Cryptographic Security Platform

Vault 10.6.1 administration and user guide

Document issue: 1.0
Issue date: October 2, 2026

© 2026, Entrust. All rights reserved

Entrust and the hexagon design are trademarks, registered trademarks and/or service marks of Entrust Corporation in Canada and the United States and in other countries. All Entrust product names and logos are trademarks, registered trademarks and/or service marks of Entrust Corporation. All other company and product names and logos are trademarks, registered trademarks and/or service marks of their respective owners in certain countries.

This information is subject to change as Entrust reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS O F THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

Contents

1 About this guide 14

Revision information 14

Other documentation 14

Documentation feedback 14

2 About Cryptographic Security Platform 15

Compliance Management 15

HSM Management 15

Certificate Management 15

Keys and Secrets Management 16

File Encryption 16

3 About Vault appliance 17

Major Components 17

Entrust Hardened OS 17

CSP Vault Clusters 18

About Entrust Policy Agent 18

Administrative Model 21

Administrative Interfaces 21

4 Release notes 26

Release notes for 10.1 26

Release notes for 10.0 27

Release notes for 10.1.1 27

Release notes for 10.2 28

Release notes for 10.3.1 28

Release notes for 10.4.1 29

Release notes for 10.4.1.1 30

Release notes for 10.4.3 30

Release notes for 10.4.5 31

Release notes for 10.4.7 32

Release notes for 10.5.1 32

Release notes for 10.5.3 33
Release notes for 10.6.1 34
5 Requirements 51
System resources 51
Network requirements 51
Browser requirements 52
Platform requirements 52
6 Installing CSP Vault 57
Installation Overview 57
CSP Vault OVA Installation 58
CSP Vault ISO Installation for Hypervisor 63
CSP Vault ISO Installation for Bare Metal Server 69
CSP Vault in Amazon Web Services 73
CSP Vault in Google Cloud Platform 83
CSP Vault in Microsoft Azure 87
7 Initializing the web GUI 95
8 User guide 96
CSP Vault authentication and user accounts 96
Vault management 119
CSP Vault for CloudKeys 123
CSP Vault for Cryptographic APIs 181
CSP Vault for Databases 253
CSP Vault for KMIP 365
CSP Vault for PKCS#11 411
CSP Vault for Secrets 431
CSP Vault for VM Encryption 533
External Authentication Provider Examples 753
Personal Access Tokens 755
Cloud Admin Groups and CSP Vault User Accounts 756
9 Upgrading CSP Vault 763

CSP Vault Upgrade Paths 763
CSP Vault Upgrade Requirements 763
Upgrading CSP Vault to 10.6.1 765
10 Installing Policy Agent 767
Preparing to Install the Policy Agent 767
Linux Policy Agent Installation 767
Windows Policy Agent Installation 774
11 Upgrading Policy Agent 785
Policy Agent Upgrade Requirements 785
Upgrading Policy Agent with the webGUI 785
Upgrading the Policy Agent on Linux 786
Upgrading the Policy Agent on Windows 787
12 CSP Vault Appliance Management 789
CSP Vault System Configuration 789
CSP Vault Cluster Maintenance 862
CSP Vault System Maintenance and Troubleshooting 881
CSP Vault Management webGUI Page Reference 901
13 CSP Vault Audit Messages 10.6.1 908
CSP Vault Audit Messages 908
CSP Vault for Cryptographic APIs Audit Messages 1032
CSP Vault for KMIP Audit Messages 1051
CSP Vault for PKCS#11 Audit Messages 1057
CSP Vault for Secrets Audit Messages 1063
Differences in CSP Vault Audit Messages 1071
14 hicli scripting guide 1073
Downloading hicli 1074
Extracting hicli 1074
Installing Python modules 1074
Setting the environment variable 1074
Enabling the python3 command 1075

Creating the configuration file 1075
Verifying 1077
Setting SSH communication 1077
15 Command reference 1078
alert detail <alertnum> 1081
alert list 1081
alert rm <alertid> 1081
create_bucket 1082
delete_bucket 1082
global set 1082
hicli byok log <group> 1082
hicli cert detail 1082
hicli cert new 1082
hicli cert rm 1082
hicli cloudkey delete_from_cloud 1082
hicli cloudkey detail 1087
hicli cloudkey disable 1087
hicli cloudkey ekm_acls 1091
hicli cloudkey enable 1095
hicli cloudkey getpublickey 1099
hicli cloudkey has_ekm_acls disable 1103
hicli cloudkey has_ekm_acls enable 1107
hicli cloudkey import 1111
hicli cloudkey kaj_policy 1115
hicli cloudkey keyops 1120
hicli cloudkey list 1124
hicli cloudkey new 1124
hicli cloudkey policy_get 1128
hicli cloudkey policy_set 1132
hicli cloudkey purge 1137
hicli cloudkey rm 1141

hicli cloudkey roles_get 1145
hicli cloudkey roles_set 1149
hicli cloudkey rotate 1153
hicli cloudkey set 1157
hicli cloudkey set_primary 1161
hicli cloudkey tag clear 1166
hicli cloudkey tag list 1170
hicli cloudkey tag set 1170
hicli cloudkey upload_to_cloud 1174
hicli cloudkey users 1178
hicli cloudkey versions 1182
hicli csp cert_auth 1186
hicli csp detail 1191
hicli csp ekm_acls 1191
hicli csp ekmconnections 1195
hicli csp get_cert_details 1199
hicli csp kaj_policy 1204
hicli csp kaj_policy_state 1208
hicli csp key_algorithms 1212
hicli csp keyrings 1216
hicli csp keyvaults 1221
hicli csp list 1225
hicli csp managedhsms 1225
hicli csp new 1230
hicli csp regions 1234
hicli csp rm 1238
hicli csp roles 1242
hicli csp rotate 1247
hicli csp set 1251
hicli csp users 1255
hicli cvm add_disk 1259

hicli cvm decrypt_task 1260
hicli cvm detail 1260
hicli cvm detail_disk 1260
hicli cvm encrypt_task 1260
hicli cvm list 1260
hicli cvm list_tasks 1261
hicli cvm new 1261
hicli cvm reauth 1261
hicli cvm rekey_task 1261
hicli cvm renew clone 1261
hicli cvm revoke 1261
hicli cvm revoke_disk 1261
hicli cvm rm 1261
hicli cvm rm_disk 1262
hicli cvm s3 add_file 1262
hicli cvm s3 get_file 1262
hicli cvm s3 rm_file 1262
hicli cvm select 1262
hicli cvmset 1262
hicli cvm set 1262
hicli cvm set_disk expiration 1262
hicli cvm set_mapping 1262
hicli cvmset add_kek 1262
hicli cvmset detail 1263
hicli cvmset kek_edit 1263
hicli cvmset kek_state_change 1263
hicli cvmset list 1263
hicli cvmset list_tasks 1263
hicli cvmset new 1263
hicli cvm set rekey 1264
hicli cvmset select 1264

hicli cvmset set 1264
hicli cvmset set grace 1264
hicli cvmset set heartbeat 1264
hicli cvmset set name 1264
hicli cvmset set rekey 1264
hicli cvmset set rekeybucket 1265
hicli cvm status 1265
hicli cvm unrevoke_disk 1265
hicli domain detail 1265
hicli domain list 1266
hicli domain select 1266
hicli domain set 1266
hicli domain set allow_reconnect 1266
hicli domain set description 1266
hicli domain set hide_passphrase 1267
hicli generate_csr 1267
hicli group add_user 1267
hicli group detail 1267
hicli group list 1267
hicli group new 1267
hicli group rm 1268
hicli group rm_user 1268
hicli group set 1268
hicli group set description 1268
hicli group set name 1269
hicli kc 1269
hicli kc select <kchost> 1269
hicli keyid new 1269
hicli keyid revoke 1269
hicli keyid rm 1270
hicli keyid set expiration 1270

hicli keyid set onexpiry 1270
hicli keyid unrevoke 1270
hicli keyset add_tde_connector 1270
hicli keyset container_purge 1270
hicli keyset create_tde_connector_token 1273
hicli keyset detail 1276
hicli keyset keyrings 1276
hicli keyset list 1278
hicli keyset list_tde_connectors 1279
hicli keyset new 1281
hicli keyset rm 1284
hicli keyset select 1287
hicli keyset set 1290
hicli keyset set_sync_schedule 1292
hicli keyset tde_connector delete 1295
hicli keyset tde_connector disable 1298
hicli keyset tde_connector enable 1301
hicli keyset verify_hsm 1303
hicli keyset verify_tde_connector_token 1306
hicli mapping detail 1309
hicli mapping list 1309
hicli mapping new 1309
hicli mapping rm 1309
hicli mapping select 1309
hicli mapping set description 1309
hicli mapping set group 1309
hicli mapping set newname 1310
hicli mapping set servers 1310
hicli server auth 1310
hicli server auth 1310
hicli server default_csr_values 1310

hicli server detail 1310
hicli server install_cert 1310
hicli server install_cert_status 1310
hicli server show_cert 1310
hicli server use_default_certs 1310
hicli server webserver_restart 1310
hicli user defaults 1311
hicli user detail <username> 1311
hicli user list 1311
hicli user login <name> 1312
hicli user new <username> 1312
hicli user rm <username> 1315
hicli user set <username> 1316
kmipsrv_obj action uuid 1316
kmipsrv_obj fetch 1318
kmipsrv_user 1320
kmipsrv set 1321
list_bucket 1323
s3 add_file 1323
s3 get_file 1323
s3 rm_file 1323
set aws_access_key_id 1323
set aws_secret_access_key 1323
16 Customer license 1324
Authorized Use 1324
License 1324
Deployment 1327
External Dependencies 1327
Trade Compliance 1327
Standard Compliance Packs Limitations 1328
Support and Record-Keeping 1328

17 CSP Vault with VSAN and VMware vSphere VM Encryption.....1329
CSP Vault with VSAN and VMware vSphere VM Encryption Overview 1329
Configuring a KMIP Server for vSphere KMS 1330
Adding a KMS Cluster in vSphere.....1333
Establishing a Trusted Connection with a vSphere-Generated CSR.....1334
Establishing a Trusted Connection with a CSP Vault-Generated CSR 1336
Troubleshooting 1337

1 About this guide

This guide describes how to install and manage Vault.

- Revision information
- Other documentation
- Documentation feedback

Revision information

See the table below for changes in each document issue.

Issue	Date	Section	Changes
1.1	Oct 2026	CSP Vault for PKCS#11	New section
		Configuring Role-Based Access Control	New page
		CSP Vault for PKCS#11 Audit Messages	New page
		CSP Vault Audit Messages 10.6.1	Updated all the audit messages pages
1.0	Aug 2026	All	Document release

Other documentation

For instructions on using Vault, see:

https://api.managed.entrust.com/vaultaas

The options described apply to both on-premises and cloud-based product versions.

Documentation feedback

You can rate and provide feedback about product documentation by completing the online feedback form:

https://go.entrust.com/documentation-feedback

Any information you provide goes directly to the documentation team and is used to improve and correct the information in our guides.

2 About Cryptographic Security Platform

The Cryptographic Security Platform (CSP) software solution provides a unified platform for managing, protecting, and assessing cryptographic assets. CSP provides functionalities in the following categories:

- Compliance Management
- HSM Management
- Certificate Management
- Keys and Secrets Management
- File Encryption

Compliance Management

These capabilities assist with assessing and managing compliance of identified keys, secrets, and certificates with specified requirements. May be deployed in a clustered configuration and includes:

- **Compliance Manager**: A CSP component that provides **centralized visibility, compliance, and risk governance** of the enterprise's cryptographic assets. It connects data sources—such as vaults and security object repositories—from which it imports metadata about security objects (keys, secrets, and certificates), aggregates this information into a centralized inventory, and evaluates assets against compliance requirements.
- **Discovery**: A CSP feature for **asset discovery and data collection**, used to collect information about cryptographic assets so they can be brought under centralized visibility. Discovery operates through configuration-based scans, which can be run manually or on a schedule. Scan results integrate directly with Compliance Manager to populate the inventory of certificates, keys, and secrets.
- **Standard Compliance Packs**: Pre-configured collections of compliance requirements designed to assist organizations in assessing cryptographic assets against commonly adopted industry standards and best practices.
- **Third-party Objects**: An optional functionality that allows metadata for keys, secrets, or certificates not created or stored directly by CSP components or Entrust's non-CSP Certificate Authority ("ECA") software to be imported into the Compliance Manager inventory. Imported third-party objects are included in compliance assessments and reporting but remain externally managed.

HSM Management

Provides centralized management, monitoring, and visibility for Entrust HSMs. It is deployed as part of the Compliance Management configuration and includes:

- **KeySafe 5:** Centralized management of Entrust HSMs (Security Worlds, card sets, soft cards, firmware, host applications) with cryptographic asset visibility via Compliance Manager.
- **KeySafe 5 Monitoring**: Optional capability for centralized monitoring of Entrust HSMs with live and historical health, performance, alerts, and utilization metrics.

Certificate Management

CSP optional add-on capabilities for deploying Public Key Infrastructure (PKI) functionality in clustered configurations, with usage limitations depending on the purchased license packages:

- **Certification Authority Package, includes:**
  - **Certificate Authority** solution providing certificate issuance, management, and validation, with built-in RESTful APIs for the CAs created and managed within the CSP.
  - **Certificate Enrollment Gateway** (CEG): a collection of certificate enrollment protocols. In this package, CEG may only be used for certificates created and managed within CSP.

- **Advanced PKI Package, includes**:
  - **Timestamping Authority**: software to prove that data existed at a specific time.
  - **Validation Authority**: certificate validation (OCSP) software specifically for (non-CSP) ECA.
  - **CA Gateway**: software consisting of RESTful APIs for integrating CAs. In this package, CA Gateway may only be used to integrate CSP with ECA.
- **Advanced CLM Package, includes**:
  - **Certificate Manager (formerly Certificate Hub)**: Certificate lifecycle management and automation across CAs created and managed within the CSP and third-party CAs, excluding CA functionality.
  - **CA Gateway**: In this package, it is permissible to use CA Gateway for integration with CSP CAs and non-CSP CAs.
  - **Certificate Enrollment Gateway**: In this package, it is permissible to use Certificate Enrollment Gateway for certificates created by both CSP and non-CSP CAs.

Keys and Secrets Management

CSP optional add-on capability for deploying multiple vault appliances in active-active Vault Clusters. Appears on Orders as "Compliance Manager - 2 Nodes Virtual Appliance Cluster for Vaults." A Vault Cluster is a secure CSP software component that provides an isolated environment for managing cryptographic keys, secrets, and related objects. Vault Clusters securely generate, store, protect, and control access to cryptographic material while enforcing strong security controls and auditability.

Each Vault Cluster can manage one or more of the following vault types:

- **Vault for KMIP Keys**: Cryptographic keys, secrets, and certificates managed using the Key Management Interoperability Protocol (KMIP), enabling standardized and interoperable key lifecycle management across heterogeneous environments and applications.
- **Vault for Cloud Keys**: Encryption keys used in cloud key management services—such as AWS KMS, Azure Key Vault, and Google Cloud KMS—to protect cloud-native workloads and data. CSP supports bring-your-own-key (BYOK), hold-your-own-key (HYOK), and native key management models, depending on the target cloud service.
- **Vault for Secrets**: Sensitive data such as passwords, API keys, access tokens, and credentials that require secure storage, access control, and lifecycle management.
- **Vault for Application Keys**: Cryptographic keys used by applications to perform cryptographic operations—such as encryption, digital signatures, and hashing—via CSP cryptographic APIs or command-line interfaces.
- **Vault for TDE Database Keys**: Encryption keys used to protect databases with Transparent Data Encryption (TDE), including Oracle, Microsoft SQL Server, MariaDB, and open-source PostgreSQL, ensuring data at rest is encrypted.
- **Vault of Virtual Machine Encryption Keys:** Cryptographic keys used to encrypt Windows and Linux virtual machine operating system disks and attached data volumes in virtualized environments.

File Encryption

File Encryption is a CSP software component that encrypts file-based data and may be deployed in a clustered configuration. File Encryption supports both:

- Software-based encryption, where hardware HSM protection is not required, and
- Hardware-based encryption, leveraging Entrust HSMs for enhanced key protection.

The File Encryption capability includes 10 GB of protected data capacity. Additional encrypted data capacity may be added by purchasing 1 TB add-on annual subscriptions.

3 About Vault appliance

See below for an overview of the Cryptographic Security Platform Vault appliance,

- Major Components
- Entrust Hardened OS
- CSP Vault Clusters
- About Entrust Policy Agent
- Administrative Model
- Administrative Interfaces

Major Components

Entrust Cryptographic Security Platform Vault® provides encryption and key management for virtual machines located in data centers or private, public, or hybrid clouds. Entrust Cryptographic Security Platform Vault works with:

- VMware vSphere
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

Entrust Cryptographic Security Platform Vault consists of two main components:

- **Entrust Cryptographic Security Platform Vault** (CSP Vault)—CSP Vault stores encryption keys, policies, and configuration for any number of virtual machines with the Entrust Policy Agent installed. You can configure CSP Vault directly through one of the browser-based webGUIs using HTTPS, or remotely through the `hicli` command line interface (CLI) or a set of REST-based APIs.

  You can install multiple CSP Vault nodes in an active-active cluster to provide load balancing and high availability support. Because this is an active-active cluster, you can make changes to the settings on any CSP Vault node in the cluster and those changes are immediately reflected on all CSP Vault nodes in the cluster.

- **Entrust Policy Agent** (Policy Agent)—A software module that runs inside Windows and most Linux operating systems that provides encryption of virtual disks, filesystems, and individual files. All VMs that have the Policy Agent installed can also securely share encrypted files and disks as long as those VMs are registered with the same Cloud VM Set.

  You must install a copy of the Policy Agent on each VM that you plan to use with the CSP Vault for Databases or the CSP Vault for VM Encryption.

Entrust Hardened OS

The base of every Cryptographic Security Platform Vault node is the Entrust-hardened version of Oracle Linux, a locked-down version of the operating system that has no run-time login/SSH access to the system. This prevents tampering or attempts to access clear-text data and/or encryption keys. Each Cryptographic Security Platform Vault node can be installed as a virtual machine.

The main features are:

- An ISO, OVA, AMI (Amazon Web Services marketplace), VHD (Microsoft Azure marketplace), or Google Cloud Platform Image that supports installation of a Cryptographic Security Platform Vault node, from which the Entrust Policy Agent can be downloaded.

- Optional automatic mirroring of the root partition to provide high availability for CSP Vault servers, preventing downtime from disk failures.
- Encryption of the Entrust software on the installation media, to prevent tampering.
- All major system software protected from tampering by whitelisting.
- No login or SSH access to CSP Vault, preventing key snooping or clear-text data snooping.
- Minimal OS software installed with industry standard lock-down capabilities built in.
- Ability to extract debug information via the webGUI or through a restricted support access. The debug information does not contain any sensitive data or encryption keys.
- GUI-based extraction of log / support information.
- Built-in VMtools.

CSP Vault Clusters

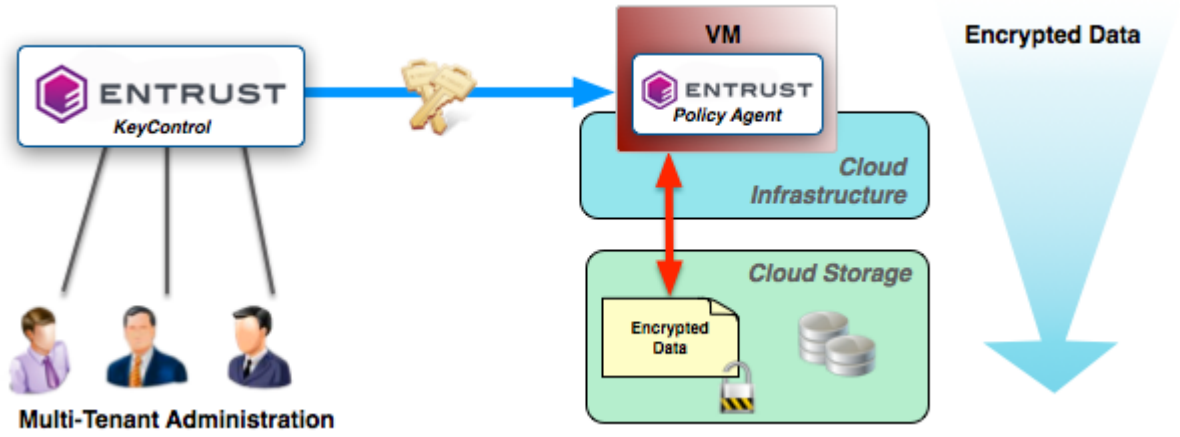
At the heart of every Entrust Cryptographic Security Platform Vault deployment is an active-active cluster of Cryptographic Security Platform Vault nodes that manage encryption keys for virtual Linux and Windows machines.

CSP Vault features include:

- An active-active cluster for high availability. Any changes made to any Cryptographic Security Platform Vault node in the cluster are automatically reflected on all nodes in the cluster.
- Clustered object store protecting keys, policies and configuration data. All objects are encrypted and ultimately wrapped with an Admin Key.
  The Admin Key uses a software-based "n of m" backup. This prevents Cryptographic Security Platform Vault backups from being stolen and installed on new hardware.
- Nodes can join or leave the cluster without affecting Cryptographic Security Platform Vault's ability to deliver encryption keys.
- A Cryptographic Security Platform Vault cluster moves into degraded mode (read only) on network disconnect or failure. While in degraded mode, any Cryptographic Security Platform Vault node can still serve requests for existing keys and policies from VMs where the Policy Agent is installed. However, new encryption keys cannot be created.
- Each Policy Agent communicates with any Cryptographic Security Platform Vault node, switching between them if they detect a non-responsive Cryptographic Security Platform Vault node.
- All system components of the Cryptographic Security Platform Vault are encrypted.
- Support for admin authentication via local accounts with strict password controls or via accounts stored in LDAP (including Microsoft AD).
- Support for Alerts in environments with and without email access.
- Full-featured command line utilities (`hicli` and `hcl`).
- A rich RESTful API.

About Entrust Policy Agent

The Entrust Policy Agent provides for encryption of disks, filesystems and files within a virtual machine.



There are a number of features provided in the Policy Agent, including:

- Full encrypted path from the VM, through the hypervisor to the storage.
- Support for cloning and replication.
- Dynamic rekey on Windows and Linux, allowing initial encryption or rekey without taking the VM or applications offline.
- Filesystem resize for encrypted devices.
- Support for Amazon S3 storage.
- Linux file-level and folder-level encryption.
- Migration of encrypted disks between VMs in the same Cloud VM Set.
- Support for Windows failover clusters.
- Root and swap encryption for Linux and boot drive (C:) encryption for Windows.

This section includes:

- Encryption Key Sizes and Algorithms
- Secure File Migration

Encryption Key Sizes and Algorithms

You can specify a specific cipher type when disks are encrypted or when KeyIDs are created. By default, the Policy Agent uses AES-XTS-512 encryption to take advantage of the performance improvements that come with AES-NI (Advanced Encryption Standard New Instructions).

Policy Management encryption keys:

- Support AES and AES-XTS encryption. Specifically:

Algorithm	Mode	Notes
AES-128	CBC	Available *only* for KeyIDs. Not available when encrypting Linux or Windows disks. Uses a single 128-bit encryption key.

Algorithm	Mode	Notes
AES-256	CBC	Uses a single 256-bit encryption key.
AES-XTS-256	XTS	Not available on Windows boot drives. Uses a pair of 128-bit encryption keys.
AES-XTS-512	XTS	Uses a pair of 256-bit encryption keys, one data AES key and one tweak AES key. The IV is generated using aes-xts-essiv:sha256.
AES-XTS-512-FIPS	XTS	Uses a pair of 256-bit encryption keys, one data AES key and one tweak AES key. The IV is generated using aes-xts-plain64, which is approved by FIPS.

- Automatically detect and use hardware cryptography—AES-NI on Intel and AMD processors.
- Can be assigned an expiration date—one key per device is generated.
- Enable secure encrypted communication between Cryptographic Security Platform Vault clusters and Policy Agents.
- Allow users to revoke or restore access to all keys for a VM.
- Allow users to cache keys in the VM (encrypted with a passphrase).
- Allow users to clone VMs and authenticate cloned VMs (for backup, restore, autoscaling, and DR purposes).
- Enable the Policy Agents to share encryption keys and disks between VMs in the same Cloud VM Set, which allows these VMs to encrypt, securely transport, and decrypt data and disks.
- Allow users to rekey both Windows and Linux disk while those disks are online and accessible.
- The FIPS certified version uses the key size designation in the name instead of the overall key material size.

AES-NI is supported by all current-generation EC2 instances in Amazon Web Services (AWS) and by all Microsoft Azure instances. To check whether a specific server supports AES-NI, run `hcl status` on the server or look at the VM details in the Cryptographic Security Platform Vault webGUI under Cloud > VMs.

For additional details about AES-NI, see the Wikipedia summary at http://en.wikipedia.org/wiki/AES_instruction_set.

Secure File Migration

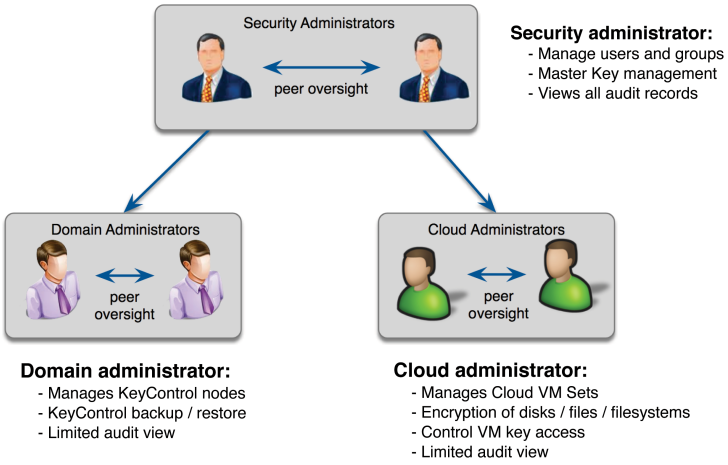
In VMs with the Policy Agent installed, we support the ability to share KeyIDs (encryption keys referenced by a symbolic name) between VMs within the same Cloud VM Set in which the KeyIDs were created. This allows you to encrypt files and move them securely between these VMs. Only the VMs within the same Cloud VM Set as the KeyIDs are able to decrypt the files. Encryption is on a file-by-file basis, so movement of larger amounts of data can be achieved by zipping/tarring groups of files and then encrypting them.

These mechanisms can also be used to encrypt files and move them to cloud storage knowing that only you will be able to decrypt the files on return.

As an extension to the KeyID notion, we also provide interfaces for migrating encrypted files between VMs and through Amazon Web Services (AWS) S3 storage.

Administrative Model

Entrust Cryptographic Security Platform Vault provides a rich administrative framework that can be leveraged by multiple organizations of different sizes. This approach is useful for organizations ranging from the single-administrator IT shop to a large, multi-tenant cloud service provider who needs to support secure customer environments.



The administration model provides:

- Multi-tenancy support. Administrative roles allow for need-to-know and separation of duties. There are three distinct administrative roles (Security, Domain, and Cloud). Roles can be combined and there are no limits to the number of administrators. Administrators can be placed in administrative groups to provide peer oversight. All objects in the system are owned by one or more administrative groups, not by individual administrators.
- Support for multiple administrative roles per admin.
- Alerts presented through the Cryptographic Security Platform Vault webGUI and, optionally, sent through email.
- Audit records that can be displayed in the Cryptographic Security Platform Vault webGUI, downloaded, or exported through syslog to an external log server.

> The Security Admin, Cloud Admin, Domain Admin model is being retired in favor of RBAC. Currently, the model has been retired only for appliance logins.

Administrative Interfaces

Entrust provides several administrative interfaces that allow you to configure and maintain Cryptographic Security Platform Vault and the encrypted VMs registered with Cryptographic Security Platform Vault.

Interface	Description
Cryptographic Security Platform Vault webGUI	A browser-based HTTPS interface to Cryptographic Security Platform Vault that lets you perform Cryptographic Security Platform Vault configuration and VM management. You can log into the webGUI on any Cryptographic Security Platform Vault node in the cluster. Any changes you make on that node are automatically disseminated to all other Cryptographic Security Platform Vault nodes in the cluster. For more information, see CSP Vault Management web GUI Overview.
Entrust Cryptographic Security Platform Vault System Console	The Entrust Cryptographic Security Platform Vault System Console is available on each Cryptographic Security Platform Vault node in the cluster. It lets you set local configuration options for the node and perform basic functions such as joining the node to an existing Cryptographic Security Platform Vault cluster and managing support access to the node. For more information, see CSP Vault System Console Overview.
`hicli`	CLI (command line interface) commands that allow you to configure and maintain both Cryptographic Security Platform Vault and the VMs registered with Cryptographic Security Platform Vault. For more information, see hicli scripting guide.
Entrust Policy Agent GUI	A Windows-only GUI installed with the Entrust Policy Agent. The Entrust Policy Agent GUI allows you to register and authenticate the VM on which it is installed. It also lets you encrypt and decrypt the disks on that VM. Unlike the other interfaces, the Entrust Policy Agent GUI is limited to the VM on which it is installed. You cannot use the Entrust Policy Agent GUI on one VM to manage the disks on a different VM, even if both VMs are registered with Cryptographic Security Platform Vault. For more information, see Entrust Policy Agent GUI Overview.
REST or Python APIs	Cryptographic Security Platform Vault can be configured and maintained through REST-based or Python-based API calls. The API documentation is located at https://<IP-Address>/apidoc/.

- CSP Vault Management web GUI Overview
- CSP Vault System Console Overview
- Entrust Policy Agent GUI Overview

CSP Vault Management web GUI Overview

When you configure a CSP Vault Management cluster, you assign each node a static IP address. When you navigate to one of those static IP addresses in a web browser, CSP Vault displays the CSP Vault Management web GUI. The CSP Vault Management web GUI lets you configure the CSP Vault Management appliance and manage the VMs registered with the cluster.

You can log into the CSP Vault Management web GUI on any CSP Vault node in the cluster, and the changes will be automatically disseminated to all nodes in the cluster.

> ⚠ Always explicitly log out of the CSP Vault Management web GUI when you are finished. If you close the browser without logging out first, CSP Vault keeps your session active until the Session Timeout is reached. For details, see Setting the CSP Vault Management web GUI Session Timeout.

The main features of the CSP Vault web GUI are:

- A Top Menu Bar that provides access to the main CSP Vault features. The icons you see in this bar depend on the user privileges associated with your account.
- A User menu next to the Top Menu Bar that lets you set your user preferences, log out from the web GUI, or open the product online help. The **Help** link in this menu is context-sensitive, so the help page displayed when you select this link depends on the currently-displayed page in the web GUI.
- A Dashboard that gives you an overview of your VMs in one place. For details, see Using the Dashboard.
- A **Refresh** button that allows you to control when the web GUI fetches updates from the network.

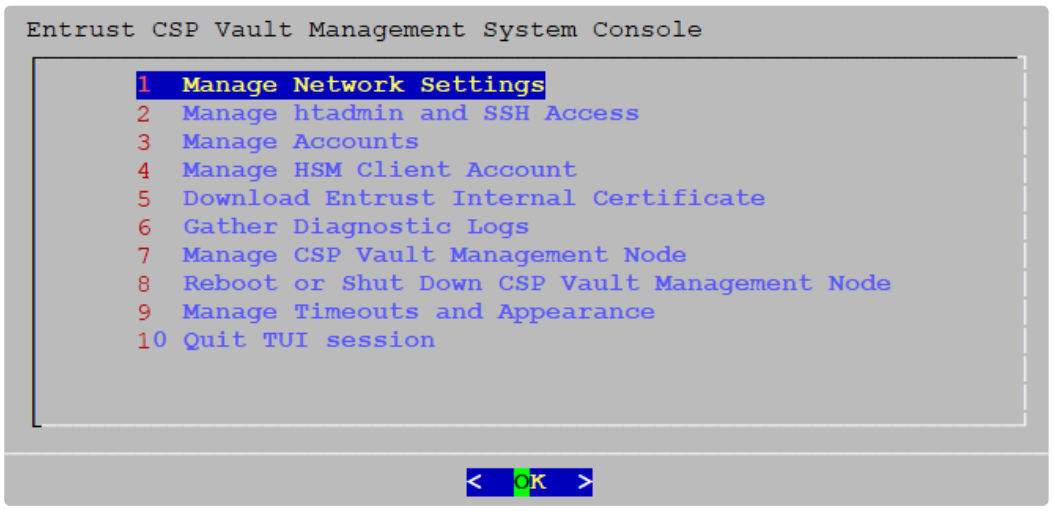
For all tables in the web GUI, you can:

- Display additional information for any object by clicking on that object.
- Sort by any column by clicking the column header.
- Select which columns are displayed by clicking the **Column Display Options** button.
- Toggle multi-select mode by clicking the **Multi-Select** button. If you select multiple objects, any action you take applies to all selected objects.

For information about logging into the web GUI for the first time, see Initializing the CSP Vault Management web GUI. For information about administering CSP Vault using the web GUI, see CSP Vault System Configuration.

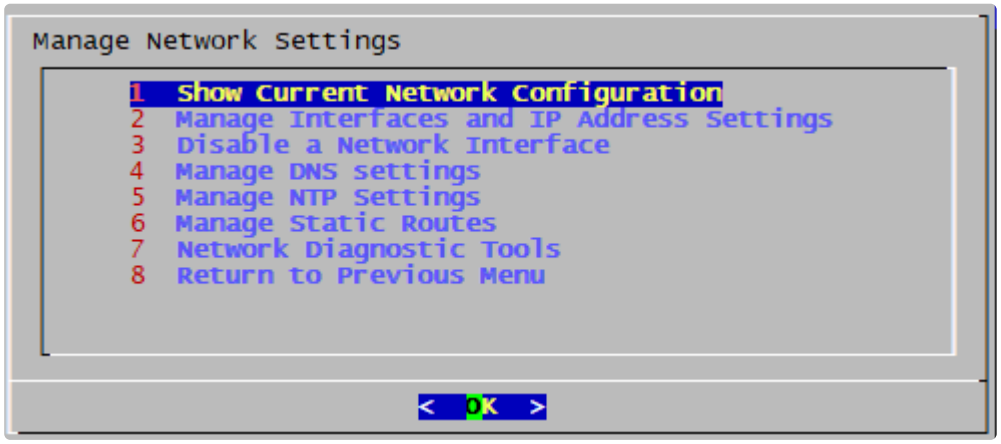
CSP Vault System Console Overview

When you log into the Cryptographic Security Platform Vault VM console as `htadmin`, Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console. This menu lets you configure the local Cryptographic Security Platform Vault server. In general, the changes you make here do not apply to any other Cryptographic Security Platform Vault node in the cluster.



The menu is a TUI (Text-based User Interface). You navigate through the TUI using the Tab key to move between fields and pressing Enter when the correct choice is highlighted. If the TUI screen has numbers at the start of the line, you can also press the corresponding number key and then press Enter to navigate through the menus.

In the screenshot above, pressing Enter goes to the Manage Network Settings screen of the TUI.

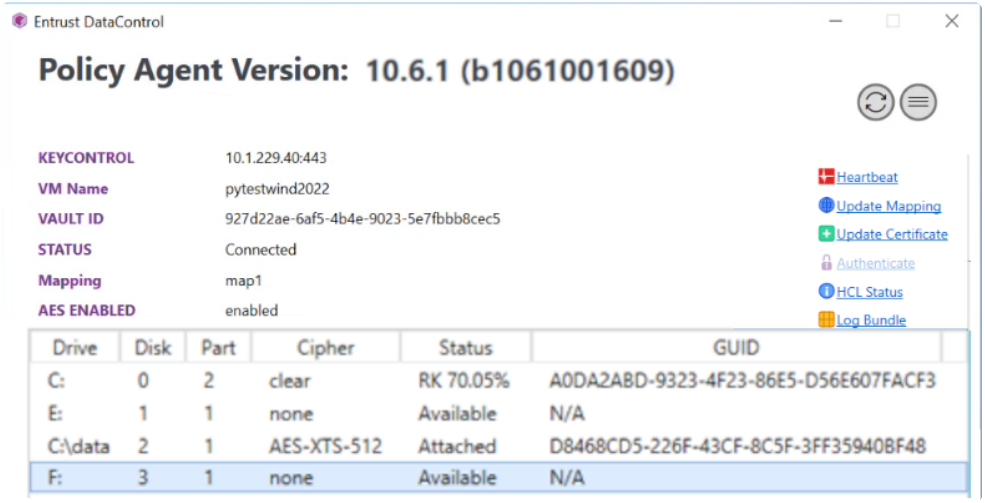


To return to the main Entrust Cryptographic Security Platform Vault System Console screen, press Esc (Escape). Based on where you are in the menus, you may need to press Esc several times.

For more information, see Using the Entrust CSP Vault System Console.

Entrust Policy Agent GUI Overview

The Entrust Policy Agent GUI is installed locally on the Windows server with the Entrust Policy Agent. It provides basic encryption, decryption, and rekeying functionality by sending requests to the CSP Vault for VM Encryption so that you do not need to log into the CSP Vault for VM Encryption webGUI.



The Entrust Policy Agent GUI allows you to register or authenticate the VM with CSP Vault for VM Encryption, and it displays the following information:

- the connection information.
- the status of each disk or folder mount on the VM.

In the Policy Agent,you can click the Heartbeat button to manually force a heartbeat connection, click the Update Mapping button to use the mapping that you created in the CSP Vault for VM Encryption webGUI, or right-click any of the listed disks or folder mounts to encrypt or decrypt them. In the screenshot above, the GUI shows that the folder mount `C:\data` is encrypted and attached to the CSP Vault for VM Encryption while `C:` is being encrypted and the encryption process has completed 70.05% of the disk.

If you had not yet registered the Policy Agent, then the screen would show a Register button that you can click to register it.

For details, see Windows Encryption Management with the Entrust Policy Agent GUI.

4 Release notes

The following changes were made in past Cryptographic Security Platform Vault releases.

- Release notes for 10.1
- Release notes for 10.0
- Release notes for 10.1.1
- Release notes for 10.2
- Release notes for 10.3.1
- Release notes for 10.4.1
- Release notes for 10.4.1.1
- Release notes for 10.4.3
- Release notes for 10.4.5
- Release notes for 10.4.7
- Release notes for 10.5.1
- Release notes for 10.5.3
- Release notes for 10.6.1

For details about the current Cryptographic Security Platform Vault release and previous releases, visit trustedcare.entrust.com. If you do not have a login, please contact trustedcaresupport@entrust.com.

Release notes for 10.1

See the release notes below for Vault 10.1

- Upgrade path
- Changes in this release

Upgrade path

You can only deploy Entrust Cryptographic Security Platform Vault 10.1 as a new installation. Upgrading from previous versions of Entrust Cryptographic Security Platform Vault is not supported.

Changes in this release

See below for the changes in this Vault release.

- New Entrust Cryptographic Security Platform Vault Architecture. The Entrust Cryptographic Security Platform Vault family of products has been divided into two components:
  - Cryptographic Security Platform Compliance Manager—This application handles all global requirements for your vaults, such as licensing and authorization.
  - Entrust Cryptographic Security Platform Vault—All of the Entrust Cryptographic Security Platform Vault applications have been separated and moved into individual vaults.
- You manage licensing for all Entrust Cryptographic Security Platform Vaults using Cryptographic Security Platform Compliance Manager.
- You can now use Cryptographic Security Platform Vault as an external key manager (EKM) provider for Oracle Server.
- You can now use Cryptographic Security Platform Vault as an AWS KMS External Key Store (XKS).
- You can now use the new Tokenization Vault and APIs for tokenization, masking, and data encryption.
- You can now use Cryptographic Security Platform Vault with Azure-managed HSMs.
- You can now configure Syslog Server to use ArcSight Common Event Format (CEF) for logging.

- Cryptographic Security Platform Vault now supports Remote Administration Ready Smartcards for nShield HSMs.
- Cryptographic Security Platform Vault now includes the Luna HSM library v10.5.1-174

Release notes for 10.0

See the release notes below for Vault 10.0

- Upgrade path
- Changes in this release

Upgrade path

See below for the versions that support upgrading to 10.0.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	5.5 and 5.5.1
Entrust Policy Agent	5.3, 5.4, 5.5, and 5.5.1

Changes in this release

See below for the changes in this Vault release.

- You can now use Cryptographic Security Platform Vault as an EKM provider for Microsoft SQL.
- You can now use Cryptographic Security Platform Vault to manage your SSH keys.
- You can now use Bring Your Own Key (BYOK) with Google Cloud Platform.
- You can now use Cryptographic Security Platform Vault with nShield HSMs that are enrolled in FIPS 140 Level 3 Security Worlds.

Release notes for 10.1.1

See the release notes below for Vault 10.1.1.

- Upgrade path
- Changes in this release

Upgrade path

See below for the versions that support upgrading to 10.1.1.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	10.0 and 10.1
Entrust Policy Agent	10.0 and 10.1

Changes in this release

See below for the changes in this Vault release.

- You can now upgrade KeyControl version 10.0 to KeyControl Vault 10.1.1.
- You no longer need to enable SMTP in the Appliance Manager UI when adding KeyControl Vaults. We removed this restriction in the 10.1 release.
- KeyControl Vault PASM vaults now support Ansible.

Release notes for 10.2

See the release notes below for Vault 10.2.

- Upgrade path
- Changes in this release

Upgrade path

See below for the versions that support upgrading to 10.2.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	10.1 and 10.1.1
Entrust Policy Agent	10.1 and 10.1.1.

Changes in this release

See below for the changes in this Vault release.

- You can now use hardware security modules with the Cryptographic Security Platform Vault for Secrets.
- You can now use BYOK with GCP in the Cryptographic Security Platform Vault for Cloud Keys.
- You can now use MariaDB with TDE in the Cryptographic Security Platform Vault for Databases.
- You can now use the HTTPS proxy server with BYOK for AWS and Azure.
- Support for Double Key Encryption for Microsoft 365 in the Cryptographic Security Platform Vault for Cloud Keys.
- Two-factor authentication is now available with each Cryptographic Security Platform Vault.

Release notes for 10.3.1

See the release notes below for Vault 10.3.1.

- Upgrade path
- Changes in this release

Upgrade path

See below for the versions that support upgrading to 10.3.1.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	10.2.
Entrust Policy Agent	10.2, 10.1.1, and 10.1.

Changes in this release

See below for the changes in this Vault release.

- Version 10.4.1 is the first KeyControl release on Oracle Linux. The transition from CentOS to Oracle Linux allows Entrust to improve KeyControl operating system security. The main KeyControl components were ported directly to Oracle Linux and will continue to work as they did in earlier releases. The same applies to the KeyControl APIs.
- You can now use OpenID Connect (OIDC) Authentication without configuring Active Directory in your individual KeyControl vaults.
- You can now use Active Directory (AD) or OpenLDAP for authentication in the KeyControl Vault Management appliance.
    - AD users are supported, but not AD groups.
    - Two-factor authentication is supported for local users only.

Release notes for 10.4.1

See the release notes below for Vault 10.4.1.

- Upgrade path
- Changes in this release

Upgrade path

See below for the versions that support upgrading to 10.4.1.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	10.3.1
Entrust Policy Agent	10.3.1

Changes in this release

See below for the changes in this Vault release.

- Version 10.4.1 is the first KeyControl release on Oracle Linux. The transition from CentOS to Oracle Linux allows Entrust to improve KeyControl operating system security.
- The main KeyControl components were ported directly to Oracle Linux and will continue to work as they did in earlier releases. The same applies to the KeyControl APIs.
- Entrust KeyControl now runs on the Entrust-hardened version of Oracle Linux.

- You can now use OpenID Connect (OIDC) Authentication with Active Directory in the KeyControl Vault Management appliance.
- You can now use OpenID Connect (OIDC) Authentication without configuring Active Directory in the KeyControl Vault Management appliance.
- AWS multi-Region keys are AWS KMS keys in different AWS Regions that can be used interchangeably. The KeyControl Vault for Cloud Keys now supports using AWS multi-region keys in BYOK.
- The KeyControl Vault for Cloud Keys now supports Azure role-based access control (Azure RBAC) and the access policy model authorization system.
- You can now use secondary approval with the KeyControl Vault for Secrets.
- You can now use Personal Access tokens in your KeyControl Vaults that use OIDC for authentication as a password for API and CLI commands.
- Added support for TLS 1.3 and Extended Master Secret (TLS). TLS 1.3 is the default for all new KeyControl installations.
- You can now set KeyControl to use self-signed certificates for all nodes in a cluster.
- The KeyControl appliance AMI now only supports Instance Metadata Service (IMDS) version 2 for AWS Cloud.

Release notes for 10.4.1.1

See the release notes below for Vault 10.4.1.1.

- Upgrade path
- Changes in this release

Upgrade path

See below for the versions that support upgrading to 10.4.1.1.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	10.3.1, 10.3.3, and 10.4.1
Entrust Policy Agent	10.3.1, 10.3.3, and 10.4.1.

Changes in this release

Release 10.4.1.1 is a cumulative release containing bug fixes and all new features from 10.4.1.

Release notes for 10.4.3

See the release notes below for Vault 10.4.3.

- Upgrade path
- Changes in this release

Upgrade path

See below for the versions that support upgrading to 10.4.3.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	10.3.1, 10.3.3, 10.4.1, and 10.4.1.1
Entrust Policy Agent	10.3.1, 10.3.3, 10.4.1, and 10.4.1.1

Changes in this release

See below for the changes in this Vault release.

- You can now use BYOK with Oracle Cloud Infrastructure (OCI).
- You can now assign API users the BACKUP_USER role, which lets them manage backups but does not grant any other admin privileges.

Release notes for 10.4.5

See the release notes below for Vault 10.4.5.

- Upgrade path
- Changes in this release

Upgrade path

See below for the versions that support upgrading to 10.4.5.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	10.4.1, 10.4.1.1, and 10.4.3
Entrust Policy Agent	10.3.1, 10.3.3, 10.4.1, 10.4.1.1, and 10.4.3

Changes in this release

See below for the changes in this Vault release.

- KeyControl and KeyControl Compliance Manager have changed names.
  - KeyControl is now known as Cryptographic Security Platform Vault.
  - KeyControl Compliance Manager is now known as Cryptographic Security Platform Compliance Manager.
  - The KeyControl Vault for Application Security is now known as the Cryptographic Security Platform Vault for Cryptographic APIs.
- If a CloudKey's cloud status is unavailable, you can remove it immediately using the Force Purge command.
- You can now use certificate-based authentication with Azure BYOK.
- You can now use BYOK and cache-only keys (HYOK) with Salesforce.
- You can set up an automatic synchronization schedule to import all CloudKeys in a Key Set.
- You can now cache your keys in the Cryptographic Security Platform Vault for Cryptographic APIs.
- The Cryptographic Security Platform Vault for Secrets now supports Terraform secrets.
- Cryptographic Security Platform Vault for Databases now supports column-level encryption for PostgreSQL.

- You can now use mTLS authentication in the Cryptographic Security Platform Vault for Cryptographic APIs.

Release notes for 10.4.7

See the release notes below for Vault 10.4.7.

- Upgrade path
- Changes in this release

Upgrade path

See below for the versions that support upgrading to 10.4.7.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	10.4.1, 10.4.1.1, 10.4.3, and 10.4.5
Entrust Policy Agent	10.3.1, 10.3.3, 10.4.1, 10.4.1.1, 10.4.3, and 10.4.5

Changes in this release

See below for the changes in this Vault release.

- The Cryptographic Security Platform Vault for Secrets now supports AWS user credential secrets.
- The Cryptographic Security Platform Vault for Secrets now supports Postgres secrets.
- Added support for EnterpriseDB (EDB) PostgreSQL Advanced Server.
- Added support for AD groups.
- Added mTLS authentication support for the Cryptographic Security Platform Vault for Cryptographic APIs and the Cryptographic Security Platform Vault for Secrets.

Release notes for 10.5.1

See the release notes below for Vault 10.5.1.

- Upgrade path
- Changes in this release

Upgrade path

See below for the versions that support upgrading to 10.5.1.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	10.4.3, 10.4.5, and 10.4.7
Entrust Policy Agent	10.4.3, 10.4.5, and 10.4.7

Changes in this release

See below for the changes in this Vault release.

- Licenses are now enforced in the Cryptographic Security Platform. You will see pop-up warnings in the webGUI when there are important license issues.
- Expanded support for Post-Quantum Encryption and Key Management, including support for ML-KEM, ML-DSA, and SLH-DSA keys, as well as encapsulation, decapsulation, sign, and verify operations using these keys. Also added improved PQ security for KMIP Server with support for PQ-TLS.
- You can now use KeySafe5 (part of the CSP appliance) to monitor your nShield HSM when configured with the Cryptographic Security Platform Vault.

  > You can view the KeySafe5 GUI through the Cryptographic Security Platform Compliance Manager.

- Azure updates, including Multi-Vault keys and the ability to manage multiple Azure
- The Cryptographic Security Platform Vault for Cloud Keys now supports on-demand key rotation for AWS key versions with BYOK.
- The Cryptographic Security Platform Vault for Secrets now supports Microsoft SQL Server
- The Cryptographic Security Platform Vault for Secrets now supports EnterpriseDB Postgres.
- Added the Batch Encrypt, Batch Decrypt, and Batch Encrypt-Decrypt API and CLI commands in the Cryptographic Security Platform Vault for Cryptographic APIs.
- Added support for OCI users in non-default identity
- Added Authentication Inheritance, which enables Security Administrators to configure the Cryptographic Security Platform Vault Appliance with AD, OIDC, or OIDC with AD Authentication, and allows Vault Administrators to inherit that configuration in their vaults.
- Added the ImportClearKey API command in the Cryptographic Security Platform Vault for Cryptographic
- Made multiple enhancements to the Windows Policy Agent GUI, including support for TLS 3, increased launch speed, and reduced application size. You can also update mappings, perform encryption tasks on drives, and view encryption details.

Release notes for 10.5.3

See the release notes below for Vault 10.5.3.

- Upgrade path
- Changes in this release

Upgrade path

See below for the versions that support upgrading to 10.5.3.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	10.5.1 and 10.5.3
Entrust Policy Agent	10.4.5, 10.4.7, 10.5.1, and 10.5.3

Changes in this release

Changes in this release:

- You can now encrypt multiple databases with one command.
- If you use geographically distributed nodes in your cluster and have performance issues, you can switch your master node to the server closest to where most data is generated.
- You can now choose which node becomes the master node after you remove the master node from the cluster.
- You can now choose whether or not you want to enable audit logging for HYOK, EKM, and XKS operations at the Key Set level.

Release notes for 10.6.1

See the release notes below for Vault 10.6.1.

- Upgrading to 10.6.1
- Changes in 10.6.1
- Fixed in 10.6.1
- Vault issues in 10.6.1
- Windows-specific Policy Agent issues in 10.6.1
- Linux-specific Policy Agent issues in 10.6.1

Upgrading to 10.6.1

See below for the versions that support upgrading to 10.6.1.

Product	Supported source versions
Entrust Cryptographic Security Platform Vault	10.5.1, 10.5.3, 10.5.3-P1, 10.5.3-P2, and 10.4.3-P2
Entrust Policy Agent	10.6.1 from versions 10.5.1 and 10.5.3

Before you upgrade:

- You must upgrade the Cryptographic Security Platform Compliance Manager before you upgrade Cryptographic Security Platform Vault.
- You must be connected to the CSP Compliance Manager and must have a valid

⚠ Beginning with version 10.4.7, you will no longer be allowed to upgrade if your license is not current. If you see an error message during the upgrade, please contact support at trustedcare.entrust.com

Changes in 10.6.1

See below for the changes in the 10.6.1 release.

- SNMP v3 Support
- Lenovo SR250/SR630 Appliance Deployment Support
- PKCS#11 Vault Support
- Microsoft External Key Manager Support
- Fine-Grained Administrative Roles and Permissions
- GitLab Secrets Vault Integration
- AWS IAM and STS Secrets Vault Integration
- Azure Entra ID Secrets Vault Integration
- Offline Cloud Encryption Key Generation

- OCI EKM Management Interface Decoupling
- Generic Authentication Error Responses
- ECDSA 384-bit Certificate and Trust Validation Enhancements
- Database Vault TDE and Platform Support Enhancements
- Vault Administrator Continuity and Alert Recipient Enhancements
- CSR Country Code Flexibility
- Interactive Swagger API Documentation

SNMP v3 Support

Added support for SNMP v3, SNMP v2c is no longer supported.

Lenovo SR250/SR630 Appliance Deployment Support

Added support for the deployment of the CSP Vault appliance on Lenovo SR250/SR630 physical server models.

PKCS#11 Vault Support

Implemented a new vault type and a lightweight client to add support for the PKCS#11 Cryptographic Token Interface Base Specification.

Microsoft External Key Manager Support

Added support for Microsoft's External Key Manager protocol.

Fine-Grained Administrative Roles and Permissions

Introduced fine-grained administrative roles and permission controls for CSP Vault appliance management tasks.

GitLab Secrets Vault Integration

Added GitLab integration for Secrets Vault, enabling CI/CD pipelines to securely retrieve and inject application credentials directly from Secrets Vault at runtime.

AWS IAM and STS Secrets Vault Integration

Introduced a dedicated Secrets Vault integration that enables secure storage and rotation of AWS IAM user access keys, as well as on-demand issuance of short-lived AWS STS session tokens and AssumeRole credentials with federated console sign-in.

Azure Entra ID Secrets Vault Integration

Added a dedicated Secrets Vault integration for securely storing and rotating Azure Entra ID (App Registration and Service Principal) credentials, including client secrets and certificates, and for issuing short-lived Azure AD access tokens on demand for Azure management and Microsoft Graph scopes.

Offline Cloud Encryption Key Generation

Added support for generating cloud encryption keys for AWS, Azure, GCP, Salesforce, and OCI offline within CSP Vault, eliminating the need for direct connectivity to the respective cloud providers.

OCI EKM Management Interface Decoupling

Decoupled Oracle Cloud Infrastructure External Key Management (OCI EKM) from the Cloud Key Vault management interface.

Generic Authentication Error Responses

Enhanced security by using generic authentication error responses across vaults to help prevent username enumeration.

ECDSA 384-bit Certificate and Trust Validation Enhancements

Enhanced certificate management and trust validation by adding support for ECDSA 384-bit certificates across internal and external web servers and KMIP servers, optimizing certificate chains to include only the required intermediate certificates, and enabling the use of custom CA certificates for email notification trust verification.

Database Vault TDE and Platform Support Enhancements

Enhanced Database Vault platform support by extending Transparent Data Encryption (TDE) capabilities to Oracle Exadata Cloud@Customer (ExaCC) environments, adding key export and import functionality for seamless TDE key forwarding between database instances, and expanding the officially tested database platform matrix to include PostgreSQL 18.

Vault Administrator Continuity and Alert Recipient Enhancements

Enhanced administrative continuity by allowing organizations to update or replace the primary Vault Administrator account when personnel changes occur, and by enabling email distribution lists (DLs) to be configured as alert recipients across all Vaults and appliances.

CSR Country Code Flexibility

Enhanced CSR generation flexibility by allowing empty or period ('.') values in the Country Code field during Web GUI certificate signing request (CSR) creation, improving compatibility with enterprise CA policies.

Interactive Swagger API Documentation

Replaced the API documentation at /apidoc with an interactive Swagger (OpenAPI 3.1) UI that lets you run APIs directly from the browser.

Fixed in 10.6.1

See below for the issues fixed by the 10.6.1 release.

- VME Vault Certificate Renewal
- KMIP and Postgres Service Restart
- Multi-Node Cluster Upgrade Reliability
- Azure Managed HSM AES Cloud Keys
- CA-Chain Certificate Filtering
- NVMe Root Disk Selection
- Database Vault Race Condition
- Key Cache Invalidation After HSM Connectivity Loss
- KMIP Certificate Expiration Alerts

- Audit Configuration Concurrent Access
- SMTP Custom CA Certificate Trust
- OIDC Configuration Concurrency
- Rotated System Log Compression
- kmipcli Explicit Logout
- Failed Upgrade Disk Space Visibility
- Database Vault Access Token Validation
- Database Vault TDE Prerequisite Validation
- HTTP/2 API Compliance
- kmipcli UUID Case Sensitivity
- Scheduled Backup Alerting
- KeySafe5 Setting Management
- Access Policy Self-Removal
- Windows Policy Agent UI Name
- Tokenization Database Upgrade Recovery
- TUI High CPU Error Handling
- Simultaneous Node Reboot Race Condition
- Local User Force-Delete Warning
- hcl attach Interrupted Operations

VME Vault Certificate Renewal

Fixed an issue where VME Vault was creating a renewal certificate on every heartbeat even when there is an unadopted certificate.

KMIP and Postgres Service Restart

The KMIP and Postgres services now restart correctly after renewing the self-signed server certificate.

Multi-Node Cluster Upgrade Reliability

Improved the upgrade reliability of the multi-node CSP Vault appliance cluster.

Azure Managed HSM AES Cloud Keys

Added the AES key option while creating Azure cloud keys with a managed HSM key vault.

CA-Chain Certificate Filtering

Added a fix to trim down the CA chain and keep only the relevant certificates, such as intermediate and root CA certificates, that are used to verify the server certificate.

NVMe Root Disk Selection

Added support for selecting NVMe disks as the root disk of the CSP vault appliance.

Database Vault Race Condition

Fixed a race condition in the Database Vault libraries for Microsoft SQL Server and Oracle databases.

Key Cache Invalidation After HSM Connectivity Loss

Added support for automatically invalidating the key cache after a configurable timeout when HSM connectivity is lost.

KMIP Certificate Expiration Alerts

Added advanced email and SNMP alerts for upcoming KMIP certificate expirations.

Audit Configuration Concurrent Access

Fixed an issue that could cause audit configuration file corruption during concurrent access operations.

SMTP Custom CA Certificate Trust

Resolved SMTP certificate trust verification issues by allowing custom CA certificates to be uploaded during SMTP configuration.

OIDC Configuration Concurrency

Fixed an issue that could create duplicate OIDC configuration entries when multiple configuration requests were processed concurrently.

Rotated System Log Compression

Improved log management by automatically compressing rotated system logs to reduce disk space consumption.

kmipcli Explicit Logout

Added an explicit logout option to kmipcli, allowing users to immediately terminate active sessions.

Failed Upgrade Disk Space Visibility

Enhanced the WebGUI to display nodes with insufficient disk space during failed upgrade validation checks.

Database Vault Access Token Validation

Fixed an issue where invalid access tokens or identities were not properly validated when connecting to the Database Vault.

Database Vault TDE Prerequisite Validation

Added prerequisite validation checks to Database Vault TDE installation scripts.

HTTP/2 API Compliance

Modified CSP Vault APIs to conform to HTTP/2 standards.

kmipcli UUID Case Sensitivity

Resolved an issue causing kmipcli to incorrectly enforce case-sensitive UUID matching.

Scheduled Backup Alerting

Improved scheduled backup alerting by suppressing notifications for the first backup failure and generating alerts only for consecutive failures.

KeySafe5 Setting Management

Added support for enabling or disabling the KeySafe5 setting from any cluster node through the HSM details page.

Access Policy Self-Removal

Removed restrictions that prevented users from removing themselves from access policies in Secrets Vault, KMIP Vault, and Tokenization Vault.

Windows Policy Agent UI Name

Modified the Windows policy agent to display "Entrust KeyControl Agent" in the UI.

Tokenization Database Upgrade Recovery

Added a `hicli` option to rerun Tokenization Database upgrades, providing additional recovery capabilities for upgrade failures.

TUI High CPU Error Handling

Fixed an issue that could cause the TUI to become stuck indefinitely under certain error conditions, resulting in high CPU usage on the Vault appliance node.

Simultaneous Node Reboot Race Condition

Resolved a race condition that could occur when multiple nodes rebooted simultaneously.

Local User Force-Delete Warning

Enhanced user management by displaying a force-delete warning when deleting a local user who is assigned to one or more access policies.

hcl attach Interrupted Operations

Fixed an issue where hcl attach could incorrectly report interrupted encrypt, decrypt, or rekey operations.

Vault issues in 10.6.1

See below for the known Vault issues in 10.6.1

- Upgrade failures during ISO upload on slow networks
- PKCS#11 vault metadata export fails with non-unicode labels
- SNMP trap delivery does not match the configured SNMP state
- Temporary password not displayed when SMTP is disabled
- OIDC unsupported for PKCS#11 Vault deployments
- VMware virtual hardware changes trigger Admin Key Recovery
- KeySafe5 agent runs only on the Compliance Manager master node

- Upgrade prerequisites for Vault Management and vault appliances
- KMIP TLS 1.3 selection restricts the protocol version
- Key-value text secrets cannot be checked out in the Secrets web GUI
- Multi-node upgrades can fail because of latency
- Clear Cache clears all Cryptographic APIs caches
- Unsupported SSH key algorithms and sizes
- Unsupported KMIP RSA key sizes
- vSAN trust requires an IP address when no FQDN DNS entry exists
- AD administrators require a rescue user
- Reverting a Vault cluster requires all prior-version nodes
- AWS XKS network latency limit
- Restore recovery can take a long time
- Two-factor authentication is limited to local users
- Upgrade must be completed on the initiating node
- OIDC is unavailable during backup restoration
- Browser cache must be cleared after upgrading
- System Recovery cannot restore access after simultaneous hardware and IP changes
- KC node hostname and domain name cannot be changed
- Cloud VM Set names must be unique
- Degraded-cluster alerts are delayed
- Custom SSL certificates require a webserver restart from the web GUI
- Expiration date changes can fail because of UTC time
- Corrupted audit log entries do not display correctly
- Longer cluster timeouts delay degraded-state processing

Upgrade failures during ISO upload on slow networks

On slow network connections, upgrades may fail during ISO upload. Retrying the upgrade usually resolves the issue.

> This issue is fixed in the 10.6.1 release.

PKCS#11 vault metadata export fails with non-unicode labels

Metadata export for PKCS#11 vaults fails when object labels contain non-Unicode characters.

SNMP trap delivery does not match the configured SNMP state

For vaults, SNMP trap delivery is inverted. Traps are not received by the NNMi SNMP server when SNMP trap settings are enabled, but continue to be received when SNMP is disabled. As a result, SNMP-based alerting does not reflect the configured SNMP state of the vault.

Temporary password not displayed when SMTP is disabled

When SMTP is disabled, the system-generated temporary password is not displayed in the CSP Vault WebGUI after an administrator resets another user's password. As a workaround, retrieve the password using the API/Postman scripts or from the browser's Network tab. When SMTP is enabled, the system-generated temporary password is sent to the user's email address following a password reset.

OIDC unsupported for PKCS#11 Vault deployments

This release does not support OIDC authentication for PKCS#11 Vault deployments.

VMware virtual hardware changes trigger Admin Key Recovery

Changing the VMware virtual hardware version of a CSP Vault appliance will trigger the Admin Key Recovery process.

KeySafe5 agent runs only on the Compliance Manager master node

Because the KeySafe5 agent does not support clustering, it only runs on the master node of the Cryptographic Security Platform Compliance Manager cluster. If you remove that node, the KeySafe5 agent will stop working.

To fix this issue:

1. Disconnect and reconnect your connection to Cryptographic Security Platform Compliance Manager.
2. You must be connected as an Appliance Cluster, not a Data Source.
3. Create the connection using the Compliance Manager master node IP, not a load balancer IP or hostname.
4. Disable and re-enable the KeySafe5 agent from the HSM settings page.

This will reestablish the connection between the KeySafe5 agent and the Compliance Manager.

Upgrade prerequisites for Vault Management and vault appliances

Before you can upgrade to 10.6.1:

- The Cryptographic Security Platform Vault Management appliance and all vaults must be connected to the Cryptographic Security Platform Compliance Manager at version 10.6.1 or 10.5.3.
- All appliances and vaults must be able to fetch the relevant license information from the Cryptographic Security Platform Compliance Manager
- The license should not be expired. If you are not in compliance with your current license, you will not be able to upgrade.

KMIP TLS 1.3 selection restricts the protocol version

By default, the Cryptographic Security Platform Vault for KMIP enables both TLS 1.2 and TLS 1.3. If you select the TLS 1.3 option, the protocol will be restricted to TLS 1.3 only.

Key-value text secrets cannot be checked out in the Secrets web GUI

If you create a text secret with a key-value value, you will get an error when checking it out from the Cryptographic Security Platform Vault for Secrets web GUI. However, you can still check out the secret from the CLI. To fix this issue, delete the secret and re-create it, specifying the secret type as "Key-Value". This should allow checkouts to succeed from the web GUI.

Multi-node upgrades can fail because of latency

If you attempt to upgrade multiple nodes, the upgrade may fail due to latency. Contact Support if this happens.

Clear Cache clears all Cryptographic APIs caches

If you run the Clear Cache command in the Cryptographic Security Platform Vault for Cryptographic APIs web GUI, all caches are cleared no matter which cache type you specify.

Unsupported SSH key algorithms and sizes

Cryptographic Security Platform Vault for Secrets administrators can no longer create SSH secrets that contain SSH keys with the ED25519 algorithm and RSA keys with a 1024-bit length.

Unsupported KMIP RSA key sizes

The Cryptographic Security Platform Vault for KMIP no longer supports creating 512-bit or 1024-bit RSA keys.

vSAN trust requires an IP address when no FQDN DNS entry exists

If you do not have the DNS entry for the FQDN for a Cryptographic Security Platform Vault node, use the IP address when establishing trust between vSAN and the KMIP Vault.

AD administrators require a rescue user

In the Cryptographic Security Platform Vault for Application Security, Cryptographic Security Platform Vault for KMIP, and Cryptographic Security Platform Vault for Secrets, when the authentication type is set to AD and the AD group is set up as an admin principal in the Admin Policy, set up a corresponding AD user from the group as a rescue user and add that user to the admin principal list as well as the AD Group.

Reverting a Vault cluster requires all prior-version nodes

Before reverting a Cryptographic Security Platform Vault cluster to an older version, ensure that all of the nodes that existed in the older version are available.

AWS XKS network latency limit

For AWS XKS, the maximum round-trip network latency between KMS in the AWS region and Cryptographic Security Platform Vault is 250 milliseconds. The KMS times out if it does not receive a response back from Cryptographic Security Platform Vault within 250 milliseconds. For more details, see the AWS documentation.

Restore recovery can take a long time

After restore, Cryptographic Security Platform Vault may display errors on the login screen. The recovery process works but takes a long time.

Two-factor authentication is limited to local users

Two-factor authentication is supported only for local users, not AD users.

Upgrade must be completed on the initiating node

Complete the Cryptographic Security Platform Vault upgrade on the same node where you initiated the upgrade.

OIDC is unavailable during backup restoration

When restoring a backup, the OpenID Connect (OIDC) service will not be available until the restore operation completes. Refreshing the login page will display the OIDC login once the process completes. Rebooting the node after the login page is available will also restore the OIDC service.

Browser cache must be cleared after upgrading

You must clear your browser's cache after upgrading Cryptographic Security Platform Vault.

System Recovery cannot restore access after simultaneous hardware and IP changes

If the hardware configuration and the IP address for a node change simultaneously, you cannot use the System Recovery option in the Cryptographic Security Platform Vault web GUI to restore access to Cryptographic Security Platform Vault. If this happens, contact Entrust Support.

KC node hostname and domain name cannot be changed

You cannot change a KC node's hostname or domain name once the system has been fully initialized. This is due to object store requirements. If you must make a change, remove the node from the cluster and reinstall it with the new hostname or domain name. Then you can add the node back to the cluster.

Cloud VM Set names must be unique

All Cloud VM Sets that the logged-in Cloud Admin can access must have unique names. If a Cloud Admin tries to edit or delete an existing VM Set with a duplicate name, they will first be prompted to change the VM Set name before they can continue with the edit or delete operation.

Degraded-cluster alerts are delayed

If a Cryptographic Security Platform Vault cluster is in the degraded state, alerts are not posted until the cluster becomes healthy. Email notifications and remote syslog messages, however, are delivered immediately even if the cluster is degraded.

Custom SSL certificates require a webserver restart from the web GUI

When you install a custom SSL certificate on a Cryptographic Security Platform Vault node, you must restart the webserver from the web GUI to use the new certificate. A Cryptographic Security Platform Vault node reboot does not have the same effect. After a node reboot, you must restart the web server from the web GUI to use the newly installed SSL certificate.

Expiration date changes can fail because of UTC time

The Cryptographic Security Platform Vault time zone is set to UTC (Coordinated Universal Time), whereas the web GUI translates the time to the browser's local time zone. While changing a key, device, or certificate expiration date from the browser, the operation might fail with the error "Expiration date must be in the future". This happens when the administrator sets the expiration date to the next day in local time, but the UTC date has already passed. For example, in Pacific Daylight Time (PDT), which is 7 hours behind UTC during daylight saving time, the UTC date has moved to the next day after 5 PM, so setting the expiration date to the next day fails.

Corrupted audit log entries do not display correctly

If the audit log contains corrupted entries, it will not display properly in the Cryptographic Security Platform Vault web GUI. If this issue arises, contact Entrust Support.

Longer cluster timeouts delay degraded-state processing

You can lengthen the Cryptographic Security Platform Vault cluster timeout to improve scalability. This causes delays when the cluster is degraded equal to twice the timeout value. These delays end a few minutes after the cluster enters the degraded state.

Windows-specific Policy Agent issues in 10.6.1

See below for the Windows-specific Policy Agent issues in 10.6.1.

- Windows Server 2025 MBR VM installation is unsupported
- VM does not boot after bootloader installation
- KVM bootloader support is unavailable
- Imported disk rekey does not restart automatically
- Bootloader installation error during Windows boot encryption
- MBR to GPT conversion is unsupported
- Shrinking a partition during rekey fails
- VM cloning with an encrypted Active Directory drive is unsupported
- Background encryption requires Vault availability after reboot
- Partition extension leaves unallocated space
- Encrypted disks do not attach after reauthorization or certificate expiry
- Encrypted data drives require the HCLD service
- Bootloader network interface configuration error
- Imported disks can receive conflicting drive letters
- Migrated encrypted disks can receive incorrect drive letters
- Boot volume extension can show an incorrect size in the web GUI
- PendingFileRename can prevent SEP installation
- Early Attach requires a gateway with a static first NIC
- Paging files on encrypted data drives are unsupported
- Encrypted boot partitions and Policy Agent binaries require C:
- Azure instance restarts prevent Early Attach on first boot
- Do not reboot or shut down while a disk is decrypting

Windows Server 2025 MBR VM installation is unsupported

Windows policy agent installation is not allowed in Windows Server 2025 MBR (Legacy BIOS) VMs.

VM does not boot after bootloader installation

If the Windows VM installed with the Entrust policy agent's bootloader does not boot:

1. Disable the OS secure boot option and retry.
2. Update to the latest Microsoft patch, as this behavior may have been fixed.

KVM bootloader support is unavailable

Windows policy agent does not support bootloaders in the Windows VM created on the KVM hypervisor.

Imported disk rekey does not restart automatically

Importing an encrypted disk with a pending rekey does not automatically restart the rekey. Reboot the system after importing the disk to resume the rekeying process.

Bootloader installation error during Windows boot encryption

If the following error is seen during Windows boot encryption, "Please install the Windows bootloader before encrypting," and the bootloader is already installed, then perform the following steps:

1. Verify that the HyTrust Bootloader partition is available on the boot disk (labeled "HTBOOTLDR" or "HTEFIBL").
2. Mount the Bootloader partition with the Drive Letter specified at HKLM\Software\HyTrust\bootldr_driveletter in the registry.
3. If the HyTrust bootloader partition is not available, install it using the InstallHTBootloader.ps1 script.

MBR to GPT conversion is unsupported

Converting MBR boot disk to GPT using MBR2GPT utility is not supported.

Shrinking a partition during rekey fails

Shrinking an encrypted partition during rekey fails. After rekey completes, extend the file system using the diskpart command and then shrink the partition.

VM cloning with an encrypted Active Directory drive is unsupported

You cannot clone a VM if one of the encrypted data drives on that VM contains a Windows Active Directory (AD) Server and its AD Database.

Background encryption requires Vault availability after reboot

If the system reboots while a drive is being encrypted in the background, the drive becomes inaccessible if the Cryptographic Security Platform Vault is not accessible. Workaround: Reboot the system again after the Cryptographic Security Platform Vault becomes available.

Partition extension leaves unallocated space

If unallocated space exists between two partitions, extending a partition will leave 10MB of unallocated space after the extended partition.

Encrypted disks do not attach after reauthorization or certificate expiry

If a system is rebooted after the grace period has expired, when reauthorization is required, or if the VM certificate has expired, Cryptographic Security Platform Vault does not attach the encrypted data disks. If the Active Directory Database (AD DB) is located on one of the encrypted data disks, the system will not boot.

Workaround for AD DB issue:

1. Boot the system into Directory Services Restore Mode (DSRM)
2. Take the appropriate corrective action
3. Ensure the data disks are correctly attached
4. Reboot the system

Workaround for all other cases:

1. Take the appropriate corrective action
2. Reboot the system or restart any services that failed because disks were not available
3. Restart the 'LanManServer' service for File Sharing

Encrypted data drives require the HCLD service

Encrypted data drives will become inaccessible if the Entrust KeyControl Service 'HCLD' is stopped.

Bootloader network interface configuration error

If you see the error message: "HyTrust Bootloader is configured to use a network interface which is different from the one used to connect to the Cryptographic Security Platform Vault server. Please reconfigure HyTrust bootloader network configuration to use the correct network interface. If you do not wish to update the network configuration (not recommended), please use option 'N'."

1. Verify the network setting using htblconf.exe or the PowerShell `SetupHTBootloaderNetwork.ps1` script.
2. If you do not want to update the network configuration, or you determine that networking is configured correctly for the bootloader, use the -N option (as suggested) to force encryption in those cases. For example:

```
hcl encrypt -N C:
```

Imported disks can receive conflicting drive letters

When importing disks to a Windows VM, Windows may assign a conflicting drive letter to the newly imported partitions. In Windows Disk Manager, reassign the drive letters as needed before using hcl import to incorporate the new drive.

Migrated encrypted disks can receive incorrect drive letters

Migrating an encrypted disk from one VM to another VM may cause incorrect/invalid drive letter assignments. To correct the drive letter assignments:

1. Remove current drive letter assignments for all the encrypted data disks.
2. Assign drive letters to the encrypted data disks that were already present on the VM. Each drive letter assignment must be the same as what it was before.
3. Assign any available drive letter to the migrated encrypted data disk.

Boot volume extension can show an incorrect size in the web GUI

If Cryptographic Security Platform Vault is unreachable when you extend the boot volume using the MoveHTBootloader.ps1 script, the new size of the disk may not be accurately displayed in the Cryptographic Security Platform Vault web GUI. Workaround: Manually update the volume size in the web GUI using the following command.

```
hcl extend C:.
```

PendingFileRename can prevent SEP installation

A `PendingFileRename` registry entry is created on HCLD startup with a location for the following file:

```
hcs\hcld.boot
```

SEP might refuse to install if this registry key is present. See https://support.symantec.com/en_US/article.TECH98292.html for details.

If `hcs\hcld.boot` is the only entry in the `PendingFileRename` registry entry:

1. Back up the following entry

   ```
   Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
   Manager\PendingFileRename
   ```

2. Restart SEP installation
3. Wait while the installation completes
4. Restore the backup before any system restart.

Early Attach requires a gateway with a static first NIC

Early Attach requires the Gateway to be configured if the first network interface has a Static IP address. NIC teaming is not supported.

Paging files on encrypted data drives are unsupported

Windows Policy Agent does not support the paging file on encrypted data drives.

Encrypted boot partitions and Policy Agent binaries require C:

Windows Policy Agent requires the boot partition to be on C: if it is to be encrypted. Also, encryption of a non-C: device that contains the Policy Agent binary is not supported.

Azure instance restarts prevent Early Attach on first boot

Azure replaces the Network Interface and assigns a new MAC address on VM Instance restart. Early Attach cannot set up access to encrypted data disks on the first boot. Workaround: Reboot the guest OS.

Do not reboot or shut down while a disk is decrypting

Do not reboot or shut down while a disk is being decrypted. If the system reboots while a disk is being decrypted, it might not reboot, or the data disk might become inaccessible due to File System corruption.

Linux-specific Policy Agent issues in 10.6.1

See below for the Linux-specific Policy Agent issues in 10.6.1.

- RHEL 10 root disk encryption requires Dropbear
- SUSE15 Dropbear and debug console configuration
- Amazon Linux 2 root drive encryption
- RHEL 8.5 DHCP root encryption requires dhclient

- RHEL 8 access control requires Python 3.9
- Do not revert a VM during a root-device rekey
- Update GRUB and shim before secure boot
- Red Hat 8 shim-x64 compatibility
- Azure RHEL 8.1 Gen 1 LVM root encryption
- BTRFS multiple-disk encryption
- Online rekey filesystem display after reboot
- Linux Access Controls on LVM devices
- AWS BIOS boot partition
- HTCrypt Driver during encryption operations
- HTCrypt Driver kernel taint message
- Access Control Policy filesystem support
- Rebuilding HTCrypt Driver after kernel package updates
- WebGUI root partition encryption
- Amazon and Azure root encryption boot disk swap

RHEL 10 root disk encryption requires Dropbear

Linux root disk encryption on RHEL 10 may fail because EPEL does not include Dropbear. To fix this issue:

1. Manually install Dropbear using the following command:

```
yum install https://dl.fedoraproject.org/pub/epel/10.2/Everything/x86_64/
Packages/d/dropbear-2025.88-1.el10_1.x86_64.rpm
```

2. Restart the root disk encryption script, htroot.
3. When you are prompted to install Dropbear, select No.

SUSE15 Dropbear and debug console configuration

On SUSE15, either install dropbear manually or do not enable the debug console in the htroot setup.

Amazon Linux 2 root drive encryption

Root drive encryption does not work for Amazon Linux 2 AMI - Kernel 5.10.

RHEL 8.5 DHCP root encryption requires dhclient

For RHEL 8.5 and later, you must install "dhclient" to configure htroot with DHCP.

RHEL 8 access control requires Python 3.9

On RHEL 8. x machines, the Linux policy agent access control policy requires Python 3.9 or greater.

Do not revert a VM during a root-device rekey

Do not revert to a VM snapshot when a system/root device has a rekey in progress.

Update GRUB and shim before secure boot

Update the grub and shim packages before running "htdrv secure-boot".

Red Hat 8 shim-x64 compatibility

On Red Hat 8.x, the online encryption driver does not work with the default "shim-x64" package. To fix this issue, downgrade the shim-x64 package version to 15-11.

Azure RHEL 8.1 Gen 1 LVM root encryption

Root drive encryption is not supported in the RHEL 8.1 (LVM) - Gen 1 image on Azure.

BTRFS multiple-disk encryption

If you use BTRFS with multiple disks for root or any system mount, only the disk shown in `/etc/fstab` can be encrypted.

Online rekey filesystem display after reboot

If the VM is rebooted in the middle of an online rekey, the rekey completes successfully after the VM reboots. However, the lsblk -fs command no longer shows the correct file system for the clear text device. To fix this, the admin can run partprobe manually.

Linux Access Controls on LVM devices

Linux Access Controls is currently not supported on LVM devices. Users should refrain from applying Access Control Policy on LVM devices.

AWS BIOS boot partition

Linux Policy Agent on AWS will show the BIOS boot partition as an available device. This partition should not be encrypted.

HTCrypt Driver during encryption operations

Do not install the HTCrypt Driver on a VM if any device in the VM is being encrypted, rekeyed, or decrypted. If you do so, you will need to remove the HTCrypt Driver rpm before you can finish encrypting, rekeying, or decrypting the devices in the VM. After these processes finish, you can reinstall the HTCrypt Driver.

HTCrypt Driver kernel taint message

When the HTCrypt Driver is loaded, it may show the following kernel message: "htcrypt: loading out-of-tree module taints kernel". You can safely ignore this message because Entrust provides and supports the HTCrypt Driver.

Access Control Policy filesystem support

On Linux, you can't enforce an Access Control Policy on an encrypted disk unless it uses one of the supported filesystems.

Rebuilding HTCrypt Driver after kernel package updates

If the kernel-devel and kernel-headers packages are updated separately from the kernel package, then a reboot is required to rebuild the HTCrypt Driver for the updated kernel.

WebGUI root partition encryption

Encryption of the Linux root partition from the Cryptographic Security Platform Vault webGUI using the Encrypt Disk action is not supported.

Amazon and Azure root encryption boot disk swap

The Linux Policy Agent in Amazon and Azure requires a manual swap of boot and root disks for root encryption before rebooting. See the Administration Guide for more information.

5 Requirements

See below for the Vault requirements.

- System resources
- Network requirements
- Browser requirements
- Platform requirements

System resources

Entrust recommends the following system resources based on your installation size. If your system does not meet these requirements, the installation may fail, or you may encounter performance issues.

Resource	Standard installation	Large installation
CPUs	2	4
RAM	8 GB	16 GB
Disk	65 GB	150 GB

Entrust recommends that you select a large installation if your system meets one or more of the following criteria:

- More than four nodes in the Cryptographic Security Platform Vault cluster.
- More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
- More than 100,000 secrets stored.

Network requirements

All Cryptographic Security Platform Vault IP addresses must use IPv4. Cryptographic Security Platform Vault does not support IPv6 addresses.

For Cryptographic Security Platform Vault to Cryptographic Security Platform Vault, Cryptographic Security Platform Vault to Cryptographic Security Platform Compliance Manager, and Policy Agent to Cryptographic Security Platform Vault, the following ports need to be open:

- **Internal protocol**—The Cryptographic Security Platform Vault nodes must be able to communicate on `TCP/443`, `TCP/8443`, and `TCP/5432`. If you have a firewall between one or more nodes, make sure these ports are open.
- **Cryptographic Security Platform Compliance Manager**—The Cryptographic Security Platform Vault nodes must be able to communicate `TCP/443` outbound to the Cryptographic Security Platform Compliance Manager.
- **Cryptographic Security Platform Vault webGUI**—Inbound TCP/443 to administrator systems from any Cryptographic Security Platform Vault server in the cluster.
- **Cryptographic Security Platform Vault support-level access**—Inbound TCP/22 from administrator systems to any Cryptographic Security Platform Vault server in the cluster.
- **Policy Agent to Cryptographic Security Platform Vault**—Inbound TCP/443 from the Policy Agent to each of the Cryptographic Security Platform Vault nodes in the cluster.

For Cryptographic Security Platform Vault infrastructure services, the following ports need to be open:

- **DNS**—Outbound UDP/53
- **SMTP**—Outbound mail server, typically TCP/25.

  > If you disable SMTPS and the server supports StartTLS, it will use StartTLS when the connection is made. SMTPS is not compatible with StartTLS, and only one can be used.

- **SYSLOG**—An outbound TCP/UDP port between 25 and 65535 if you want to use a remote syslog server. Cryptographic Security Platform Vault supports both TCP and UDP for syslog.
- **Backup and Restore via NFS**—If you want to access the Cryptographic Security Platform Vault-generated backup files via NFS, you need to open the following ports: 2046 (lockd), 2047 (rpc statd), 2048 (rcp mountd), and 2049 (default NFS port).
  If you need to check the port status, you can run one of the following commands:
  `rcpinfo <KeyControl_Vault_IP_Address>` or `rcpinfo <KeyControl_Vault_Name>`
- **NTP**—Outbound NTP servers, typically UDP/123 or TCP/123

  > The network ports indicated for SMTP, syslog, and NTP are the typical ports for these services. If you need to change those ports, consult with the administrators of these services.

To configure Cryptographic Security Platform Vault as a KMIP server, open the port you plan to use. The default KMIP port is 5696.

Browser requirements

The Cryptographic Security Platform Vault webGUI administrative interface requires HTTPS access and has been tested on the following browsers:

- Chrome
- Firefox
- Edge

Platform requirements

We support the 64-bit versions of the Linux and Windows platforms listed below. 32-bit versions are *not* supported.

- Hypervisors supported for Vault
- Linux platforms supported for Policy Agent
- Windows platforms supported for Policy Agent
- Hypervisors Supported for Policy Agent

> The following information is for virtual machines only. Physical servers are not supported.

Hypervisors supported for Vault

See below for the hypervisors supported for Entrust Cryptographic Security Platform Vault.

Hypervisor	Versions supported	Notes
KVM hypervisor	Red Hat 7.8 and above	To access the System Console in KVM on Redhat 10.0, please use the RHEL web console (Cockpit).
VMware ESXi	VMware ESXi 8.0 (HW version 20) and above	
AWS	Latest Entrust version available in the marketplace	
Azure	Latest Entrust version available in the marketplace	
Google Cloud Platform	Latest Entrust version available in the marketplace	
Nutanix AHV	Nutanix AOS 7.3 and above	Documentation for deploying Entrust Cryptographic Security Platform on Nutanix is available on the nShield Documentation site. Search on Nutanix to locate it on the page.
Microsoft Hyper-V and Hyper-V 2025	Microsoft Windows Server 2019, 2022, 2025	

Linux platforms supported for Policy Agent

All supported Linux versions also support XFS (Extent File System). If the Linux version you are running is not listed, contact Entrust Support and provide information about the Linux version and the problems encountered.

Linux Online Encryption is only supported for RHEL 8.0 or later, or Ubuntu 20.04 or later. For details, see Linux Online Encryption Prerequisites and Considerations

Platform	Data encryption	Root/Swap encryption	Online encryption	Offline encryption
RHEL10.0 - 10.2	✔	✔	✔	✔

Platform	Data encryption	Root/Swap encryption	Online encryption	Offline encryption
RHEL 9.0 - 9.8	✓	✓	✓	✓
RHEL 8.10	✓	✓	✓	✓
Ubuntu 26.4	✓	✓	✓	✓
Ubuntu 24.04	✓	✓	✓	✓
Ubuntu 22.04	✓	✓	✓	✓
Rocky Linux 10.0 - 10.2	✓	✓	✓	✓
Rocky Linux 9.4 - 9.8	✓	✓	✓	✓
Rocky Linux 8.10	✓	✓	✓	✓
Oracle Linux 10	✓	✓	✓	✓
Oracle Linux 9.1 - 9.8	✓	✓	✓	✓
Oracle Linux 8.10 - 10.2	✓	✓	✓	✓
SUSE Linux Enterprise Server 15 SP7	✓	✓	✗	✓
SUSE Linux Enterprise Server 12 SP5	✓	✓	✗	✓

Windows platforms supported for Policy Agent

All Windows operating systems listed below are supported on Amazon Web Services and Microsoft Azure. For data encryption:

- Only Windows basic disks are supported. Windows dynamic disks are *not* supported.

- To use the `hicli` command line interface with Windows, you need to enable WinRM (Windows Remote Management), which is disabled by default. The Python `pywinrm` package must also be installed on the Windows control node on which `hicli` is running.
- In AWS, Azure, and Google Cloud, Entrust does not support Secure Boot on Windows.

⚠ Make sure that you have the latest Microsoft patches on your Windows operating system.

Platform	Data drive and Folder encryption	Boot drive encryption	Online encryption
Microsoft Windows Server 2025 (OS build 26100) (UEFI Enabled)	✔	✔	✔
Microsoft Windows Server 2022 (OS build 20348)	✔	✔	✔
Microsoft Windows Server 2019 (OS build 17763)	✔	✔	✔
Microsoft Windows Server 2016 (OS build 14393)	✔	✔	✔
Server Core for Microsoft Windows Server 2019	✔	✔	✔
Server Core for Microsoft Windows Server 2016	✔	✔	✔

Hypervisors Supported for Policy Agent

Both Linux and Windows clients are supported with the following Hypervisors.

Hypervisor	Data encryption	Root/Swap and Boot Encryption
VMware ESXi 8.0 (HW version 20) and above	✔	✔
Microsoft Hyper-V	✔	✔
KVM (on RHEL 8 and above)	✔	✔
Proxmox	✔	✔

Hypervisor	Data encryption	Root/Swap and Boot Encryption
AWS	✓	✓ Secure Boot is not supported.
Azure	✓	✓ Secure Boot is not supported.
Google Cloud Platform	✓	✓ Secure Boot is not supported.
Nutanix AHV	✓	✓

6 Installing CSP Vault

- Installation Overview
- CSP Vault OVA Installation
- CSP Vault ISO Installation for Hypervisor
- CSP Vault ISO Installation for Bare Metal Server
- CSP Vault in Amazon Web Services
- CSP Vault in Google Cloud Platform
- CSP Vault in Microsoft Azure

Installation Overview

This document contains the standard installation procedures for Entrust Cryptographic Security Platform Vault.

- For installation on Amazon Web Services, see CSP Vault in Amazon Web Services.
- For installation on Microsoft Azure, see CSP Vault in Microsoft Azure.
- For installation on Google Cloud Platform, see CSP Vault in Google Cloud Platform.

To configure a basic Cryptographic Security Platform Vault cluster and register one or more VMs with that cluster, you need to install Cryptographic Security Platform Vault on one or more servers and then install the Policy Agent on each VM you want to register. To do so:

Step	Description	Notes
1	Verify that the systems you want to use meet the basic system requirements.	See Requirements.
2	Install the Cryptographic Security Platform Vault software on the target system. Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.	If you want to use VMware vCenter to deploy Cryptographic Security Platform Vault using an OVA template, see CSP Vault OVA Installation. If you want to install Cryptographic Security Platform Vault on an existing VM, see CSP Vault ISO Installation for Hypervisor.
3	Configure the first Cryptographic Security Platform Vault node and initialize the Cryptographic Security Platform Vault webGUI.	For OVA, see Configuring the First CSP Vault Node (OVA Install). For ISO, see Installing the First CSP Vault Node from an ISO Image.

Step	Description	Notes
4	If desired, install additional Cryptographic Security Platform Vault nodes and join them to the cluster. The number of nodes you can install is dictated by your Cryptographic Security Platform Vault license.	For OVA, see CSP Vault OVA Installation followed by Adding a New CSP Vault Node to an Existing Cluster (OVA Install). For ISO, see Installing a New Cryptographic Security Platform Vault Cluster Node from an ISO Image.

CSP Vault OVA Installation

- OVA installation overview
- Installing CSP Vault from an OVA Template
- Configuring the First CSP Vault Node (OVA Install)
- Adding a New CSP Vault Node to an Existing Cluster (OVA Install)

OVA installation overview

For deployment in a vSphere environment with vCenter, Entrust provides a single virtual node in OVA format. You use the same OVA file to install as many Cryptographic Security Platform Vault nodes as you need.

> If you are running directly on ESX and not through vCenter, install from an ISO image as described in CSP Vault ISO Installation for Hypervisor.

Installing CSP Vault from an OVA Template

Before You Begin

Make sure that:

- You know the IP address and any required network connection information, such as the domain name and the DNS and gateway IP addresses, for the machine on which you are installing Cryptographic Security Platform Vault.
  Note: You must use an IPv4 address. Cryptographic Security Platform Vault does not support IPv6 addresses.
- You have the required permissions to install software on the target system.
- The target system meets the basic system requirements described in System Requirements.
- If you are using VMware, ensure that all of your CSP Vault deployments have VM-to-Host affinity enabled. This allows you to avoid Admin Key Recovery due to host migration. We recommend that you select 'Should run on hosts in group' for the rule specification. The group should contain only the one ESXi host that you are using for this Cryptographic Security Platform Vault VM.

Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.

Procedure

1. Log in to your vSphere Client.
2. Navigate to **Hosts and Clusters**.

3. Select **Actions > Deploy OVF Template**.
   Note: In this context, OVF and OVA are synonymous.
4. On the **Select template** page of the **Deploy OVF Template** wizard, browse to the location of your OVA file.
5. Select the file and click **Next**.
6. Specify the appropriate installation information in the remaining pages of the **Deploy OVF Template** wizard. Required fields are shown in red.
   On the **Select configuration** page, the configuration options use the following resources:

Resource	Standard Installation	Large Installation
CPUs	2	4
RAM	8 GB	16 GB
Disk	65 GB	150 GB

   Entrust recommends that you select a **large** installation if your system meets one or more of the following criteria:
   - More than four nodes in the Cryptographic Security Platform Vault cluster.
   - More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
   - More than 100,000 secrets stored.

   Note: The OVA deployment method creates the disk as 60 GB, even for large configurations. After Cryptographic Security Platform Vault is configured, please follow the vSphere instructions on increasing the disk size and increase it to 140 GB. This will require a reboot of Cryptographic Security Platform Vault. You must increase the size for each node. For details, see Increasing CSP Vault Storage in a VM.

   On the **Customize template** page:
   - If you want to specify multiple DNS servers, enter their IP addresses as a comma-separated or space-separated list.
   - Specify a static IPv4 address in the **Host IP address** field. If you have an internal IP address that differs from your external IP address due to your firewall configuration, use the internal IP address. You *cannot* change the IP address for the node after it has been deployed.
     Note: You must use an IPv4 address. Cryptographic Security Platform Vault does not support IPv6 addresses.
   - Do *not* use spaces or special characters in the **Hostname** and **Domain Name** fields. Only use alphanumeric characters or hyphens (-). You *cannot* change the hostname after the node has been deployed.
     Note: Any uppercase letters in the hostname will be translated to lowercase after the node has been deployed.

   For information about the other fields in this wizard, see your vSphere Client documentation.
7. After you have finished entering the deployment information, click **Next** and review your choices on the **Ready to complete** page.
8. Click **Finish** to deploy the Cryptographic Security Platform Vault node.
9. Wait until you receive a message that the installation is complete.
   You can view the installation progress in the **Recent Tasks** tab in the vSphere Client.
10. If you selected the large installation configuration earlier in this procedure, you need to manually change the disk size allotted to the VM from the standard 65 GB to 150 GB. The OVA template sets the appropriate number of CPUs and the memory allocation but it *cannot* automatically change the standard disk size.
11. Power on the Cryptographic Security Platform Vault VM.

12. Configure the node as needed. For details, see one of the following:
    - If this is the first Cryptographic Security Platform Vault node in the system or if you want this to be a standalone node, follow the steps in Configuring the First CSP Vault Node (OVA Install).
    - If you are adding this node to an existing Cryptographic Security Platform Vault cluster, follow the steps in Adding a New CSP Vault Node to an Existing Cluster (OVA Install).

Configuring the First CSP Vault Node (OVA Install)

This procedure explains how to use this console to configure this system as the first Cryptographic Security Platform Vault node in the system. If you want to join this node with an existing Cryptographic Security Platform Vault node, see Adding a New CSP Vault Node to an Existing Cluster (OVA Install).

1. Log into the system on which you installed the Cryptographic Security Platform Vault software.
   The Cryptographic Security Platform Vault installer will automatically start running as soon as the VM is powered on.
2. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings.
   This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
   Important: Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.

The installer configures Cryptographic Security Platform Vault and then starts the appropriate services. This process will take a few minutes to complete. When the installer has finished, Cryptographic Security Platform Vault displays a confirmation dialog stating that the setup was completed successfully.

1. Review the confirmation dialog that provides the URL of the Cryptographic Security Platform Vault webGUI (also known as the Management IP Address). You will need this URL in the next step.
   When you are done, press **Enter** to finish the installation. Cryptographic Security Platform Vault displays the login prompt.
2. To initialize the Cryptographic Security Platform Vault webGUI and finish the configuration of the first node, do the following:
   a. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the Management IP address. For security reasons, you must explicitly specify `https://` in the URL.
   b. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
      Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
   c. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for both the username and password.
   d. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
   e. On the Welcome to Cryptographic Security Platform Vault screen, click **Continue as a Standalone Node**.
   f. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.
   g. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.

If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.

h. When you are done, click **Continue**.
i. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.
j. When you are finished, click **Continue**.
Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI. For details about the tasks you can perform from the webGUI, see the CSP Vault Management webGUI Page Reference.

What to Do Next

- To add additional Cryptographic Security Platform Vault nodes to form a cluster, see CSP Vault OVA Installation followed by Adding a New CSP Vault Node to an Existing Cluster (OVA Install).
- To create a dedicated webGUI account with Cloud Admin privileges that you can use to install the Entrust Policy Agent, see Preparing to Install the Policy Agent.

Adding a New CSP Vault Node to an Existing Cluster (OVA Install)

When you log into the target system for the first time after installing the Cryptographic Security Platform Vault software, Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault System Menu. This procedure explains how to use this menu to configure this system as a new node in an existing Cryptographic Security Platform Vault cluster.

Before You Begin

- Make sure you know the IP address of any Cryptographic Security Platform Vault node that is already part of the cluster you want to join.
- If Startup Authentication is enabled, you cannot add a new Cryptographic Security Platform Vault node. You must disable Startup Authentication on the existing Cryptographic Security Platform Vault node, add the new node, and then re-enable Startup Authentication.

Procedure

1. Log into the VM on which you installed the Cryptographic Security Platform Vault software.
2. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings.
This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
Important: Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.
3. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the Management IP address you specified during installation. For security reasons, you must explicitly specify `https://` in the URL.

Tip: If you do not know the Management IP address for the node, log into the system on which the node is installed as `htadmin`. Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console. From the menu, select **Manage Network Settings > Show Current Network Configuration**.

4. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault webGUI.
   Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
5. On the **Entrust Cryptographic Security Platform Vault Login** page, enter `secroot` for both the username and password.
6. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
7. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
   The Join Existing Cluster window displays.
8. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
   - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
9. Click **Continue**.
10. On the Download CSR page, click **Generate and Download CSR**.
11. Click **Continue**.
12. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
13. Select **Actions > Add a Node**.
14. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
15. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
16. Click **OK** to close the Add a Node window.
17. Return to the new node and click **Continue**.
18. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.
19. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
20. When the node has successfully restarted, click **Login**.

What to Do Next

To create a dedicated webGUI account with Cloud Admin privileges that you can use to install the Entrust Policy Agent, see Preparing to Install the Policy Agent.

CSP Vault ISO Installation for Hypervisor

- ISO Installation Overview
- Installing the First CSP Vault Node from an ISO Image
- Installing an Additional CSP Vault Cluster Node from an ISO Image

ISO Installation Overview

Entrust provides an ISO image that allows you to install the first Cryptographic Security Platform Vault node or add a Cryptographic Security Platform Vault node to an existing cluster.

If you are installing Cryptographic Security Platform Vault on an existing VM, make sure that there is no important data currently on the target system. The installer will overwrite all data on the selected disks.

> Note: If you want to deploy Cryptographic Security Platform Vault using an OVA template, see CSP Vault OVA Installation.

Installing the First CSP Vault Node from an ISO Image

This procedure describes how to use the Entrust-provided ISO image to install and configure a standalone Cryptographic Security Platform Vault node or the first node in new Cryptographic Security Platform Vault cluster. If you want to add a Cryptographic Security Platform Vault node to an existing cluster, see Installing a New CSP Vault Cluster Node from an ISO Image.

If you want to deploy the node from an OVA template, see Installing CSP Vault from an OVA Template.

Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.

Before You Begin

- If you are installing Cryptographic Security Platform Vault on an existing VM, make sure that there is no important data currently on the target system. The installer will overwrite all data on the selected disks.
- Make sure that the target VM can access the Entrust Cryptographic Security Platform Vault ISO image.
- Make sure the target VM meets the basic system requirements described in Requirements.
- If you are using VMware, ensure that all of your CSP Vault deployments have VM-to-Host affinity enabled. This allows you to avoid Admin Key Recovery due to host migration. We recommend that you select 'Should run on hosts in group' for the rule specification. The group should contain only the one ESXi host that you are using for this Cryptographic Security Platform Vault VM.

Procedure

1. Log into the vSphere Client.
2. Create a new virtual machine using the settings appropriate to your environment.
3. At the Select Compatibility prompt, select your ESXi version.
   For more information on versions, see the Platform requirements.
4. When you are prompted to select a guest OS, set the following according to the Guest OS version that you are using:

Field	Setting
Guest OS Family	Linux
Guest OS Version	Oracle Linux 8 or 9 (64-bit)

5. Click **Next**.
6. On the Virtual Hardware tab of the Customize hardware page, make sure the VM configuration meets the following system resource recommendations:

Resource	Standard Installation	Large Installation
CPUs	2	4
RAM	8 GB	16 GB
Disk	65 GB	150 GB

   Entrust recommends that you select a **large** installation if your system meets one or more of the following criteria:
   - More than four nodes in the Cryptographic Security Platform Vault cluster.
   - More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
   - More than 100,000 secrets stored.

   The rest of the options on this tab should be configured to match your vSphere environment.
   Note:
   - For the SCSI controller, we suggest that you use VMware Paravirtual. While other choices should work, VMware Paravirtual is used regularly in our testing.
   - For the network adapter type, we suggest that you use VMXNET 3. While other choices should work, VMXNET3 is used regularly in our testing.
7. On the VM Options tab of the Customize hardware page, expand Boot Options and set the Firmware to EFI.
8. For **Secure Boot**, deselect **Enabled**.
9. Connect the Cryptographic Security Platform Vault version 10.5.1 installation ISO image to the VM so that the VM will boot from this ISO image when you power on the VM. How you do this depends on how your vSphere environment is configured and what options you have available.
   For example, you could upload the Cryptographic Security Platform Vault ISO image to a datastore that vSphere can access and then attach the datastore ISO image as a CD/DVD drive that is connected when the VM powers on.
10. Power on the Cryptographic Security Platform Vault VM and have it boot from the Cryptographic Security Platform Vaultversion 10.5.1 installation ISO image .
11. When the VM boots from the ISO image, it will begin installing Oracle Linux.
    Note: The installer will post messages as the Oracle Linux operating system install proceeds. Some parts of the OS take longer to install than others, and there may be times when no new messages appear for over ten minutes. Do not attempt to cancel or restart the installation procedure during this time.
    The installer will automatically reboot the VM as needed.
    When then installer has finished, it displays a prompt asking for a password for the `htadmin` account.

12. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by an Cryptographic Security Platform Vault administrator in the System Settings.
    This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
    Important: Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.
13. The System Configuration page asks if you want to use DHCP for the node. We highly recommend that you do *not* do this, as the Cryptographic Security Platform Vault node should always be available at a set IP address. Make sure **No** is selected and press **Enter** to acknowledge this message.
14. On the Confirm Network Configuration page, enter the appropriate network information for the Cryptographic Security Platform Vault node. When you are done, press **Enter** to save this information.
15. On the System Configuration page, review the configuration settings and press **Enter** if you are ready to configure the node.
    The installer configures Cryptographic Security Platform Vault and then starts the appropriate services. This process will take a few minutes to complete. When the installer has finished, Cryptographic Security Platform Vault displays a confirmation dialog stating that the setup was completed successfully.
16. Review the confirmation dialog that provides the URL of the Cryptographic Security Platform Vault webGUI (also known as the Management IP Address). You will need this URL in the next step.
    When you are done, press **Enter** to finish the installation. Cryptographic Security Platform Vault displays the Oracle Linux login prompt.
17. After the configuration is complete, power off your VM, detach the ISO, and reset the boot order. Then you can safely power on your VM again.
18. To initialize the Cryptographic Security Platform Vault webGUI and finish the configuration of the first node, do the following:
    a. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the Management IP address. For security reasons, you must explicitly specify `https://` in the URL.
    b. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
    Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
    c. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for both the username and password.
    d. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
    e. On the Welcome to Cryptographic Security Platform Vault screen, click **Continue as a Standalone Node**.
    f. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.
    g. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.
    If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
    To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.
    h. When you are done, click **Continue**.
    i. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts

for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.

j. When you are finished, click **Continue**.
Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI.

- To add additional Cryptographic Security Platform Vault nodes to form a cluster, see Installing an Additional CSP Vault Cluster Node from an ISO Image.
- To create a dedicated webGUI account with Cloud Admin privileges that you can use to install the Entrust Policy Agent, see Preparing to Install the Policy Agent.

Installing an Additional CSP Vault Cluster Node from an ISO Image

This procedure describes how to use the Entrust-provided ISO image to install and configure a new Cryptographic Security Platform Vault that you want to add to an existing cluster. If you want to configure a standalone Cryptographic Security Platform Vault node or the first node in the cluster, see Installing the First CSP Vault Node from an ISO Image.

Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.

Before You Begin

- If you are installing Cryptographic Security Platform Vault on an existing VM, make sure that there is no important data currently on the target system. The installer will overwrite all data on the selected disks.
- Make sure that the target VM can access the Entrust Cryptographic Security Platform Vault ISO image.
- Make sure the target VM meets the basic system requirements described in Requirements.
- If EMS is disabled, you will need to configure the node as a standalone node, disable EMS, and then join the cluster.
  For more information on EMS, see Configuring TLS. For more information on joining a cluster, see Joining a CSP Vault Cluster.

Note: If your version of vCenter is different from what is described below, please see your vCenter documentation for details about the ISO deployment process.

Procedure

1. Log into the vSphere Client.
2. Create a new virtual machine using the settings appropriate to your environment.
3. At the Select Compatibility prompt, select your ESXi version.
   For more information on versions, see the Platform requirements.
4. When you are prompted to select a guest OS, set the following according to the Guest OS version that you are using:

Field	Setting
Guest OS Family	Linux
Guest OS Version	Oracle Linux 8 or 9 (64-bit)

5. Click **Next**.

6. On the Virtual Hardware tab of the Customize hardware page, make sure the VM configuration meets the following system resource recommendations:

Resource	Standard Installation	Large Installation
CPUs	2	4
RAM	8 GB	16 GB
Disk	65 GB	150 GB

   Entrust recommends that you select a **large** installation if your system meets one or more of the following criteria:
   - More than four nodes in the Cryptographic Security Platform Vault cluster.
   - More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
   - More than 100,000 secrets stored.

   The rest of the options on this tab should be configured to match your vSphere environment.
   Note:
   - For the SCSI controller, we suggest that you use VMware Paravirtual. While other choices should work, VMware Paravirtual is used regularly in our testing.
   - For the network adapter type, we suggest that you use VMXNET 3. While other choices should work, VMXNET3 is used regularly in our testing.
7. On the VM Options tab of the Customize hardware page, expand Boot Options and set the Firmware to EFI.
8. For **Secure Boot**, deselect **Enabled**.
9. Connect the Cryptographic Security Platform Vault version 10.5.1 installation ISO image to the VM so that the VM will boot from this ISO image when you power on the VM. How you do this depends on how your vSphere environment is configured and what options you have available.
   For example, you could upload the Cryptographic Security Platform Vault ISO image to a datastore that vSphere can access and then attach the datastore ISO image as a CD/DVD drive that is connected when the VM powers on.
10. Power on the Cryptographic Security Platform Vault VM and have it boot from the Cryptographic Security Platform Vault version 10.5.1 installation ISO image .
11. When the VM boots from the ISO image, it will begin installing Oracle Linux.
    Note: The installer will post messages as the Oracle Linux operating system install proceeds. Some parts of the OS take longer to install than others, and there may be times when no new messages appear for over ten minutes. Do not attempt to cancel or restart the installation procedure during this time.
    The installer will automatically reboot the VM as needed.
    When then installer has finished, it displays a prompt asking for a password for the `htadmin` account.
12. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings.
    This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
    Important: Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.

13. The System Configuration page asks if you want to use DHCP for the node. We highly recommend that you do *not* do this, as the Cryptographic Security Platform Vault node should always be available at a set IP address. Make sure **No** is selected and press **Enter** to acknowledge this message.
14. On the Confirm Network Configuration page, enter the appropriate network information for the Cryptographic Security Platform Vault node. When you are done, press **Enter** to save this information.
15. On the System Configuration page, review the configuration settings and press **Enter** if you are ready to configure the node.
    The installer configures Cryptographic Security Platform Vault and then starts the appropriate services. This process will take a few minutes to complete. When the installer has finished, Cryptographic Security Platform Vault displays a confirmation dialog stating that the setup was completed successfully.
16. Review the confirmation dialog that provides the URL of the Cryptographic Security Platform Vault webGUI (also known as the Management IP Address).
    When you are done, press **Enter** to finish the installation. Cryptographic Security Platform Vault displays the Oracle Linux login prompt.
17. After the configuration is complete, power off your VM, detach the ISO, and reset the boot order. Then you can safely power on your VM again.
18. Log into the webGUI on the Cryptographic Security Platform Vault node you want to join with the cluster using `secroot` for both the username and password.
19. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
    The Join Existing Cluster window displays.
20. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
    - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
    - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
    - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
    - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
21. Click **Continue**.
22. On the Download CSR page, click **Generate and Download CSR**.
23. Click **Continue**.
24. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
25. Select **Actions > Add a Node**.
26. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
27. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
28. Click **OK** to close the Add a Node window.
29. Return to the new node and click **Continue**.
30. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.
31. Click **Join**.

During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
The cluster will automatically be placed in maintenance mode.
The node will restart after the join is complete.

32. When the node has successfully restarted, click **Login**.

What to Do Next

To create a dedicated webGUI account with Cloud Admin privileges that you can use to install the Entrust Policy Agent, see Preparing to Install the Policy Agent.

CSP Vault ISO Installation for Bare Metal Server

- ISO Installation Overview for Bare Metal Server
- Prerequisites and Requirements for Installing CSP Vault on a Bare Metal Server
- Installing the First CSP Vault Node on a Bare Metal Server from an ISO
- Installing an Additional CSP Vault Node on a Bare Metal Server from an ISO

ISO Installation Overview for Bare Metal Server

Entrust provides an ISO image that allows you to install the first Cryptographic Security Platform Vault node or add a Cryptographic Security Platform Vault node to an existing cluster.

To install CSP Vault on a bare metal server, see the following:

Prerequisites and Requirements for Installing CSP Vault on a Bare Metal Server

Before you begin the installation process, ensure that you meet the requirements in this section.

Hardware Prerequisites

Lenovo ThinkSystem SR250 or SR630 with:

- 8-core CPU
- 16 GB RAM
- Broadcom Ethernet Controller
- Intel VROC/VMD for NVMe RAID

Note: Only fresh installations are supported with this release.

Installation Requirements

- Configure RAID 1 so that 1 virtual disk is visible to the Operating System.
  When you deploy the ISO, the system will detect if the destination disk already has a formatted partition table. If so, you will be prompted to type 'delete my data' to proceed.
- Ensure that at least 1 NIC is connected. If you have multiple NICs, you will be prompted to select the primary interface.
- Ensure that UEFI is enabled.
- Ensure that UEFI secure boot is disabled. If not, you can disable it in XClarity Provisioning Manager by navigating to the UEFI Setup page and selecting **System Settings > Security > Secure Boot Configuration > Secure Boot Setting**.
  The deployment will not continue if UEFI Secure Boot is detected.
- If you plan to use network bonding, the primary bonded interface needs to be created with both members when you deploy the ISO. After the system setup is complete, you can create the secondary bonded interface.

Installing the First CSP Vault Node on a Bare Metal Server from an ISO

Note: Installing the ISO file will delete all existing data on the disk.

1. Mount the CSP Vault installation ISO in the media browser.
2. Make sure to change the one time boot option to CD/DVD by selecting F12 in the boot screen.
3. Start the installation.
4. When prompted, select the primary network interface for the installation.
5. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by an Cryptographic Security Platform Vault administrator in the System Settings.
   This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
   Important: Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.
6. If you want to configure a bonded interface, press **Yes** to enable bonding on the primary interface. Otherwise, press **No**.
   If you selected Yes, complete the following to configure the system with the bonded network interface:
   a. Choose the desired network bonding mode based on your network requirements, and press **OK**.
   b. Add the additional network interfaces that will participate in the bond and press **OK**.
   c. Enter any optional bonding parameters, such as link monitoring or failover settings, and press **OK**.
7. On the Confirm Network Configuration page, enter the appropriate network information for the CSP Vault node. When you are done, press **Enter** to save this information.
8. On the System Configuration page, review the configuration settings and press **Yes** if you are ready to configure the node.
   The installer configures Cryptographic Security Platform Vault and then starts the appropriate services. This process will take a few minutes to complete. When the installer has finished, Cryptographic Security Platform Vault displays a confirmation dialog stating that the setup was completed successfully.
9. Review the confirmation dialog that provides the URL of the Cryptographic Security Platform Vault webGUI (also known as the Management IP Address). You will need this URL in the next step.
   When you are done, press **Enter** to finish the installation. Cryptographic Security Platform Vault displays the Oracle Linux login prompt.
10. After the configuration is complete, unmount the ISO from the media browser, and ensure that the boot order is reset.
11. To initialize the Cryptographic Security Platform Vault webGUI and finish the configuration of the first node, do the following:
    a. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the Management IP address. For security reasons, you must explicitly specify `https://` in the URL.
    b. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
    Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
    c. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for both the username and password.
    d. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
    e. On the Welcome to Cryptographic Security Platform Vault screen, click **Continue as a Standalone Node**.

f. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.
g. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.
If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.
h. When you are done, click **Continue**.
i. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.
j. When you are finished, click **Continue**.
Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI. For details about the tasks you can perform from the webGUI, see the CSP Vault Management webGUI Page Reference.

12. If you would like to add an additional NIC or a bonded interface, you can configure it in the CSP Vault System Console by doing the following:
a. From the System Console, navigate to Manage Network Settings and select Manage Interfaces and IP Address Settings.
b. Choose one of the available unconfigured network interfaces and press **OK**.
c. Select **Configure as secondary or bonded secondary interface** and press **OK**.
d. Select **Yes** if you want to configure a bonded secondary interface, or select **No** if you want to configure an unbonded secondary interface.
e. If you selected a bonded secondary interface, select the appropriate network bonding mode based on your network setup requirements and press **OK**.
Note: If you selected unbonded, this step will not appear.
f. If you selected a bonded secondary interface, add the additional interfaces that you want to be included in the secondary bond and press **OK**.
Note: If you selected unbonded, this step will not appear.
g. If you selected a bonded secondary interface, add any additional options for the bond, or leave blank if there are no additional options, and press **OK**.
Note: If you selected unbonded, this step will not appear.
h. When prompted to configure the selected interface, click **Yes**.
i. Configure the secondary network and press **OK**.
j. Verify that the secondary interface or network bond is successfully created and operational.

What to Do Next

- Connect the CSP Vault Appliance to CSP Compliance Manager.
- To add additional Cryptographic Security Platform Vault nodes to form a cluster, see Installing an Additional CSP Vault Node on a Bare Metal Server from an ISO.

Installing an Additional CSP Vault Node on a Bare Metal Server from an ISO

Note: Installing the ISO file will delete all existing data on the disk.

1. Mount the CSP Vault installation ISO in the media browser.
2. Make sure to change the one time boot option to CD/DVD by selecting F12 in the boot screen.
3. Start the installation.
4. When prompted, select the primary network interface for the installation.

5. Enter a password for the Cryptographic Security Platform Vault system administration account `htadmin` and press **Enter**. Password requirements are configured by an Cryptographic Security Platform Vault administrator in the System Settings.
   This password controls access to the Entrust Cryptographic Security Platform Vault System Console that allows users to perform some Cryptographic Security Platform Vault administration tasks. It does not permit a Cryptographic Security Platform Vault user to access the full OS.
   Important: Make sure you keep this password in a secure place. If you lose the password, you will need to contact Entrust Support. For security reasons, Cryptographic Security Platform Vault does not provide a user-accessible password recovery mechanism.
6. If you want to configure a bonded interface, press **Yes** to enable bonding on the primary interface. Otherwise, press **No**.
   If you selected Yes, complete the following to configure the system with the bonded network interface:
   a. Choose the desired network bonding mode based on your network requirements, and press **OK**.
   b. Add the additional network interfaces that will participate in the bond and press **OK**.
   c. Enter any optional bonding parameters, such as link monitoring or failover settings, and press **OK**.
7. On the Confirm Network Configuration page, enter the appropriate network information for the Cryptographic Security Platform Vault node. When you are done, press **Enter** to save this information.
8. On the System Configuration page, review the configuration settings and press **Yes** if you are ready to configure the node.
   The installer configures Cryptographic Security Platform Vault and then starts the appropriate services. This process will take a few minutes to complete. When the installer has finished, Cryptographic Security Platform Vault displays a confirmation dialog stating that the setup was completed successfully.
9. Review the confirmation dialog that provides the URL of the Cryptographic Security Platform Vault webGUI (also known as the Management IP Address). You will need this URL in the next step.
   When you are done, press **Enter** to finish the installation. Cryptographic Security Platform Vault displays the Oracle Linux login prompt.
10. After the configuration is complete, unmount the ISO from the media browser, and ensure that the boot order is reset.
11. Log into the webGUI on the CSP Vault node you want to join with the cluster using `secroot` for both the name and the password.
12. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
    The Join Existing Cluster window displays.
13. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
    - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
    - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
    - A passphrase to use during the joining process. Passphrase requirements are configured by a CSP Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
    - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
14. Click **Continue**.
15. On the Download CSR page, click **Generate and Download CSR**.
16. Click **Continue**.
17. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
18. Select **Actions > Add a Node**.
19. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.

20. Click **OK** to close the Add a Node window.
21. Return to the new node and click **Continue**.
22. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.
23. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode. The node will restart after the join is complete.
24. When the node has successfully restarted, click **Login**.

CSP Vault in Amazon Web Services

The following topics explain how to deploy one or more Cryptographic Security Platform Vault nodes in Amazon Web Services (AWS).

- AWS Deployment Overview
- Deploying the First CSP Vault Node in AWS
- Associating an Elastic IP Address with the CSP Vault Instance
- Configuring the First CSP Vault Node in AWS
- Deploying Additional CSP Vault Nodes in AWS
- Configuring Additional CSP Vault Nodes in AWS

AWS Deployment Overview

To create a Cryptographic Security Platform Vault node in AWS, you need to launch a Entrust Cryptographic Security Platform Vault for AWS instance and then configure that instance using SSH.

After the first Cryptographic Security Platform Vault node is configured, you can then add additional nodes from other AWS availability zones or regions, or from other environments such as VMware vSphere or Microsoft Azure. All configuration information from the first node is copied to any subsequent nodes that you add to the cluster.

Note:

- CSP Vault now supports AWS Instance Metadata Service Version 2 (IMDSv2) to access EC2 instance metadata.
- CSP Vault does not support SSM manager. To access the console, use the EC2 console.

To create a Cryptographic Security Platform Vault cluster in AWS, perform the following tasks:

Step	Task	Details
1	Launch a Entrust Cryptographic Security Platform Vault for AWS instance that will become the initial Cryptographic Security Platform Vault node in the cluster.	Deploying the First CSP Vault Node in AWS.

Step	Task	Details
2	Associate an Elastic IP (EIP) address with the instance.	Associating an Elastic IP Address with the CSP Vault Instance.
3	Configure the first Cryptographic Security Platform Vault node and initialize the Cryptographic Security Platform Vault webGUI.	Configuring the First CSP Vault Node in AWS.
4	If desired, deploy additional Cryptographic Security Platform Vault nodes in AWS.	Deploying Additional CSP Vault Nodes in AWS.
5	Configure the additional nodes and join them to the existing cluster.	Configuring Additional CSP Vault Nodes in AWS.

Deploying the First CSP Vault Node in AWS

In order to deploy the first Cryptographic Security Platform Vault node on AWS, you need to launch a Entrust Cryptographic Security Platform Vault for AWS instance on a new or existing VPC. After you have configured the first Cryptographic Security Platform Vault node, you can add other Cryptographic Security Platform Vault nodes to your Cryptographic Security Platform Vault cluster as desired.

Note: The following procedure is based on the 2019 AWS Console interface. If your version of the AWS Console is different from what is described below, please see your AWS documentation.

1. Open a web browser and navigate to the Amazon Web Services login page for your company. The default login page is https://aws.amazon.com/.
2. Log in to the AWS Management Console with your AWS user name and password.
3. In the top menu bar just after your login name, verify that the deployment region is correct. If you need to change it, click the current region and select the new region from the drop-down list.
4. Create a new VPC to use for the Cryptographic Security Platform Vault node, or select an existing VPC.
5. In the top menu bar, select **Services > Compute > EC2**.
6. Click the blue **Launch Instance** button.
7. In the Step 1: Choose an Amazon Machine Image (AMI) page, click **AWS Marketplace** in the left-hand pane.
8. Search the Marketplace for "Entrust" and select Entrust Cryptographic Security Platform Vault **for AWS BYOL** (Bring Your Own License).
9. Review the details and click **Continue**.
10. In the Step 2: Choose an Instance Type page, select an instance type. For optimal performance, we recommend that you select a general purpose or compute optimized instance type with SSD Instanced storage, such as **m3.large** or **c3.large**. The Cryptographic Security Platform Vault system resource recommendations are:

Resource	Standard Installation	Large Installation
CPUs	2	4

Resource	Standard Installation	Large Installation
RAM	8 GB	16 GB
Disk	65 GB	150 GB

Entrust recommends that you select a **large** installation if your system meets one or more of the following criteria:

- More than four nodes in the Cryptographic Security Platform Vault cluster.
- More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
- More than 100,000 secrets stored.

11. After you have selected the type, click **Next: Configure Instance**
12. On the Step 3: Configure Instance Details page, set the following options:
    - Number of Instances —Specify the number of instances you want to launch in this field. All instances will run in the same region using the same VPC and instance settings.
      Tip: You can use this option to create a multi-node Cryptographic Security Platform Vault cluster on this VPC without needing to launch additional instances, but you can also add additional Cryptographic Security Platform Vault nodes to the cluster at any time after the initial node has been configured.
    - Network —Select the VPC you want to use for the Cryptographic Security Platform Vault node.
    - Set all other options on this page according to your corporate standards.
13. When you are done, click **Next: Add Storage**.
14. On the Step 4: Add Storage page, set the following options:
    - Volume Size —Set the size of the disk based on your configuration requirements. The default setting of65 GB should work for most Cryptographic Security Platform Vault installations.
    - Volume Type—For optimal performance, we recommend setting the volume type to one of the SSD options instead of the default Magnetic volume.
    - Delete on Termination—If you select this option and the instance is deleted, all keys stored on this Cryptographic Security Platform Vault node will be deleted as well. In a single node configuration, this means that encrypted data cannot be decrypted, as the keys will be lost. If you want to use this option, make sure all data is decrypted before the instance is deleted.
15. When you are done, click **Next: Add Tags**.
16. On the Step 5: Add Tags page, click **Add Tag** and enter a Name tag for the instance:
    - Key —Enter "Name".
    - Value—Enter the name for this Cryptographic Security Platform Vault node.

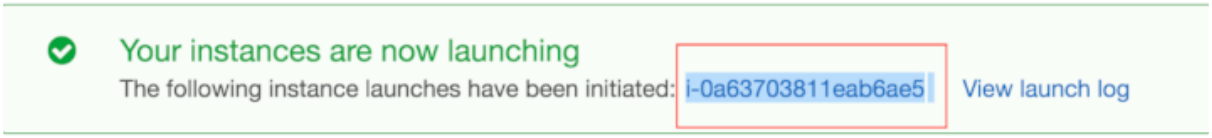
    Add any other tags as desired.
17. When you are done, click **Next: Configure Security Group**.
18. In the Step 6: Configure Security Group page, do the following:
    a. Make sure that the **Assign a security group** field is set to **Create a new security group**.
       Note: You can use an existing security group as long as all of the required ports are open in that security group.
    b. Optionally enter a custom security group name and description in the **Security group name** and **Description** fields.
    c. For each of the required entries in the security group, set the Source IP addresses or security groups that can communicate with Cryptographic Security Platform Vault through the associated ports. We strongly recommend that you do *not* use the default 0.0.0.0/0 notation, which indicates that the ports are open to the world.

    Cryptographic Security Platform Vault requires the following ports:

Type	Protocol	Port Range	Source
SSH (22)	TCP	22	*IP address list or another security group*
HTTPS (443)	TCP	443	*IP address list or another security group*
Custom TCP Rule	TCP	5432	*IP address list or another security group*
Custom TCP Rule	TCP	8443	*IP address list or another security group*
Custom UDP Rule	UDP	123	*IP address list or another security group*

For details about specifying the source IP addresses or security groups, see your AWS documentation.

19. When you are done, click **Review and Launch**.
20. In the Step 7: Review Instance Launch page, verify your selections and click **Launch**.
21. At the prompt, either select an existing key pair or select **Create a new key pair**, specify a key pair name, and download the new private key file for the new key pair.
22. When you are done, click **Launch Instances**. AWS displays a confirmation page stating that your instance is being launched and displays the instance ID. Make a note of the ID, as it will be your initial Cryptographic Security Platform Vault password.



To verify the status of the instance, select **Services > EC2 > Instances** and locate the new instance in the table.

Tip: If you requested multiple instances on the Step 3: Configure Instance Details page, you will see multiple Cryptographic Security Platform Vault instances with the same name listed in the table. We recommend that you give each instance a unique name at this point so that you can tell them apart as you configure them. To do so, mouse over an instance name and click the pencil icon when it appears.

What to Do Next

Associate an Elastic IP address with the instance as described in Associating an Elastic IP Address with the CSP Vault Instance. An elastic IP address is required for every Cryptographic Security Platform Vault instance so that you can configure and maintain the Cryptographic Security Platform Vault instance using a static IPv4 address.

If you created multiple instances, you need to assign a different Elastic IP to each copy of the instance.

Associating an Elastic IP Address with the CSP Vault Instance

An elastic IP address is a static IPv4 address that allows you to access the Cryptographic Security Platform Vault AWS instance from a web browser. An elastic IP address is required in order to configure and maintain the Cryptographic Security Platform Vault node using the Cryptographic Security Platform Vault webGUI and the Entrust Cryptographic Security Platform Vault System Console.

Note: The following procedure is based on the 2019 AWS Console interface. If your version of the AWS Console is different from what is described below, please see your AWS documentation.

1. In the Amazon Management Console's top menu bar, select **Services > EC2**.
2. In the EC2 Dashboard, select **Network & Security > Elastic IPs**.
3. Click the blue **Allocate new address** button.
4. Click **Allocate**.
5. Make a note of the new IP address and click **Close**.
6. In the table of elastic IP addresses, select the EIP address you just created.
7. Select **Actions > Associate address**.
8. On the Associate Address page, select the Cryptographic Security Platform Vault instance in the **Instance** drop-down list, then click **Associate**.
9. On the confirmation page, click **Close**.
10. Repeat this procedure for any other Cryptographic Security Platform Vault instance that does not have an associated IPv4 Public IP address.
11. When you have assigned all Cryptographic Security Platform Vault instances an EIP address, from the EC2 Dashboard, select **Instances**.
12. In the table, locate your Cryptographic Security Platform Vault instances and make sure the correct elastic IP addresses appear in the **IPv4 Public IP** column.

What to Do Next

If this is the first Cryptographic Security Platform Vault node in the cluster, configure it as described in Configuring the First CSP Vault Node in AWS.

If you are adding this node to an existing Cryptographic Security Platform Vault cluster, see Configuring Additional CSP Vault Nodes in AWS.

Configuring the First CSP Vault Node in AWS

You need to configure the Cryptographic Security Platform Vault instance using SSH before you can use the Cryptographic Security Platform Vault webGUI to configure and maintain your Cryptographic Security Platform Vault cluster.

The following procedure describes how to configure the first Cryptographic Security Platform Vault node in the cluster. If you are adding this node to an existing cluster, see Configuring Additional CSP Vault Nodes in AWS.

Before You Begin

Make sure you have the following information:

- The Amazon instance ID for the Cryptographic Security Platform Vault instance.
- The Elastic (Public) IP address associated with the instance.
- The private key file (in pem format) that was used when the instance was created.

Tip: To find this information, select Instances from the Amazon Management Console EC2 Dashboard, then select the Cryptographic Security Platform Vault instance in the table. In the Description tab, look at the Instance ID, IPv4 Public IP, and Key pair name fields.

Procedure

1. To initialize Cryptographic Security Platform Vault for this cluster, do the following:
   a. Use a web browser to navigate to `https://<Elastic-IP-addy>`, where `<Elastic-IP-addy>` is the Elastic IP address associated with the Cryptographic Security Platform Vault AWS instance. For security reasons, you must explicitly specify `https://` in the URL.
   b. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.

Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.

c. On the **Entrust Cryptographic Security Platform Vault Management** login, enter `secroot` for the username and the AWS instance ID as the password.
d. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
e. On the Welcome to Cryptographic Security Platform Vault screen, click **Continue as a Standalone Node**.
f. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.
g. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.
If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.
h. When you are done, click **Continue**.
i. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.
j. When you are finished, click **Continue**.
Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI. For details about the tasks you can perform from the webGUI, see the CSP Vault Management webGUI Page Reference.

2. Optional. Log into the `htadmin` account on the keycontrol System Console using the private key file. For example:
`ssh -i <key-file>.pem htadmin@<Elastic-IP-addy>`
The password is the same as the secroot password that you changed in step **f** above.
Important: The secroot password is used for this first login. You can either change it, or leave it as is. If you change the `htadmin` password in the System Console, it only changes the password for this particular node, and does not affect the secroot password.

What to Do Next

- To add additional Cryptographic Security Platform Vault nodes to form a cluster, see Deploying Additional CSP Vault Nodes in AWS.
- For information about configuring and maintaining your Cryptographic Security Platform Vault cluster, see the CSP Vault Cluster Maintenance.

Deploying Additional CSP Vault Nodes in AWS

The following procedure describes how to deploy a Cryptographic Security Platform Vault node that you intend to add to an existing Cryptographic Security Platform Vault cluster. If you want to deploy a Cryptographic Security Platform Vault node that will become the first node in a new cluster, see Configuring the First CSP Vault Node in AWS.

Note: The following procedure is based on the 2019 AWS Console interface. If your version of the AWS Console is different from what is described below, please see your AWS documentation.

Before You Begin

If you want to use a existing VPC for the new node that is different from the VPC used for the first Cryptographic Security Platform Vault node, make sure that you have set up VPC-to-VPC communication between the VPCs. This includes configuring a Peering Connection and setting the correct Routing Table information. For details, see your AWS documentation.

If you want to use the same VPC for the new node as you used for the first node, make sure you know the following information:

- The region in which the first node is deployed.
- The VPC assigned to the first node.
- The Security Group assigned to the first node.

Tip: To find this information, select Instances from the Amazon Management Console EC2 Dashboard, then select the first Cryptographic Security Platform Vault node in the table. In the Description tab, look at the VPC ID and Security groups fields.

Procedure

1. Open a web browser and navigate to the Amazon Web Services login page for your company. The default login page is https://aws.amazon.com/.
2. Log in to the AWS Management Console with your AWS user name and password.
3. In the top menu bar just after your login name, select the Region into which you want to deploy the Cryptographic Security Platform Vault node. If you want to use the same VPC as the first Cryptographic Security Platform Vault node, you must deploy the new node in the same region as the first node.
4. If you intend to use the same VPC as you used for the first Cryptographic Security Platform Vault node, proceed to the next step. Otherwise, make sure that you have configured VPC-to-VPC communication between the two VPCs as per your AWS documentation.
5. In the top menu bar, select **Services > Compute > EC2**.
6. Click the blue **Launch Instance** button.
7. In the Step 1: Choose an Amazon Machine Image (AMI) page, click **AWS Marketplace** in the left-hand pane.
8. Search the Marketplace for "Entrust" and select Entrust Cryptographic Security Platform Vault **for AWS BYOL** (Bring Your Own License).
9. Review the details of the version you selected and click **Continue**.
10. In the Step 2: Choose an Instance Type page, select an instance type. For optimal performance, we recommend that you select a general purpose or compute optimized instance type with SSD Instanced storage, such as **m3.large** or **c3.large**. The Cryptographic Security Platform Vault system resource recommendations are:

Resource	Standard Installation	Large Installation
CPUs	2	4
RAM	8 GB	16 GB
Disk	65 GB	150 GB

Entrust recommends that you select a **large** installation if your system meets one or more of the following criteria:

- More than four nodes in the Cryptographic Security Platform Vault cluster.
- More than 500 virtual machine heartbeats OR more than 10,000 KMIP keys across all KMIP vaults together.
- More than 100,000 secrets stored.

11. After you have selected the type, click **Next: Configure Instance Details**.

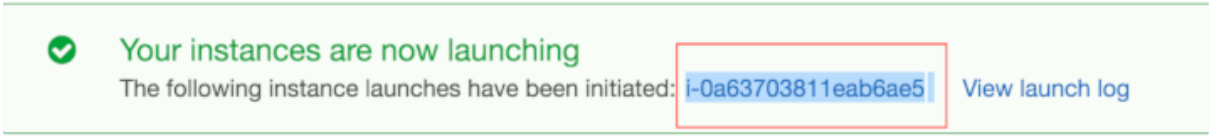
12. On the Step 3: Configure Instance Details page, set the following options:
    - Number of Instances—Specify the number of instances you want to launch in this field. All instances will run in the same region using the same VPC and instance settings.
    - Network —Select the VPC you want to use for the Cryptographic Security Platform Vault node.
    - Set all other options on this page according to your corporate standards.
13. When you are done, click **Next: Add Storage**.
14. On the Step 4: Add Storage page, set the following options:
    - Volume Size —Set the size of the disk based on your configuration requirements. The default setting of 20 GB should work for most Cryptographic Security Platform Vault installations.
    - Volume Type—For optimal performance, we recommend setting the volume type to one of the SSD options instead of the defaut Magnetic volume.
    - Delete on Termination—If you select this option and the instance is deleted, all keys stored on this Cryptographic Security Platform Vault node will be deleted as well. In a single node configuration, this means that encrypted data cannot be decrypted, as the keys will be lost. If you want to use this option, make sure all data is decrypted before the instance is deleted.
15. When you are done, click **Next: Add Tags**.
16. On the Step 5: Add Tags page, click **Add Tag** and enter a Name tag for the instance:
    - Key —Enter "Name".
    - Value—Enter the name for this Cryptographic Security Platform Vault node.

    Add any other tags as desired.
17. When you are done, click **Next: Configure Security Group**.
18. In the Step 6: Configure Security Group page **Assign a security group** field, do one of the following:
    - Select **Select an existing security group** and then select the security group you assigned to the first Cryptographic Security Platform Vault node.
      Note: You can use any existing security group as long as all of the required ports are open in that security group.
    - Select **Create a new security group**. For each of the required entries in the security group, set the Source IP addresses or security groups that can communicate with Cryptographic Security Platform Vault through the associated ports. We strongly recommend that you do *not* use the default 0.0.0.0/0 notation, which indicates that the ports are open to the world.
      Cryptographic Security Platform Vault requires the following ports:

Type	Protocol	Port Range	Source
SSH (22)	TCP	22	*IP address list or another security group*
HTTPS (443)	TCP	443	*IP address list or another security group*
Custom TCP Rule	TCP	5432	*IP address list or another security group*
Custom TCP Rule	TCP	8443	*IP address list or another security group*
Custom UDP Rule	UDP	123	*IP address list or another security group*

      For details about specifying the source IP addresses or security groups, see your AWS documentation.
19. When you are done, click **Review and Launch**.
20. In the Step 7: Review Instance Launch page, verify your selections and click **Launch**.
21. At the prompt, either select an existing key pair or select **Create a new key pair**, specify a key pair name, and download the new private key file for the new key pair.

22. When you are done, click **Launch Instances**. AWS displays a confirmation page stating that your instance is being launched and displays the instance ID. Make a note of the ID, as it will be your initial Cryptographic Security Platform Vault password.



23. To verify the status of the instance, select **Services > EC2 > Instances** and locate the new instance in the table.
Tip: If you requested multiple instances on the Step 3: Configure Instance Details page, you will see multiple Cryptographic Security Platform Vault instances with the same name listed in the table. We recommend that you give each instance a unique name at this point so that you can tell them apart as you configure them. To do so, mouse over an instance name and click the pencil icon when it appears.

What to Do Next

Associate an Elastic IP address with the instance as described in Associating an Elastic IP Address with the CSP Vault Instance. An elastic IP address is required for every Cryptographic Security Platform Vault instance so that you can configure and maintain the Cryptographic Security Platform Vault instance using a static IPv4 address.

If you created multiple instances, you need to assign a different Elastic IP to each copy of the instance.

Configuring Additional CSP Vault Nodes in AWS

After the AWS instance is deployed, you need to configure the Cryptographic Security Platform Vault node using SSH. The following procedure describes how to configure the node as part of an existing Cryptographic Security Platform Vault cluster. If you want to configure this node as the first node in the Cryptographic Security Platform Vault cluster, see Configuring the First CSP Vault Node in AWS.

Before You Begin

Make sure that the new Cryptographic Security Platform Vault node can communicate with the Cryptographic Security Platform Vault nodes in the existing Cryptographic Security Platform Vault cluster. For details, see your AWS documentation.

Make sure you have the following information:

- The Amazon instance ID for the new Cryptographic Security Platform Vault instance.
- The Elastic (Public) IP address associated with the new instance.
- The private key file (in pem format) that was used when the new instance was created.
Tip: To find this information, select **Instances** from the Amazon Management Console EC2 Dashboard, then select the Cryptographic Security Platform Vault instance in the table. In the **Description** tab, look at the **Instance ID**, **IPv4 Public IP**, and **Key pair name** fields.
- The private IP address of one of the existing Cryptographic Security Platform Vault nodes in the cluster.
Tip: To find this IP address, log into the Cryptographic Security Platform Vault webGUI on one of the existing nodes and click **Cluster** in the top menu bar. Go to the **Servers** tab and look at the IP address in the table.

Procedure

1. Use a web browser to navigate to `https://<Elastic-IP-addy>`, where `<Elastic-IP-addy>` is the Elastic IP address associated with the Cryptographic Security Platform Vault AWS instance. For security reasons, you must explicitly specify `https://` in the URL.
2. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault webGUI.

Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.

3. On the **Entrust Cryptographic Security Platform Vault Login** page, enter `secroot` for the username and the AWS instance ID as the password.
4. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
5. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
   The Join Existing Cluster window displays.
6. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
   - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
7. Click **Continue**.
8. On the Download CSR page, click **Generate and Download CSR**.
9. Click **Continue**.
10. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
11. Select **Actions > Add a Node**.
12. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
13. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
14. Click **OK** to close the Add a Node window.
15. Return to the new node and click **Continue**.
16. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.
17. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
18. When the node has successfully restarted, click **Login**.
19. Optional. Log into the `htadmin` account on the keycontrol System Console using the private key file. For example:
    `ssh -i <key-file>.pem htadmin@<Elastic-IP-addy>`
    The password is the Amazon instance ID.
    After logging in, you can change this password. The change applies only to the `htadmin` login on this node.

CSP Vault in Google Cloud Platform

The following topics explain how to deploy one or more Cryptographic Security Platform Vault nodes in Google Cloud Platform (GCP).

- GCP Deployment Overview
- Deploying the First CSP Vault Node in GCP
- Configuring Firewall Rules for the CSP Vault Instance
- Configuring the First GCP Node
- Configuring Additional GCP Nodes

GCP Deployment Overview

To create a Cryptographic Security Platform Vault cluster in GCP, perform the following tasks:

Step	Task	Details
1	Launch an Entrust Cryptographic Security Platform Vault for GCP instance that will become the initial Cryptographic Security Platform Vault node in the cluster.	Deploying the First CSP Vault Node in GCP.
2	Configure firewall rules for the Cryptographic Security Platform Vault instance.	Configuring Firewall Rules for the CSP Vault Instance.
3	Configure the first Cryptographic Security Platform Vault node and initialize the Cryptographic Security Platform Vault webGUI.	Configuring the First GCP Node.
4	If desired, deploy additional Cryptographic Security Platform Vault nodes in GCP using the same instructions as the first node.	Deploying the First CSP Vault Node in GCP.
5	Configure the additional nodes and join them to the existing cluster.	Configuring Additional GCP Nodes.

Deploying the First CSP Vault Node in GCP

In order to deploy the first Cryptographic Security Platform Vault node on GCP, you need to launch Entrust Cryptographic Security Platform Vault for GCP from the Google Cloud Marketplace.

1. Log in to the GCP Console.
2. Select your project.
3. Search for the **Entrust Cryptographic Security Platform Key & Secrets Vault BYOL** image in the Google Cloud Marketplace.
4. Click **Launch**.
5. On the New deployment page, enter the Deployment name, the Service Account information, and the Zone. For Machine type, we recommend using n1-standard-2 (2 vCPU, 1 core, 7.5 GB memory).
6. In the firewall section, ensure that you select **Allow HTTPS traffic from the Internet**.

Note: You will need to enter additional firewall rules. For details, see Configuring Firewall Rules for the CSP Vault Instance.

7. Click **Deploy**.
8. After the instance is created, locate your new VM on the **Compute Engine > VM Instances** page and copy the External IP address.

Configuring Firewall Rules for the CSP Vault Instance

Before configuring Cryptographic Security Platform Vault, ensure that the following ports are open in your GCP firewall.

Type	Protocol	Port Range
SSH (22)	TCP	22
HTTPS (443)	TCP	443
Custom TCP Rule	TCP	8443
Custom TCP Rule	TCP	5432
Custom UDP Rule	UDP	123

If you are going to use Cryptographic Security Platform Vault as a KMIP server or want to use the SNMP polling feature for Cryptographic Security Platform Vault, you must open related ports for the Cryptographic Security Platform Vault instance.

Type	Protocol	Default Port
KMIP	TCP	5696
SNMP	UDP	161

Note: These feature specific ports are configurable, and you must ensure you configure the firewall rules accordingly.

To set up the firewall, select VPC network > Firewall in the GCP Console. The Dashboard shows you a set of firewall rules. Select the Create Firewall Rules button to configure additional firewall rules.

Configuring the First GCP Node

Follow this procedure if you are configuring the first Cryptographic Security Platform Vault node in the cluster. If you are adding the node to an existing cluster, see Configuring Additional GCP Nodes.

Before You Begin

Make sure you have the following information:

- The instance ID for the Cryptographic Security Platform Vault instance. This is located in the Basic Information section on the Details page of the instance.

- The External IP associated with the instance.

Procedure

To initialize Cryptographic Security Platform Vault for this cluster, do the following:

1. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the External IP address. For security reasons, you must explicitly specify `https://` in the URL.
2. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
   Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
3. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for the username and the Instance ID for the password.
4. Click **Login**.
5. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
6. On the Welcome to Appliance Management screen, click **Continue as a Standalone Node**.
7. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.
8. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.
   If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
   To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.
9. When you are done, click **Continue**.
10. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
    Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.
11. When you are finished, click **Continue**.
    Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI. For details about the tasks you can perform from the webGUI, see the Administration Guide.

What to Do Next

If you want to add another Cryptographic Security Platform Vault node to this cluster, create another instance as described in Deploying the First CSP Vault Node in GCP and then configure it as described in Configuring Additional GCP Nodes.

Configuring Additional GCP Nodes

If you deploy an additional Cryptographic Security Platform Vault on GCP, you can add it to your existing Cryptographic Security Platform Vault cluster.

Before You Begin

- Ensure that the new Cryptographic Security Platform Vault node can communicate with the nodes in the existing Cryptographic Security Platform Vault cluster.
- Ensure that you have the following information:
  - The instance ID for the new Cryptographic Security Platform Vault instance. This is located in the Basic Information section on the Details page of the instance.
  - The External IP associated with the new instance.

- The private IP address of one of the existing Cryptographic Security Platform Vault nodes in the cluster.
  Tip: To find this IP address, log into the Cryptographic Security Platform Vault webGUI and click Switch to Appliance Management. Click Clusters in the top menu bar, then navigate to the Servers tab to see the IP address.

Procedure

1. Use a web browser to navigate to `https://<Public-IP-addy>`, where `<Public-IP-addy>` is the Public IP address assigned to the Cryptographic Security Platform Vault VM. For security reasons, you must explicitly specify `https://` in the URL.
2. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
   Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
3. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for the username and the Instance ID for the password.
4. Click **Login**.
5. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
6. On the Welcome to Appliance Management screen, click **Join an Existing Cluster.**.
   The Join Existing Cluster window displays.
7. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so that you can download and import the required certificates and files.
   - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
   - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
8. Click **Continue**.
9. On the Download CSR page, click **Generate and Download CSR**.
10. Click **Continue**.
11. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
12. Select **Actions > Add a Node**.
13. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
14. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
15. Click **OK** to close the Add a Node window.
16. Return to the new node and click **Continue**.
17. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the IP address of any node in the existing cluster, and enter the passphrase that you selected.
18. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.

The cluster will automatically be placed in maintenance mode.
The node will restart after the join is complete.

19. When the node has successfully restarted, click **Login**.
20. Optional. Log into the `htadmin` account on the Cryptographic Security Platform VaultSystem Console using the private key file. For example:
    `ssh -i <key-file>.pem htadmin@<Public-IP-addy>`
    The password is the VM unique ID (vmId).
    After logging in, you can change this password. The change applies only to the `htadmin` login on this node.

CSP Vault in Microsoft Azure

The following topics explain how to deploy one or more Cryptographic Security Platform Vault nodes in Microsoft Azure.

- Azure Deployment Overview
- Recommendations
- Deploying a CSP Vault Node in Azure
- Configuring the First CSP Vault Node in Azure
- Configuring Additional CSP Vault Nodes in Azure

Azure Deployment Overview

In order to deploy a Cryptographic Security Platform Vault node in a Microsoft Azure environment, you need to:

1. Deploy a Entrust Cryptographic Security Platform Key & Secrets Vault BYOL (KeyControl) virtual machine (VM) resource from the Azure Marketplace. For details, see Deploying a CSP Vault Node in Azure.
2. Use SSH to configure the new Cryptographic Security Platform Vault node. How you do this depends on whether this is the first Cryptographic Security Platform Vault node in the cluster or if you are adding this node to an existing Cryptographic Security Platform Vault cluster.
    - If this is the first node in the cluster, configure the node and initialize the Cryptographic Security Platform Vault webGUI. For details, see Configuring the First CSP Vault Node in Azure.
    - If you are adding this node to an existing Cryptographic Security Platform Vault cluster, configure the node and authenticate it with the existing cluster. For details, see Configuring Additional CSP Vault Nodes in Azure.

Recommendations

When working with Microsoft Azure, Entrust recommends the following:

- If your corporate Azure subscription is shared among multiple users, we recommend you use the Azure Resource Manager to lock the Cryptographic Security Platform Vault resources in the resource group so that they are not accidentally deleted.
- If you deploy multiple Cryptographic Security Platform Vault nodes in Azure to create your Cryptographic Security Platform Vault cluster, we recommend that the nodes be in different regions and resource groups to provide high availability.
- If you need to move a Cryptographic Security Platform Vault node to another region, we recommend that you deploy a new Cryptographic Security Platform Vault node in the new region, add that node to the existing cluster, and then delete the old Cryptographic Security Platform Vault node.

Deploying a CSP Vault Node in Azure

To deploy a Cryptographic Security Platform Vault node in Microsoft Azure, you need to create a virtual machine (VM) resource that has a Public IP address and SSH access. After Azure has started the new VM, you can configure it to either become the first node in a Cryptographic Security Platform Vault cluster or you can join the new node with an existing cluster.

The following procedure describes how to create the VM resource. Configuration details, see Configuring Additional CSP Vault Nodes in Azure.

> Note: If your version of ARM is different from what is described below, please see your Azure documentation.

Before You Begin

Make sure you have access to a public SSH key pair that you can use for this instance. You will be required to paste the public portion of the key pair into the Create Virtual Machine wizard and you will need the private portion of the key pair when you configure the new VM.

Important: The private part of the SSH key file cannot be reset or recovered once the VM is configured, even if you use the Azure "Reset Password" method. Please ensure that you keep it in a safe place.

Procedure

1. Log into your Microsoft Azure account.
2. In the left-hand pane, click **Create a resource**.
3. In the Search bar, enter "Entrust".
4. Select **Entrust Cryptographic Security Platform Key & Secrets Vault BYOL (KeyControl)**.
5. Review the information and then click **Create** at the bottom of the right-hand pane.
6. On the **Basics** page, specify the options you want to use:

Field	Description
Project Details Section	
Subscription	Select the Azure subscription that you want to use.
Resource group	If this is the first Cryptographic Security Platform Vault node you are deploying, you can create a new resource group or use an existing group as desired. If you want to connect this Cryptographic Security Platform Vault node with an existing node, make sure you select the same resource group as the existing Cryptographic Security Platform Vault node.
Instance Details	
Virtual machine name	The name of the VM that will host the Cryptographic Security Platform Vault node.

Field	Description
Region	Select the region in which this Cryptographic Security Platform Vault node should be deployed. If you want to connect this node to an existing Azure Cryptographic Security Platform Vault node, select the same region as the existing node or make sure a communication channel exists between the two regions.
Availability options	Select the desired availability option. Cryptographic Security Platform Vault does *not* require any special infrastructure redundancy.
Image	Make sure this is set to Entrust Cryptographic Security Platform Key & Secrets Vault BYOL (KeyControl).
Size	Select the size of the VM that you want to use for Cryptographic Security Platform Vault. Entrust recommends the following for standard and large deployments: • VCPUs: 2 for standard, 4 for large. • RAM: 8 GB for standard, 16 GB for large.
Administrator Account	
Authentication type	Select SSH public key.
Username	Enter `htadmin` as the username. The username must be in lower case.
SSH public key	Paste in the public portion of the SSH key pair you want to use for this node. Cryptographic Security Platform Vault implementation only works with SSH key authentication but not Password.

7. When you are done, click **Next: Disks**.
8. On the **Disks** tab, specify the options you want to use. For optimum performance, we recommend you select an SSD disk type. Cryptographic Security Platform Vault does not require additional data disks.
9. When you are done, click **Next: Networking**.
10. On the **Networking** page, specify the options you want to use based on your corporate standards. Cryptographic Security Platform Vault only requires the following:
    - The Public IP address must be static, which it is *not* by default. To use a static IP address, click **Create New** under the **Public IP** field. On the **Create public IP address** page, enter a name for the IP address and select the **Static** radio button under **Assignment**. When you are done, click **OK**.
    - If you create a new Network Security Group in this step (which is the Azure default action), Cryptographic Security Platform Vault automatically creates the correct port settings. If you

select an existing Network Security Group, you need to make sure the security group allows network communication with Cryptographic Security Platform Vault over the following ports and protocols:

Type	Protocol	Port Range
SSH	TCP	22
HTTPS	TCP	443
Custom	TCP	5432
Custom	TCP	8443
Custom	UDP	123

If you plan to connect this node with an existing Cryptographic Security Platform Vault cluster, you may need to open additional ports if the nodes are running in different Azure regions or in different environments.

11. If you want to set any other options for the VM, do so. When you are done, click **Review + Create**.
12. Review the settings for the resource and click **Create**. Wait for the success message from Azure confirming that the new resource is running and ready to use.
13. After Azure has created the virtual machine, determine the public IP address. To do so:
    a. In the left-hand pane, select **Resource groups**.
    b. Click the name of the resource group you specified on the **Basics** page.
    c. Click the virtual machine name in the table.
    Tip: If you do this before Azure has deployed the new VM, it may take a few minutes for the VM name to appear in this table.

    Azure displays the public IP address in the **Public IP address** field in the VM Details area.
14. Configure the node as the first Cryptographic Security Platform Vault node in the cluster or add it to an existing Cryptographic Security Platform Vault cluster. For details, see:
    - Configuring the First CSP Vault Node in Azure
    - Configuring Additional CSP Vault Nodes in Azure

Configuring the First CSP Vault Node in Azure

To deploy a Cryptographic Security Platform Vault node in Microsoft Azure, you need to create a virtual machine (VM) resource that has a Public IP address and SSH access. After Azure has started the new VM, you can configure it to either become the first node in a Cryptographic Security Platform Vault cluster or you can join the new node with an existing cluster.

The following procedure describes how to create the VM resource. Configuration details, see Configuring Additional CSP Vault Nodes in Azure.

> Note: If your version of ARM is different from what is described below, please see your Azure documentation.

Before You Begin

Make sure you have access to a public SSH key pair that you can use for this instance. You will be required to paste the public portion of the key pair into the Create Virtual Machine wizard and you will need the private portion of the key pair when you configure the new VM.

Important: The private part of the SSH key file cannot be reset or recovered once the VM is configured, even if you use the Azure "Reset Password" method. Please ensure that you keep it in a safe place.

Procedure

1. Log into your Microsoft Azure account.
2. In the left-hand pane, click **Create a resource**.
3. In the Search bar, enter "Entrust".
4. Select **Entrust Cryptographic Security Platform Key & Secrets Vault BYOL (KeyControl)**.
5. Review the information and then click **Create** at the bottom of the right-hand pane.
6. On the **Basics** page, specify the options you want to use:

Field	Description
Project Details Section	
Subscription	Select the Azure subscription that you want to use.
Resource group	If this is the first Cryptographic Security Platform Vault node you are deploying, you can create a new resource group or use an existing group as desired. If you want to connect this Cryptographic Security Platform Vault node with an existing node, make sure you select the same resource group as the existing Cryptographic Security Platform Vault node.
Instance Details	
Virtual machine name	The name of the VM that will host the Cryptographic Security Platform Vault node.
Region	Select the region in which this Cryptographic Security Platform Vault node should be deployed. If you want to connect this node to an existing Azure Cryptographic Security Platform Vault node, select the same region as the existing node or make sure a communication channel exists between the two regions.
Availability options	Select the desired availability option. Cryptographic Security Platform Vault does *not* require any special infrastructure redundancy.
Image	Make sure this is set to Entrust Cryptographic Security Platform Key & Secrets Vault BYOL (KeyControl).
Size	Select the size of the VM that you want to use for Cryptographic Security Platform Vault. Entrust recommends the following for standard and large deployments: • VCPUs: 2 for standard, 4 for large. • RAM: 8 GB for standard, 16 GB for large.

Field	Description
Administrator Account	
Authentication type	Select SSH public key.
Username	Enter `htadmin` as the username. The username must be in lower case.
SSH public key	Paste in the public portion of the SSH key pair you want to use for this node.

7. When you are done, click **Next: Disks**.
8. On the **Disks** tab, specify the options you want to use. For optimum performance, we recommend you select an SSD disk type. Cryptographic Security Platform Vault does not require additional data disks.
9. When you are done, click **Next: Networking**.
10. On the **Networking** page, specify the options you want to use based on your corporate standards. Cryptographic Security Platform Vault only requires the following:
    - The Public IP address must be static, which it is *not* by default. To use a static IP address, click **Create New** under the **Public IP** field. On the **Create public IP address** page, enter a name for the IP address and select the **Static** radio button under **Assignment**. When you are done, click **OK**.
    - If you create a new Network Security Group in this step (which is the Azure default action), Cryptographic Security Platform Vault automatically creates the correct port settings. If you select an existing Network Security Group, you need to make sure the security group allows network communication with Cryptographic Security Platform Vault over the following ports and protocols:

Type	Protocol	Port Range
SSH	TCP	22
HTTPS	TCP	443
Custom	TCP	5432
Custom	TCP	8443
Custom	UDP	123

      If you plan to connect this node with an existing Cryptographic Security Platform Vault cluster, you may need to open additional ports if the nodes are running in different Azure regions or in different environments.
11. If you want to set any other options for the VM, do so. When you are done, click **Review + Create**.
12. Review the settings for the resource and click **Create**. Wait for the success message from Azure confirming that the new resource is running and ready to use.
13. After Azure has created the virtual machine, determine the public IP address. To do so:
    a. In the left-hand pane, select **Resource groups**.
    b. Click the name of the resource group you specified on the **Basics** page.
    c. Click the virtual machine name in the table.

Tip: If you do this before Azure has deployed the new VM, it may take a few minutes for the VM name to appear in this table.

Azure displays the public IP address in the **Public IP address** field in the VM Details area.

14. Configure the node as the first Cryptographic Security Platform Vault node in the cluster or add it to an existing Cryptographic Security Platform Vault cluster. For details, see:
    - Configuring the First CSP Vault Node in Azure
    - Configuring Additional CSP Vault Nodes in Azure

Configuring Additional CSP Vault Nodes in Azure

You can add a Cryptographic Security Platform Vault node running in the Azure environment to any other Cryptographic Security Platform Vault nodes running in any other environments as long as the Azure node can communicate with the other nodes in the cluster.

Before You Begin

- Make sure you have the private SSH key file that matches the public SSH key that was specified when the instance was created.
  Important: The private part of the SSH key file cannot be reset or recovered once the VM is configured, even if you use the Azure "Reset Password" method. Please ensure that you keep it in a safe place.
- Make sure you know the static public IP address associated with the Azure node.
  To find the public IP address, select **All resources** from the Azure Resource Manager dashboard, then click on the virtual machine name on which the Cryptographic Security Platform Vault node is running. The public IP address is displayed in the VM details section at the top of the page.
- Make sure you know the IP address of one of the Cryptographic Security Platform Vault nodes already in the cluster.
  This IP address may *not* be the same as the public IP address. Make sure you verify the IP address before you attempt to add the node to the cluster.
  To find the correct IP address, log into the Cryptographic Security Platform Vault webGUI with Domain Admin privileges and go to **Cluster > Servers**. The IP address for each Cryptographic Security Platform Vault node is listed in the table.
- Make sure that the Azure node can communicate with the Cryptographic Security Platform Vault cluster in which you want to add the node. For details on setting up communication between the Azure VM and a Cryptographic Security Platform Vault VM running in a different Azure location or a different environment such as vSphere or AWS, see your Azure documentation.

Important: Azure might disconnect ssh sessions if idle for more than 5 minutes. To prevent this, please use the ServerAliveInterval and ServerAliveCountMax opens in the ssh client command line to keep the session active during Cryptographic Security Platform Vault management.

We recommend using ssh CLI options to send a KeepAlive packet with a frequency duration of less than 5 minutes. Please refer to the sshd_config man page for how to use the ServerAliveInterval and ServerAliveCountMax options. For example:

```
ssh -o ServerAliveInterval=180 -o ServerAliveCountMax=10 user@host
```

Procedure

1. Use a web browser to navigate to `https://<Public-IP-addy>`, where `<Public-IP-addy>` is the Public IP address Azure assigned to the Cryptographic Security Platform Vault VM. For security reasons, you must explicitly specify `https://` in the URL.
2. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault webGUI.

Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.

3. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for the username and enter the VM unique ID (vmId) for the password.
4. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
5. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
   The Join Existing Cluster window displays.
6. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
   - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
7. Click **Continue**.
8. On the Download CSR page, click **Generate and Download CSR**.
9. Click **Continue**.
10. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
11. Select **Actions > Add a Node**.
12. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
13. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
14. Click **OK** to close the Add a Node window.
15. Return to the new node and click **Continue**.
16. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.
17. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
18. When the node has successfully restarted, click **Login**.
19. Optional. Log into the `htadmin` account on the Cryptographic Security Platform Vault System Console using the private key file. For example:
    `ssh -i <key-file>.pem htadmin@<Public-IP-addy>`
    The password is the VM unique ID (vmId).
    After logging in, you can change this password. The change applies only to the `htadmin` login on this node.

7 Initializing the web GUI

The first time you log into the Cryptographic Security Platform Vault Management webGUI for a Cryptographic Security Platform Vault node, you need to do some basic initialization. After this process is complete, you can log directly into the Cryptographic Security Platform Vault Management webGUI without going through these steps.

1. Use a web browser to navigate to `https://node-ip-address`, where `node-ip-address` is the Management IP address you specified during installation. For security reasons, you must explicitly specify `https://` in the URL.
   Tip: If you do not know the Management IP address for the node, log into the system on which the node is installed as `htadmin`. Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console. From the menu, select **Manage Network Settings > Show Current Network Configuration**.
2. If prompted, add a security exception for the Cryptographic Security Platform Vault IP address and proceed to the Cryptographic Security Platform Vault Management webGUI.
   Cryptographic Security Platform Vault uses its own Root Certificate Authority to create its security certificate, which means that certificate will not be recognized by the browser. For details, see CSP Vault Certificates.
3. On the **Entrust Cryptographic Security Platform Vault Management** login page, enter `secroot` for both the username and password.
4. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
5. On the Welcome to Cryptographic Security Platform Vault screen, click **Continue as a Standalone Node**.
6. On the **Change Password** page, enter a new password for the `secroot` account and click **Update Password**.
7. On the **Configure E-Mail and Mail Server Settings** page, specify your email settings.
   If you specify an email address, Cryptographic Security Platform Vault sends an email with the Admin Key for the new node. It also sends system alerts to this email address.
   To disable alerts, select the **Disable e-mail notifications** checkbox. You are then prompted to download the Admin Key.
8. When you are done, click **Continue**.
9. On the Download Admin Key page, click the **Download** button to save the admin key locally. Please keep the admin key in a safe place for later use. When Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data.
   Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.
10. When you are finished, click **Continue**.
    Cryptographic Security Platform Vault displays the Cryptographic Security Platform Vault Management webGUI. For details about the tasks you can perform from the webGUI, see CSP Vault Management webGUI Page Reference.

What to Do Next

- To add additional Cryptographic Security Platform Vault nodes to form a cluster:
  - For OVA, see CSP Vault OVA Installation followed by Adding a New CSP Vault Node to an Existing Cluster (OVA Install).
  - For ISO, see CSP Vault ISO Installation for Hypervisor.
- If you plan to use the Entrust Policy Agent on either the Cryptographic Security Platform Vault for Databases or the Cryptographic Security Platform Vault for VM Encryption, see Preparing to Install the Policy Agent.

.

8 User guide

See below for the Vault console user options.

- CSP Vault authentication and user accounts
- Vault management
- CSP Vault for CloudKeys
- CSP Vault for Cryptographic APIs
- CSP Vault for Databases
- CSP Vault for KMIP
- CSP Vault for PKCS#11
- CSP Vault for Secrets
- CSP Vault for VM Encryption
- External Authentication Provider Examples
- Personal Access Tokens
- Cloud Admin Groups and CSP Vault User Accounts

CSP Vault authentication and user accounts

There are two types of CSP Vault user accounts:

- Cryptographic Security Platform Vault-managed user accounts. These are individual accounts created and administered locally in Cryptographic Security Platform Vault. A Cryptographic Security Platform Vault-managed account can be authenticated locally (with a password stored in Cryptographic Security Platform Vault) or externally (with a password stored in an LDAP server), and it can have any combination of the available user roles: Security Admin, Domain Admin, and Cloud Admin. These three user roles and their privileges are described below.
  With Cryptographic Security Platform Vault-managed accounts, a Cryptographic Security Platform Vault Security Admin should create one user account for each person who needs access to Cryptographic Security Platform Vault, being careful to assign each account the appropriate user roles and access rights.
- Active Directory (AD)-managed user accounts. Unlike Cryptographic Security Platform Vault-managed accounts where you have to create one account for each Cryptographic Security Platform Vault user, AD-managed users are granted access at the AD Security group level. When a Cryptographic Security Platform Vault Security Admin creates a Cloud Admin Group, they can assign one or more AD Security groups to that Cloud Admin Group. When they do so, every individual in every explicitly-named AD Security group is automatically granted Cloud Admin access to Cryptographic Security Platform Vault. (For more information, see Considerations When Using AD Security Groups.)
  AD Security groups can only be associated with a Cloud Admin Group, and the only available user role for an AD-managed user account is Cloud Admin. This means you cannot use an AD group to specify users that need Security Admin or Domain Admin access to Cryptographic Security Platform Vault. Those users must have their own Cryptographic Security Platform Vault-managed user account.

By default, the Cryptographic Security Platform Vault installer creates the Cryptographic Security Platform Vault-managed user account `secroot`, which is automatically assigned all three user roles and placed in the default Cloud Admin Group. You can change the password and group membership for `secroot`, but you cannot delete the account or change its assigned Security Admin user role. We recommend you only give the `secroot` password to a very small number of administrators who need root-level access. If you need to change the `secroot` password, see Resetting the secroot Account Password.

User Roles and Privileges

Security Admin

- Can manage the Cryptographic Security Platform Vault license.
- Can create or delete Cryptographic Security Platform Vault-managed user accounts and Cloud Admin Groups.
- Can specify the LDAP server that Cryptographic Security Platform Vault will use to authenticate AD user accounts.
- Can assign Cryptographic Security Platform Vault-managed users or AD groups to Cloud Admin Groups.
- Can manage the master Admin key and set up KMIP or HSM as a external key server.
- Can back up, restore, and upgrade Cryptographic Security Platform Vault.
- Can manage the Cryptographic Security Platform Vault KMIP server settings, accounts, and objects.
- Can enable Cryptographic Security Platform Vault features such as email settings and BoundaryControl.
- Can view all audit records. These records can be exported to an external syslog server.
- Can view and delete alerts.
- *Cannot* view any policies or virtual machines, and cannot modify any associated settings.

Domain Admin

- Can manage Entrust Cryptographic Security Platform Vault clusters by adding, removing, and authorizing Cryptographic Security Platform Vault nodes.
- Can configure Cryptographic Security Platform Vault node settings such as Cryptographic Security Platform Vault heartbeat.
- Can view audit log records and alerts generated by Domain Admin actions.

Cloud Admin

- Can manage the encryption of virtual machines that have the Entrust Policy Agent installed.
- Can create and manage Cloud VM Sets, which separate the encrypted VMs into logical groups such as "VMs running in AWS" or "UK Data Center VMs". The configuration settings selected for a Cloud VM Set are automatically applied to all VMs in that set.
- Can set options for specific VMs that override the default options specified in the Cloud VM Set.
- Can create certificates for VMs and specify key expiration dates.
- Can revoke access to individual encrypted disks/filesystems, or the whole VM. When access to disks is revoked, filesystems are forcibly unmounted, thus removing access to clear-text data.
- Can create encryption keys to securely move encrypted data between specified VMs in the same Cloud VM Set.
- Can view audit records and alerts generated from the all VMs in the Cloud VM Sets to which they have access.

The Security Admin, Cloud Admin, Domain Admin model is being retired in favor of RBAC. Currently, the model has been retired only for appliance logins.

This section includes:

- Authentication for CSP Vault User Accounts
- Configuring local authentication
- Configuring Local Authentication Settings
- Configuring Active Directory
- Adding an Active Directory Group
- Configuring OIDC
- Specifying an LDAP/AD Authentication Server
- Specifying an OpenLDAP Authentication Server
- Configuring OIDC with Active Directory for CSP Vault

- Configuring OIDC for Vault
- Configuring an OpenID Connect Provider
- Setting the CSP Vault Management webGUI Session Timeout
- Setting the Default Account Expiration
- Creating a New CSP Vault-Managed User Account
- Setting webGUI User Preferences
- Changing Your CSP Vault User Account Settings
- Setting the secroot Account Expiration
- Resetting the secroot Account Password
- Changing CSP Vault Account Details as a Security Administrator
- Re-enabling a CSP Vault-Managed User Account
- Configuring Role-Based Access Control

Authentication for CSP Vault User Accounts

Cryptographic Security Platform Vault-Managed Account Authentication

Cryptographic Security Platform Vault-managed accounts can be authenticated locally, with a password stored in the Cryptographic Security Platform Vault Management webGUI. Security Admins can configure the password requirements and expiration options, as well as the maximum number of login attempts that are allowed before the user account is disabled and an expiration date after which the account will be automatically disabled.

- Locally, with a password stored in Cryptographic Security Platform Vault. Cryptographic Security Platform Vault Security Admins can configure the password requirements and expiration options, as well as the maximum number of login attempts that are allowed before the Cryptographic Security Platform Vault account is disabled and an expiration date after which the account will be automatically disabled.
- Externally, through a LDAP/Active Directory authentication server. Security Admins cannot change the password requirements or expiration options, but they can set the maximum number of login attempts that are allowed before the Cryptographic Security Platform Vault-managed account is disabled and they can set an expiration date on the account itself so that it cannot be used after a certain date.
  For LDAP and Active Directory servers, Security Admins can specify one and only one domain for all user account authentication. You can, however, configure multiple domain controllers to provide failover in case one controller becomes unreachable.
- Cryptographic Security Platform Vault also supports user authentication through an OpenID Connect provider. If a provider is configured, the Cryptographic Security Platform Vault login dialog contains not only the **Sign In** button but also a configurable button to start the authentication process using the provider. When the user has been authenticated via the OpenID Connect provider, the same username is used to obtain the LDAP permissions to Cryptographic Security Platform Vault.

Active Directory-Managed Account Authentication

Cryptographic Security Platform Vault requires customers to provide a service account in Active Directory settings. The service account is used for retrieving the list of AD objects to help Security Administrators configure members in KeyControl Groups. The service account configured in Active Directory settings requires the following read permissions in AD:

- User object: attributes distinguishedName, cn, sAMAccountName, userPrincipalName, mail
- Group object: attributes objectGUID, distinguishedName, cn, sAMAccountName

All Active Directory (AD)-managed accounts must belong to AD Security groups that are defined in the same AD domain. While you can specify multiple domain controllers to provide failover, all of the Security groups you want to use must be part of the same domain.

> Note: An AD-managed user account *cannot* log into Cryptographic Security Platform Vault for the first time if the Cryptographic Security Platform Vault cluster is degraded. AD accounts that have already

successfully logged in at least once will continue to work, but, in a degraded state, Cryptographic Security Platform Vault cannot process a new AD user login.

If you plan to use a mix of Cryptographic Security Platform Vault-managed user accounts that are authenticated through LDAP along with AD Security groups, you must use the same AD domain for both the Cryptographic Security Platform Vault-managed accounts and the AD Security groups.

Configuring local authentication

Local authentication is enabled by default when you create a vault. If you use local authentication, you don't need to configure any additional authentication. Next, configure your access policies and users.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all users but keep local authentication available for admin users.

Configuring Local Authentication Settings

This procedure describes how to configure the password and account security options for all locally-authenticated Cryptographic Security Platform Vault-managed user accounts. Password requirements for externally-authenticated accounts is managed in your LDAP authentication server.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Type** drop-down list, select **Local (Password)**.
6. On the **Basic** tab, change the options as desired, then click **Apply** when finished.

Field	Description
Password Expiration	The maximum number of days that a password can be used before it expires. Cryptographic Security Platform Vault also uses this value to calculate the default password expiration date when a new local Cryptographic Security Platform Vault user is created. (Default: 60.) Once a password expires, the user is prompted to change their account password the next them they log into the webGUI.
Max Failed Logins	The number of failed login attempts allowed before the user account is locked. (Default: 5.) If the maximum number of logins is exceeded, the next time the user attempts to log in they receive a message informing them that the account is disabled and telling them to talk to a Security Administrator. The Security Administrator must then re-enable the account as described in Re-enabling a CSP Vault-Managed User Account. Note: This option applies to all Cryptographic Security Platform Vault-managed accounts, even ones that are authenticated using LDAP.

Field	Description
Minimum Previous Passwords	The number of unique new passwords that must be associated with a user account before an old password can be used. (Default: 5.)

7. On the **Strength** tab, click the desired value to change the setting, then click **Save** when finished. If you change one of these settings, Cryptographic Security Platform Vault applies the new requirements to any new passwords created for a Cryptographic Security Platform Vault account. It does *not* apply the requirements to any existing Cryptographic Security Platform Vault account passwords.

Field	Description
Minimum Password Length	The minimum number of characters that must be in a password. (Default: 8.)
Minimum Uppercase Characters	The minimum number of characters that must be upper case. (Default: 1.)
Minimum Special Characters	The minimum number of characters that must be something other than a-z, A-Z,or 0-9. (Default: 1.)
Minimum Lowercase Characters	The minimum number of characters that must be lowercase. (Default: 1.)
Minimum Required Digits	The minimum number of characters that must be numeric. (Default: 1.)

8. When you are finished, click **Close**.

Configuring Active Directory

See below for configuring Active Directory for the Vault.

> By default, the vault uses local authentication. You can change the authentication method as required.

To configure Active Directory

1. Log in to the CSP Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. On the Authentication page, select **LDAP** as the Authentication Type.
5. On the **Domain** tab, enter:
   - Domain Name—Enter the domain name for the service account.
   - Directory Service Type—Select **Microsoft AD** if you plan to use Microsoft AD directory services, or **OpenLDAP** for all non-Microsoft AD directory services.

- Service Account Name—Enter the name of the service account for the given domain (for example, Administrator).

  > The service account needs read-only access to users and groups on the domain and any subdomain used.

- Service Account Password —Enter the password for the service account.
- UID Attribute—Enter the Security Manager Account Name (sAMAccountName) for the user.

  > This is the attribute of the user or group object that would be queried during search.

6. Click **Apply** to save the changes.
7. Click the **Domain Controllers** tab.
8. Click **+**
9. Add the following details in the **Add Domain Controller** window.
   - Server URL
   - STARTTLS
   - CA Certificate
   - User Search Context (Base DN)
   - Group Search Context (Base DN)
   - Timeout
10. Click **Save and Close**.

Server URL

Select LDAP or LDAPS and enter the domain name or IP address. To include a port number, use the following syntax:

```
<ip>:<port>
```

STARTTLS

If you selected LDAP, check the checkbox if you want to use LDAP over TLS.

CA Certificate

The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller.

- The CA certificate must be in Base64-encoded PEM format.
- If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates.

Click Load File to select the CA certificate that you want to use.

User Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the user search should start. For performance reasons, make the base DN as specific as possible. For example:

```
dc=ldapserver,dc=com
```

This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP.

Group Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the search for Security groups should start.

This option applies to AD Security groups being associated with an admin group.

Timeout

Set the timeout in seconds before connecting to an alternate domain controller.

- If multiple domain controllers are specified, this is how long the Cryptographic Security Platform Vault waits for a response before re-sending the request to another domain controller.
- If the DNS server is down, Cryptographic Security Platform Vault may take longer than the time specified here before it fails over to the next domain controller in the list or considers the authentication request failed.

This option only applies to the TCP/LDAP request. It does not apply to the DNS request before the LDAP server has been successfully contacted.

Adding an Active Directory Group

If you want to add an Active Directory Group, complete the following.

To add an Active Directory Group

1. Log in to the Vault web GUI
2. Click **Security**.
3. Click the **Groups** tab.
4. Select **Actions > Create Group**.
5. On the **Group** tab, enter the name of the group and click **Next**.
6. On the Active Directory Groups tab, type the first three letters of the group to fetch the group name from the AD server.
7. Click **Next**.
8. On the KeyControl Managed User Members tab, select the managed users that you want to assign and click the right arrow icon.
9. Click **Create**.

Configuring OIDC

By default, the vault uses local authentication. You can change the authentication method as required, and you can have multiple authentication modes active at the same time. However, OIDC without Active Directory cannot be used with Active Directory, and OIDC with Active Directory cannot be used without Active Directory.

> ⚠ You cannot disable OIDC authentication once it is configured. After you enable OIDC, you can no longer sign in with AD credentials. However, you can sign in using local authentication credentials without any issues.

To configure OIDC

1. Log in to the Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. In the **Choose Authentication Type** drop-down menu, select:
   - **OpenID Connect** to configure OIDC without Active Directory
   - **OpenID Connect (with AD)** to configure OIDC with Active Directory
5. Click the **Learn more about configuring the OIDC Provider** link to view the OIDC provider's login redirect URL and logout redirect URL.
6. Specify the OpenID Connect Configuration settings:
   - Name
   - Client ID
   - Client Secret
   - Base URL
7. Optionally, click **Load File** to upload the CA certificate in base64-encoded PEM format.
8. Click **Apply**.
9. Select **Verify and Enable**. After verification, a message appears confirming OpenID Connect has been successfully enabled. Vault is set for OIDC authentication.
10. Sign out from the vault and sign in to the vault as an OIDC user by selecting **Sign in with IDAAS** and entering your OIDC credentials.

Name

A user-defined name for the OpenID Connect provider.

> ℹ Cryptographic Security Platform Vault displays this name on the button in the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

> ⚠ This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Specifying an LDAP/AD Authentication Server

For Cryptographic Security Platform Vault-managed user accounts, you can use any LDAP server. If you want to specify AD-managed Security groups whose members will have Cloud Admin access to the VMs registered with Cryptographic Security Platform Vault, you must specify a Windows Active Directory (AD) server.

Cryptographic Security Platform Vault uses the same settings for both local account authentication and AD Security group authentication. You can specify up to two AD domain controllers for failover, but both controllers must manage the same AD domain.

For OpenLDAP, see Specifying an OpenLDAP Authentication Server.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Type** drop-down list, select **LDAP**.
6. On the **Domain** tab, specify the options you want to use. When you are done, click **Apply**.

Field	Description
Domain Name	The Domain name to use for account authentication. You cannot specify multiple domain names.
Directory Service Type	If you plan to use Microsoft AD directory services, then select Microsoft AD. Select OpenLDAP for all non-Microsoft AD directory services.
Service Account	The AD account that Cryptographic Security Platform Vault should use when logging into the AD server. Specify the account using one of the following formats: • Distinguished Name (DN). For example, `CN=Administrator,CN=users,DC=<company-name>,DC=com` • User Principal Name (UPN). For example, `administrator@<company-name>.com`. • Account username. For example, `administrator`. The AD account is usually an administrative user and it can have read only permissions on the AD server.
Service Account Password	The password for the Service Account.
UID Attribute	The Security Manager Account Name (sAMAccountName) for the user. This is the attribute of the user or group object that would be queried during search.

7. If you want to add or change a Domain Controller, go to the **Domain Controllers** tab. To add a controller, click the blue **+** (Plus) sign. You can add up to two domain controllers per Cryptographic Security Platform Vault cluster.
   If you specify two domain controllers, make sure your primary controller appears first in this list. Cryptographic Security Platform Vault always tries to authenticate an AD user through the first domain controller listed.
   To edit an existing domain controller, select that controller and then click the edit button. You can specify the following basic options:

Field	Description
Server URL	The LDAP server IP address or hostname. Select `ldap://` or `ldaps://` from the drop-down list and enter the URL in the text field. To include a port number, specify *`:port`* after the name. For example, `ldaps://10.238.66.33:389`.
STARTTLS	Enable this option if you want Cryptographic Security Platform Vault to use Transport Layer Security (TLS) protocol when communicating with the LDAP server. Note: This option is only available if the Server URL starts with `ldap://`.
CA Certificate	The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller. The CA certificate must be in Base64-encoded pem format. Cryptographic Security Platform Vault uses the CA certificate to verify the SSL certificate used by the LDAP server/Active Directory. If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates. If you are using `ldaps://` or have selected the STARTTLS option for `ldap://`, click Load File and select the CA (Certificate Authority) certificate for the LDAP server.
User Search Context	The Distinguished Name (DN) of the node where the search for users should start. This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP. For performance reasons, the base DN should be as specific as possible. For example, `dc=ldapserver,dc=com`.
Group Search Context	The Distinguished Name (DN) of the node where the search for Security groups should start. This option applies to AD Security groups being associated with a Cloud Admin Group.

Field	Description
Timeout	If multiple domain controllers have been specified, this is the amount of time Cryptographic Security Platform Vault should wait for a response before it re-sends the request to another domain controller. This option only applies to the TCP/LDAP request. It does *not* apply to the DNS request before the LDAP server has been successfully contacted. If the DNS server is down, Cryptographic Security Platform Vault may take longer than the length of time specified here before it fails over to the next domain controller in the list or it considers the authentication request to have failed.

8. When you are finished, click **Save & Close**. Cryptographic Security Platform Vault automatically verifies that it can reach the specified domain controller using the service account credentials you specified on the **Domain** tab.

Specifying an OpenLDAP Authentication Server

You can now use OpenLDAP for Cryptographic Security Platform Vault-managed user accounts.

For Microsoft AD services, see Specifying an LDAP/AD Authentication Server.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Type** drop-down list, select **LDAP**.
6. On the **Domain** tab, specify the options you want to use. When you are done, click **Apply**.

Field	Description
Domain Name	The Domain name to use for account authentication. You cannot specify multiple domain names.
Directory Service Type	Select OpenLDAP.
Service Account	The service account that Cryptographic Security Platform Vault should use when logging into the OpenLDAP server. We recommend that you specify the account using the following format: `<CN>@<DOMAIN NAME>` Important: OpenLDAP does not support the UPN parameter. Using the `<CN>@<DOMAIN NAME>` format allows you to import OpenLDAP users correctly into the provider's database. The users can then authenticate with the provider in Cryptographic Security Platform Vault.

Field	Description
Service Account Password	The password for the Service Account.
UID Attribute	The Security Manager Account Name (sAMAccountName) for the user.

7. If you want to add or change a Domain Controller, go to the **Domain Controllers** tab. To add a controller, click the blue **+** (Plus) sign. You can add up to two domain controllers per Cryptographic Security Platform Vault cluster.
   If you specify two domain controllers, make sure your primary controller appears first in this list.
   To edit an existing domain controller, select that controller and then click the edit button. You can specify the following basic options:

Field	Description
Server URL	The LDAP server IP address or hostname. Select `ldap://` or `ldaps://` from the drop-down list and enter the URL in the text field. To include a port number, specify *:port* after the name. For example, `ldaps://10.238.66.33:389`.
STARTTLS	Enable this option if you want Cryptographic Security Platform Vault to use Transport Layer Security (TLS) protocol when communicating with the LDAP server. Note: This option is only available if the Server URL starts with `ldap://`.
CA Certificate	The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller. The CA certificate must be in Base64-encoded pem format. Cryptographic Security Platform Vault uses the CA certificate to verify the SSL certificate used by the LDAP server/Active Directory. If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates. If you are using `ldaps://` or have selected the STARTTLS option for `ldap://`, click Load File and select the CA (Certificate Authority) certificate for the LDAP server.

   If you want to specify advanced domain controller options, click **Show Advanced Settings** and specify the options you want to use.

Field	Description
User Search Context	The Distinguished Name (DN) of the node where the search for users should start. This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through OpenLDAP. For performance reasons, the base DN should be as specific as possible. For example, `dc=ldapserver,dc=com`.
Group Search Context	The Distinguished Name (DN) of the node where the search for Security groups should start. This option applies to AD Security groups being associated with a Cloud Admin Group.
Timeout	If multiple domain controllers have been specified, this is the amount of time Cryptographic Security Platform Vault should wait for a response before it re-sends the request to another domain controller. This option only applies to the TCP/LDAP request. It does *not* apply to the DNS request before the LDAP server has been successfully contacted. If the DNS server is down, Cryptographic Security Platform Vault may take longer than the length of time specified here before it fails over to the next domain controller in the list or it considers the authentication request to have failed.

8. When you are finished, click **Save & Close**. Cryptographic Security Platform Vault automatically verifies that it can reach the specified domain controller using the service account credentials you specified on the **Domain** tab.

Configuring OIDC with Active Directory for CSP Vault

By default the KeyControl Vault Management application is configured for local authentication. You can change the authentication method as required.

This topic explains how to configure OIDC authentication.

Active Directory authentication is a prerequisite for OIDC. Ensure Active Directory Authentication is configured for the vault before configuring OIDC. See Specifying an LDAP/AD Authentication Server. For OpenID Connect login to be successful across all vaults, you must provide AD/OpenLDAP service credentials, and the credentials must be active.

Each vault can be configured with a separate OIDC server or a separate application from same server.

For an example of how to configure an OIDC provider, see Example: Configuring Entrust Identity as a Service. If you are using a cluster, even though you configure OIDC for only one node, you will need to enter the Callback URIs (the Login Redirect URIs and Logout Redirect URIs) for all nodes in the cluster.

Important: OIDC with AD is a legacy authentication mode that relies on Active Directory (AD) where the OIDC provider manages authentication and Active Directory manages identity. This option should be used only for existing OIDC configurations that are already integrated with AD. If you are not using AD, we recommend that you use OIDC without AD as your OIDC authentication method.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.

2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Choose Authentication Type** drop-down list, select **OpenID Connect (with LDAP)**.
6. Specify the OpenID Connect Configuration settings:

Field	Description
Name	A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.
Client ID	The organizational identity assigned by the OpenID Connect provider when you sign up for the service.
Client Secret	A cryptographic component used to secure the organization's access to the OpenID Connect provider. Important: This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.
Base URL	The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

7. Click **Browse** to upload the CA Certificate.
   Note: The certificate needs to be in base64 encoded pem format.
8. Click **Apply**.
   A dialog box displays the configuration.
9. Click **Verify and Enable**.
10. After the verification, ensure the OpenID Connector Configuration Status is set to **Enabled**.
11. The vault is now set for OIDC authentication.

Configuring OIDC for Vault

By default, the KeyControl Vault Management application is configured for local authentication. You can change the authentication method as required, but you can use only one type of authentication per vault at a time.

- If you want to use OIDC without AD, you can only change to that mode from the local authentication mode.
- If you have configured AD or OIDC with AD, you cannot change to OIDC without AD. You must first delete all AD users and groups, then remove the AD and/or OIDC configuration before configuring OIDC without AD.

Each vault can be configured with a separate OIDC server or a separate application from same server.

> ⚠ OIDC without AD is the recommended mode of OIDC authentication method where the OIDC provider independently manages identity and authentication. For new OIDC setups, this is the preferred option.

To configure OIDC

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.

2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Choose Authentication Type** drop-down list, select **OpenID Connect**.
6. Specify the OpenID Connect Configuration settings:
    - Name
    - Client ID
    - Client Secret
    - Base URL
7. Optional. Click **Browse** to upload the CA Certificate.

    The certificate needs to be in base64 encoded pem format.

8. Click **Apply**. The OpenID Connect Configuration window appears showing the current configuration.
9. Click **Verify and Enable**. After verification, a message appears confirming that OpenID Connect has been successfully enabled. The vault is now configured for OIDC authentication.

Name

A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Configuring an OpenID Connect Provider

Cryptographic Security Platform Vault supports user authentication through an OpenID Connect provider. If a provider is configured, the Cryptographic Security Platform Vault login dialog contains not only the Cryptographic Security Platform Vault Sign In button but also a configurable button to start the authentication process using the provider.

Important:

- For OpenID Connect login to be successful across all vaults, you must provide AD/OpenLDAP service credentials, and the credentials must be active.
- When the user has been authenticated via the OpenID Connect provider, the same username is used to obtain the LDAP permissions to Cryptographic Security Platform Vault. Therefore, the User Principal Name (UPN) used for the OpenID Connect provider must match a configured user on the LDAP server.

- OpenLDAP does not support the UPN parameter. This might cause problems because the OpenID Connect provider might be unable to authenticate users if it cannot return a valid UPN. **Workaround**: Set the `sn` field in the OpenLDAP server to the UPN for the registered user. This allows you to import OpenLDAP users correctly into the provider's database. The users can then authenticate with the provider in Cryptographic Security Platform Vault.

Before You Begin

The OpenID Connect provider must be configured to accept the Cryptographic Security Platform Vault URLs. Each login dialog requires both a login and a logout URL, so for Cryptographic Security Platform Vault, you have to configure 2 URLs for each node in the cluster. You have to configure the login and logout URL for Cryptographic Security Platform Vault, these 2 URLs are also sufficient for all types of vaults.

In the following example of URL list for OpenID Connect provider, `KC_IP` is the hostname or IP address of the Cryptographic Security Platform Vault agent:

<https://KC_IP/v5/oidc/callback>
<https://KC_IP/v5/kc/oidc/logout>

From Cryptographic Security Platform Vault 10.1.1, the Cryptographic Security Platform Vault appliance and the various types of vaults support multiple IDP servers. Each vault can have a separate IDP configured or can have different applications of same IDP configured for OIDC authentication.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **Type** drop-down list, select **OpenID Connect**.

Specify the options you want to use. When you are done, click Apply.

Field	Description
Client ID	The organizational identity assigned by the OpenID Connect provider when you sign up for the service.
Client Secret	A cryptographic component used to secure the organization's access to the OpenID Connect provider. Important: This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.
Base URL	The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Field	Description
Name	A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs. Only one global OIDC provider can be configured per Cryptographic Security Platform Vault cluster. The same button appears and the same OIDC authentication method is used on the login dialogs to Cryptographic Security Platform Vault, the Cryptographic Security Platform Vault for KMIP webGUI, and the Cryptographic Security Platform Vault for Secrets webGUI.

Setting the CSP Vault Management webGUI Session Timeout

By default, a Cryptographic Security Platform Vault Management webGUI session is logged out automatically after 30 minutes of inactivity. You can shorten the timeout but you cannot lengthen it.

> Note: If the user closes the browser without explicitly logging out from Cryptographic Security Platform Vault Management webGUI first, Cryptographic Security Platform Vault Management webGUI does not end the session until the session timeout is reached.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Session Timeout**.
4. Use the slider to set the desired value. You can set the timeout to be between 1 and 30 minutes.
5. Click **Apply** to save your changes.

Setting the Default Account Expiration

When you create a Cryptographic Security Platform Vault-managed user account, Cryptographic Security Platform Vault automatically assigns an account expiration date 365 days from the date the account is created. If you change this default, the expiration date for existing accounts is not changed. The new value is only applied to future accounts.

The default expiration date can also be overridden on an account by account basis when you create a new user account. For details, see Creating a New CSP Vault-Managed User Account.

> Note: This option applies only to Cryptographic Security Platform Vault-managed accounts. It does not apply to AD-managed user accounts. For details, see CSP Vault Authentication and User Accounts.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **KeyControl Account**.
5. In the **Account Expires After** field, click the existing value and enter a number of days between 1 and 999. The default is 365 days.
6. Click **Save** and close the General Settings dialog box.

Creating a New CSP Vault-Managed User Account

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.

2. In the top menu bar, click **Users**.
3. Select **Actions > Create User**.
4. Enter the following information. All fields are required.

Field	Description
Full Name	The full name of the user associated with the account. This name is included on any audit log messages generated by that user's activity. Therefore, we recommend that you specify a unique full name for each Cryptographic Security Platform Vault user.
Email	If your system is configured to send email alerts, they will be sent to this email address. The alerts a user sees depends on their user role and group access.
Account Decay	The amount of time an account can stay enabled without logging in. The default and maximum value is 10 years from the last login date. If the user does not log in within that time period, Cryptographic Security Platform Vault automatically disables the account, but does not delete it. You will need to contact Entrust Support to re-enable the account.
Account Enabled	Check this box to have the account be available as soon as you create it. If you clear this check box, Cryptographic Security Platform Vault sets the account status to Disabled and you will need to manually enable it through the webGUI.

5. Click **Add**.
6. When you see the **User Successfully Added** message, click **Close**.

Setting webGUI User Preferences

The webGUI user account preferences are saved in Cryptographic Security Platform Vault so that your preferences are available even if you log in from a new location or using a different browser.

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, open the **User Menu** by clicking the down arrow following your login name.
4. Select **User Preferences**.
5. On the **User Preferences** page, you can:
    - Select the page you want Cryptographic Security Platform Vault to display automatically whenever you log into the webGUI by selecting it in the **Default Landing Page** drop-down list. The pages available depend on the privileges associated with your user account.
    - Reset the initial landing page to the Entrust default by clicking the **Reset Initial Landing Page to Default** button. The default page depends on the privileges associated with your account.
    - Have Cryptographic Security Platform Vault remember your table column settings between sessions by checking the **Save Column Preferences** check box. This option is enabled by default.
    - Restore all default table settings and remove any customizations by clicking the **Reset All Grids to Default Configuration** button.

- Change the webGUI skin by selecting a theme in the **Theme** drop-down list.

6. When you are done, click **Save Preferences**.

Changing Your CSP Vault User Account Settings

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
   Note: AD-managed account users can view their account settings but they cannot change them.
2. In the top right, click the Switch to **Appliance Management** link.
3. Click **Settings**.
4. To change your account settings, click the contents of the appropriate field. Cryptographic Security Platform Vault-managed account users can change:
   - Full Name—Click the current name and enter the new information. When you are done, click **Save**. The full name can contain letters, digits, hyphens (-), or underscores (_).
     Note: The full name is associated with any audit log messages generated by the activity on this account. We recommend that every user be assigned a unique full name. Before you change this information consult your Cryptographic Security Platform Vault Administrator to make sure the full name you want to use is available.
   - Password—Click the **Change Password** button and enter your new password in the **Change Password** dialog box. When you are done, click **Update Password**. You can only change the password for a locally authenticated Cryptographic Security Platform Vault-managed user account. All other account passwords must be changed through the external LDAP, or Active Directory authentication server.
   - Email Address—Click the current email address and enter the new information. When you are done, click **Save**.
   - Send Alert Notifications—If this is set to **On**, any alert notifications are emailed to the address associated with the account. If it is **Off**, alert notifications can only be viewed in the webGUI.
   - Two-Factor Authentication—If this is set to **On**, you are required to have an authentication token when logging into the webGUI. If it is set to **Off**, you can log in using your standard username/password combination. For details and supported accounts, see About Two-Factor Authentication.

Setting the secroot Account Expiration

You can set an expiration for the Security Administrator (`secroot`) user account or set it to never expire.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Users**.
3. Select the Security Administrator (`secroot`) user account in the list. The Cryptographic Security Platform Vault webGUI displays the details for the selected account below the table.
4. In the Account Expiration field, choose one of the following:
   - **Never**—The `secroot` user account will never expire. This is the default.
   - **Choose a date**—The `secroot` user account will expire on the date that you set. Click **Apply** to save the date that you selected.

Resetting the secroot Account Password

The Cryptographic Security Platform Vault webGUI has a default Cryptographic Security Platform Vault-managed user account called secroot. If you do not remember the credentials of any Cryptographic Security Platform Vault user account with Security Administrator privilege, or if you are locked out of

the Cryptographic Security Platform Vault webGUI, you can reset the secroot credentials with a temporary password. You can reset the password using one of the following methods:

- **Generate random password and send it via email to secroot**—Use this option to generate a random temporary password for the `secroot` user and securely send it to their email account that is registered in Cryptographic Security Platform Vault. The `secroot` user must have an email account configured in the Cryptographic Security Platform Vault webGUI and have access to email. We recommend that you use this option if secroot has email configured and has access to email.
- **Enter new temporary password for secroot**—Use this option to enter a temporary password. You can either pass it to the `secroot` user outside of Cryptographic Security Platform Vault, or email it to the `secroot` user directly from Cryptographic Security Platform Vault.

Note: If you have Two-Factor Authentication enabled configured for `secroot`, you will be provided an option to optionally reset the `secroot` user's Two-Factor Authentication state/secret.

Procedure

1. Log into the Cryptographic Security Platform Vault VM console as `htadmin`.
   Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Manage Accounts**.
3. In the Manage Accounts page, select **secroot (**Cryptographic Security Platform Vault webGUI **default account)**.
4. On the Cryptographic Security Platform Vault - Reset `secroot` Account page, choose the option that you want and complete the following:
   - To use Cryptographic Security Platform Vault to generate a random password and send it to the `secroot` user:
     i. Select **Generate random password and send it via email to secroot**.
     ii. On the Generate random password and send it via email to secroot page, optionally choose **Reset Two-Factor Authentication**.
     iii. Select **OK**.

     The `secroot` user will receive an email with the temporary password. When they log into the Cryptographic Security Platform Vault webGUI with the temporary password, they are immediately prompted to update the password.
   - To enter your own temporary password for `secroot`:
     i. Select **Enter new temporary password for secroot**.
     ii. On the Enter new temporary password for secroot page, optionally choose **Reset Two-Factor Authentication** and **Send Temporary password to secroot via email**.
     Note: If you choose to email the temporary password, the `secroot` user must have an email account configured in the Cryptographic Security Platform Vault webGUI and have access to emails.
     iii. Select **OK**.
     iv. Enter and confirm the temporary password.
     v. Select **OK**.
     vi. On the confirmation screen, select **OK**.

     When the `secroot` user receives the temporary password and logs into the Cryptographic Security Platform Vault webGUI, they are immediately prompted to update the password.

Changing CSP Vault Account Details as a Security Administrator

This procedure is for Cryptographic Security Platform Vault-managed user accounts only. You cannot change the account details for any AD-managed user accounts. For details, see CSP Vault authentication and user accounts.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Security**.
4. Click the **KeyControl Managed Users** tab.
5. Select the account you want to modify in the list. The Cryptographic Security Platform Vault webGUI displays the details for the selected account below the table.
6. Click the tab containing the information you want to change.
   Note: For a full description of all information in the tabs, see Creating a New CSP Vault-Managed User Account.
   - The full name, account status, account expiration, and email information is on the **User** tab. The **User** tab also lets you disable two-factor authentication for another user's account. If you do so, however, the user will need to re-enable it themselves. You cannot enable two-factor authentication for any other user's account. For more information, see About Two-Factor Authentication.
     Note: Beginning with 5.2, the security administrator can globally enforce two-factor authentication for all users. For more information, see Managing Two-Factor Authentication.
   - The authentication method and password, including the password expiration, for locally-authenticated accounts is on the **Authentication** tab.
   - The user role and group membership information is on the **Privileges and Groups** tab.
7. Click the field that you want to change and enter the new value in that field. When you are done, click **Save**. Your changes are immediately applied to the account.

Re-enabling a CSP Vault-Managed User Account

A Cryptographic Security Platform Vault-managed user account can become disabled for the following reasons:

- The number of consecutive unsuccessful login attempts has exceeded the value set for **Max Failed Logins**. For more information, see Configuring Local Authentication Settings.
- A Cryptographic Security Platform Vault Security Admin has manually disabled the account.
- The expiration date associated with the account has passed.
- The **Account Enabled** check box was not selected when the user account was created.

Important: If you cannot log into any Cryptographic Security Platform Vault accounts with Security Admin privileges, contact Entrust Support.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Security**.
4. Select the account you want to re-enable in the list. The Cryptographic Security Platform Vault webGUI displays the details for the selected account below the table.
5. In the **Account Status** field, click **Disabled**.
6. Check the **Enabled?** check box and click **Save**.
7. Verify the expiration date in the **Account Expiration** field.
8. To change the account password, click the **Authentication** tab then click **Change Password**.

Your changes take effect immediately.

Configuring Role-Based Access Control

Role-Based Access Control (RBAC) allows you to assign permissions through roles instead of granting access directly to users. Users and Active Directory (AD) groups can be assigned one or more roles, and the permissions associated with those roles determine the actions they can perform. When upgrading to Release 10.6.1 from an earlier release, existing users are automatically migrated to the RBAC model. Existing access levels are preserved during migration.

> The introduction of RBAC to Compliance Manager is being implemented in phases. Release 10.6.1 includes Phase 1, which applies only to Vault appliance users. Vault users for all types of vaults are currently unchanged.

This page provides information on the following topics:

- Viewing Assigned Roles
- Viewing Available Roles
- Assigning Roles to a New User
- Assigning Roles to an AD Group
- Modifying Assigned Roles
- Role Assignment Restrictions

Viewing Assigned Roles

1. Log in to the Cryptographic Security Platform Vault Management webGUI.
2. In the top right, click Switch to **Appliance Management**.
3. In the **Account Settings** section, view the **Assigned Roles** field to see the roles assigned to you.

> The Account Settings section displays a read-only list of the roles assigned to your user account.

Viewing Available Roles

1. Log in to the Cryptographic Security Platform Vault Management webGUI.
2. In the top right, click Switch to **Appliance Management**.
3. From the top menu, select **Users**.
4. Select the **Roles** tab. A list of roles and their descriptions appear.

> The Roles tab is a read-only view that lists the available roles and the operations each role can perform.

Assigning Roles to a New User

When creating a user, you can assign roles during user creation. The selected roles determine the permissions available to the new user. Complete the steps below to assign roles to a new user.

1. Log in to the Cryptographic Security Platform Vault Management webGUI.
2. In the top right, click Switch to **Appliance Management**.
3. From the top menu, select **Users**.
4. From the **Actions** dropdown list, select **Add User**. The **Add a New User** dialog box appears.
5. Select the **User** tab and complete the following fields:
    a. **Full Name**: Enter the full name of the user.
    b. **Email**: Enter the email address of the user.
6. Click **Next.** The system takes you to the **Roles** tab.

> An alternative is to select the Roles tab.

7. Select the role to assign to the user based on your requirements.

> You can select one or more roles for each user that you created.

8. Click **Add**. A **User Successfully Added** dialog box appears.
9. Click **Close**.

Assigning Roles to an AD Group

1. Log in to the Cryptographic Security Platform Vault Management webGUI.
2. In the top right, click Switch to **Appliance Management**.
3. From the top menu, select **Users**.
4. Select the **AD Groups** tab.
5. From the **Actions** dropdown list, select **Add AD Group**. The **Add AD Group** dialog box appears.
6. Select the **Group** tab.
7. In the **AD Group** field, enter an AD group name based on your requirements.
8. Click **Next.** The system takes you to the **Roles** tab.

> An alternative is to select the Roles tab.

9. Select the role to assign to the group based on your requirements.

> You can select one or more roles for each group.

10. Click **Add**. An **AD Group Added Successfully** message appears.

Modifying Assigned Roles

1. Log in to the Cryptographic Security Platform Vault Management webGUI.
2. In the top right, click Switch to **Appliance Management**.
3. From the top menu, select **Users**. A list of users appears.
4. Select the user whose assigned roles you want to modify.
5. Select the **Roles** tab.
6. Select or deselect roles as required.

7. Click **Apply**.

> The operations available to a user are determined by the roles assigned to the user. The Roles tab displays the operations and level of access associated with the selected roles.

Role Assignment Restrictions

- A user must already have a role to assign that role to another user.
- The role assignments for the `secroot` user and the currently signed-in user cannot be modified.
- Adding or removing permissions related to admin key management generates a new admin key.

Vault management

The Vault Management dashboard in the CSP Vault Management web GUI shows all configured vaults.

- Creating a Vault
- Rescuing a Vault
- Editing a Vault
- Viewing Vault Details
- Renaming a Vault
- Deleting a Vault
- Connecting CSP Vault and CSP Compliance Manager

> The vault administrator configures and manages the vault. CSP Vault administrators create vaults and assign a vault administrator to each vault but do not have access to the vaults.

Creating a Vault

CSP Vault security administrators create vaults and assign an administrator to each vault.

> CSP Vault sends the vault administrator a URL and a temporary password, allowing them to access and configure the vault. The vault administrator is responsible for the vault and has full control. CSP Vault administrator does not have access to the vault by default.

To create a vault

1. Log in to the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Select **Create Vault**. The Create Vault page appears.
3. Enter the vault details:
    - Type
    - Name
    - Description
    - Email Notifications
    - Admin Name
    - Admin Email
4. Select **Create Vault**.

Type

Select the vault type.

Name

Enter the name for the vault.

Description

Enter an optional description for the vault.

Email Notifications

Select ON or OFF to enable email notifications. If SNTP is not configured, you cannot use email.

- If email is turned on, then an email is sent to the vault administrator. The email includes the vault URL and a temporary password. The vault administrator logs in with the temporary password and is prompted to change their password.
- If email is turned off, you will see the temporary passwords and need to give them to the Vault Admins.

Admin Name

Enter the name of the vault administrator.

Admin Email

Enter the email address of the vault administrator. We send an email to this address, inviting the vault administrator to configure and manage the vault.

Rescuing a Vault

If a vault administrator is locked out of a vault, the CSP Vault administrator can Rescue the vault.

Rescuing a vault resets the vault authentication to local authentication. Each vault administrator is sent an email with a new temporary password. They can then log on to the vault using the temporary password and reconfigure the vault.

Important: If two-factor authentication is enforced for the vault, then the user will need to add the one time password after the temporary password.

To rescue a vault

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Locate the required vault and select **Edit**.
3. In the Rescue Vault section, select **Rescue**.
   You are asked to confirm that you want to continue as rescuing the vault resets authentication to local authentication.
4. Select **Yes, Reset Authentication**.

The vault authentication is reset and a confirmation message appears.

An email is sent to vault administrators confirming that the vault has been rescued. The email includes a new temporary password to use to sign in to the vault.

Editing a Vault

You can change the vault name or description for a vault.

To edit a vault

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Locate the required vault and select **Edit**.
3. Edit the vault name and/or description.
4. Select **Apply**.

The vault details are updated and a confirmation message appears.

Viewing Vault Details

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Locate the required vault and click **View Details**.
   The Vault Details window displays the following information:
   - The name of the vault.
   - The type of vault.
   - The date that the vault was created.
   - The URL for the vault.
   - The URL for the Vault API.
   - The administrator name and user name.
3. Click **Close**.

Renaming a Vault

You can change the name of a CSP Vault after it has been created.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Locate the required vault and select **Edit**.
3. In the Name field, update the name.
4. Click **Apply**.
5. Log into the Cryptographic Security Platform Vault for whose name you just changed.

The updated name should display in the top right of the CSP Vault Management webGUI. If the old name still appears, log out of the CSP Vault and log back in again.

Deleting a Vault

If a vault is no longer required, you can delete the vault and remove it from the vault management dashboard.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Locate the required vault and select **Edit**.
3. Select **Delete Vault**.
   You are asked to confirm that you want to delete the vault.
4. Select **Yes, Delete**.

The vault is deleted and a confirmation message appears.

Connecting CSP Vault and CSP Compliance Manager

When you connect your CSP Vault to CSP Compliance Manager, the licensing for this vault will be tracked and maintained through Compliance Manager.

You will need to connect each vault that you have created to CSP Compliance Manager by importing a token file that was downloaded in Compliance Manager. The token file will be supplied by your CSP Compliance Manager administrator.

If you are also the administrator for CSP Compliance Manager, perform the tasks in Initializing a Data Source Connection in CSP Compliance Manager.

If you are not the admin for Cryptographic Security Platform Compliance Manager, request the Compliance Manager Token from the administrator and perform the tasks in Connecting a CSP Vault to CSP Compliance Manager.

- Initializing a Data Source Connection in CSP Compliance Manager
- Connecting a CSP Vault to CSP Compliance Manager
- Disconnecting a CSP Vault from CSP Compliance Manager

Initializing a Data Source Connection in CSP Compliance Manager

If you are the admin for CSP Compliance Manager, you will need to download the CSP Compliance Manager token file in CSP Compliance Manager and upload it into your CSP Vault.

1. Log into your Cryptographic Security Platform Compliance Manager webGUI.
2. In the side bar, click **Data Sources**.
3. Select **Actions > Initialize Connection**.
4. On the Initialize Connection to a Data Source page, enter the URL for the data source that you want to ad
5. Click **Create and Download File**.
   The Cryptographic Security Platform Compliance Manager downloads a file in .JSON format that will be used to connect to your data source.
   Important: This file should be considered a password. Please save it in a safe location in case you need to reconnect the same data source.

Connecting a CSP Vault to CSP Compliance Manager

After you have obtained the CSP Compliance Manager token file, you can upload it into your CSP Vault.

1. Log into your Cryptographic Security Platform Vault.
2. Click the **Settings** icon.
3. Click Cryptographic Security Platform Compliance Manager.
   Note: Alternatively, in the yellow 'This vault is not connected to Cryptographic Security Platform Compliance Manager' area on the Home page, click **Connect Now** to be taken directly to the Cryptographic Security Platform Compliance Manager page.
4. On the Connect Cryptographic Security Platform Compliance Manager page, click **Connect**.
5. Upload the token file that you downloaded from the Cryptographic Security Platform Compliance Manager or received from the Cryptographic Security Platform Compliance Manager administrator.

Disconnecting a CSP Vault from CSP Compliance Manager

1. Log into your Cryptographic Security Platform Vault.
2. Click the **Settings** icon.
3. Click Cryptographic Security Platform Compliance Manager.
4. On the Cryptographic Security Platform Compliance Manager page, click **Disconnect**.
5. In the confirmation screen, click **Disconnect**.

CSP Vault for CloudKeys

The Cryptographic Security Platform Vault for Cloud Keys lets you manage keys for use with providers such as AWS, Azure, and GCP in Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) environments. You can use Cryptographic Security Platform Vault as

- External Key Store (XKS) for AWS,
- External service for Double Key Encryption (DKE),
- External Key Manager (EKM) provider

See below for the required steps.

- Managing Cloud Service Provider accounts
- Managing key sets
- Managing CloudKeys
- Managing Vault BYOK
- Managing AWS XKS
- Using CSP Vault as a GCP EKM Provider
- Using double key encryption with Vault
- Managing Authentication for Vault for Cloud Keys

> ⚠ If you plan to manage Elliptic Curve Cryptography (ECC) keys in a Cryptographic Security Platform Vault for Cloud Keys that is protected by an nShield HSM, the ECC feature must be enabled on the HSM.

Managing Cloud Service Provider accounts

See below for managing Cloud Service Provider accounts.

- Adding a Cloud Service Provider account for AWS
- Adding a Cloud Service Provider account for Azure
- Adding a Cloud Service Provider account for GCP
- Adding a Cloud Service Provider account for OCI
- Adding a Cloud Service Provider account for SFDC
- Deleting a Cloud Service Provider account

> ⚠ Only one account per Cloud Service Provider can be associated with a Vault account.

Adding a Cloud Service Provider account for AWS

See below for adding a Cloud Service Provider account for AWS (Amazon Web Services).

> ⚠ If you set the rotation schedule during Cloud Service Provider account creation, the access key will rotate immediately after the account is created. The access key used to set up the Cloud Service Provider account will be deleted.

To add an account for AWS

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CSP Accounts** tab and select **Actions > Add Cloud Service Provider Account**.

4. On the Details tab of the Add CSP dialog box, enter the account details.
    - Name
    - Description
    - Admin Group
    - Type
    - AWS Access Key ID
    - AWS Secret Access Key
    - Default Region
5. Click **Continue**.
6. On the **Schedule** tab, determine the rotation schedule for the access keys.
    - Never
    - Every x days
    - Every x weeks
    - Every x months
    - Every x years
7. Click **Add**.

Name

The name you want to use for the Cloud Service Provider Account.

Description

An optional description of the Cloud Service Provider Account.

Admin Group

Select the Admin Group that you want to use for the account.

Type

Select AWS.

AWS Access Key ID

Enter the AWS Access Key ID.

AWS Secret Access Key

Enter the AWS Secret Access Key.

Default Region

Select the region where this Cloud Service Provider Account will be used.

Adding a Cloud Service Provider account for Azure

See below for adding a Cloud Service Provider account for Azure.

> ⚠ When the service account keys are rotated, the Cryptographic Security Platform Vault for Cloud Keys creates a new key and replaces the key that was used when you registered the Cloud Service Provider account. Please do not delete the service account key.

To add an account for Azure

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CSP Accounts** tab and select **Actions > Add Cloud Service Provider Account**.
4. On the Details tab of the Add CSP dialog box, enter the account details.
    - Name
    - Description
    - Admin Group
    - Type
    - Microsoft Entra Tenant ID
    - Subscription ID
    - Application (Client) ID
    - Application Object ID
    - Authentication Method
    - Common Name
    - Passphrase
    - Client Secret
5. Click **Continue**.
6. On the Schedule tab, determine the rotation schedule for the access keys.
    - Never
    - Every x days
    - Every x weeks
    - Every x months
    - Every x years
7. Click **Add**.

Name

The name you want to use for the Cloud Service Provider Account.

Description

An optional description of the Cloud Service Provider Account.

Admin Group

Select the admin group you want to use for the account.

Type

Select AZURE.

Microsoft Entra Tenant ID

Enter the Microsoft Entra tenant ID.

> You can find this value in Azure under Azure > Azure Active Directory.

Subscription ID

The Azure subscription ID.

> You can find this in Azure under Azure > Subscriptions.

Application (Client) ID

The Service Principal client ID. Click the link to update the Client ID and Client Secret.

> You can find this in Azure under Azure > Azure Active Directory > App Registrations

Application Object ID

The Object ID of your BYOK application. This is required if you don't have Microsoft Graph permissions.

> You can find this in Azure under Azure > Azure Active Directory > App Registrations

Authentication Method

The authentication method. Select:

- **Client Secret** to use the Azure Service Principal secret that you created for authentication.
- **Internally generated CSR / Certificate** to use certificate-based authentication and optionally generate a self-signed certificate. You can accept the generated certificate expiration, or choose your own expiration date. You will need to upload the certificate to the Azure App Service.

  > If you do not allow the self-signed certificate to be generated, a certificate signing request will be generated, which you must sign and upload to both Azure and Vault.

- **Externally Signed Certificate** to upload a certificate file and private key in PEM format.

  > Upload the certificate file to the Azure App Service before you create the Cloud Service Provider Account.

Common Name

If you selected Internally generated CSR / Certificate, enter the common name to be used for the certificate.

> If you are using client secret-based or externally signed certificate-based authentication, then this field is hidden.

Passphrase

If you selected Externally Signed Certificate, you can enter a passphrase to encrypt the private key.

> If you are using client secret-based or internally generated certificate-based authentication, then this field is hidden.

Client Secret

The Azure Service Principal secret that you created.

> If you are using certificate-based authentication, then this field is hidden.

Adding a Cloud Service Provider account for GCP

See below for adding a Cloud Service Provider account for GCP (Google Cloud Platform).

> ⚠ When the service account keys are rotated, the Cryptographic Security Platform Vault for Cloud Keys creates a new key and replaces the key that was used when you registered the Cloud Service Provider account. Please do not delete the service account key.

To add an account for GCP

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CSP Accounts** tab and select **Actions > Add Cloud Service Provider Account**.
4. On the Details tab of the Add CSP dialog box, enter the account details.
    - Name
    - Description
    - Admin Group
    - Type
    - Service Account Key File
5. Click **Continue**.
6. On the **Schedule** tab, determine the rotation schedule for the access keys.
    - Never
    - Every x days
    - Every x weeks
    - Every x months
    - Every x years
7. Click **Add**.

Name

The name you want to use for the Cloud Service Provider Account.

Description

An optional description of the Cloud Service Provider Account.

Admin Group

Select the Admin Group that you want to use for the account.

Type

Select GCP.

Service Account Key File

Click Load File to upload the service account key in JSON format that you downloaded from GCP.

Adding a Cloud Service Provider account for OCI

See below for adding a Cloud Service Provider account for OCI (Oracle Cloud Infrastructure).

> ⚠ It may take up to 5 minutes for a new OCI API key to become active. If you attempt to create your Cloud Service Provider account before the API key is active, it will fail with the "Failed to validate Access Credentials OCI" error.

To add an account for OCI

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CSP Accounts** tab and select **Actions > Add Cloud Service Provider Account**.
4. On the Details tab of the Add CSP dialog box, enter the account details.
    - Name
    - Description
    - Admin Group
    - Type
    - OCI User ID
    - OCI Tenancy ID
    - OCI Region
    - OCI API Key Fingerprint
    - OCI API Key Content
    - OCI API Key Passphrase
    - OCI Storage Bucket
    - OCI Storage Namespace
5. Click **Continue**.
6. On the **Schedule** tab, determine the rotation schedule for the access keys.
    - Never
    - Every x days
    - Every x weeks
    - Every x months
    - Every x years
7. Click **Add**.

Name

The name you want to use for the Cloud Service Provider Account.

Description

An optional description of the Cloud Service Provider Account.

Admin Group

Select the Admin Group that you want to use for the account.

Type

Select OCI.

OCI User ID

Copy the user information (everything after `user=`) from the configuration file preview.

OCI Tenancy ID

Copy the tenancy information (everything after `tenancy=`) from the configuration file preview.

OCI Region

Copy the region information (everything after `region=`) from the configuration file preview.

OCI API Key Fingerprint

Copy the fingerprint information (everything after `fingerprint=`) from the configuration file preview.

OCI API Key Content

Click Load File to upload the key file that you generated.

OCI API Key Passphrase

If you generated an RSA Key Pair with a passphrase, enter the passphrase here.

OCI Storage Bucket

If you are using a virtual private vault, enter the bucket name. This is where backups of HSM-protected keys in a virtual private vault will be stored.

> If you have a virtual private vault, imported keys will not be stored in the Cryptographic Security Platform Vault for Cloud Keys.

OCI Storage Namespace

If you are using a virtual private vault, enter the storage bucket namespace.

Adding a Cloud Service Provider account for SFDC

See below for adding a Cloud Service Provider account for SFDC.

To add an account for SFDC

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CSP Accounts** tab and select **Actions > Add Cloud Service Provider Account**.
4. On the Details tab of the Add CSP dialog box, enter the account details.
   - Name
   - Description
   - Admin Group
   - Type
   - KeySet
   - Client ID
   - Salesforce Domain
   - Wrapping Certificate Name
   - Named Credential ID
5. Click **Continue**.
6. On the **Schedule** tab, determine the rotation schedule for the Salesforce connection credentials.

   > Because the Cryptographic Security Platform Vault for Cloud Keys cannot rotate SDFC credentials, this allows you to create reminders for when you should plan to rotate

7. Click **Add**.

Name

The name you want to use for the Cloud Service Provider Account.

Description

An optional description of the Cloud Service Provider Account.

Admin Group

Select the Admin Group that you want to use for the account.

Type

Select SFDC.

KeySet

If you have a keyset, enter the name of the keyset associated with this CSP account.

Client ID

The Consumer Key from SFDC.

Salesforce Domain

Enter the domain for your Salesforce instance. You will need to copy everything after the `https://` and end with `salesforce.com`. For example, if the URL was:

```
https://my-company.development.salesforce.com
```

You would enter:

```
my-company.development.salesforce.com
```

Wrapping Certificate Name

Enter the name of an existing wrapping certificate, or the name to be used for a wrapping certificate.

Named Credential ID

If you plan to use cache-only keys, enter the ID for the named credential used by Salesforce to make cache-only key callout requests.

Deleting a Cloud Service Provider account

See below to delete a Cloud Service Provider account.

⚠ You can only delete a Cloud Service Provider Account if it is not associated with a Key Set.

To delete a Cloud Service Provider account

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.

3. Click the **CSP Accounts** tab.
4. On the **CSP Accounts** tab, select the Cloud Service Provider Account that you want to delete.
5. On the confirmation screen, click **Delete**.

Managing key sets

See below to manage key sets.

- Creating a key set
- Importing CloudKeys
- Deleting a key set

Creating a key set

See below for creating a key set.

To create a key set

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **Key Sets** tab.
4. Select the type of key to be contained in the Key Set. This can be one of the following:
    - AWS Key
    - Azure Key
    - GCP Key
    - OCI Key
    - SFDC Key
5. On the **Details** tab of the **Create Key Set** dialog box, enter the following:
    - Name—Enter the name for the Key Set.
    - Description—Enter the optional description for the Key Set.
    - Admin Group—Select the Admin Group.
6. Choose whether or not you want to enable audit logging for HYOK, EKM, and XKS operations.

    ⚠ Enabling audit logging for these operations could affect performance. Please be aware before you enable this. You can enable or disable this feature at any time from the Key Set Details tab.

7. Click **Continue**.
8. On the **Cloud Service Provider Account** tag, choose an existing Cloud Service Provider Account or add a new account to use with this Key Set.
9. Check the **Yes, import all keys** checkbox to import all pre-existing Customer Managed Keys (CMKs) in the Cloud Service Provider Account.

    ⚠ If your imported keys are deleted in the CSP, they cannot be restored by Cryptographic Security Platform Vault.

10. Click **Continue**.
11. On the **HSM** tab, check the **Enable HSM** checkbox if you plan to use an HSM to create CloudKeys that can be uploaded to the cloud.

    ⚠ Once the key material is in the KMS, you no longer need the HSM. However, if you remove the CloudKey from the cloud, you will need to use the HSM to upload the key again.

12. If you selected **Enable HSM**, click **Verify HSM connection** to test the connectivity and suitability of the configured HSM. Cryptographic Security Platform Vault checks whether the HSM is accessible and supports creating and exporting relevant keys.

    > ⚠ Some HSM servers with older firmware versions do not support key creation and wrapping. If the connection test fails, check the HSM server's firmware version. If it is old, update it to the latest version.

13. Click **Continue**.
14. On the Schedule tab, determine the default rotation schedule for the CloudKeys created in this Key Set. This can be one of the following:
    - Never
    - Once a year
    - Every 6 months
    - Every 30 days
    - Other
15. Click **Apply**.

Importing CloudKeys

See below for importing CloudKeys.

> ⚠ Importing some types of CloudKeys will not cause Vault to back up the key material, as the operation is not permitted. We highly recommend rotating keys after importing them to ensure backups are available.

To import CloudKeys

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **Key Sets** tab.
4. Select **Actions > Import Cloud Keys**.
5. In the **Import CloudKeys** window, select the type of vault to import.
6. Click **Import**.

Deleting a key set

See below for deleting a key set.

> ⚠ You can delete a key set as long as you haven't added any Cloud Keys.

To delete a key set

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **Key Sets** tab.
4. On the **Key Sets** page, select the key set that you want to delete.
5. Select **Actions > Delete Key Set**.
6. On the confirmation screen, click **Delete**.

Managing CloudKeys

See below for managing CloudKeys.

- Creating a CloudKey
- Enabling a CloudKey
- Disabling a CloudKey
- Uploading a CloudKey
- Modifying a CloudKey
- Setting a syncing schedule
- Removing a CloudKey
- Deleting a CloudKey
- Canceling a CloudKey deletion
- Purging a CloudKey
- Forcing a CloudKey purge
- Replicating an AWS multi-region CloudKey
- Changing the primary region for an AWS multi-region CloudKey
- Creating a replica key for Azure
- Disabling an Azure multi-vault CloudKey

Creating a CloudKey

See below for creating a CloudKey.

- Creating a CloudKey for AWS
- Creating a CloudKey for Azure
- Creating a CloudKey for GCP
- Creating a CloudKey for OCI
- Creating a CloudKey for SFDC

Creating a CloudKey for AWS

See below for creating a CloudKey for AWS.

To create a CloudKey for AWS

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab and select the **Key Set** and **Region**.

   > If you do not complete the selections on the CloudKeys page, add them on the Details tab of the Create CloudKey dialog box.

4. Select **Actions > Create CloudKey**.
5. On the **Details** tab of the Create **CloudKey** dialog box, enter the following:
   - Purpose
   - Algorithm
6. Create as Multi-Region Key—Check the Multi-Region checkbox if you are using AWS Multi-Region keys. Otherwise, leave it unchecked.
   - Region—If you selected **Multi-Region**, this field changes to the Primary Region. If you did not finish selecting the key set prompts, select the region here.
   - Name—Enter the name for the CloudKey.
   - Description—Enter the optional description for the CloudKey
7. Click **Continue**.
8. On the Purpose tab, complete the following:
9. Click **Continue**.
10. On the **Access** tab, enter the following:
    - Administrators—Choose the users who have administrative rights to the CloudKey.

- Users—Choose the users who can use the CloudKey for encryption or decryption.

11. On the Schedule tab, set the CloudKey rotation schedule. This can be one of the following:
    - Inherit from Key Set—The CloudKey will use the default schedule from the Key Set. If the Key Set schedule changes after you create the CloudKey, the CloudKey schedule will not update.
    - Never—The CloudKey will never be rotated.
    - Once a year—The CloudKey will be rotated once a year.
    - Every 6 months—The CloudKey will rotate every 6 months.
    - Every 30 days—The CloudKey will rotate every 30 days.
    - Other—The CloudKey will be rotated at the interval you select.
12. Choose when this CloudKey version should expire. The per-version expiration can be one of the following:
    - Never—The CloudKey version will never expire.
    - Fixed Date—All CloudKey versions will expire on the date that you set.
    - Relative Expiry—Each CloudKey version will expire after the number of days that you set.
13. Choose when the CloudKey should expire. This can be Never, or you can choose a specific date.
14. If you selected an expiration date, choose the Expire Action to define what happens to the CloudKey when it expires. This can be one of the following:
    - Disable—The key will remain in the cloud, but is disabled and cannot be used by any applications.
    - Delete—The key is disabled in the cloud and cannot be used by any applications. You can set the date for permanent deletion.
    - Delete from Cloud—Removes the key material from the KMS, and applications can no longer use this key from the cloud. However, the Cryptographic Security Platform Vault retains a copy of the key, which you can upload back to the cloud.
15. Click **Apply**.

Purpose

This can be one of the following:

- Symmetric Encrypt and decrypt
- Generate and verify MAC
- Asymmetric Encrypt and decrypt
- Asymmetric Sign and verify
- Use on-demand key rotation for new versions (for AES keys only)

Algorithm

Choose the algorithm that matches the purpose you selected. T

- For Symmetric Encrypt and decrypt or On-demand key rotation:
    - AES-256
- For Generate and verify MAC:
    - HMAC - SHA224 Digest
    - HMAC - SHA256 Digest
    - HMAC - SHA384 Digest
    - HMAC - SHA512 Digest
- For asymmetric encryption and decryption:
    - 2048-bit RSA
    - 3072-bit RSA
    - 4096-bit RSA
- For asymmetric signing and verification:
    - Elliptic Curve P-256
    - Elliptic Curve P-384
    - Elliptic Curve P-521
    - Elliptic Curve secp256k1
    - 2048-bit RSA

- 3072-bit RSA
- 4096-bit RSA

Creating a CloudKey for Azure

See below for creating a CloudKey for Azure.

To create a CloudKey for Azure

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab
4. Select the **Key Set** and the **Type**.
5. Select **Actions > Create CloudKey**.
6. On the Details tab of the **Create CloudKey** dialog box, enter the following:
   - Key Vault or Managed HSM—If you did not finish selecting the Key Set prompts, you will need to select the Key Vault or Managed HSM here.
   - Create as Multi-Vault Key—Select this option if you want this CloudKey to be available in multiple vaults. Otherwise, leave it unchecked.
   - Name—Enter the name for the CloudKey.
   - Description—Enter the optional description for the CloudKey
7. Click **Continue**.
8. On the **Access** tab, enter the following:
   - Hardware Protected—Select whether or not to create a hardware-protected key in Azure. For premium vaults only. This field is visible only for CloudKeys of type Key Vault and DKE.
   - Cipher—Select the RSA or EC key that you want to use. For DKE keys, only RSA is supported.
   - Permitted operations (for Key Vault only)—Check the checkboxes for the allowed key operations.
   - Azure Accounts (for DKE Keys only)—Select **Allow all** or **Specific tenants**.
9. Click **Continue**.
10. On the **Schedule** tab, determine the rotation schedule for the CloudKey. This can be one of the following:
    - Inherit from Key Set—The CloudKey will use the Key Set's default schedule. If the Key Set schedule changes after you create the CloudKey, the CloudKey schedule will not update.
    - Never—The CloudKey will never be rotated.
    - Once a year—The CloudKey will be rotated once a year.
    - Every 6 months—The CloudKey will rotate every 6 months.
    - Every 30 days—The CloudKey will rotate every 30 days.
    - Other—The CloudKey will be rotated at the interval you select.
11. Select the Activation Date for the CloudKey.
12. Choose when this CloudKey version should expire. The per-version expiration can be one of the following:
    - Never—The CloudKey version will never expire.
    - Fixed Date—All CloudKey versions will expire on the date that you set.
    - Relative Expiry—Each CloudKey version will expire after the number of days that you set.
13. Choose when the CloudKey should expire. This can be Never, or you can choose a specific future date for all versions of the key to expire.

    ⚠ For Azure CloudKeys, once you set an expiration date, you can not change the value back to Never.

14. If you selected an expiration date, choose the Expire Action to define what happens to the CloudKey when it expires. This can be one of the following:
    - Disable—The key will remain in the cloud, but is disabled and cannot be used by any applications.
    - Delete—The key is disabled in the cloud and cannot be used by any applications. You can set the date for permanent deletion.

- Delete from Cloud—Removes the key material from the KMS, and applications can no longer use this key from the cloud. However, Cryptographic Security Platform Vault retains a copy of the key which can be uploaded back to the cloud.

15. Click **Apply**.

Creating a CloudKey for GCP

See below for creating a CloudKey for GCP.

To create a CloudKey for GCP

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab.
4. Select the **Key Set** and **Key Ring**.

   If you do not finish the selections on the CloudKeys page, add them on the Details tab of the Create CloudKey dialog box.

5. Select **Actions > Create CloudKey**.
6. On the Details tab of the Create CloudKey dialog box, enter the following:
   - Key Ring—If you did not finish selecting the Key Set prompts, select the **Region** here.
   - Name—Enter the name for the CloudKey.
   - Description—Enter the optional description for the CloudKey.
   - Key Management—Choose **Customer Managed Key**.
7. Click **Continue**.
8. On the Purpose tab, complete the following:
   - Protection Level
   - Purpose
   - Algorithm
9. Click **Continue**.
10. On the Schedule tab, determine the rotation schedule for the CloudKey. This can be one of the following:
    - Inherit from Key Set—The CloudKey will use the key set default schedule. If the Key Set schedule changes after you create the CloudKey, the CloudKey schedule will not update.
    - Never—The CloudKey will never be rotated.
    - Once a year—The CloudKey will be rotated once a year.
    - Every 6 months—The CloudKey will rotate every 6 months.
    - Every 30 days—The CloudKey will rotate every 30 days.
    - Other—The CloudKey will be rotated at the interval you select.
11. Choose when this CloudKey version should expire. The per-version expiration can be one of the following:
    - Never—The CloudKey version will never expire.
    - Fixed Date—All CloudKey versions will expire on the date that you set.
    - Relative Expiry—Each CloudKey version will expire after the number of days that you set.
12. Choose when the CloudKey should expire. This can be Never, or you can choose a specific date.
13. If you selected an expiration date, choose the Expire Action to define what happens to the CloudKey when it expires. This can be one of the following:
    - Disable—The key will remain in the cloud, but is disabled and cannot be used by any applications.
    - Delete—The key is disabled in the cloud and cannot be used by any applications. You can set the date for permanent deletion.
    - Delete from Cloud—Removes the key material from the KMS, and applications can no longer use this key from the cloud. However, the Cryptographic Security Platform Vault retains a copy of the key, which you can upload back to the cloud.
14. Click **Apply**.

Protection Level

Choose whether to protect your key with software or an HSM.

Purpose

This can be one of the following:

- Symmetric encrypt/decrypt
- Asymmetric decrypt
- Asymmetric Sign
- MAC signing/verification

Algorithm

Choose the algorithm that matches the purpose you selected. This can be one of the following:

- For Symmetric encrypt/decrypt:
  - Google symmetric key
- For asymmetric decryption:
  - 2048-bit RSA - OAEP Padding - SHA1 Digest
  - 2048-bit RSA - OAEP Padding - SHA256 Digest
  - 3072-bit RSA - OAEP Padding - SHA1 Digest
  - 3072-bit RSA - OAEP Padding - SHA256 Digest
  - 4096-bit RSA - OAEP Padding - SHA1 Digest
  - 4096-bit RSA - OAEP Padding - SHA256 Digest
  - 4096-bit RSA - OAEP Padding - SHA512 Digest
- For Asymmetric Sign:
  - Elliptic Curve P-256 - SHA256 Digest
  - Elliptic Curve P-384 - SHA384 Digest
  - 2048 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest
  - 3072 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest
  - 4096 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest
  - 4096 bit RSA - PKCS#1 v1.5 padding - SHA512 Digest
  - 2048 bit RSA - PSS Padding - SHA256 Digest
  - 3072 bit RSA - PSS Padding - SHA256 Digest
  - 4096-bit RSA - PSS Padding - SHA256 Digest
  - 4096-bit RSA - PSS Padding - SHA512 Digest
- For MAC signing/verification:
  - HMAC - SHA256 Digest

Creating a CloudKey for OCI

See below for creating a CloudKey for OCI

To create a CloudKey for OCI

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab and select the **Key Set**, and **KeyVault**.

   If you do not complete the selections on the CloudKeys page, add them on the Details tab of the Create CloudKey dialog box.

4. Select **Actions > Create CloudKey**.
5. On the Details tab of the Create CloudKey dialog box, enter the following:

- Key Vault—If you did not finish selecting the Key Set prompts, you will need to select the OCI Key Vault here.
- Compartment— Enter the OCI compartment.
- Name—Enter the name for the CloudKey.
- Description—Enter the optional description for the CloudKey.

6. Click **Continue**.
7. On the Settings tab, enter the following:
   - Hardware Protected—Select whether the key will be stored in an HSM or in software in OCI.
   - Cipher—Select the AES or RSA key that you want to use.
8. Click **Continue**.
9. On the Schedule tab, determine the rotation schedule for the CloudKey. This can be one of the following:
   - Inherit from Key Set—The CloudKey will use the Key Set's default schedule. If the Key Set schedule changes after you create the CloudKey, the CloudKey schedule will not update.
   - Never—The CloudKey will never be rotated.
   - Once a year—The CloudKey will be rotated once a year.
   - Every 6 months—The CloudKey will be rotated once every 6 months.
   - Every 30 days—The CloudKey will rotate every 30 days.
   - Other—The CloudKey will be rotated at the interval you select.
10. Choose when this CloudKey version should expire. The per-version expiration can be one of the following:
    - Never—The CloudKey version will never expire.
    - Fixed Date—All CloudKey versions will expire on the date that you set.
    - Relative Expiry—Each CloudKey version will expire after the number of days that you set.
11. Choose when the CloudKey should expire. This can be Never, or you can choose a specific date.
12. If you selected an expiration date, choose the Expire Action to define what happens to the CloudKey when it expires. This can be one of the following:
    - Disable—The key will remain in the cloud, but is disabled and cannot be used by any applications.
    - Delete—The key is disabled in the cloud and cannot be used by any applications. You can set the date for permanent deletion.
    - Delete from Cloud—Removes the key material from the KMS, and applications can no longer use this key from the cloud. However, Cryptographic Security Platform Vault retains a copy of the key, which can be uploaded back to the cloud.
13. Click **Apply**.

Creating a CloudKey for SFDC

See below for creating a CloudKey for SFDC.

To create a CloudKey for SFDC

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab and select the **Key Set** where you want to create the CloudKey.
4. Select **Actions > Create CloudKey**.
5. On the Details tab of the Create CloudKey dialog box, enter the following:
6. SFDC Key Type—Select **Fields and Files** (Probabilistic), **Fields** (Deterministic), or **Event Bus**
7. Use Key Derivation—Check if you want Salesforce to derive the encryption key. Otherwise, Salesforce will use the key material that you upload for encryption.
8. Cache-Only Key—Check if you want Salesforce to derive the encryption key. Otherwise, Salesforce will use the key material that you upload for encryption.
9. Click **Continue**.
10. On the Schedule tab, determine the rotation schedule for the CloudKey. This can be one of the following:
    - Inherit from Key Set—The CloudKey will use the Key Set's default schedule. If the Key Set schedule changes after you create the CloudKey, the CloudKey schedule will not update.

- Never—The CloudKey will never be rotated.
- Once a year—The CloudKey will be rotated once a year.
- Every 6 months—The CloudKey will be rotated once every 6 months.
- Every 30 days—The CloudKey will rotate every 30 days.
- Other—The CloudKey will be rotated at the interval you select.

11. Choose when this CloudKey version should expire. The per-version expiration can be one of the following:
    - Never—The CloudKey version will never expire.
    - Fixed Date—All CloudKey versions will expire on the date that you set.
    - Relative Expiry—Each CloudKey version will expire after the number of days that you set.
12. Choose when the CloudKey should expire. This can be Never, or you can choose a specific date.
13. If you selected an expiration date, choose the Expire Action to define what happens to the CloudKey when it expires. This can be one of the following:
    - Disable—The key will remain in the cloud, but is disabled and cannot be used by any applications.
    - Delete—The key is disabled in the cloud and cannot be used by any applications. You can set the date for permanent deletion.
    - Delete from Cloud—Removes the key material from the KMS, and applications can no longer use this key from the cloud. However, Cryptographic Security Platform Vault retains a copy of the key, which can be uploaded back to the cloud.
14. Click **Apply**.

Enabling a CloudKey

See below for enabling a CloudKey.

To enable a CloudKey

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab.
4. Select the CloudKey that you want to enable.
5. Click **Actions > Enable CloudKey**.
6. On the confirmation screen, click **Enable**.

Disabling a CloudKey

See below for disabling a CloudKey.

⚠ Once disabled, a CloudKey remains in the cloud but cannot be used by any applications.

To disable a CloudKey

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab.
4. Select the CloudKey that you want to disable.
5. Click Actions > **Disable CloudKey**.
6. On the confirmation screen, click **Disable**.

Uploading a CloudKey

See below for uploading a CloudKey to the cloud.

To upload a CloudKey

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.

2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab.
4. Select the CloudKey that you want to upload to the cloud.
5. Click **Actions > Upload to Cloud**.
6. On the confirmation screen, click **Upload**.

Modifying a CloudKey

After you create a CloudKey, you can only modify the following settings:

- Description,
- Rotation schedule,
- The expiry date

> You cannot edit inherited permissions (for example, for Google Cloud Platform CloudKeys) at the CloudKey level. Only custom-added permissions are editable.

To modify a CloudKey

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab.
4. Select the CloudKey that you want to modify.
5. Scroll down to the **Details** section.
6. Change the parameters as required.

Setting a syncing schedule

See below for how to set up an automatic synchronization schedule that imports all CloudKeys into a key set.

To set a synchronization schedule

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **Key Sets** tab.
4. Select the key set you want to schedule for syncing.
5. Select **Actions > Set Schedule for Syncing CloudKeys**.
6. Specify the subcontainer to set the schedule on by selecting it from the drop-down list. This depends on the key set type.
    - AWS—Select a Region or All.
    - Azure—Select Managed HSM, Key Vault, or All.
    - GCP—Select a Key Ring or All.
    - OCI—Select a Key Vault or All.
    - SFDC—Not applicable.
7. Select **Define Schedule** and choose how often you want to sync the CloudKeys. Alternatively, select **Never** to disable automatic syncing.
8. Click **Apply**.

Removing a CloudKey

See below to remove a CloudKey.

Removing a CloudKey removes the key material from the KMS, and applications can no longer use this key from the cloud. However, the Cryptographic Security Platform Vault retains a copy of the key that you can upload back to the cloud.

To remove a CloudKey

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab.
4. Select the CloudKey that you want to remove from the cloud.
5. Click **Actions > Remove from Cloud**.
6. On the confirmation screen, enter the CloudKey name, then type **Remove**.

Deleting a CloudKey

After a key is disabled in the cloud and cannot be used by any applications, you can set the date for permanent key deletion.

To delete a CloudKey

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab.
4. Select the key set for the CloudKey that you want to delete. For Azure, you must also select the Type.
5. Select the CloudKey that you want to delete.
6. Click **Actions > Delete CloudKey**.
7. On the confirmation screen, enter the number of days when the CloudKey will be permanently deleted.
   - The maximum number of days is 30 for AWS, 90 for Azure, and 120 for GCP.
   - The minimum is 7 days or, on Azure, if Purge Protection is enabled.
8. Click **Delete**.

   You can cancel the deletion at any time before the CloudKey is permanently deleted.

Canceling a CloudKey deletion

See below for how to cancel a scheduled CloudKey deletion.

To cancel a CloudKey deletion

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab.
4. Select the CloudKey you want to stop deleting.
5. Click **Actions > Cancel Deletion**.
6. On the confirmation screen, click **Cancel Deletion**.

Purging a CloudKey

If you don't want to wait for the CloudKey to be permanently deleted, you can purge it.

CloudKeys created using External Key Manager (EKM) cannot be purged the same day they are deleted. You must wait at least 24 hours.

To purge a CloudKey

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab.
4. Select the key set for the CloudKey that you want to purge.

   For Azure, you must also select the type.

5. Select the deleted CloudKey that you want to purge.
6. Click **Actions > Purge CloudKey**.
7. On the confirmation screen, enter the CloudKey name and click **Purge**.

Forcing a CloudKey purge

If the Cloud status of a CloudKey is unavailable, you can force-purge the CloudKey.

To force a CloudKey purge

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab.
4. Select the key set for the CloudKey that you want to force purge.

   For Azure, you must also select the Type.

5. Check that the Cloud Status is effectively **Not Available**.
6. Click **Actions > Purge**.
7. On the Force Purge CloudKey screen, type the name of the CloudKey and click **Continue**.
8. On the confirmation screen, type "Delete this key" and click **Purge**.

Replicating an AWS multi-region CloudKey

After creating a Multi-Region CloudKey, you can replicate it into different regions.

To replicate a multi-region CloudKey

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab, then select the multi-region CloudKey you want to replicate.
4. Select **Actions > Create Replica Key**.
5. In the **Create Replica Key** dialog box, select the region where you want to replicate the CloudKey.
6. Click **Create Replica Key**.

   After the CloudKey is replicated, the multi-region section under the Details tab displays both the Primary and Replica locations.

Changing the primary region for an AWS multi-region CloudKey

After you replicate an AWS Multi-Region CloudKey to an additional region, you can change the Primary region.

To change the primary region for an AWS multi-region CloudKey

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.

2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab and select the multi-region CloudKey you want to change primary regions for.
4. On the **Details** tab, scroll down to the multi-region section.
5. Click **Change Primary Region**.
6. In the Change Primary Region dialog box, select the new Primary Region.
7. Click **Change Primary Region**.

> The Multi-Region section under the Details tab now displays the new Primary Region.

Creating a replica key for Azure

See below for creating a replica key for Azure.

> The replica CloudKey is created in the Key Vault that you select. You cannot use Key Vaults with purge protection enabled for replica keys.

To create a replica key for Azure

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab and select the Key Set and Type.
4. Select the multi-vault CloudKey that you want to replicate.
5. Select **Actions > Create Replica CloudKey**.
6. In the **Create Replica Key** dialog box, select the key vault where you want to replicate the CloudKey.
7. Click **Create Replica Key**.

Disabling an Azure multi-vault CloudKey

If you have created a multi-vault CloudKey in Azure, and it has not been duplicated into any other vaults yet, you can disable the multi-vault properties and turn it into a single-vault CloudKey. The CloudKey itself is not affected.

> If the CloudKey has replicas, you must delete the replicas before you can disable multi-vault.

To disable an Azure multi-vault CloudKey

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab and select the Key Set and Type.
4. Select the Multi-Vault CloudKey that you want to disable.
5. Select **Actions > Disable Multi-Vault**.
6. In the **Create Replica Key** dialog box, select the region where you want to replicate the CloudKey.
7. Click **Create Replica Key**.

Managing Vault BYOK

Many Cloud service providers allow users to bring their own cryptographic key material to the key management service. This is called Bring Your Own Key (BYOK). With the Cryptographic Security Platform Vault BYOK functionality, you can use CSP Vault to manage BYOK for your cloud providers.

When you use an HSM with BYOK, keys are never stored as plaintext.

- CSP Vault also encrypts (wraps) in-memory keys, except for software-protected keys in Azure.

- When a software-protected key has to be uploaded to Azure, CSP Vault unwraps it before upload.
- For other keys, including hardware-protected keys on Azure, when CSP Vault uploads them to the cloud, it encrypts (wraps) them in the HSM using the master key and the cloud provider's wrapping key before uploading the wrapped keys.

See below for managing BYOK.

- Configuring AWS for Vault BYOK
- Configuring Azure for Vault BYOK
- Configuring GCP for CSP Vault BYOK
- Configuring OCI for Vault BYOK
- Configuring SFDC for CSP Vault BYOK
- Viewing BYOK audit logs

Configuring AWS for Vault BYOK

Before you can use Bring Your Own Key (BYOK) with AWS, you will need to configure AWS to communicate with the Cryptographic Security Platform Vault. You can use symmetric or asymmetric keys for encryption and decryption. All key types are supported.

- AWS requirements for BYOK
- AWS BYOK process
- AWS BYOK access policy
- On-demand key rotation for AWS AES keys with BYOK

⚠ If you plan to use on-demand key rotation, only AES keys are supported.

AWS requirements for BYOK

See below for the AWS requirements for Vault BYOK.

- AWS account requirements
- AWS endpoint access requirements

AWS account requirements

To use AWS with BYOK, you must create a new, unique service account user in your AWS account.

- Do not use an existing user account or existing access key. Create the service account with the required permissions.
- Create an access key by logging in to AWS using the service account.
- Do not use the access key more than one time.
- Do not delete any access keys from the service account.
- Do not attach the same AWS account to multiple Cryptographic Security Platform Vault clusters.
- Do not share the AWS BYOK service account.
- Use the following permissions to create the AWS service account:
    - KMS:FullAccess
    - IAM:GetUser
    - IAM:ListUsers
    - IAM:ListAccessKeys
    - IAM:CreateAccessKey
    - IAM:DeleteAccessKey
    - IAM:UpdateAccessKey
    - EC2:DescribeRegions
    - SSM:GetParameter

- tag:GetResources

Your JSON file should look like the following:

```
{
  "Version": "2022-10-17",
  "Statement": [
    {
      "Sid": "ServiceAccountPolicy",
      "Effect": "Allow",
      "Action": [
        "kms:*",
        "ec2:DescribeRegions",
        "ssm:GetParameter",
        "iam:ListUsers",
        "iam:GetUser",
        "iam:CreateAccessKey",
        "iam:UpdateAccessKey",
        "iam:ListAccessKeys",
        "iam:DeleteAccessKey"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS endpoint access requirements

If your organization restricts outbound access to the public internet, whitelist the following endpoints for AWS BYOK to work correctly.

```
https://iam.amazonaws.com
```

Whitelist the following endpoints individually for each region you want to use.

```
https://kms.<region>.amazonaws.com
```

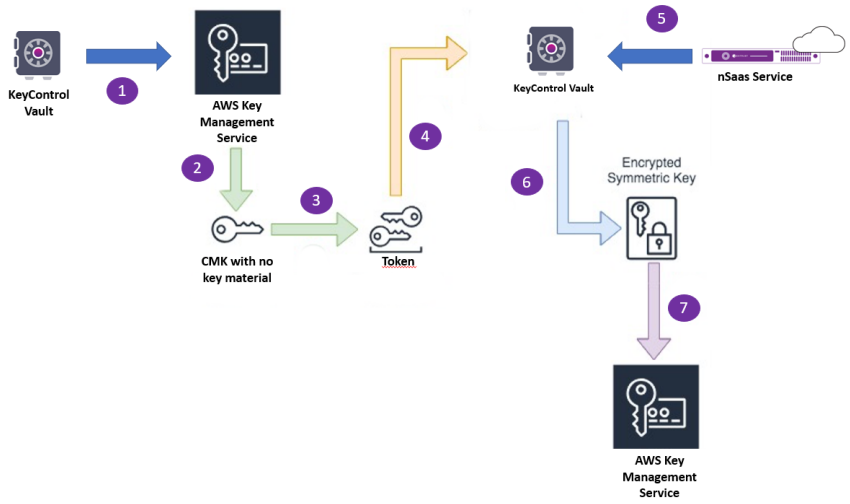
```
https://ssm.<region>.amazonaws.com
```

```
https://ec2.<region>.amazonaws.com
```

If a proxy is in use in the network, you can test these endpoints in the Vault application on the Settings > Proxy Settings Vault page.

AWS BYOK process

This section describes the workflow that occurs in the Cryptographic Security Platform Vault for Cloud Keys when you use BYOK for AWS.



To bring your own key

1. Vault creates a Cloud Key with key material. If HSM is configured, the key is generated and wrapped with a root key on the HSM.
2. AWS Key Management Service (KMS) creates a customer master key (CMK) with no key material associated.
3. Download the RSA-2048 wrapping public key and the import token from AWS KMS.
4. Import the RSA-2048 wrapping public key and the import token into Vault.
5. The imported wrapping key rewraps the symmetric key. If an HSM is configured, the HSM performs the wrapping.
6. Import the symmetric key into AWS KMS using the import token.

AWS BYOK access policy

Vault uses the AWS Key Policy to control IAM users' access to BYOK keys. The default key policy template used by the CSP Vault for Cloud Keys defines the following roles:

- An administrator with full administrative rights to the key
- A user that can use the key for encryption or decryption.

CSP Vault for Cloud Keys admins can assign IAM users as administrator and/or user to a specific CloudKey. The default key policy template Vault uses matches the default policy template used by the AWS KMS console.

> If you change a CloudKey's key policy in KMS, you will not be able to update or view its access information in CSP Vault for Cloud Keys.

On-demand key rotation for AWS AES keys with BYOK

Starting with release 10.5.3, you can use on-demand key rotation with BYOK, with native AWS support for key versions. The following caveats apply to on-demand key rotation:

- Only AES keys can be rotated using on-demand rotation. Non-symmetric encryption keys and HMAC keys are not supported.
- You can rotate a key using on-demand rotation only 10 times, for a total of 11 versions.
- You can delete key versions created using on-demand rotation only from the cloud or by uploading them to the cloud. You cannot disable them or schedule them for deletion.
- When the master key is scheduled for deletion, all versions of the key created using on-demand rotation are also scheduled for deletion.

⚠ If AWS created the initial key versions, CSP Vault cannot rotate this key using on-demand rotation after it is imported. This is because each on-demand rotation must have the same key material source. Therefore, you must create any subsequent key versions in AWS and then sync them to CSP using the import functionality. For example, if the key source is AWS KMS, you can import the key but cannot use on-demand rotation in the CSP Vault. You will need to rotate the key in AWS and then re-import the key.

To enable on-demand key rotation for AWS AES keys with BYOK

1. Create a CloudKey for AWS BYOK.
2. On the Purpose tab, select AES-256 for the algorithm.
3. Check the **Use on-demand key rotation for new versions** checkbox.
4. Continue creating the key as normal.
5. After the key is created, click the **Details** tab and scroll down to the Rotation Schedule section.
6. Check that the new **Use on-demand rotations** field reads **True**.
    - If this value is set to **False**, you can change it to **True** if the key only has a single version.
    - If it is set to **True**, you cannot modify its value.

Configuring Azure for Vault BYOK

Before you can use Bring Your Own Key (BYOK) with Microsoft Azure, you will need to configure Azure to communicate with the Cryptographic Security Platform Vault.

- Azure requirements for BYOK
- Azure BYOK process
- Creating a service principal
- Setting permissions for each Azure Key Vault
- Creating a client secret in Azure Active Directory

Azure requirements for BYOK

See below for the Azure requirements for Vault BYOK.

- Supported Azure environments
- Azure account requirements
- Azure endpoint access requirements

Supported Azure environments

Vault supports only the Azure public cloud. The following Azure environments are not supported:

- Azure China
- Azure Germany
- Azure Government

Azure account requirements

See below for the Azure account requirements for Vault BYOK.

- Use only one service principal per Azure account; however, you can use multiple subscriptions in the same Azure tenant with the same service principal.
- Do not share the Azure BYOK service principal credentials.
- Do not enable Purge Protection on Key Vaults.
- Do not connect more than one Cryptographic Security Platform Vault cluster to the same Azure account.

Azure endpoint access requirements

If your organization restricts outbound access to the public internet, whitelist the following endpoints for Azure BYOK to work correctly.

```
https://login.microsoftonline.com
```

```
https://management.azure.com
```

```
https://azure.net
```

Whitelist this endpoint individually for each key vault you want to use.

```
https://<keyvault>.vault.azure.net
```

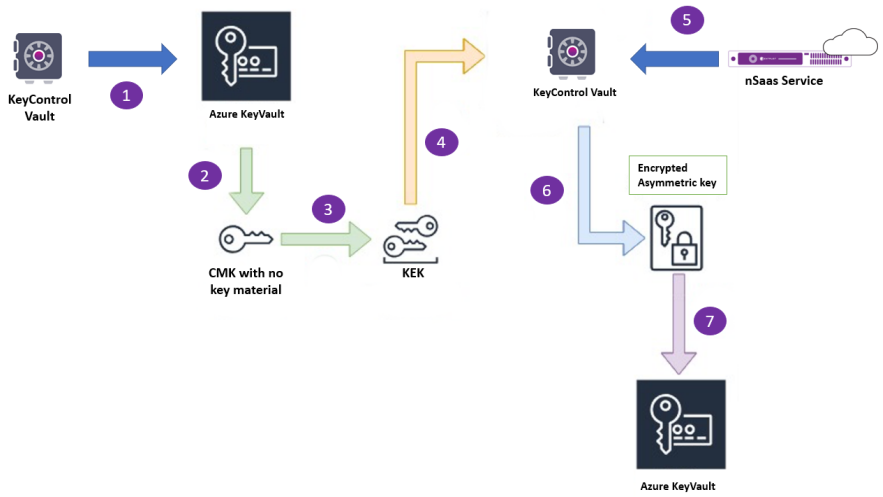
Whitelist this endpoint individually for each managed HSM you want to use.

```
https://<managedhsm>.managedhsm.azure.net
```

If a proxy is in use in the network, you can test these endpoints in the Vault application on the Settings > Proxy Settings Vault page.

Azure BYOK process

This section describes the workflow that occurs in the Cryptographic Security Platform Vault for Cloud Keys when you use BYOK for Azure.



Azure keys can be hardware-protected or software-protected.

- Hardware-protected key
- Software-protected Key

Hardware-protected key

See below for managing hardware-protected keys.

To manage hardware-protected keys

1. Create a Cloud Key with key material in the Cryptographic Security Platform Vault for Cloud Keys.

   If you configure an HSM, the HSM generates the key and wraps it with a root key.

2. A Key Encryption Key (KEK) is created in Azure Key Vault in your chosen key vault.
3. Download the RSA-2048 wrapping public key and the KEK ID from Azure Key Vault.
4. Import the RSA-2048 wrapping public key and the KEK ID into the Cryptographic Security Platform Vault for Cloud Keys.
5. Use the imported wrapping key to wrap the asymmetric key and create a blob.
6. Import the asymmetric key into Azure Key Vault using the KEK ID from Step 3.

Software-protected Key

See below for managing software-protected keys.

To manage software-protected keys

1. Create a Cloud Key with key material in the Cryptographic Security Platform Vault for Cloud Keys.

   If an HSM is configured, the HSM generates the key and wraps it with a root key, then stores it in the Cryptographic Security Platform Vault for Cloud Keys.

2. The asymmetric key is imported into Azure Key Vault.

> SSL/TLS protects communication between Cryptographic Security Platform Vault for Cloud Keys and Azure.

Creating a service principal

See below for creating a service principal.

- Creating and registering an Azure application
- Setting rotation permissions
- Selecting the Azure application
- Reviewing services

> If you wish to use DKE, you will need to create a separate registered application to provide access to the Azure Key Vaults. If you only wish to manage DKE keys, then the service principal does not need access to any Azure Key Vaults.

Creating and registering an Azure application

Create a service application in Azure and register it in Azure Active Directory using App Registrations.

Use New Registration to create the BYOK service application with the following parameters:

Parameter	Value
name	Select a name, for example, `mybyokapp`.
account type	Select Accounts in this organizational directory only (only - Single tenant). This option restricts access to users and services in the current Azure AD tenant.
application type	Web

Setting rotation permissions

Optionally, add the following permissions to allow auto rotation of client secrets.

> This configuration is recommended for enhanced security and requires admin consent.

If your Azure license allows role assignments:

1. Navigate to **Azure Active Directory > App Registrations > <mybyokapp> > Roles and Administrators**.
2. Click the **Cloud Application Administrator** role.
3. Click **Add Assignments**.
4. Start typing the name of the BYOK service application in the search box, and check the checkbox for the corresponding Enterprise application.
5. Click **Add**.

If your Azure license does not allow role assignments:

1. Navigate to **Azure Active Directory > App Registrations > <mybyokapp> > API Permissions**.
2. Click **Add a permission**

3. Add the following permission:

```
Application.ReadWrite.All Type:Application
```

4. Use **Grant Admin Consent for <directory name>** to grant permissions.

> ⚠ You will need global administrator rights to grant these permissions.

Selecting the Azure application

To select the Azure application:

1. Navigate to **Azure > Subscriptions > <your subscription> > Access Control (IAM)**.
2. In **Role Assignments**, select **Role > Reader > Members**.
3. Select your application. for example, **mybyokapp**.

Reviewing services

Navigate to Azure > <directory name> > Enterprise Applications > mybyokapp > Permissions and check that the service principal, which has the same name as the BYOK application, has all required permissions.

Setting permissions for each Azure Key Vault

You must set permissions for the BYOK service by configuring each Azure Key Vault that you want to manage.

- Setting permissions for the Azure RBAC permission model
- Setting permissions for Vault Access Policies

> ℹ Azure Key Vault now offers Azure role-based access control (Azure RBAC) in addition to the previous access policy model. If you are upgrading from a previous Cryptographic Security Platform Vault release, you will have used the access policy model.

Setting permissions for the Azure RBAC permission model

Repeat the following steps for each key vault that uses the Azure RBAC permission model.

To set permissions for the Azure RBAC permission model

1. Navigate to **Azure > Key vaults > <Key Vault name> > Access control (IAM)**.
2. Click **Add role assignment** to assign the Key Vault Crypto Officer role to the BYOK application.
3. In **Job function roles**, select **Key Vault Crypto Officer** and then click **Next**.
4. Click + **Select Members**.
5. Search for the BYOK application and click the **+** next to it, then click **Select**.
6. Click **Review + assign** to move to the final step of **Add role assignment**.
7. Review the settings and then click **Review + assign**.

Setting permissions for Vault Access Policies

Repeat the following steps for each Key Vault that uses Vault Access Policies.

To set permissions for Vault Access Policies

1. Navigate to **Azure > Key vaults > <Key Vault name> > Access control (IAM).**
2. Use **Add Access Policy** to add permissions to the BYOK application.

3. In the **Key Permissions** column, click **Select All** for both the Key Management Operations and Privileged Key Operations lists of permissions.
4. Select **Principal > BYOK application**.
5. Select **Add**.

Creating a client secret in Azure Active Directory

See below for creating a client secret in Azure Active Directory.

To create a client secret

1. Navigate to **Azure > Azure Active Directory > App Registrations > <the BYOK application> > Certificates & Secrets**.
2. Select **New client secret** to create the client secret.
3. Add the description and set the expiration period. The recommended period is 24 months.

   > You will have to update the secret in CSP Vault before the expiration date that you set here in order to have uninterrupted access to Azure Key Vaults from Cryptographic Security Platform Vault.

4. Copy the **Value** of the new client secret and paste it into a text file. Use this value to create a Cloud Service Provider Account in CSP Vault.

   > This value is displayed in the Azure Portal only temporarily. Once the portal hides it, you can't retrieve it, and you will need to create a new client secret.

Configuring GCP for CSP Vault BYOK

Before you can use Bring Your Own Key (BYOK) with GCP (Google Cloud Platform), you will need to configure GCP to communicate with the Cryptographic Security Platform Vault.

- GCP requirements for BYOK
- GCP BYOK access policy

> GCP supports symmetric and asymmetric keys.

GCP requirements for BYOK

See below for the requirements to use BYOK with GCP.

- GCP service account requirements
- GCP endpoint access requirements

GCP service account requirements

To use GCP with BYOK, create a new, unique service account user on the IAM & Admin > Service Account page.

- Do not use an existing user account or existing access key.
- Create an access key by logging in to GCP using the service account.
- Do not use the access key more than one time.
- Do not delete any access keys from the service account.
- Do not attach the same GCP account to multiple Cryptographic Security Platform Vault clusters.
- Do not share the GCP BYOK service account.
- Assign the following roles to the GCP service account:

- Required project-level roles:
  - `roles/browser`
  - one of `roles/cloudkms.admin` or `roles/cloudkms.viewer`

    > If `roles/cloudkms.admin` is not granted at the project level, you must add the service account as a principal with `roles/cloudkms.admin` access to any keyrings that you want to manage with this connection.
- For access-key rotation, configure one of the following permissions:
  - `roles/iam.serviceAccountKeyAdmin` : Grant this role at the project level
  - `service account` : Add the service account as a principal with `serviceAccountKeyAdmin` to the service account IAM policy as a binding.

Download the JSON file from the Key tab of the IAM & Admin > Service Account page. This JSON file will be your access key. For example:


```
{
     "type": "service_account",
     "project_id": "my-project",
     "private_key_id": "1c2f3ca8f0aactj23cj653ca12c4abf09052j2ca",
     "private_key": "-----BEGIN PRIVATE KEY-----
      agbcjeiosaghklte23jbaNBgkqhkiG9w0BAQEFAASCBKkwggSAoIBAQDl1T/WCYd
      VbzFaiVqx8i/SHHKgVbEeyKfjkl123cji3lsjtjlk231VLcyXESGfaDWQprStxKu
      J2ItEO5sDrWVajVkMpiDHNKDrHBdlahxvvx2JJNhm5loteclqMub5i6KgXpP+J8T
      uGbZCDHqfCBIIPH123ro3MxOUWVzrpEysLSVPOXJIltRajbPF98B5bK5y3i4FB++
      0KgeRgwbVjfRpzxr/Xe6clm5YIwL7spDNlpaSO5yB/pJitrLxydTRB1qnHlSZ25u
      nBUThj6Z1xCPJ3gjk3sJK783placje45oH8rLEYokdpO0rtSUJzm8U2OS7BVd0Jd
      6vHaCHhdAgMBAAECggEAA3mOXvG61qhLqdeQ5tM7DFJ0PuiOX7n/meZ9O46Vz7iD
      4UhnAUQVeWZbOfH7PJG7JNEB5GFwX5EAHhhUAMZSnucXh/lwSMrjCuoPGBH5bfqS
      PWvkHqDG7Mrhw/49h6PaCaR/tEDFJJ+vbeAAfqCaVcCQr830HLQ/2WY4mE7Es7t1
      yRNVfl81f3niea2CGYtM217UOUMM3tEE58+OL47ZOm7O8g1TWVtrs3tvQNqL06Pb
      Nv+N2SZRDUz2sTXpZtvzrQ3uKGmiW2jdasG50nbSR6Z/koCePWsyuHc3wTF2adLz
      +zrzHH7KfaCWuHL6HxqyCIt8huGcxECHYXkL3CjlsQKBgQDvD6fR6RRf8rshXCdT
      UQFTSMc0n4eaLiQfVXy9B5X9PzNrEM7HqAkceYJPQhD7wdO9jNJX19O6xY5puHbz
      GfpZPYqgLg4mbRLh6DgHgg/kLrWFgkESmSuP1ABISRY+wDWCCBfoO2VIsrhn155k
      BmiMigSKg6AiWavMGgu6Gbv+kQKBgQDrwnVNte3srXfugN3RsGtcSmQokngsKxXT
      OHQ4hmrDnXMtfZjfFVhZTDsbuz4vt80/9EiI/Jph/L+n4OFMZsbJUsAB7ig1YDho
      I3VSGL8PIbJ75c5BW5Aq0fWGqvh4QHXJIyWPy0pciZu8Ze4jrLQ+Ep+Rf3nVlUbw
      cDlJtY9bDQKBgQDABSI2gHJmM1FOFXhc+ucGn6Gqyi0gkclgBcmhCFPYzAggCqsd
      QgK3hX4+7YE4x1KtoUxfVLP0BLVEg++/ivFE9yK/UN76zIfrPxyqIzVigoY5jAt6
      xd9wssfbSCF/G+Ke5KNXXUYYo71tY4sNKvyVTlMhc2KP1NkioxUiUYNokQKBgQDW
      PJUgEuysIE5Vu2DXBbvp1+gAPmlZqaVhlXF3VB58t/1MH0/lmJ36N52W66Xs8tdf
      AHtRkEoyNN1sjpvtM4/8rmew2VxMdK2NZHteKQKlm3d3wzKUjcIKR1UYFRFJJTpj
      lr6xVoiyYpHUt8OZQ31e0smSDAcIoWgfYbuNUaF9mQKBgQDof8RNDNYVAeMUnAr1
      EkJoUrnu6dmApJajrm+QInxcR6QAXqBIvXjTkx+k+K+BMfXYW3J978Ux+uJW/ZXL
      Dh098jk7v4newIVuRrAOJKyTLVWROAg/VJC0IPVagI0JBwzyNuPlrcL4HcgwPWtv
      DefSTvCnsHGy1dYBGf0AZ6tRhg==
      -----END PRIVATE KEY-----",
     "client_email": "gcp-byok@my-project.iam.gserviceaccount.com",
     "client_id": "687456956321489204860",
```

```
    "auth_uri": "https://accounts.google.com/o/oauth2/auth",
    "token_uri": "https://oauth2.googlecerts.com/token",
    "auth_provider_x509_cert_url": "https://www.googlecerts.com/oauth2/v1/certs",
    "client_x509_cert_url": "https://www.googlecerts.com/robot/v3/metadata/x509/
gcpbyok@my-project.iam.gserviceaccount.com",
    "universe_domain": "googlecerts.com"

}
```

GCP endpoint access requirements

If your organization restricts outbound access to the public internet, the following endpoints must be whitelisted for GCP BYOK to function correctly:

```
https://www.googleapis.com/auth/cloud-platform
```

```
https://oauth2.googleapis.com
```

```
https://cloudresourcemanager.googleapis.com
```

```
https://iam.googleapis.com
```

```
https://cloudkms.googleapis.com
```

```
https://accounts.google.com
```

If a proxy is in use in the network, you can test these endpoints in the Vault application on the Settings > Proxy Settings Vault page.

GCP BYOK access policy

Cryptographic Security Platform Vault uses the AWS Key Policy to control IAM users' access to BYOK keys. The default key policy template used by Cryptographic Security Platform Vault defines the following roles:

- An administrator with full administrative rights to the key
- A user that can use the key for encryption or decryption.

Cryptographic Security Platform Vault admins can assign IAM users as administrator and/or user to a specific CloudKey. The default key policy template used by Cryptographic Security Platform Vault is the same as the default policy template that is used by the AWS KMS console.

If you change a CloudKey's key policy in KMS, you will not be able to update or view its access information in Vault.

Configuring OCI for Vault BYOK

Before you can use Bring Your Own Key (BYOK) with Oracle Cloud Infrastructure (OCI), you will need to configure Oracle to communicate with the Cryptographic Security Platform Vault.

- OCI requirements for BYOK
- Adding an API Key for the OCI user

OCI requirements for BYOK

See below for the requirements to use BYOK with OCI.

- User requirements
- User Group requirements
- Compartment requirements
- Policy requirements
- Vault requirements
- OCI endpoint access requirements

User requirements

The user you use to connect to CSP Vault can be new or existing.

User Group requirements

The user group used for BYOK management users can be new or existing.

You must add the selected user to this group.

Compartment requirements

If you plan to use compartments, you must create the appropriate compartments before you connect to the CSP Vault. Create vaults and keys in this compartment or subcompartment.

Access permissions for compartments are controlled at the user group level.

If you are not using compartments, please ensure that your vault, keys, user group, and users are all in the root tenancy.

Policy requirements

The policy grants the user group the appropriate permissions to manage keys and vaults.

- Set the Policy use cases drop-down under Policy Builder to 'Key and Secret Management'.
- The 'Let security admins manage vaults, keys and secrets' policy must be selected.
- Under Identity Domain, select the user group you created for Groups, and the compartment you created for Location.

Vault requirements

The OCI keys reside inside vaults. Create the vault you want to use inside your compartment. The user group that you selected must have permissions to manage this vault.

> You can choose to use a virtual private vault. If you do, you must have a storage bucket configured and accessible in the same compartment as the vault.

OCI endpoint access requirements

If your organization restricts outbound access to the public internet, the following endpoints must be whitelisted for OCI BYOK to function correctly:

```
https://cloud.oracle.com
```

Whitelist the following endpoint individually for each region you want to use.

```
https://kms.<region>.oraclecloud.com
```

```
https://identity.region>.oci.oraclecloud.com
```

You must whitelist this endpoint individually for each vault you want to use. You can find the URL on the vault information tile in the OCI console.

```
https://<vaultid>-management.kms.us-phoenix-1.oraclecloud.com
```

> If a proxy is in use in the network, you can test these endpoints in the Vault application on the Settings > Proxy Settings Vault page.

Adding an API Key for the OCI user

The API key provides a configuration file snippet with the connection information you need to connect to CSP Vault.

> It may take up to 5 minutes for a new API key to become active on OCI. If you attempt to create your Cloud Service Provider account before the API key is active, it will fail with the "Failed to validate Access Credentials OCI returned" error.

To add an API Key for the OCI user

1. In OCI, navigate to the user that you created.
2. On the user page, under **Resources** in the left pane, click **API Keys**.
3. Under API Keys, click **Add API Key**.
4. Add the key using your preferred method.
    - Generate the key pair here and download the private key
    - Upload or paste your public key file
5. Click **Add**. The Configuration file preview window will display the information that you will need to connect to CSP Vault.

6. Click **Copy** to copy the file.

Configuring SFDC for CSP Vault BYOK

Before you can use Bring Your Own Key (BYOK) with Salesforce (SFDC), you will need to configure Salesforce to communicate with the Cryptographic Security Platform Vault.

- SFDC requirements for BYOK
- Creating a connected app in SFDC
- Using cache-only keys with SFDC

SFDC requirements for BYOK

See below for the requirements to use BYOK with SFDC.

- Salesforce app requirements
- Salesforce endpoints access requirements

Salesforce app requirements

To use SFDC with BYOK, you must create a new connected app in Salesforce.

- Only one Connected App and external credential should be used per Salesforce organization
- Do not share the Salesforce BYOK connected app credentials.
- Do not connect more than one Cryptographic Security Platform Vault cluster to the same Salesforce account.

Salesforce endpoints access requirements

If your organization restricts outbound access to the public internet, you must individually whitelist each Salesforce domain that you want to use.

> If a proxy is in use in the network, you can test these endpoints in the Vault application on the Settings > Proxy Settings Vault page.

Creating a connected app in SFDC

BYOK requires an app to connect to the Cloud Service Provider Account created in the CSP Vault.

To create a connected app

1. In Salesforce, start the App Manager.
2. Click **New Connected App**.
3. In the Create a Connected App window, select **Create a Connected App** and click **Continue**.
4. In the New Connected App window, complete the following:
    - Basic Information
    - API (Enable OAuth Settings)
5. At the bottom of the window, click **Save**.
6. On the New Connected App page, click **Continue**.

    > It may take up to 10 minutes to finish creating the connected app.

7. In the sidebar, click **Manage Connected Apps**.
8. On the **Connected Apps** page, locate the connected app that you created and click **Edit**.
9. On the **Connected App Details** page, click **Edit Policies**.

10. In the **Run As section under Client Credentials Flow**, select a user with the permissions to manage keys and secrets and click **Save**.
11. In the sidebar, click **App Manager**.
12. Locate the app that you just created and select **View**.
13. In the **API (Enable OAuth Settings)** section, click **Manage Consumer Details**.
14. Wait for Salesforce to email you a verification code.
15. Enter the verification code and click **Verify**.
16. Copy the Consumer Key and the Consumer Secret.

    Use these values to connect to the CSP Vault.

Basic Information

Configure the following settings.

Field	Description
Connected App Name	Enter the name to use for the connected app.
API Name	Enter the connected app API name.
Contact Email	Enter your email address.

API (Enable OAuth Settings)

Configure the following settings and click OK in the confirmation box.

Field	Value
Enable OAuth Settings	Check this box
Enable for Device Flow	Check this box
Callback URL	Accept the default URL
OAuth Scopes	Select Manage User Data via APIs (api)
Require Proof Key for Code Exchange (PKCE)	Check this box
Require Secret for Web Server Flow	Check this box
Require Secret for Refresh Token Flow	Check this box
Enable Client Credentials Flow	Check this box.

Using cache-only keys with SFDC

You can create Salesforce keys as cache-only keys.

- Creating external named credentials
- Enabling cache-only keys
- Creating cache-only keys

When you create a cache-only key in CSP Vault, it creates a new tenant secret in Salesforce, but specifies no key material. Instead, the Cryptographic Security Platform Vault for Cloud Keys provides Salesforce with:

- The CloudKey GUID to use in callouts
- The name of the wrapping certificate it will use
- The named credential to use to retrieve the key

Creating external named credentials

See below for creating an external named credential in SFDC.

> ⚠ CSP Vault must have a publicly routable address and a publicly signed certificate in order to communicate with Salesforce.

Creating an external named credential in SFDC

1. In Salesforce, navigate to **Named Credentials**.
2. In the **External Credentials** tab, click **New**.
3. In the **New External Credential** window, enter the Label and the Name, and select JWT for the Authentication Protocol.
4. Complete the following:
    - Issuer (iss)
    - Subject (sub)
    - Audience (aud)
    - JWT Expiration (in seconds)
    - Signing Certificate
    - Signing Algorithm
5. Click **Save**.
6. In the **Principals** section, click **New**.
7. In the **Create Principal** window, complete the following:
    - Parameter Name—Enter a name for the principal.
    - Identity Type—Select **Named Principal**.
8. Click **Save**.
9. Return to **Named Credentials**.
10. Click the **Named Credentials** tab, and click **New**.
11. In the **Named Credentials** window, enter the Label and the Name.
12. Enter the URL that you want to use for the callouts in the following format:

```
https://<vault>/v5/sfdc
```

13. Under **Authentication**, select the External Credential that you created.
14. Click **Save**.
15. Navigate to **Users > Permission Sets**.
16. Create a permission set that gives the user permission to access external credentials.
17. Return to the named credential that you created and copy the ID from the URL.

> The ID is located after `/NamedCredential/`

Issuer (iss)

Enter the Salesforce Organization ID.

> You can find this value on the Company Information page in Salesforce.

Subject (sub)

Enter the Client ID that you used when you created the Cloud Service Provider Account for SFDC.

> This value was referred to as "Customer Key" in Salesforce.

Audience (aud)

Enter the name of the Cloud Service Provider Account that you created.

JWT Expiration (in seconds)

Set to 600 seconds (10 minutes).

Signing Certificate

Enter the name of the wrapping certificate that you used when you created the Cloud Service Provider Account for SFDC.

Signing Algorithm

Select RS256.

Enabling cache-only keys

Update the Cloud Service Provider to accept cache-only keys:

To enable cache-only keys

1. In the Vault web GUI, find the SFDC Cloud Service Provider account that you created.
2. Update the Named Credential ID with the ID that you copied from Salesforce.
3. Click **Save**.

Creating cache-only keys

To create the cache-only keys you can:

- Create a new CloudKey as a cache-only key by checking the Cache-Only Key checkbox.
- Rotate a BYOK key and create a new cache-only version by checking the Use Cache Only Key on rotating the keys checkbox.

Viewing BYOK audit logs

See below to view BYOK audit logs.

> The audit logs are view-only.

To view BYOK audit logs

1. Log in to the Vault web GUI.
2. In the top menu bar, click **CloudKeys**.
3. Click the **Audit Log** tab.
4. On the **Audit Log** page, check the BYOK activity.
5. Click the arrow at the end of each row for more details on the specific activity.

Managing AWS XKS

CSP Vault supports AWS (Amazon Web Services) External Key Store (XKS), allowing administrators to protect data in AWS with 256-bit AES keys.

- AWS XKS Requirements
- AWS XKS Limitations
- Configuring certificates and DNS for AWS XKS
- Creating a Cloud Service Provider Account for AWS XKS
- Creating a key set for AWS XKS
- Creating a CloudKey for AWS XKS
- Creating an external key store in AWS
- Connecting AWS XKS to the CSP Vault XKS Proxy
- Rotating XKS access keys
- Troubleshooting AWS XKS deployment

For more information about AWS XKS, see https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html

AWS XKS Requirements

To configure CSP Vault as an AWS XKS, ensure you have the following:

- AWS account with KMS access allowed
- Public certificate
- Public DNS entry for the common name in the certificate
- Publicly accessible IP address

AWS XKS Limitations

The following limitations currently exist:

- AWS currently supports only 256-bit AES keys.
- Amazon recommends a round-trip time latency of under 35 milliseconds between the AWS region and the CSP Vault.
- The maximum request timeout in KMS is set to 250 milliseconds.
- External key stores are supported in MOST AWS Regions in which AWS KMS is supported. Prior to selecting the region, make sure XKS is supported in that region.
- Only the XKS Public endpoint connection option is supported.

Configuring certificates and DNS for AWS XKS

See below for configuring certificates and DNS for AWS XKS.

To configure certificates and DNS for AWS XKS

1. In AWS, select a region geographically closest to the CSP Vault node.
2. Install a public certificate on the Cryptographic Security Platform Vault node.

   ⚠ The certificate chain must include the intermediate and root CA.

3. On your external/public DNS Server, add a DNS record for the CSP Vault node common name as specified in the certificate.

   ℹ The FQDN in the DNS record must match the common name in the server certificate.

4. Verify the server certificate, CA chain, and DNS record entries.

Creating a Cloud Service Provider Account for AWS XKS

You will need to create a new Cloud Service Provider account in the Cryptographic Security Platform Vault for Cloud Keys with cloud admin privileges for your AWS XKS deployment:

ℹ In the current release, a Cloud Service Provider account is tied to a single keyset.

To create a Cloud Service Provider Account for AWS XKS

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, select **CloudKeys**.
3. Select the **CSP Accounts** tab.
4. Select **Actions > Add Cloud Service Provider Account**.
5. On the Details tab, enter the account details.
   - Name
   - Description
   - Admin Group
   - Type
   - AWS Access Key ID
   - AWS Secret Access Key
   - Default Region
6. Select **Continue**.
7. On the Schedule tab, determine the rotation schedule for the access keys. This can be one of the following:
   - Never—The access keys will never be rotated.
   - Once a year—The access keys will be rotated once a year.
   - Every 6 months—The access keys will be rotated once every 6 months.
   - Every 30 days—Access keys will be rotated every 30 days.
   - Other—Access keys will rotate at the interval you select.
8. Select **Apply**.

Name

The name you want to use for the Cloud Service Provider Account.

Description

An optional description of the Cloud Service Provider Account.

Admin Group

Select the Cloud Admin Group.

Type

Select AWS.

AWS Access Key ID

Enter the AWS Access Key ID.

AWS Secret Access Key

Enter the AWS Secret Access Key.

Default Region

Select the target region (the AWS XKS region) as the default region.

Creating a key set for AWS XKS

See below for creating a key set for AWS XKS.

To create a key set for AWS XKS

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, select **CloudKeys**.
3. Select the **Key Sets** tab and select **Actions > Create Key Set**.
4. Select **AWS Key** as the key set type.
5. On the **Details** tab of the **Create Key Set** dialog box, enter the following:
    - Name—Enter the name for the key set.
    - Description—Enter the optional description for the key set.
    - Admin Group—Select **Cloud Admin Group**.
6. Click **Continue**.
7. On the **Cloud Service Provider Account** tab, enter the following:
    - Cloud Service Provider Account—Select the newly created Cloud Service Provider account to use with this key set.
    - Enable External Key Store—Select **Enable External Key Store**
8. Copy the AWS XKS Access Key ID and Secret Access Key to a notepad.
9. Select **Continue**.
10. On the **HSM** tab, you can optionally enable an HSM.
11. Select **Continue**.
12. On the **Schedule** tab, determine the default rotation schedule for the CloudKeys created in this Key Set. This can be one of the following:
    - Never—The CloudKey will never be rotated.
    - Once a year—The CloudKey will be rotated once a year.
    - Every 6 months—The CloudKey will be rotated once every 6 months.
    - Every 30 days—The CloudKey will rotate every 30 days.
    - Other—The CloudKey will be rotated at the interval you select.
13. Click **Apply**.

Creating a CloudKey for AWS XKS

Create a CloudKey in the AWS XKS Key Set you created earlier.

> AWS services use this CloudKey to encrypt objects in AWS.

To create a CloudKey for AWS XKS

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, select **CloudKeys**.
3. Select the **CloudKeys** tab.
4. From the **Key Set** menu, select the AWS XKS Key Set that you created earlier.
5. Select **Actions > Create CloudKey**.
6. On the Details tab, enter the following:
    - Region—Select the AWS XKS region.
    - Name—Enter the name for the CloudKey.
    - Description—Enter the optional description for the CloudKey.
7. Click **Continue**.
8. On the Access tab, enter the following.
    - Administrators—Choose the users who have administrative rights to the CloudKey.
    - Users—Choose the users who can use the CloudKey for encryption or decryption.
9. Click **Continue**.
10. On the Schedule tab, determine the rotation schedule for the CloudKey. This can be one of the following:
    - Inherit from Key Set—The CloudKey will use the Key Set's default schedule. If the Key Set schedule changes after you create the CloudKey, the CloudKey schedule will not update.
    - Never—The CloudKey will never be rotated.
    - Once a year—The CloudKey will be rotated once a year.
    - Every 6 months—The CloudKey will rotate every 6 months.
    - Every 30 days—AWS will rotate the CloudKey every 30 days.
    - Other—Rotate the CloudKey at the interval you select.
11. Click **Apply**.

Creating an external key store in AWS

See below to create an external key store in AWS.

To create an external key store in AWS

1. From the AWS portal, select **Key Management Service (KMS)**.
2. In the left pane, select **External key stores**.
3. Select **Create external key store**. The Create external key store screen appears.
4. In the Custom key store name section, enter the Cryptographic Security Platform Vault node FQDN.
5. In the Proxy connectivity section, select **Public endpoint** and enter the Proxy URI endpoint in the following format:

    ```
    https://<vault_fqdn>
    ```

6. In the Proxy configuration section:
    - Skip the Proxy URI path prefix
    - In **Enter proxy credentials,** type the access key ID copied from CSP Vault.
    - In **Enter Proxy credential**, enter the secret access key copied from Cryptographic Security Platform Vault.
7. Select **Create external key store**.

Connecting AWS XKS to the CSP Vault XKS Proxy

See below for connecting AWS XKS to the CSP Vault XKS Proxy.

To connect AWS XKS to the XKS Proxy

1. Log in to the AWS portal
2. On the **External key stores** screen, select **Custom key store**.

3. From the **Key store actions** menu, select **Connect**.
4. Wait until the external key store connection state is **Connected**.
5. Delete the copy of the access credential.

Rotating XKS access keys

We recommend that you rotate your access keys when:

- You have lost the access key ID or the secret access key.
- You have lost connection between the external keystore and the Cryptographic Security Platform Vault for Cloud Keys.
- You suspect a security compromise.
- You have a policy that requires you to rotate your keys periodically.

To rotate the XKS access keys

1. Log in to the CSP Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. In the **Key Sets** tab, select the Key Set that contains the key you want to rotate.
4. On the **Details** tab, locate the External Key Store row.
5. Click **Rotate Key**.

Troubleshooting AWS XKS deployment

If you have problems with your AWS XKS deployment, check the following settings.

Setting	Expected configuration
Server Certificate	The certificate is valid
Certificate Authority Chain	The certificate authority chain is complete, with a valid root CA certificate, intermediate certificate, and server certificate
DNS record	The DNS record is valid
Certificate common name	The certificate common name matches the FQDN specified in the DNS record
Port 443 (HTTPS)	Port 443 is open on your firewall to allow HTTPS traffic

Contact Entrust Support for help.

Using CSP Vault as a GCP EKM Provider

You can now use the Cryptographic Security Platform Vault for Cloud Keys as an External Key Manager (EKM) provider for GCP Cloud Key Management Service (KMS). GCP supports the following types of EKM:

- Manual key creation—The keys are created in the Cryptographic Security Platform Vault for Cloud Keys, and the key URI is copied to the GCP console to establish the link.
- Coordinated keys—The keys are created using the interface in the GCP console.

The key resides in the Cryptographic Security Platform Vault for Cloud Keys and is never moved to GCP, no matter which EKM type you choose.

- Prerequisites for using CSP Vault as a GCP EKM provider
- Manually creating EKM CloudKeys
- Creating coordinated EKM CloudKeys

Prerequisites for using CSP Vault as a GCP EKM provider

Before you can use CSP Vault as a GCP EKM provider, you must set up the following parameters on the Cloud Service Provider Account details page.

- EKM URI
- Key Access Justification Policy
- EKM Access Control List

EKM URI

The EKM URI is the URI GCP uses to access keys from the CSP Vault.

- If you deploy a single CSP Vault, set the EKM URI directly to that vault.
- If you deploy a cluster with multiple nodes, set the EKM URI to the load balancer.

For EKM via Internet, use the following format:

```
https://example.server.com
```

For EKM via VPC, use the following format:

```
https://<hostname>
```

Key Access Justification Policy

We highly recommend creating a Key Access Justification policy at the Cloud Service Provider and KeySet level that specifies access justification reasons. These apply to all the keys created in this KeySet, unless the policy is specified at the key level, which overrides this policy.

The supported justification reasons are:

- Customer initiated access
- Modified Customer initiated access
- Google initiated system operation
- Modified Google initiated system operation
- No justification reason expected
- Customer initiated support
- Google initiated service
- Third party data request
- Google initiated review
- Google response to production alert
- No justification reason specified
- Customer Authorized Workflow Servicing
- Allow missing access justification

For more information, see https://cloud.google.com/blog/products/identity-security/control-access-to-gcp-data-with-key-access-justifications

EKM Access Control List

This policy applies to all of the keys that are created in the associated KeySet for this Cloud Service Provider account, unless a policy at the key level overrides it. For coordinated keys, only the Cloud Service Provider-level permissions apply. The EKM access control list specifies the GCP identities and the permissions they have. You can specify identities by their service account email, for example:

```
apbyok2@kcv-project.iam.gserviceaccount.com
```

The supported permissions are:

- wrap
- unwrap
- asymmetricSign
- getPublicKey
- checkCryptoSpacePermissions
- createKey
- destroyKey

Manually creating EKM CloudKeys

See below for manually creating Cloud Keys.

To manually create Cloud Keys

1. Log into the CSP Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab and select the **Key Set** and **Key Ring**.
4. Select **Actions > Create CloudKey**.
5. On the **Details** tab of the **Create CloudKey** dialog box, enter the following:
    - Key Ring—If you did not finish selecting the key set prompts, select the **Region** here.
    - Name—Enter the name for the CloudKey.
    - Description—Enter the optional description for the CloudKey
    - Key Management—Choose **External Key Manager (EKM)**.
6. Click **Continue**.
7. On the Purpose tab, complete the following:
    - Connection Type
    - EKM Connection
    - Purpose
    - Algorithm
8. Click **Continue**.
9. On the Schedule tab, set the CloudKey rotation schedule. This can be one of the following:
    - Inherit from Key Set—The CloudKey will use the Key Set's default schedule. If the Key Set schedule changes after you create the CloudKey, the CloudKey schedule will not update.
    - Never—The CloudKey will never be rotated.
    - Once a year—The CloudKey will be rotated once a year.
    - Every 6 months—The CloudKey will rotate every 6 months.
    - Every 30 days—The CloudKey will rotate every 30 days.
    - Other—The CloudKey will be rotated at the interval you select.

10. Choose when this CloudKey version should expire. The per version expiration can be one of the following:
    - Never—The CloudKey version will never expire.
    - Fixed Date—All CloudKey versions will expire on the date that you set.
    - Relative Expiry—Each CloudKey version will expire after the number of days that you set.
11. Choose when the CloudKey should expire. This can be Never, or you can choose a specific date.
12. If you selected an expiration date, choose the Expire Action to define what happens to the CloudKey when it expires. This can be one of the following:
    - Disable—The key will remain in the cloud, but is disabled and cannot be used by any applications.
    - Delete—The key is disabled in the cloud and cannot be used by any applications. You can set the date for permanent deletion.
    - Delete from Cloud—Removes the key material from the KMS, and applications can no longer use this key from the cloud. However, the Cryptographic Security Platform Vault retains a copy of the key, which you can upload back to the cloud.
13. Click **Apply**.

Connection Type

Choose one of the following:

- External via VPC—Connect the Cryptographic Security Platform Vault for Cloud Keys via a Virtual Private Cloud (VPC) network.

  > You must create a VPC connection in GCP before you can use this option.

- External via Internet—Connect the Cryptographic Security Platform Vault for Cloud Keys via the internet.

EKM Connection

If you selected External via VPC, select the EKM connection that you created.

Purpose

This can be one of the following:

- Symmetric encrypt/decrypt
- Asymmetric Sign

Algorithm

Choose the algorithm that matches the purpose you selected. This can be one of the following:

- For Symmetric encrypt/decrypt:
  - Google symmetric key
- For Asymmetric Sign:
  - Elliptic Curve P-256 - SHA256 Digest
  - Elliptic Curve P-384 - SHA384 Digest
  - 2048 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest
  - 3072 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest
  - 4096 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest
  - 4096 bit RSA - PKCS#1 v1.5 padding - SHA512 Digest
  - 2048 bit RSA - PSS Padding - SHA256 Digest
  - 3072 bit RSA - PSS Padding - SHA256 Digest
  - 4096 bit RSA - PSS Padding - SHA256 Digest
  - 4096 bit RSA - PSS Padding - SHA512 Digest

Creating coordinated EKM CloudKeys

Upload coordinated external keys using VPC to store them in your crypto space. You can manage most coordinated external keys in Google Cloud using

- Google Cloud console
- gcloud CLI
- Cloud KMS API
- Cloud KMS client libraries
- Procedure

To create coordinated EKM CloudKeys

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Create a Cloud Service Provider account and a KeySet.
    - The KeySet UUID becomes the crypto space ID.
    - The Crypto Space Path is displayed on the Key Sets details tab:

    ```
    v5/cryptospaces/<keyset_uuid>
    ```
4. Create an EKM connection in the Google Cloud console
5. Set the EKM management node to Cloud KMS.
6. During setup, authorize your Google Cloud project service account to access your crypto space in CSP Vault for Cloud Keys using the EKM access control list in the Cloud Service Provider account.

    For more information on creating an EKM connection, see https://cloud.google.com/kms/docs/create-ekm-connection
7. Optionally, create a Key Access Justification policy in the Cloud Service Provider account.

Using double key encryption with Vault

Double Key Encryption (DKE) is a Microsoft security feature that encrypts Office documents with a symmetric key protected by a Microsoft-managed key and a second key managed by an external service such as CSP Vault.

- Labels configured in the Microsoft Purview Compliance Portal control Office document encryption.
- An Azure-registered application provides authentication.
- DKE keys are stored in an Azure key set in the Cloud Cryptographic Security Platform Vault for Cloud Keys. These keys are stored in the dke_keys key vault, separate from Azure key vaults and managed HSMs. The DKE keys are never uploaded to Azure.

See the required configuration steps below.

- CSP Vault prerequisites for DKE
- Creating a key set for DKE
- Creating a CloudKey for DKE
- Viewing CloudKey details
- Creating compliance labels
- Using compliance labels with MS Office
- Register with Azure Entra

To use DKE with CSP Vault, set TLS to TLSv1.2 and TLSv1.3, and set EMS to Do not enforce EMS.

CSP Vault prerequisites for DKE

Before you can configure DKE, you must have the following:

- To provide high availability, we recommend using a Cryptographic Security Platform Vault behind a load balancer. For load-balanced clusters, the compliance label should specify the load balancer FQDN. Also include the FQDN in the SAN records for the Cryptographic Security Platform Vault certificate and when registering the Azure application that authenticates the service.

  If you use a single Cryptographic Security Platform Vault instance, you can access it directly and use its FQDN.

- The Cryptographic Security Platform Vault certificate should be issued by a public CA so all client systems running Microsoft Office applications trust it.

Creating a key set for DKE

See below for creating a key set for DKE.

If you have an existing Azure Key Set that isn't in use, you can use that instead of creating a new one.

To create a key set for DKE

1. Log in to the CSP Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **Key Sets** tab.
4. Select **Actions > Create Key Set**.
5. Select **Azure Key** for the key set type.
6. On the Details tab of the **Create Key Set** dialog box, enter the following:
   - Name–Enter the name for the Key Set.
   - Description–Enter the optional description for the Key Set.
   - Admin Group–Select the Admin Group.
7. Click **Continue**.
8. On the **Cloud Service Provider Account** tab of the **Create Key Set** dialog box, enter your Azure Cloud Service Provider account.
9. Click **Continue**.
10. On the **HSM** tab of the **Create Key Set** dialog box, optionally enter the information for your HSM.
11. Click **Continue**.
12. On the Schedule tab, determine the default rotation schedule for the CloudKeys created in this Key Set. This can be one of the following:
    - Never—The CloudKey will never be rotated.
    - Once a year—The CloudKey will be rotated once a year.
    - Every 6 months—The CloudKey will be rotated once every 6 months.
    - Every 30 days—The CloudKey will rotate every 30 days.
    - Other—The CloudKey will be rotated at the interval you select.
13. Click **Apply**.

Creating a CloudKey for DKE

See below for creating a CloudKey for DKE.

To create a CloudKey for DKE

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKey** tab.
4. Select the Azure Key Set that you just created, and then select **DKE Keys**.
5. Select **Actions > Create CloudKey**.
6. On the **Details** tab of the **Create CloudKey** dialog box, enter the following:
    - Name–Enter the name for the CloudKey.
    - Description–Enter the optional description for the CloudKey.
7. Click **Continue**.
8. On the Access tab, enter the following:
    - Cipher
    - DKE Cache
    - Azure Accounts
9. Click **Continue**.
10. On the Schedule tab, determine the rotation schedule for the CloudKey. This can be one of the following:
    - Inherit from Key Set—The CloudKey will use the Key Set's default schedule. If the Key Set schedule changes after you create the CloudKey, the CloudKey schedule will not update.
    - Never—The CloudKey will never be rotated.
    - Once a year—The CloudKey will be rotated once a year.
    - Every 6 months—The CloudKey will rotate every 6 months.
    - Every 30 days—The CloudKey will rotate every 30 days.
    - Other—The CloudKey will be rotated at the interval you select.
11. Click **Apply**.

Cipher

This can be one of the following:

- RSA-2048
- RSA-3072
- RSA-4096

DKE Cache

Enter the number of days to cache your RSA public key.

Azure Accounts

Select one of the followig:

- Allow All
- Specific Tenants (enter the tenant GUIDs to give access to the Azure accounts)

Viewing CloudKey details

See below to view your CloudKey details.

To view CloudKey details

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab and select the CloudKey that you created.
4. Click on the following tabs to view the details of that CloudKey.
    - Details
    - DKE Permissions
    - Tags
    - Versions

Details

Check the following details:

- The name of the CloudKey.
- The Key ID of the CloudKey.
- The DKE URI of the CloudKey.
- The description of the CloudKey.
- The Key Type of the CloudKey.
- The Cipher Type of the CloudKey.
- The DKE Cache, or the number of days the RSA public key is cached.
- The status of the CloudKey. This can be one of the following:
    - Available—The CloudKey is available to use.
    - Disabled—The CloudKey is disabled, and applications cannot use it. If you enable the CloudKey, it will become available again.
    - Pending Delete—The CloudKey is scheduled for deletion.
- The Key Source of the CloudKey.
- The Key Set where the CloudKey belongs.
- The Key Vault from which the CloudKeys were imported.
- The Rotation Schedule for the CloudKey.

DKE Permissions

Check whether all tenants or specific tenants are assigned to the CloudKey. You can add or remove tenants from here.

Tags

Displays any tags (key-value pairs) that have been assigned to a CloudKey.

- Click **Add** to add new tags
- Click **Remove** to remove existing tags

Versions

Displays the different versions of each CloudKey, including the version currently in use.

- You can enable, disable, or delete versions
- Keys with a download arrow icon have been imported

Creating compliance labels

See below for instructions on creating a compliance label in the Microsoft Purview Portal.

⚠ You must have an account in order to access this page.

To create a compliance label

1. Navigate to https://purview.microsoft.com
2. In the menu on the left side of the page, select the **Information Protection** section.
3. Click **Sensitivity Labels**.
4. On the **Sensitivity Labels** page, click **Create a Label**.
5. On the Label details page, enter the following:
    - Name
    - Display name
    - Label priority
    - Description for users
    - Description for admins
    - Select a label color. This color will be displayed in Microsoft Office.
6. Click **Next**.
7. On the Scope page, define the label scope. Include all items except 'meetings'.
8. Click **Next**.
9. On the Items page, define your protection settings. Include 'Control access'.
10. Click **Next**.
11. On the Access control page, specify your encryption settings. You must check the 'Use Double Key Encryption' checkbox and enter the DKE URI value from the CloudKey details.

    ⚠ If you did not access that Cryptographic Security Platform Vault for Cloud Keys webGUI using the service FQDN, replace the IP or FQDN portion of the URI with the service FQDN.

12. Click **Assign Permissions** and choose the appropriate permissions. You must add permissions for at least one user or group.
13. Click **Save**.
14. Set any other values you need, then click **Next**.
15. Enter any other values that are required on the following pages and click **Create label**.
16. Select **Don't create a policy yet** and then click **Done**.
17. Repeat the steps above to create any other labels you need.
18. After creating all labels, navigate to **Information Protection > Label Policies**.
19. Edit the Global sensitivity label policy and add the new DKE key.
20. Review your settings and click **Submit**.

Using compliance labels with MS Office

Double Key Encryption (DKE) requires a Microsoft 365 enterprise account at level E5 and Windows desktop versions of Microsoft Office applications.

1. When you save a document in Microsoft Office, you see a menu of labels.
2. When you choose the DKE label, the Office application contacts the URL specified in the label to obtain the public key and a decryption URL.
3. When you open a document with a DKE label, the Microsoft Office application contacts the decryption URL with an identity token. A registered Azure application provides the token and is associated with the decryption URL FQDN.

Register with Azure Entra

In order to receive the identity token that is used to decrypt DKE, you must register with Azure Entra or the Azure Portal. You must have an account in order to access one of these pages.

To register with Azure Entra

1. Navigate to https://entra.microsoft.com/.
2. Navigate to the App registrations page by clicking on **App registrations** in the 'Entra ID' section on the left, or by searching for App registrations using the search bar at the top of the page.
3. On the App registrations page, click **New registration**.
4. On the Register an application page, enter the name to use for the application.
5. Select the supported account type. You must select one of the following:
    - Accounts in this organizational directory only (MSFT only - Single tenant)
    - Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
6. For the Redirect URI, select Web and enter the FQDN of the service.
7. Click **Register**.
8. On the App registration page for the application that you just registered, click **Expose an API**.
9. On the Expose an API page, enter the FQDN in the Application ID URI field, then click **Save**.
10. Click **Add a scope**.
11. In the Add a scope window, enter user_impersonation for the Scope name, Admin consent display name, and Admin consent description.
12. Click **Add scope** to return to the Expose an API page.
13. Click **Add a client application**.
14. In the Add a client application window, enter the Microsoft Office client ID.

```
d3590ed6-52b3-4102-aeff-aad2292ab01c
```

15. Check the checkbox for the scope you just added, then click **Add application**.
16. Click **Add a client application** again and enter the Azure Information Protection unified labeling client ID.

```
c00e9d32-3c8d-4a7d-832b-029040e7db99
```

17. Check the checkbox for the scope and click **Add application**.

Managing Authentication for Vault for Cloud Keys

By default each vault is configured for local authentication. You can change the authentication method as required. In the current release, you can choose between local authentication, Active Directory, OpenID Connect (OIDC) with AD, or OIDC without AD.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users.

For details on configuring each authentication option, see:

- Configuring local authentication for Vault for Cloud Keys
- Configuring Active Directory for the Vault for Cloud Keys
- Configuring OIDC with Active Directory for Vault for Cloud Keys
- Configuring OIDC for Vault for Cloud Keys
- Managing two-factor authentication in Vault for Cloud Keys

Configuring local authentication for Vault for Cloud Keys

Local authentication is enabled by default when you create a vault. If using local authentication, no further authentication configuration is required. The next step is to configure your access policies and users.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users

Configuring Active Directory for the Vault for Cloud Keys

See below for configuring Active Directory for the Vault for Cloud Keys.

> By default, the vault uses local authentication. You can change the authentication method as required.

To configure Active Directory

1. Log in to the CSP Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. On the Authentication page, select **LDAP** as the Authentication Type.
5. On the **Domain** tab, enter:
   - Domain Name—Enter the domain name for the service account.
   - Directory Service Type—Select **Microsoft AD** if you plan to use Microsoft AD directory services, or **OpenLDAP** for all non-Microsoft AD directory services.
   - Service Account Name—Enter the name of the service account for the given domain (for example, Administrator).

     > The service account needs read-only access to users and groups on the domain and any subdomain used.

   - Service Account Password —Enter the password for the service account.
   - UID Attribute—Enter the Security Manager Account Name (sAMAccountName) for the user.

     > This is the attribute of the user or group object that would be queried during search.

6. Click **Apply** to save the changes.
7. Click the **Domain Controllers** tab.
8. Click **+**
9. Add the following details in the **Add Domain Controller** window.
   - Server URL
   - STARTTLS
   - CA Certificate
   - User Search Context (Base DN)
   - Group Search Context (Base DN)
   - Timeout
10. Click **Save and Close**.

Server URL

Select LDAP or LDAPS and enter the domain name or IP address. To include a port number, use the following syntax:

```
<ip>:<port>
```

STARTTLS

If you selected LDAP, check the checkbox if you want to use LDAP over TLS.

CA Certificate

The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller.

- The CA certificate must be in Base64-encoded PEM format.
- If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates.

Click Load File to select the CA certificate that you want to use.

User Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the user search should start. For performance reasons, make the base DN as specific as possible. For example:

```
dc=ldapserver,dc=com
```

This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP.

Group Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the search for Security groups should start.

This option applies to AD Security groups being associated with an admin group.

Timeout

Set the timeout in seconds before connecting to an alternate domain controller.

- If multiple domain controllers are specified, this is how long the Cryptographic Security Platform Vault waits for a response before re-sending the request to another domain controller.
- If the DNS server is down, Cryptographic Security Platform Vault may take longer than the time specified here before it fails over to the next domain controller in the list or considers the authentication request failed.

This option only applies to the TCP/LDAP request. It does not apply to the DNS request before the LDAP server has been successfully contacted.

Configuring OIDC with Active Directory for Vault for Cloud Keys

By default, the vault uses local authentication. You can change the authentication method as required, and you can have multiple authentication modes active at the same time. However, OIDC without Active Directory cannot be used with Active Directory, and OIDC with Active Directory cannot be used without Active Directory.

> ⚠ You cannot disable OIDC authentication once it is configured. After you enable OIDC, you can no longer sign in with AD credentials. However, you can sign in using local authentication credentials without any issues.

To configure OIDC

1. Log in to the Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. In the **Choose Authentication Type** drop-down menu, select:
   - **OpenID Connect** to configure OIDC without Active Directory
   - **OpenID Connect (with AD)** to configure OIDC with Active Directory
5. Click the **Learn more about configuring the OIDC Provider** link to view the OIDC provider's login redirect URL and logout redirect URL.
6. Specify the OpenID Connect Configuration settings:
   - Name
   - Client ID
   - Client Secret
   - Base URL
7. Optionally, click **Load File** to upload the CA certificate in base64-encoded PEM format.
8. Click **Apply**.
9. Select **Verify and Enable**. After verification, a message appears confirming OpenID Connect has been successfully enabled. Vault is set for OIDC authentication.
10. Sign out from the vault and sign in to the vault as an OIDC user by selecting **Sign in with IDAAS** and entering your OIDC credentials.

Name

A user-defined name for the OpenID Connect provider.

> ℹ Cryptographic Security Platform Vault displays this name on the button in the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

> ⚠ This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Configuring OIDC for Vault for Cloud Keys

By default, the KeyControl Vault Management application is configured for local authentication. You can change the authentication method as required, but you can use only one type of authentication per vault at a time.

- If you want to use OIDC without AD, you can only change to that mode from the local authentication mode.
- If you have configured AD or OIDC with AD, you cannot change to OIDC without AD. You must first delete all AD users and groups, then remove the AD and/or OIDC configuration before configuring OIDC without AD.

Each vault can be configured with a separate OIDC server or a separate application from same server.

To configure OIDC

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Choose Authentication Type** drop-down list, select **OpenID Connect**.
6. Specify the OpenID Connect Configuration settings:
    - Name
    - Client ID
    - Client Secret
    - Base URL
7. Optional. Click **Browse** to upload the CA Certificate.

    The certificate needs to be in base64 encoded pem format.

8. Enter the Admin Name and Admin Email for OIDC user. This user will be created and will act as the Vault Administrator. They will be assigned to the admin policy and receive the email with the registration URL.
9. Click **Apply**. The OpenID Connect Configuration window appears showing the current configuration.
10. Click **Verify and Enable**. The OpenID Connect Successfully Configured window displays the new login URL.
11. Copy the URL, and click **Log Out and Sign in with IDP**.
12. After you are logged out, paste the URL into the browser window.
13. Log in to the Identity Provider using the name and password that you created.

Name

A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Managing two-factor authentication in Vault for Cloud Keys

Two-factor authentication requires you to enter two forms of identification before you can access your CSP Vault.

- The first form is your standard username and password combination,
- The second is a one-time password (OTP) generated by an authorization app. The OTP is appended to your existing password.

See below for how to enable and manage it.

- Requirements for enabling two-factor authentication in Vault for Cloud Keys
- Enforcing two-factor authentication in Vault for Cloud Keys
- Disabling two-factor authentication in Vault for Cloud Keys

> Two-factor authentication is supported with local authentication only. If you want to use two-factor authentication for non-local users, we recommend enabling it in your remote authentication provider.

Requirements for enabling two-factor authentication in Vault for Cloud Keys

Make sure you have access to an authentication app that can generate HOTP or TOTP passwords. For example:

- For TOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. These applications continuously generate passwords valid for 30 seconds. If the current password expires before you can submit the login request, you must wait for it to generate a new password, then use that to log in.
- For HOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. A password generated through the application is valid from the time you create it until you use it to log in. To log in again, click **Next** in the app to generate a new password.

Enforcing two-factor authentication in Vault for Cloud Keys

See below for enforcing two-factor authentication in Vault for Cloud Keys.

- Enforcing two-factor authentication for the current user
- Enforcing two-factor authentication for all users

Enforcing two-factor authentication for the current user

See below for enforcing two-factor authentication for the current user.

To enforce two-factor authentication for the current user

1. Log in to the Cryptographic Security Platform Vault for Cloud Keys webGUI.
2. In the top menu bar, click **Settings**.
3. In the **Two-Factor Authentication** field, click **Set up Two-Factor Authentication**.
4. In the **Enable Two-Factor** dialog box, select the HOTP or TOTP radio button.
5. Scan the generated barcode with your authorization app.
6. Enter the six-digit verification code from your app in the dialog box.

7. Click **Continue**. Cryptographic Security Platform Vault verifies the code and displays a message indicating success or failure. If the code is not correct, re-enter it.
8. After the code has been accepted, click **Done**.
9. When you log into the Vault web GUI:
    - Enter a valid OTP along with your standard account password on the login page. Do not add any characters or spaces between your account password and the one-time password generated by your authorization app. For example, if your password is `XyZ123$`, and your OTP is `32325`, you enter `XyZ123$32325` in the password field.
    - If you use TOTP, make sure your password doesn't expire before you submit the login request.

Enforcing two-factor authentication for all users

See below for enforcing two-factor authentication for all Vault users

To enforce two-factor authentication for all users

1. Log into the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the **Two-Factor Authentication Settings** page, select **ENFORCED**.
5. Click **Apply**.

Disabling two-factor authentication in Vault for Cloud Keys

See below for disabling two-factor authentication in Vault for Cloud Keys.

- Disabling two-factor authentication for a user
- Disabling two-factor authentication for all users

Disabling two-factor authentication for a user

See below to disable two-factor authentication for a single Vault user.

To disable two-factor authentication

1. Log in to the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Security**.
3. Select the **Users** tab
4. Select the user for whom you want to disable two-factor authentication.
5. In the **Details** tab below the table, click the **Enabled** link for the **Two-Factor Authentication** row.
6. In the **Disable Two-Factor Authentication** window, click **Proceed**.

Disabling two-factor authentication for all users

See below to disable two-factor authentication for all Vault users.

To disable two-factor authentication for all users

1. Log into the Cryptographic Security Platform Vault for Cloud Keys webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the Two-Factor Authentication Settings page, select **NOT ENFORCED**.
5. Click **Apply**.

CSP Vault for Cryptographic APIs

- CSP Vault for cryptographic APIs policies
- Post quantum support in Cryptographic APIs
- Cryptographic APIs sample use case
- Signing in to the Vault for the first time
- CSP Vault for Cryptographic APIs Crypto CLI
- Managing client certificates
- Configuring mTLS for the CSP Vault for Cryptographic APIs
- About Cache Management
- Configuring CSP Vault for Cryptographic APIs Policies
- Managing Keys
- Setting the password policy for users
- Managing access policies and users
- Managing Authentication for Vault for Cryptographic APIs

CSP Vault for cryptographic APIs policies

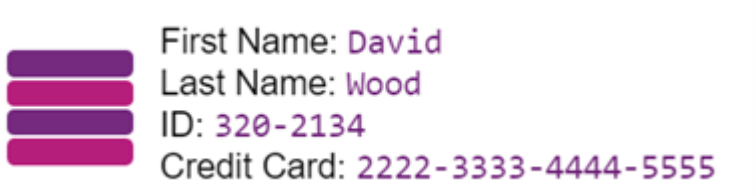
The Cryptographic Security Platform Vault for Cryptographic APIs lets you configure the following policy types.

- Tokenization
- Masking

> Beginning with release 10.2, the Encryption policy no longer exists. You can encrypt blocks of unstructured data using keys.

Tokenization

Format-preserving encryption. For example:



Tokenization (AES-FPE)	First Name: jEfWq Last Name: IfIs ID: 068-8534 Credit Card: 2222-5894-1547-5555

Tokenization can be reversed to retrieve the sensitive data from the token.

Each Cryptographic Security Platform Vault for Cryptographic APIs cluster (including all vaults in the cluster) has been tested to support 10,000 tokenization key objects, and can tokenize 1 million records at once.

Masking

Masks data. You can set the masking character, plus a prefix and suffix value if you want to preserve some of the data. For example:

```
Original credit card number: 2222-3333-4444-5555

Masked credit card number: 22##-####-####-##55
```

Masking is one-way encryption. You cannot retrieve the data from the token.

An example use case is exporting data and generating reports with the sensitive data masked.

If you plan to manage Entrust Elliptic Curve Cryptography (ECC) keys in a Cryptographic Security Platform Vault for Cryptographic APIs that is protected by an nShield XC HSM, you must have an ECC license for that HSM.

The Cryptographic Security Platform Vault for Cryptographic APIs webGUI has an automatic timeout value of 15 minutes.

Post quantum support in Cryptographic APIs

Starting with version 10.5.3, we now offer the following Post-Quantum (PQ) features in the Cryptographic Security Platform Vault for Cryptographic APIs, with and without HSM.

- PQ operations
- Import from HSM

Currently, the channel between the client and the Cryptographic Security Platform Vault for Cryptographic APIs is not using PQ-TLS. This means the channel is still vulnerable to a harvest-now, decrypt-later attack.

PQ object creation

You can create the following PQ-safe objects.

- ML-DSA
- SLH-DSA

PQ operations

The following operations are considered PQ-safe:

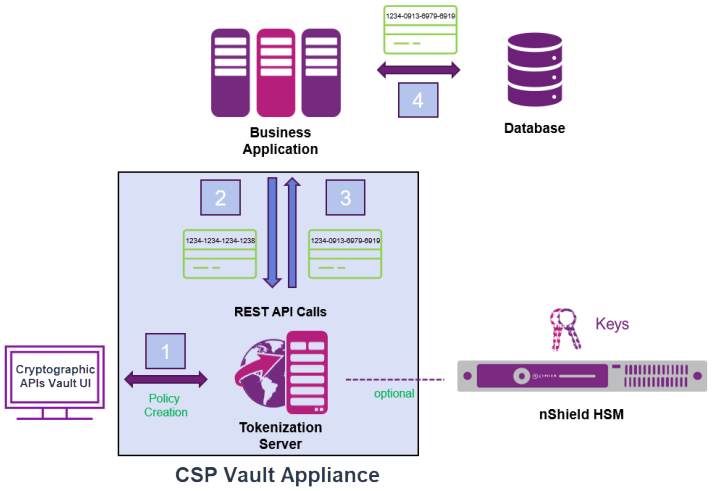
- Sign (ML-DSA, SLH-DSA)
- Verify (ML-DSA, SLH-DSA)

Import from HSM

Import from HSM (Hardware Security Module) to Cryptographic Security Platform Vault for Cryptographic APIs—You can import the public part of PQ keys from your HSM to the Cryptographic Security Platform Vault for Cryptographic APIs. This allows the Cryptographic Security Platform Vault for Cryptographic APIs to verify the PQ signature.

Cryptographic APIs sample use case

This overview explains how a business application, such as a banking application, interacts with the Cryptographic Security Platform Vault for Cryptographic APIs to tokenize data.



In summary:

- Add the relevant user (the business application's user account) to the list of vault users. You must also add this user to the relevant access policy.
- You set up the required tokenization policies.
- The keys for each policy are stored on Cryptographic Security Platform Vault or, optionally, an HSM.
- The business application interacts with the vault through REST API calls.
- The business application sends data to the vault for tokenization using the relevant policy.
- The vault tokenizes the data and returns the token to the business application.
- The business application stores and uses the token as needed.

The vault does not store the original data or the tokenized data. Applications interact with the vault using REST API calls. For example, an application sends token data to the vault to be tokenized using a specific policy:

```
{
   "policyName" :"CreditCard-1",
   "tokenData" : "1234-1234-1234-1238"
}
```

In this example,

- The tokenization policy is `CreditCard-1`.
- The data to be tokenized is `1234-1234-1234-1238`.

Signing in to the Vault for the first time

When the tokenization vault is created, the vault administrator receives the vault URL and a temporary password.

> ⚠ After signing in for the first time, the vault administrator needs to change the password.

To sign in to the Vault for the first time

1. Using the provided URL, navigate to the tokenization vault. The URL is in the format:

   ```
   https://<vault-ip-address>/tokenization/<vault-id>/<vault-name>
   ```

2. Sign in to the vault using the following information:
   - Name—Your email address. This is the email address the vault invite was sent to, or the one the vault creator provided.
   - Password—The temporary password provided in the vault invite email or sent to you by the vault creator.
3. Click **SIGN IN**.
4. On the Change Password window, enter and re-enter your new password and click **Change**.
5. On the sign-in page, enter your new credentials and click **SIGN IN**.
6. Click **Continue** to use an HSM to store the keys for the vault, or **Not Now** to configure it later.

CSP Vault for Cryptographic APIs Crypto CLI

- Wrap Command
- Version Command
- Verify Command
- Download-Audit Command
- Update-Tokenization-Settings Command
- Update-Tenant-Auth-Method-To-AD Command
- Update-Key-State Command
- Update-Audit-Settings Command
- Unwrap Command
- Tokenize Command
- Sign Command
- Set-Key-Property Command
- Schedule-Delete-Key Command
- Rotate-Key Command
- Renew Command
- Rekey Command
- Purge-Key Command
- Mask Command
- List-Tokenization-Policies Command
- List-of-Keys Command
- List-Mask-Policies Command
- List-Local-User Command
- List-Audit-Message-Templates Command

- List-Audit-Messages Command
- Import-Clear-Key Command
- Get-Tokenization-Settings Command
- Get-Tokenization-Policy Command
- Get-Tokenization-Info Command
- Get-Platform-Info Command
- Get-Local-User Command
- Get-Key-Versions Command
- Get-Key-Value Command
- Get-Keyset-Guid Command
- Get-Key-Details Command
- Get-HSM-Info Command
- Get-Audit-Settings Command
- Get-Audit-Message-Template Command
- Get-AD-User Command
- Get-AD-Group Command
- Export-Key Command
- Encrypt Command
- Enable-HSM-for-Keyset Command
- Detokenize-Mask Command
- Detokenize Command
- Delete-Tokenization-Policy Command
- Delete-Local-User Command
- Decrypt Command
- Create-Tokenization-Policy Command
- Create-Mask-Policy Command
- Create-Local-User Command
- Create-Key Command
- Change-AD-Domain Command
- Batch-Tokenize Command
- Batch-Rekey Command
- Batch-Mask Command
- Batch-Encrypt-Decrypt Command
- Batch-Encrypt Command
- Batch-Detokenize Command
- Batch-Decrypt Command
- Get-AD-Settings Command
- Update-AD-Settings Command
- List-AD-Settings Command
- Delete-Policy Command
- Update-Access-Policy Command
- Set-Policy-Version Command
- List-Policy-Versions Command
- Get-Policy Command
- Create-Access-Policy Command
- Login Command
- Accessing the Crypto CLI

Wrap Command

Use the Crypto CLI wrap command to wrap a symmetric key.

Important: Only symmetric keys can be wrapped.

Syntax

```
cryptocli wrap [options]
```

Option	Description
-h or --help	Displays usage text.
-d or --data string	The data to be wrapped. Strings must be enclosed in double quotes.
-m or --mode string	The mode to be used for wrapping. Strings must be enclosed in double quotes.
-k or --keyGuid string	The key GUID to be used for wrapping. Strings must be enclosed in double quotes.
-T or --keyType string	The key type. Strings must be enclosed in double quotes.

Version Command

Use the Crypto CLI version command to view the current version of the Crypto CLI.

Syntax

```
cryptocli version [options]
```

Option	Description
-h or --help	Displays usage text.

Verify Command

Use the Crypto CLI verify command to verify a signature.

Syntax

```
cryptocli verify [options]
```

Option	Description
-h or --help	Displays usage text.
-d or --data string	The data to be verified. Strings must be enclosed in double quotes.

Option	Description
-m or --mode string	The mode to be used for signing. Strings must be enclosed in double quotes.
-k or --keyGuid string	The key GUID to be used to verify the signature. Strings must be enclosed in double quotes.
-s or --signature string	The signature to verify. Strings must be enclosed in double quotes.

Download-Audit Command

Use the Crypto CLI download-audit command to download the vault audit logs as a bundle in tar.gz format.

Syntax

cryptocli download-audit [*options*]

Option	Description
-h or --help	

Update-Tokenization-Settings Command

Use the Crypto CLI update-tokenization-settings command to update the Cryptographic Security Platform Vault for Cryptographic APIs settings.

Syntax

cryptocli update-tokenization-settings [*options*]

Option	Description
-h or --help	Displays usage text.
-d or --degraded-mode-availability string	The degraded mode availability flag. Accepts enable or disable.
-o or --oidc-enabled string	The OIDC enabled flag. Accepts enable or disable.
-R or --revision int	The current revision number of tokenization settings.

Update-Tenant-Auth-Method-To-AD Command

Use the Crypto CLI update-tenant-auth-method-to-ad command to change the authentication mode of the vault from local to managed.

Syntax

```
cryptocli update-tenant-auth-method-to-ad [options]
```

Option	Description
-h or --help	Displays usage text.
-a or --ad-domain-name string	The Active Directory setting ID or name. Strings must be enclosed in double quotes.
-n or --ad-domain-type string	The Active Directory AD type. Strings must be enclosed in double quotes.

Option	Description

-j, -ad-servers string	The Active Directory Domain Controller List JSON File. This is an array of JSON objects, each object representing a Domain Controller. Strings must be enclosed in double quotes.
	The following keys are supported:
	• server_url - the (mandatory) full url of the Domain Controller
	• cacert (optional) - the path to the CA Certificate to verify with
	• user_base_dn (optional) - the user base DN
	• group_base_dn (optional) - the group base DN
	• timeout (optional) - the connection timeout in seconds. The default is 5 seconds.
	• tls (optional) - whether to enable StartTLS or not. The default is false.
	Example:
	[
	{
	"server_url": "ldaps://
	dc1.mycompany.eng.com",
	"cacert": "/root/cacert.pem",
	"user_base_dn":
	"DC=mycompany,DC=eng,DC=com",
	"group_base_dn":
	"DC=mycompany,DC=eng,DC=com",
	"timeout": 10,
	"tls": false,
	}
	]

-s, --ad-service-account-name string	The Active Directory service account user name. Strings must be enclosed in double quotes.
-p, --ad-service-account-pw string	The Active Directory service account user password. Strings must be enclosed in double quotes.
-u, --ad-uid string	The Active Directory UID Attribute. Strings must be enclosed in double quotes.
-k, --initial-ad-member-cn string	The initial Active Directory member CN. Strings must be enclosed in double quotes.

Option	Description
-d, --initial-ad-member-distinguished-name string	The initial Active Directory member distinguished name. Strings must be enclosed in double quotes.
-m, --initial-ad-member-mail string	The email address for the initial Active Directory member. Strings must be enclosed in double quotes.
-o, --initial-ad-member-upn string	The initial Active Directory member UPN. Strings must be enclosed in double quotes.
-t, --name string	The name of the tenant to be updated. Strings must be enclosed in double quotes.

Update-Key-State Command

Use the Crypto CLI update-key-state command to update the status of the key.

Syntax

```
cryptocli update-key-state [options]
```

Option	Description
-h or --help	Displays usage text.
-k or --key-guid string	The GUID of the key. Strings must be enclosed in double quotes.
-s or --state string	The new state for the key. This can be enable or disable.

Update-Audit-Settings Command

Use the Crypto CLI update-audit-settings command to update the audit settings.

Syntax

cryptocli update-audit-settings [*options*]

Option	Description
-h or --help	Displays usage text.

Option	Description
-m or --max-items int	The maximum number of items to be included in the response.
-r or --retention-days int32	The number of days to retain the audit logs. Retention days can be set between 30 - 365 days. Set 0 to retain all.

Unwrap Command

Use the Crypto CLI unwrap command to unwrap a symmetric key.

Syntax

```
cryptocli unwrap [options]
```

Option	Description
-h or --help	Displays usage text.
-d or --data string	The data to be unwrapped. Strings must be enclosed in double quotes.
-m or --mode string	The mode to be used for unwrapping. Strings must be enclosed in double quotes.
-k or --keyGuid string	The key GUID to be used for unwrapping. Strings must be enclosed in double quotes.
-T or --keyType string	The key type. Strings must be enclosed in double quotes.

Tokenize Command

Use the Crypto CLI tokenize command to tokenize data.

Syntax

```
cryptocli tokenize [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-n or --policyName string	The policy name to be used for tokenization. Strings must be enclosed in double quotes.
-d or --tokenData string	The data to be tokenized. Strings must be enclosed in double quotes.
-k or --keyGuid string	If you want to tokenize data using a specific version of the key, enter it here. If you do not enter a key, the latest key version will be used. Strings must be enclosed in double quotes.

Sign Command

Use the Crypto CLI sign command to sign data.

Syntax

```
cryptocli sign [options]
```

Option	Description
-h or --help	Displays usage text.
-d or --data string	The data to be signed. Strings must be enclosed in double quotes.
-m or --mode string	The mode to be used for signing. Strings must be enclosed in double quotes.
-k or --keyGuid string	The key GUID to be used for signing. Strings must be enclosed in double quotes.

Set-Key-Property Command

Use the Crypto CLI set-key-property command to set the properties of the key.

Syntax

```
cryptocli set-key-property [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-k or --key-guid string	The GUID of the key. Strings must be enclosed in double quotes.
-d or --description string	The new description of the key. Strings must be enclosed in double quotes.

Schedule-Delete-Key Command

Use the Crypto CLI schedule-delete-key command to update the status of the key.

Syntax

```
cryptocli schedule-delete-key [options]
```

Option	Description
-h or --help	Displays usage text.
-k or --key-guid string	The GUID of the key. Strings must be enclosed in double quotes.
-o or --operation string	The delete operation to use. This can be schedule-destroy or cancel-destroy.
-r or --retention-period int	The retention period for the key before it is destroyed. The minimum is 7 days, the maximum is 30 days, and the default is also 30 days.

Rotate-Key Command

Use the Crypto CLI rotate-key command to rotate a key.

Syntax

```
cryptocli rotate-key [options]
```

Option	Description
-h or --help	Displays usage text.
-k or --keyset-guid string	The GUID of the key to be rotated. Strings must be enclosed in double quotes.

Renew Command

Use the Crypto CLI renew command to renew the access token for the Cryptographic Security Platform Vault for Cryptographic APIs.

Syntax

```
cryptocli renew [options]
```

Option	Description
-h or --help	Displays usage text.

Rekey Command

Use the Crypto CLI rekey command to rekey data.

Syntax

```
cryptocli rekey [options]
```

Option	Description
-h or --help	Displays usage text.
-n or --policyName string	The policy name to be used for rekeying your data. Strings must be enclosed in double quotes.
-d or --tokenData string	The data to be rekeyed. Strings must be enclosed in double quotes.

Purge-Key Command

Use the Crypto CLI purge-key command to purge a key.

Syntax

```
cryptocli purge-key [options]
```

Option	Description
-h or --help	Displays usage text.
-k or --key-guid string	The GUID of the key. Strings must be enclosed in double quotes.

Mask Command

Use the Crypto CLI mask command to mask data.

Syntax

```
cryptocli mask [options]
```

Option	Description
-h or --help	Displays usage text.
-n or --policyName string	The policy name to be used for masking. Strings must be enclosed in double quotes.
-d or --tokenData string	The data to be masked. Strings must be enclosed in double quotes.

List-Tokenization-Policies Command

Use the Crypto CLI list-tokenization-policies command to list tokenization policies.

Syntax

```
cryptocli list-tokenization-policies [options]
```

Option	Description
-h or --help	Displays usage text.
-c or --counts string	Use True if you want the count information, otherwise use False.
-l or --limit string	The limit filter. Strings must be enclosed in double quotes.
-o or --offset string	The offset filter. Strings must be enclosed in double quotes.
-s or --sort string	How to sort the policies. Strings must be enclosed in double quotes.
-n or --nameFilter string	The name filter. Strings must be enclosed in double quotes.

List-of-Keys Command

Use the Crypto CLI list-of-keys command to list all keys present in a keyset.

Syntax

```
cryptocli list-of-keys [options]
```

Option	Description
-h or --help	Displays usage text.
-k or --keyset-guid string	Optional. The GUID of the keyset. Strings must be enclosed in double quotes.
-s or --status string	The status of the keys to list. This can be available, disable, or pending delete. Strings must be enclosed in double quotes.
-c or --cryptographic-algorithm string	The cryptographic algorithm of the keys to list. Strings must be enclosed in double quotes.

List-Mask-Policies Command

Use the Crypto CLI list-mask-policies command to list mask policies.

Syntax

```
cryptocli list-mask-policies [options]
```

Option	Description
-h or --help	Displays usage text.
-c or --counts string	Use True if you want the count information, otherwise use False.
-l or --limit string	The limit filter. Strings must be enclosed in double quotes.
-o or --offset string	The offset filter. Strings must be enclosed in double quotes.
-s or --sort string	How to sort the policies. Strings must be enclosed in double quotes.

Option	Description
-n or --nameFilter string	The name filter. Strings must be enclosed in double quotes.

List-Local-User Command

Use the Crypto CLI list-local-users command to display all local users.

Syntax

```
cryptocli list-local-users [options]
```

Option	Description
-h or --help	Displays usage text.
-f or --field stringArray	The fields to be included in the response.
-l or –filters string	The conditional expression to filter local users.
-m or --max-items int	The maximum number of items to be included in the response.
-n or --next-token string	The token from which the subsequent local users would be listed. Strings must be encased in double quotes.
-p or --prefix string	Only the local users prefixed with this string will be listed.

List-Audit-Message-Templates Command

Use the Crypto CLI list-audit-message-templates command to display all audit message templates.

Syntax

```
cryptocli list-audit-message-templates [options]
```

Option	Description
-h or --help	Displays usage text.
-m or --max-items int	The maximum number of items to be included in the response.

Option	Description
-n or --next-token string	The token from which the subsequent audit messages would be listed. Strings must be encased in double quotes.

List-Audit-Messages Command

Use the Crypto CLI list-audit-messages command to display all audit messages.

Syntax

```
cryptocli list-audit-messages [options]
```

Option	Description
-h or --help	Displays usage text.
-f or --field stringArray	The AD setting fields to be included in the response.
-l or –filters string	The conditional expression to filter AD settings.
-i or --include-info	Show additional information if available.
-j or --json-output	Show JSON-formatted audit messages.
-t or --local-time	Convert audit message timestamps to local time.
-m or --max-items int	The maximum number of items to be included in the response.
-n or --next-token string	The token from which the subsequent audit messages would be listed. Strings must be encased in double quotes.

Import-Clear-Key Command

Use the Crypto CLI clear-key command to import a clear key instead of importing a wrapped key. The import-clear-key command can be used with and without mTLS enabled.

Important: This method imports key material as base64-encoded cleartext, which is not recommended. For stronger security, use the import-key API, which wraps key material with RSA and AES keys before transmission. This provides end-to-end cryptographic protection beyond what HTTPS alone offers.

Syntax

```
cryptocli import-clear-key [options]
```

Option	Description
-h or --help	Displays usage text.
-k or --keyset-guid string	Optional. The GUID of the keyset where this key will be imported. Strings must be enclosed in double quotes.
-n or --name string	The name of the key to be imported. Strings must be enclosed in double quotes.
-d or --description string	The optional description. Strings must be enclosed in double quotes.
-c or --cipher string	The cipher of the key. This should be RSA-2048.
-m or --key_material string	The key material of the key in base64.

Get-Tokenization-Settings Command

Use the Crypto CLI get-tokenization-settings command to display the Cryptographic Security Platform Vault for Cryptographic APIs settings.

Syntax

```
cryptocli get-tokenization-settings [options]
```

Option	Description
-h or --help	Displays usage text.

Get-Tokenization-Policy Command

Use the Crypto CLI get-tokenization-policy command to fetch the specified tokenization policy.

Syntax

```
cryptocli get-tokenization-policy [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-n or --name string	The name of the tokenization policy to fetch. Strings must be enclosed in double quotes.

Get-Tokenization-Info Command

Use the Crypto CLI get-tokenization-info command to display the Cryptographic Security Platform Vault for Cryptographic APIs information.

Syntax

```
cryptocli get-tokenization-info [options]
```

Option	Description
-h or --help	Displays usage text.

Get-Platform-Info Command

Use the Crypto CLI get-platform-info command to display the Cryptographic Security Platform Vault for Cryptographic APIs platform information.

Syntax

```
cryptocli get-platform-info [options]
```

Option	Description
-h or --help	Displays usage text.

Get-Local-User Command

Use the Crypto CLI get-local-user command to fetch a local user.

Syntax

```
cryptocli get-local-user [options]
```

Option	Description
-h or --help	Displays usage text.
-u or --username string	The username of the user to be fetched. Strings must be enclosed in double quotes.

Get-Key-Versions Command

Use the Crypto CLI get-key-versions command to get the versions of a key.

Syntax

```
cryptocli get-key-versions [options]
```

Option	Description
-h or --help	Displays usage text.
-k or --key-guid string	The GUID of the key. Strings must be enclosed in double quotes.

Get-Key-Value Command

Use the Crypto CLI get-key-value command to get the value of a key.

Syntax

```
cryptocli get-key-value [options]
```

Option	Description
-h or --help	Displays usage text.
-k or --key-guid string	The GUID of the key. Strings must be enclosed in double quotes.

Get-Keyset-Guid Command

Use the Crypto CLI get-keyset-guid command to display the Cryptographic Security Platform Vault for Cryptographic APIs default keyset GUID.

Syntax

```
cryptocli get-keyset-guid [options]
```

Option	Description
-h or --help	Displays usage text.

Get-Key-Details Command

Use the Crypto CLI get-key-details command to get the details of a key.

Syntax

```
cryptocli get-key-details [options]
```

Option	Description
-h or --help	Displays usage text.
-k or --key-guid string	The GUID of the key. Strings must be enclosed in double quotes.

Get-HSM-Info Command

Use the Crypto CLI get-hsm-info command to display the Cryptographic Security Platform Vault for Cryptographic APIs HSM information.

Syntax

```
cryptocli get-hsm-info [options]
```

Option	Description
-h or --help	Displays usage text.

Get-Audit-Settings Command

Use the Crypto CLI get-audit-settings command to fetch the current audit settings.

Syntax

```
cryptocli get-audit-settings [options]
```

Option	Description
-h or --help	Displays usage text.

Get-Audit-Message-Template Command

Use the Crypto CLI get-audit-message-template command to fetch a specific audit message template.

Syntax

```
cryptocli get-audit-message-template [options]
```

Option	Description
-h or --help	Displays usage text.
-m or --msgid int	The message ID of the audit message template to fetch in integer format.

Get-AD-User Command

Use the Crypto CLI get-ad-user command to delete a local user.

Syntax

```
cryptocli get-ad-user [options]
```

Option	Description
-h or --help	Displays usage text.
-n or --name string	The prefix of the username for searching. Strings must be enclosed in double quotes.

Get-AD-Group Command

Use the Crypto CLI get-ad-group command to search Active Directory groups.

Syntax

```
cryptocli get-ad-group [options]
```

Option	Description
-h or --help	Displays usage text.
-n or --name string	The prefix of the group name for searching. Strings must be enclosed in double quotes.

Export-Key Command

Use the Crypto CLI export-key command to export a key.

Syntax

```
cryptocli export-key [options]
```

Option	Description
-h or --help	Displays usage text.
-k or --key-guid string	The GUID of the key to be exported. Strings must be enclosed in double quotes.

Option	Description
-p or --public-key string	The public key file. Strings must be enclosed in double quotes.

Encrypt Command

Use the Crypto CLI encrypt command to encrypt data.

Syntax

```
cryptocli encrypt [options]
```

Option	Description
-h or --help	Displays usage text.
-a or --aad	Additional authentication data. Strings must be enclosed in double quotes.
-d or --data string	The data to be encrypted. Strings must be enclosed in double quotes.
-i or --iv string	The initialization vector. Strings must be enclosed in double quotes.
-m or --mode string	The mode of encryption to use. Strings must be enclosed in double quotes.
-k or --keyGuid	The Key GUID to be used for encryption. Strings must be enclosed in double quotes.

Enable-HSM-for-Keyset Command

Use the Crypto CLI enable-hsm-for-keyset command to enable HSM for a keyset.

Syntax

```
cryptocli enable-hsm-for-keyset [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-l or --part-label string	Partition label. Strings must be enclosed in double quotes.
-p or --part-password string	Partition password. Strings must be enclosed in double quotes.
-k or --keyset-guid string	Keyset for which HSM is to be enabled. Strings must be enclosed in double quotes.

Detokenize-Mask Command

Use the Crypto CLI detokenize-mask command to detokenize and mask data.

Syntax

```
cryptocli detokenize-mask [options]
```

Option	Description
-h or --help	Displays usage text.
-n or --policyName string	The comma-separated detokenization and mask policy names. Strings must be enclosed in double quotes.
-d or --tokenData string	The data to be detokenized and masked. Strings must be enclosed in double quotes.
-k or --keyGuid string	If you want to detokenize data using a specific version of the key, enter it here. If you do not enter a key, the latest key version will be used. Strings must be enclosed in double quotes.

Detokenize Command

Use the Crypto CLI detokenize command to detokenize data.

Syntax

```
cryptocli detokenize [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-n or --policyName string	The policy name to be used for detokenization. Strings must be enclosed in double quotes.
-d or --tokenData string	The data to be detokenized. Strings must be enclosed in double quotes.
-k or --keyGuid string	If you want to detokenize data using a specific version of the key, enter it here. If you do not enter a key, the latest key version will be used. Strings must be enclosed in double quotes.

Delete-Tokenization-Policy Command

Use the Crypto CLI delete-tokenization-policy command to delete the specified tokenization policy.

Syntax

```
cryptocli delete-tokenization-policy [options]
```

Option	Description
-h or --help	Displays usage text.
-n or --name string	The name of the tokenization policy to delete. Strings must be enclosed in double quotes.

Delete-Local-User Command

Use the Crypto CLI delete-local-user command to delete a local user.

Syntax

```
cryptocli delete-local-user [options]
```

Option	Description
-h or --help	Displays usage text.
-u or --username string	The username of the user to be deleted. Strings must be enclosed in double quotes.

Decrypt Command

Use the Crypto CLI decrypt command to decrypt data.

Syntax

```
cryptocli decrypt [options]
```

Option	Description
-h or --help	Displays usage text.
-a or --aad	Additional authentication data. Strings must be enclosed in double quotes.
-d or --data string	The data to be decrypted. Strings must be enclosed in double quotes.
-i or --iv string	The initialization vector. Strings must be enclosed in double quotes.
-m or --mode string	The mode of decryption to use. Strings must be enclosed in double quotes.
-k or --keyGuid	The Key GUID to be used for decryption. Strings must be enclosed in double quotes.

Create-Tokenization-Policy Command

Use the Crypto CLI create-tokenization-policy command to create a tokenization policy.

Syntax

```
cryptocli create-tokenization-policy [options]
```

Option	Description
-h or --help	Displays usage text.
-A or --alphabet bool	Use True if data to be tokenized using this policy can contain alphabets. Otherwise use False.
-c or --charset string	The character set to be used with this policy. Strings must be enclosed in double quotes.
-o or --charsetOption stringArray	The character set option to be used for this policy. Use 1 for space, 2 for punctuation, 4 for numbers, 8 for alphabets, and 16 for fullwidth.

Option	Description
-d or --description string	The description of the policy. Strings must be enclosed in double quotes.
-D or --digit bool	Use True if data to be tokenized using this policy can contain digits. Otherwise use False.
-w or --fullwidth bool	Use True if data to be tokenized using this policy can contain fullwidth. Otherwise use False.
-k or --keyguid string	The GUID of the key to be used with this policy. Strings must be enclosed in double quotes.
-n or --name string	The name of the policy to be created. Strings must be enclosed in double quotes.
-N or --new bool	Use True if creating a new policy, or False if updating an existing policy. The default is True.
-P or --preservedPrefixLength int	The length of the prefix to be preserved.
-S or --preservedSuffixLength int	The length of the suffix to be preserved.
-U or --space bool	Use True if the data to be tokenized using this policy can contain spaces. Otherwise use False.
-s or --symbol bool	Use True if the data to be tokenized using this policy can contain symbols. Otherwise use False.

Create-Mask-Policy Command

Use the Crypto CLI create-mask-policy command to create a masking policy.

Syntax

```
cryptocli create-mask-policy [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-c or --charset string	The character set to be used with this policy. Strings must be enclosed in double quotes.
-d or --description string	The description of the policy. Strings must be enclosed in double quotes.
-m or --maskChar string	The character to use for the mask. By default, this is "#".
-n or --name string	The name of the policy to be created. Strings must be enclosed in double quotes.
-N or --new bool	Use True if creating a new policy, or False if updating an existing policy. The default is True.
-P or --preservedPrefixLength int	The length of the prefix to be preserved.
-S or --preservedSuffixLength int	The length of the suffix to be preserved.

Create-Local-User Command

Use the Crypto CLI create-local-user command to create a local user.

Syntax

```
cryptocli create-local-user [options]
```

Option	Description
-h or --help	Displays usage text.
-e or --email string	The email of the user. Strings must be enclosed in double quotes.
-p or --password string	The password for the user. Strings must be enclosed in double quotes.
-d or --password-expiration string	The date on which the password expires in yyyy-mm-dd format. Strings must be enclosed in double quotes.

Option	Description
-u or --username string	The username of the user for login purposes. Strings must be enclosed in double quotes.
-n or --name string	The full name of the user. Strings must be enclosed in double quotes.

Create-Key Command

Use the Crypto CLI create-key command to create a key.

Syntax

```
cryptocli create-key [options]
```

Option	Description
-h or --help	Displays usage text.
-d or --description string	The optional key description. Strings must be enclosed in double quotes.
-c or --cipher string	The cipher to be used for this key. Strings must be enclosed in double quotes.
-n or --name string	The name of the key to be created. Strings must be enclosed in double quotes.
-k or --keyset-guid string	Optional. The GUID of the keyset to be used for creating this key. Strings must be enclosed in double quotes.

Change-AD-Domain Command

Use the Crypto CLI change-AD-domain command to change your AD domain.

Syntax

```
cryptocli change-ad-domain [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-n or --netbios-name string	The Active Directory NetBIOS name. Strings must be enclosed in double quotes.

-j, --servers-json-file string	The Active Directory Domain Controller List JSON File. This is an array of JSON objects, each object representing a Domain Controller. Strings must be enclosed in double quotes.
	The following keys are supported:
	• server_url - the (mandatory) full url of the Domain Controller
	• cacert (optional) - the path to the CA Certificate to verify with
	• user_base_dn (optional) - the user base DN
	• group_base_dn (optional) - the group base DN
	• timeout (optional) - the connection timeout in seconds. The default is 5 seconds.
	• tls (optional) - whether to enable StartTLS or not. The default is false.
	Example:
	[
	{
	"server_url": "ldaps://
	dc1.mycompany.eng.com",
	"cacert": "/root/cacert.pem",
	"user_base_dn":
	"DC=mycompany,DC=eng,DC=com",
	"group_base_dn":
	"DC=mycompany,DC=eng,DC=com",
	"timeout": 10,
	"tls": false,
	}
	]

-s, --service-account string	The Active Directory service account user name. Strings must be enclosed in double quotes.
-p, --service-password string	The Active Directory service account user password. Strings must be enclosed in double quotes.
-u, --uid-attribute string	The Active Directory UID Attribute. Strings must be enclosed in double quotes.

Option	Description
-d, --domain-name string	The Active Directory Domain Name. Strings must be enclosed in double quotes.
-t, --type string	The domain type.

Batch-Tokenize Command

Use the Crypto CLI batch-tokenize command to tokenize multiple records at once.

Syntax

```
cryptocli batch-tokenize [options]
```

Option	Description
-h or --help	Displays usage text.
-n or --policyName string	The policy name to be used for tokenization. Strings must be enclosed in double quotes.
-d or --tokenData string	The data to be tokenized. Strings must be enclosed in double quotes.
-k or --keyGuid string	If you want to tokenize data using a specific version of the key, enter it here. If you do not enter a key, the latest key version will be used. Strings must be enclosed in double quotes.

Batch-Rekey Command

Use the Crypto CLI batch-rekey command to rekey multiple records of tokenized data using a different policy.

Syntax

```
cryptocli batch-rekey [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-n or --policyName string	The detokenization policy name used to detokenize your data, and the tokenization policy name to be used for rekeying your data using a different policy. Strings must be enclosed in double quotes.
-d or --tokenData string	The data to be rekeyed. Strings must be enclosed in double quotes.

Batch-Mask Command

Use the Crypto CLI batch-mask command to mask multiple records at once.

Syntax

```
cryptocli batch-mask [options]
```

Option	Description
-h or --help	Displays usage text.
-n or --policyName string	The policy name to be used for masking. Strings must be enclosed in double quotes.
-d or --tokenData string	The data to be masked. Strings must be enclosed in double quotes.

Batch-Encrypt-Decrypt Command

Use the Crypto CLI batch-encrypt-decrypt command to encrypt and decrypt multiple records at once.

Syntax

```
cryptocli batch-encrypt-decrypt [options]
```

Option	Description
-h or --help	Displays usage text.
-a or --aad stringArray	Enter additional authentication data if required. Enter 0 if no additional authentication data is required.

Option	Description
-d or --data stringArray	The data to be encrypted.
-i or --iv stringArray	Enter the initialization vector if required. Enter 0 if the initialization vector is not required.
-k or --keyGuid stringArray	Enter the Key GUID to be used for encryption.
-m or --mode stringArray	Enter the mode of encryption.
-o or --operation stringArray	Enter Encrypt/Decrypt for the operation type.

Batch-Encrypt Command

Use the Crypto CLI batch-encrypt command to encrypt multiple records at once.

Syntax

```
cryptocli batch-encrypt [options]
```

Option	Description
-h or --help	Displays usage text.
-a or --aad stringArray	Enter additional authentication data if required. Enter 0 if no additional authentication data is required.
-d or --data stringArray	The data to be encrypted.
-i or --iv stringArray	Enter the initialization vector if required. Enter 0 if the initialization vector is not required.
-k or --keyGuid stringArray	Enter the Key GUID to be used for encryption.
-m or --mode stringArray	Enter the mode of encryption.

Batch-Detokenize Command

Use the Crypto CLI batch-detokenize command to detokenize multiple records at once.

Syntax

```
cryptocli batch-detokenize [options]
```

Option	Description
-h or --help	Displays usage text.
-n or --policyName string	The policy name to be used for detokenization. Strings must be enclosed in double quotes.
-d or --tokenData string	The data to be detokenized. Strings must be enclosed in double quotes.
-k or --keyGuid string	If you want to detokenize data using a specific version of the key, enter it here. If you do not enter a key, the latest key version will be used. Strings must be enclosed in double quotes.

Batch-Decrypt Command

Use the Crypto CLI batch-decrypt command to decrypt multiple records at once.

Syntax

```
cryptocli batch-decrypt [options]
```

Option	Description
-h or --help	Displays usage text.
-a or --aad stringArray	Enter additional authentication data if required. Enter 0 if no additional authentication data is required.
-d or --data stringArray	The data to be decrypted.
-i or --iv stringArray	Enter the initialization vector if required. Enter 0 if the initialization vector is not required.
-k or --keyGuid stringArray	Enter the Key GUID to be used for decryption.
-m or --mode stringArray	Enter the mode of decryption.

Get-AD-Settings Command

Use the Crypto CLI get-ad-settings command to fetch the specified AD settings.

If you have only one AD account, then using the list-ad-settings command displays the same information.

Syntax

```
cryptocli get-ad-settings [options]
```

Option	Description
-h or --help	Displays usage text.
-a or --ad-setting-id string	The ID or name of the AD setting to fetch. Strings must be enclosed in double quotes.

Update-AD-Settings Command

Use the Crypto CLI update-AD-settings command to update your AD settings.

Syntax

```
cryptocli update-ad-settings [options]
```

Option	Description
-h or --help	Displays usage text.
-a or --ad-setting-id string	The Active Directory setting ID or name. Strings must be enclosed in double quotes.
-n or --netbios-name string	The Active Directory NetBIOS name. Strings must be enclosed in double quotes.
-r or --revision int	The Active Directory setting current revision.

Option	Description

-j, --servers-json-file string	The Active Directory Domain Controller List JSON File. This is an array of JSON objects, each object representing a Domain Controller. Strings must be enclosed in double quotes.
	The following keys are supported:
	• server_url - the (mandatory) full url of the Domain Controller
	• cacert (optional) - the path to the CA Certificate to verify with
	• user_base_dn (optional) - the user base DN
	• group_base_dn (optional) - the group base DN
	• timeout (optional) - the connection timeout in seconds. The default is 5 seconds.
	• tls (optional) - whether to enable StartTLS or not. The default is false.
	Example:
	[
	{
	"server_url": "ldaps://
	dc1.mycompany.eng.com",
	"cacert": "/root/cacert.pem",
	"user_base_dn":
	"DC=mycompany,DC=eng,DC=com",
	"group_base_dn":
	"DC=mycompany,DC=eng,DC=com",
	"timeout": 10,
	"tls": false,
	}
	]

-s, --service-account string	The Active Directory service account user name. Strings must be enclosed in double quotes.
-p, --service-password string	The Active Directory service account user password. Strings must be enclosed in double quotes.
-u, --uid-attribute string	The Active Directory UID Attribute. Strings must be enclosed in double quotes.
-t, --type string	The domain type.

List-AD-Settings Command

Use the Crypto CLI list-AD-settings command to display all AD settings.

Syntax

```
cryptocli list-ad-settings [options]
```

Option	Description
-h or --help	Displays usage text.
-f or --field stringArray	The AD setting fields to be included in the response.
-l or –filters string	The conditional expression to filter AD settings.
-m or --max-items int	The maximum number of items to be included in the response.
-n or --next-token string	The token from which the subsequent audit messages would be listed. Strings must be encased in double quotes.
-p or --prefix string	Only the AD settings prefixed with this string will be listed.

Delete-Policy Command

Use the Crypto CLI delete-policy command to delete the specified policy.

Syntax

```
cryptocli delete-policy [options]
```

Option	Description
-h or --help	Displays usage text.
-p or --policyid string	The ID or name of the policy to delete. Strings must be enclosed in double quotes.

Update-Access-Policy Command

Use the Crypto CLI update-access-policy command to update the properties of a policy.

Syntax

```
cryptocli update-policy-command [options]
```

Option	Description
-h or --help	Displays usage text.
-g, --ad-group stringArray	A string separated by '||' containing the DN and display name of AD groups to be added as principals.
-L or --ad-logon-name stringArray	The logon name of AD users to be added as principals. This option is repeatable.
-u, --ad-upn stringArray	The UPN of AD users to be added as principals. This option is repeatable.
-d, --description string	Short description of the policy.
-l, --local-user stringArray	Local username of users to be added as principals. This option is repeatable.
-p or --policyid string	The name or ID of the policy to update.
-P or –tokenization_permissions stringArray	Tokenization permissions for users of this policy. This option is repeatable.
-R or --revision int	The revision number of the policy.
-r or --role string	The role of the user.
-t or --tagkey stringArray	The tag key to associate with the policy. This option is repeatable.
-v or --tagvalue stringArray	The tag value to associate with the policy. This option is repeatable.

Set-Policy-Version Command

Use the Crypto CLI set-policy-version command to set a specific version of the policy to current.

Syntax

```
cryptocli set-policy-version [options]
```

Option	Description
-h or --help	Displays usage text.
-p or --policyid string	The ID or name of the policy to fetch. Strings must be enclosed in double quotes.
-v or --version int	The version of the policy to be set as current.

List-Policy-Versions Command

Use the Crypto CLI list-policy-versions command to display the specified policy versions.

Syntax

```
cryptocli list-policy-versions [options]
```

Option	Description
-h or --help	Displays usage text.
-p or --policyid string	The ID or name of the policy to fetch. Strings must be enclosed in double quotes.

Get-Policy Command

Use the Crypto CLI get-policy command to fetch a specific policy.

If you have only one policy, then using the list-policy command displays the same information.

Syntax

```
cryptocli get-policy [options]
```

Option	Description
-h or --help	Displays usage text.
-p or --policyid string	The ID or name of the policy to fetch. Strings must be enclosed in double quotes.
-v or –version int	Version of the Policy to fetch. If not specified, fetches the current version.

Create-Access-Policy Command

Use the Crypto CLI create-access-policy command to create a role-based access control policy to allow users or applications to access secrets.

Syntax

```
cryptocli create-access-policy [options]
```

Option	Description
-h or --help	Displays usage text.
-g or --ad-group stringArray	||-separated string containing the DN & display name of AD groups to be added as principals.
-L or --ad-logon-name stringArray	Logon name of AD users to be added as principals. This option is repeatable.
-u or --ad-upn stringArray	The UPN of AD users to be added as principals. This option is repeatable.
-l or --local-user stringArray	Local username of users to be added as principals. This option is repeatable.
-n or --name string	The name of the policy. Strings must be enclosed in double quotes.
-p or —-tokenization_permissions stringArray	Tokenization permissions for users of this policy. This option is repeatable.
-r or --role string	The role of the user that is being assigned.
-t or --tagkey stringArray	The tag key to associate with the policy. This option is repeatable.
-v or --tagvalue stringArray	The tag value to associate with the policy. This option is repeatable.

Login Command

Use the Crypto CLI login command to log in to your Cryptographic Security Platform Vault for Cryptographic APIs. The login expires in 30 minutes.

⚠ Ensure that you have the Cryptographic Security Platform Vault CA Certificate and the Cryptographic Security Platform Vault for Cryptographic APIs API URL before you begin. For more information, see Accessing the Crypto CLI

```
cryptocli login [options]
```

See below for a description of each option.

Option	Description
-h or --help	Displays usage text.
-C or --cacert string	The path to the Cryptographic Security Platform Vault CA Certificate file you downloaded (for example, cacert.pem). This verifies the Cryptographic Security Platform Vault server. Enclose strings in double quotes.
-l or --login-URL string	The API URL for the Cryptographic Security Platform Vault for Cryptographic APIs.
-p or --password string	The login password. If you don't provide it, you'll be prompted to enter the password. Enclose strings in double quotes.
-u or --username string	The login username. If not provided, you will be prompted to enter the username. Enclose strings in double quotes.

Example: log in to the Crypto CLI with the username and password:

```
./cryptocli -C "/home/kc-cert/240328220252_cacert" -l https://10.1.1.222/token/1.0/Login/d65138e6-b249-4587-9f24-81787babffc2/ -u "MyName@MyCompany.com" -p "MyPa$$word123"
```

Accessing the Crypto CLI

You must create a Cryptographic Security Platform Vault for Cryptographic APIs before you can use the Crypto CLI commands.

To access the Crypto CLI, you will need the following:

- The KeyControl Vault CA Certificate.
- The login URL of the vault. This is listed as the API URL on the Details page for your Cryptographic Security Platform Vault for Cryptographic APIs.

Crypto CLI is available for both Linux and Windows at https://github.com/EntrustCorporation/cryptocli

The Crypto CLI application is in the same directory as the Cryptographic Security Platform Vault CA Certificate you downloaded.

Managing client certificates

See below for instructions on managing client certificates.

- Creating a client certificate
- Downloading a client certificate
- Using the mTLS API commands
- Deleting a Client Certificate

Creating a client certificate

See below for creating a client certificate.

> Creating a client certificate automatically creates a CA certificate.

To create a client certificate

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Security > Client Certificates**.
3. On the Manage Client Certificates page, click the **Create** button.
4. On the Create Client Certificate dialog box, complete the following:

Field	Description
Name	Enter the client certificate name.
Create for	Enter the name or group for whom the certificate is created.
Certificate Expiration	Enter the date the certificate will expire or accept the default of 1 year.
Certificate Signing Request (CSR)	Optionally click Browse and select the Certificate Signing Request.
Encrypt Certificate Bundle	Optionally choose to encrypt the certificate bundle. If selected, enter an encryption password and confirm it.
Access Policy	Select the access policy to associate with this client certificate.

5. Click **Create**.

Downloading a client certificate

See below for how to download a client certificate.

To download a client certificate

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Security > Client Certificates**.
3. On the Manage Client Certificates page, select the client certificate that you want to download.
4. Click the **Client Certificate** tab.
5. Click **Download**.
6. Wait while Vault for Cryptographic APIs webGUI downloads a ZIP bundle that contains the client certificate and the CA certificate.

Using the mTLS API commands

By default, all APIs in the Cryptographic Security Platform Vault for Cryptographic APIs use the following API endpoint.

```
https://<VAULT_IP_or_FQDN>/token/1.0/key/API_COMMAND
```

When you enable mTLS, you will need to change your API endpoint to

```
https://<VAULT_IP_or_FQDN>/mtls/crypto/1.0/key/API_COMMAND
```

If you disable mTLS, switch the endpoint back to:

```
https://<VAULT_IP_or_FQDN>/token/1.0/key/API_COMMAND
```

Before you can use the mTLS APIs:

- mTLS must be enabled for the CSP Vault for Cryptographic APIs.
- You must have a CA certificate. This can be downloaded from the CSP Vault Management appliance, or it can be downloaded using the Get Client Certificate along with CA certificate API
- You must have a Client certificate. You can create this using the Create Client Cert API and download it using the Get Client Certificate along with CA certificate API.

See below for examples.

- Sample curl command
- Sample Python script
- mTLS API Examples

Sample curl command

See below for a sample curl command to use mTLS APIs.

```
[root@user1-10.1.10.10 mtls]# curl -s --cert ./client_cert.pem --key ./client_key.pem
--cacert ./ca_cert.pem -X POST -H "Content-Type: application/json" -d '{"name":
"rsa-2048", "cipher": "RSA-2048"}' https://10.1.10.10/mtls/crypto/1.0/key/
```

Sample Python script

See below for a sample Python script to use mTLS APIs.

```
import requests
```

```
import json

# Define the URL of the API endpoint
url = "https://10.1.228.140/mtls/crypto/1.0/key/"
payload = {"name": "aes-128", "cipher": "AES-128"}

# Path to the client certificate and key files
client_cert = (
    "./client_cert.pem",
    "./client_key.pem",
)  # Client key is present in the client_cert.pem if external CSR is not used. If
external CSR is used then it has to specified additionally.

# Path to the CA certificate file
ca_cert = "./ca_cert.pem"

# Make the API request with mTLS
response = requests.post(
    url, cert=(client_cert), data=json.dumps(payload), verify=ca_cert
)

# Print the response
print(response.status_code)
print(response.text.encode("utf-8").decode("unicode_escape"))
```

mTLS API Examples

See below for creating an AES key

Post

```
https://<VAULT_IP_or_FQDN>/mtls/crypto/1.0/CreateKey
```

Request payload

```
{
   "cipher": "AES-256",
    "description": "Signing key",
    "keyset_guid": "b4e6b2a8-a693-40ab-9cb3-5f34cbf2227e",
    "name": "key1"
}
```

See below to create a tokenization policy using the GUID of an AES key that you created.

Post

```
Post: https://<VAULT_IP_or_FQDN>/mtls/crypto/1.0/CreateTokenPolicy/
```

Request payload

```
{
    "charset": "Alphanumeric",
    "charsetOption": [
        1,
        4,
        8
    ],
    "description": "Tokenization Policy for SSN",
    "isNew": true,
    "keyGuid": "52bbf639-babf-47a6-a54b-bb92ad6954ad",
    "name": "Tokenization-Policy-1",
    "preservedPrefixLength": 2,
    "preservedSuffixLength": 2
}
```

See below to encrypt an AES key.

```
https://<VAULT_IP_or_FQDN>/mtls/crypto/1.0/encrypt
```

Request payload

```
{
  "aad": "VEVTVA==",
  "data": "TWFyeSBoYWQgYSBsaXR0bGUgbGFtYg==",
  "iv": "MDEyMzQ1Njc4OTAxMjM0NQ==",
  "keyGuid": "9f726ba4-3b88-48d7-8a02-df2e8472d4dc",
  "mode": "AES_ECB"
}
```

Deleting a Client Certificate

See below for how to delete a client certificate.

To delete a client certificate

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Security > Client Certificates**.
3. On the Manage Client Certificates page, select the client certificate that you want to delete.
4. Click the **Delete** button.

5. On the Delete Client Certificate screen, click **Delete**.

Configuring mTLS for the CSP Vault for Cryptographic APIs

Mutual Transport Layer Security (mTLS) adds two-way authentication and encryption using digital certificates.

Important: Once mTLS is enabled in the Cryptographic Security Platform Vault for Cryptographic APIs, only certain APIs located at a new URL will function. You will also not be able to use any webGUI functions located under the Manage section in the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.

These APIs function the same as the existing APIs, but are located at a new URL: https://<VAULT_IP_or_FQDN>/mtls/crypto/1.0/.

Enabling or Disabling mTLS Authentication

You can enable or disable mTLS from the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.

1. Log into the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. At the top right of the vault page, click the Settings icon.
3. On the Settings page, click the mTLS tab.
4. Toggle the mTLS button to Enabled or Disabled.
5. Confirm your choice.

You can also use the UpdateTokenizationSettings API to enable mTLS. The path to this API does not change when mTLS is enabled. It is always https://<VAULT_IP_Address>/token/1.0/key/UpdateTokenizationSettings.

For example:

Copy

```
{
 "2FA_enforced": false,
 "degraded_mode_availability": false,
 "mTLS_enabled": true,
 "oidc_enabled": true,
 "revision": 1
}
```

APIs Supported with mTLS

The following APIs in the Cryptographic Security Platform Vault for Cryptographic APIs can be used with mTLS:

- Key management functions, including creating keys, deleting keys, rotating keys, importing keys, and exporting keys.
- Tokenization and masking policies, including creating, editing, and deleting the policies, as well as tokenizing, detokenizing, masking or demasking the data.
  Note: Access policies are not supported in mTLS.
- Encryption and decryption functions, including encrypting and decrypting data, wrapping and unwrapping keys, signing data, and verifying signed data.

mTLS Prerequisites

Before you can use mTLS APIs, you must complete the following:

- Enable mTLS on the Cryptographic Security Platform Vault for Cryptographic APIs.
- Create and download the client certificate and the CA certificate. For more information, see Creating a client certificate.
  When you download the client certificate from the webGUI, the downloaded zip bundle contains both the client certificate and the CA certificate. For more information, see Downloading a client certificate.
  Note: If you want to use API commands, use the CreateClientCert API to create the certificate and the GetClientCertificateBundleInText API to download both the client certificate and the CA certificate.

About Cache Management

You can cache your keys in the Cryptographic Security Platform Vault for Cryptographic APIs memory to improve performance.

The Cryptographic Security Platform Vault for Cryptographic APIs creates cache tables with the following columns:

- Cache Type—This can be one of the following operation types:
  - Tokenization
  - Encryption
  - Signing
  - Wrapping
- Eviction Time (mins)—The length of time in minutes before the elements in the cache will be deleted after their last usage. The default is 30 minutes.
- Size—The number of elements that will remain in the cache. The default is 250 elements.

Caching is enabled by default, and each cache can be configured individually.

Clearing the Caches

1. Log into the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. Click the **Settings** icon at the top right of the vault page.
3. Click the **Cache Management** tab.
4. Click **Actions > Clear Cache**.
5. In the Clear Cache window, check the checkbox for each cache type that you want to clear.
   Note: If you do not select a type, all caches will be cleared.
6. Click **Confirm** to close the window.

Configuring Cache Management

1. Log into the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. Click the **Settings** icon at the top right of the vault page.
3. Click the **Cache Management** tab.
4. Choose whether to enable or disable in-memory cache.
   Note: Cache management is enabled by default. If you disable cache management, all of your caches will be cleared.
5. Click **Actions > Edit** to update the cache settings values.
6. In the Edit Cache Settings window, you can update each of the four caches individually.
7. Click **Apply** to close the window and save your changes.

Configuring CSP Vault for Cryptographic APIs Policies

You can create either a tokenization policy or a masking policy.

- To configure tokenization policies, see Creating a Tokenization Policy
- To configure masking policies, see Creating a Masking Policy

> ⚠ If you plan to manage Elliptic Curve Cryptography (ECC) keys in a Cryptographic Security Platform Vault for Cryptographic APIs that is protected by an nShield HSM, the ECC feature must be enabled on the HSM.

Deleting a Masking Policy

1. Log into the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Manage > Policies**.
3. Select the Masking tab.
4. On the Masking Policies page, select the policy that you want to delete.
5. Click **Delete**.
6. On the confirmation screen, click **OK** to delete the policy.

Editing a Masking Policy

You can edit a masking policy. This allows you to update any of the policy details except the policy name.

1. Log into the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Manage > Policies**.
3. Select the Masking tab.
4. On the Masking Policies page, select the policy that you want to edit.
5. On the Edit Masking Policy dialog box, update the necessary fields.
6. Click **Apply**.

Creating a Masking Policy

You can create and configure masking policies, which provide masked data tokens.

Vault administrators and vault users can create tokenization policies. Only vault administrators can edit and delete tokenization policies. Users are not able to edit or delete tokenization policies.

To configure a masking policy

1. Log into the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Manage > Policies**.
3. On the Tokenization Policies page, select the Masking tab.
4. Click the **Create** icon to create a masking policy.
5. On the Create Masking Policy dialog box, complete the following:

Field	Description
Policy Name	Enter the name for the policy.
Charset	Select the required character set for the policy (the format of the input data). For example, Numeric.

Field	Description
Mask Character	Enter the character for masking token data. For example, #.
Preserved Prefix	Optional: To preserve any prefix characters in the token, enter the number of characters to preserve. For example, select 2 to preserve the first two characters.
Preserved Suffix	Optional: To preserve any suffix characters in the token, enter the number of characters to preserve. For example, select 2 to preserve the last two characters.

6. Click **Create**.

Deleting a Tokenization Policy

You can delete a tokenization policy.

Vault administrators and vault users can create tokenization policies. Only vault administrators can edit and delete tokenization policies. Users are not able to edit or delete tokenization policies.

Ensure no users or applications are using the policy.

To delete a tokenization policy

1. Log into the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Manage > Policies**.
3. On the Tokenization Policies page, select the policy that you want to delete.
4. Click **Delete**.
5. On the confirmation screen, click **OK** to delete the policy.

Editing a Tokenization Policy

You can edit a tokenization policy. This allows you to update any of the policy details except the policy name.

Vault administrators and vault users can create tokenization policies. Only vault administrators can edit and delete tokenization policies. Users are not able to edit or delete tokenization policies.

Your change will apply to all applications currently using the tokenization policy.

To edit a tokenization policy

1. Log into the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Manage > Policies**.
3. On the Tokenization Policies page, select the policy that you want to edit.
4. On the Edit Tokenization Policy dialog box, update the necessary fields.
5. Click **Apply**.

Creating a Tokenization Policy

You create and configure tokenization policies, which are used to tokenize or detokenize data.

Vault administrators and vault users can create tokenization policies. Only vault administrators can edit and delete tokenization policies. Users are not able to edit or delete tokenization policies.

Note: You must create a key before you can create a tokenization policy. See Creating keys.

To configure a tokenization policy

1. Log into the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Manage > Policies**.
3. On the Tokenization Policies page, ensure the Tokenization tab is selected.
4. Click the Create icon to create a tokenization policy.
5. On the Create Tokenization Policy dialog, complete the following:

Field	Description
Policy Name	Enter the name for the policy.
Description	Optional. Enter the description for the policy.
Key	Select a key from the drop-down list. For Tokenization policies, only keys of type AES are supported.
Charset	Select the required character set for the policy (the format of the input data). Examples include: • Alphanumeric—for numbers and alphabetical characters. • Numeric—for numbers only • Numeric-Luhn—used for credit cards and ID numbers. • Chinese—for Chinese text. • Japanese—for Japanese text. • Korean—for Korean text. • Thai—For Thai text. • TWID—the Taiwan National ID format, in the form A123456789. • Vietnamese—for Vietnamese text.
Preserved Prefix	Optional. To preserve any prefix characters in the token, enter the number of characters to preserve. For example, select 2 to preserve the first two characters.
Preserved Suffix	Optional. To preserve any suffix characters in the token, enter the number of characters to preserve. For example, select 2 to preserve the last two characters.

6. Click **Create**.

Managing Keys

The Manage Keys page allows you to view all of your keys, as well as create new keys, edit or delete existing keys, rotate keys, and cancel the deletion of a key.

- Exporting keys
- Importing keys

- Creating keys
- Viewing key details
- Editing keys
- Rotating keys
- Programming key deletion
- Canceling key deletion
- Permanently deleting keys

Exporting keys

See below to wrap and export a key.

- Generating a wrapping key
- Downloading the key
- Decoding the key
- Splitting the key
- Unwrapping the temporary key
- Unwrapping the target key
- Verifying the key

Generating a wrapping key

Generate an RSA 2048 key using OpenSSL. For example:

```
$ openssl genrsa -out key.pem 2048
```

Extract the public key from the key you created, and list the key parts. For example:

Where:

- The `public.pem` public part of the key will wrap the key.
- The `key.pem` private part will unwrap the key.

Downloading the key

Export the Base64 encoding of the target AES-256 key.

To download the key

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs web GUI.
2. From the Home tab, select **Manage > Keys**.
3. On the **Manage Keys** page, select the key you want to export, then select **Actions > Export Key**.
4. On the **Export Key** page, complete the following:

Field	Description
Version	Displays the key version number. Copy this value to the clipboard. This is the key GUID.
Public Key	Click Browse and import the public part (public.pem) of the RSA 2048 key that you created.

Field	Description
Hashing Algorithm	Select SHA256 or SHA1.

5. Click **Download Key**.

Decoding the key

Base64 decode the wrapped AES key and save it in a file. For example:

```
$ openssl enc -base64 -d <<<
H2frvNvTUP+VyynwRYqo8+YEPRAgdioSyWtzYtJlQ1AqvxWW2B5EjEiJ8HxczMkxGKJPVjMJzKhYFkWgRhgWV
DUQSroDLV4PMZvcwRQ33/Z05brjJk/3I7n2aqPKlwPwAtVLy2phT8DVa4j1ozcmDI5aLKUncrdz/iY/
tuaEaFMyTHrHuLoo2jAONmyy2wJpi4tGeNoa+v+tKIzcmV9a9oE76Y7g9WHy35YDwryP2jzaK6NdMlBiABqnr
dGaa9O1mIt8HTZNMawHX9IXP7amAww0gGb4AGvOragllxUw42/
Eo2E7Nfo0JKElo2xn6NuKZ2TZRoMolTQZrDkEOrmoX6rBZb3d3HyiHlHFDbU0JPIt/
O+0EwS9tQJoBunv7gISLE1rrcLStrI= >> decoded_wrapped_key
$ ls -lrt
-rw-r--r-- 1 user1 1049089 1732 Aug 6 15:16 key.pem
-rw-r--r-- 1 user1 1049089 460 Aug 6 15:18 public.pem
-rw-r--r-- 1 user1 1049089 296 Aug 6 16:01 decoded_wrapped_key
```

Splitting the key

Split the decoded key into two parts:

- The temporary AES key
- The target key

For example:

```
$ dd if=decoded_wrapped_key of=wrapped_temp_aes_key bs=1 count=256
256+0 records in
256+0 records out
256 bytes copied, 0.0101148 s, 25.3 kB/s

$ dd if=decoded_wrapped_key of=wrapped_target_key bs=1 skip=256
40+0 records in
40+0 records out
40 bytes copied, 0.0025336 s, 15.8 kB/s

$ ls -lrt
-rw-r--r-- 1 user1 1049089 1732 Aug 6 15:16 key.pem
-rw-r--r-- 1 user1 1049089 460 Aug 6 15:18 public.pem
-rw-r--r-- 1 user1 1049089 296 Aug 6 16:01 decoded_wrapped_key
-rw-r--r-- 1 user1 1049089 256 Aug 6 16:04 wrapped_temp_aes_key
-rw-r--r-- 1 user1 1049089 40 Aug 6 16:04 wrapped_target_key
```

Unwrapping the temporary key

Unwrap the temp AES key using the private key. For example:

```
$ openssl pkeyutl -decrypt -inkey key.pem -in wrapped_temp_aes_key -out temp_aes_key
-pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha1

$ ls -lrt
-rw-r--r-- 1 bhavsac 1049089 1732 Aug 6 15:16 key.pem
-rw-r--r-- 1 bhavsac 1049089 460 Aug 6 15:18 public.pem
-rw-r--r-- 1 bhavsac 1049089 296 Aug 6 16:01 decoded_wrapped_key
-rw-r--r-- 1 bhavsac 1049089 256 Aug 6 16:04 wrapped_temp_aes_key
-rw-r--r-- 1 bhavsac 1049089 40 Aug 6 16:04 wrapped_target_key
-rw-r--r-- 1 bhavsac 1049089 32 Aug 6 16:06 temp_aes_key
```

Unwrapping the target key

Unwrap the target key using the temp AES key. The output is the unwrapped target key. If the target key is an AES key, then the output is Base64 encoded. For example:

```
$ openssl enc -d -id-aes256-wrap-pad -iv A65959A6 -K $( hexdump -v -e '/1 "%02x"' <
temp_aes_key ) -in wrapped_target_key | openssl enc -base64
0vEmbWIQnMAjP3gVJ0C4amnl+TWHymmW5ezQu5MDI+o=
```

Verifying the key

Verify the output using the Get Key Value API. For example:

```
GET: <CSP-vault-IP>/token/1.0/key/<key-guid_of_target_key>/value/
Response
{
  "result": "success",
  "value": "0vEmbWIQnMAjP3gVJ0C4amnl+TWHymmW5ezQu5MDI+o="
}
```

Importing keys

When you import a key into the Cryptographic Security Platform Vault for Cryptographic APIs, the target key must be wrapped with RSA-AES. To do this, first wrap the key with a temporary AES key, then wrap the temporary AES key with an RSA key. Concatenate the two wrapped keys and import them. If the key that you are importing was created in a different Cryptographic Security Platform Vault for Cryptographic APIs, then you can wrap that key before you export it with a key created in the new vault.

See below for the required steps.

- Importing a clear key using the API
- Importing a key from a different Cryptographic API
- Wrapping a key for import
- Importing a wrapped key using the API
- Importing a wrapped key in the web GUI

Importing a clear key using the API

See below for how to import a clear key instead of a wrapped key.

> ⚠ This method imports key material as base64-encoded cleartext, which we don't recommend. For stronger security, use the import-key API, which wraps key material with RSA and AES keys before transmission. This provides end-to-end cryptographic protection beyond what HTTPS alone offers.

Ensure you have the Import Clear Key permission on your account, then send the following POST request.

```
https://<VAULT_IP_or_FQDN>/mtls/crypto/1.0/clear_key_import /
```

Use a request payload like the following.

```
{
  "cipher": "RSA-2048",
  "description": "Signing key",
  "key_material":
"MIHuAgEAMBAGByqGSM49AgEGBSuBBAAjBIHWMIHTAgEBBEIBJ2oatGhkdy1W6pS9xygCo8cEbnV/...
ZA==",
  "keyset_guid": "b4e6b2a8-a693-40ab-9cb3-5f34cbf2227e",
  "name": "key1"
}
```

See below for each parameter.

Parameter	Value
cipher	The cipher of the key. Only RSA-2048 is supported
description	The optional description of the key
key_material	The key material of the key in base 64.
keyset_guid	The GUID (Globally Unique Identifier) of the key set where the key will be imported.
name	The name of the key to be imported.

Importing a key from a different Cryptographic API

See below to export any key from a Vault for Cryptographic APIs (Export-Vault) and then import it into a different one (Import-Vault).

> ℹ Export-Vault and Import-Vault can be different versions, as long as both are version 10.4.5 or later and support the target key type.

To import a key from a different Cryptographic API

1. Log in to the Import-Vault web GUI.
2. Create an RSA-2048 key in the web GUI.
3. Select the key that you created, and click **Download Public Key** to download the public part of the RSA-2048 key.
4. In a different browser window, log into the Export-Vault web GUI.
5. From the Home tab, select **Manage > Keys**.
6. On the **Manage Keys** page, select the RSA-2048 key that you want to export and select **Actions > Export Key**.
7. Click **Download Key**. The RSA-2048 key from the Export-Vault is now wrapped by the Import-Vault wrapping key and downloaded.
8. Return to the Import-Vault web GUI.
9. From the Home tab, select **Manage > Keys**.
10. On the **Manage Keys** page, select **Actions > Import Key**.
11. On the **Import Key** page, complete the following.

Field	Description
Name	Enter the new name for the key that you exported.
Description	Enter the optional description for the key that you exported.
Algorithm	Select AES.
Key Length	Select 256.
Key Material	Select the wrapped AES key that you exported.
Wrapping Key	Select the RSA-2048 public key that you used to wrap the AES key.
Wrapping Key Version	Select the version of the key that you exported.
Hashing Algorithm	Select SHA1.

12. Click **Import Key**.

Wrapping a key for import

When you import a key into the Cryptographic Security Platform Vault for Cryptographic APIs, the target key must be wrapped with RSA-AES.

To wrap a key for key import

1. Create an RSA-2048 key in the Cryptographic Security Platform Vault for Cryptographic APIs where you want to import the wrapped key. This will be the wrapping key.
2. Select the key that you created, and click **Download Public Key** to download the public part of the RSA-2048 key.
3. Generate the target AES-256 32-byte key using OpenSSL. For example:

```
$ openssl rand -out target_aes_key 32
```

4. Generate a temporary random AES-256 32-byte key using OpenSSL. For example:

```
$ openssl rand -out temp_aes_key 32
```

5. List the files that you've created or downloaded. For example:

```
root@machine-name-10-1-228-132 import_key_sample2]# ls -lrt
total 12
-rw-r--r--. 1 root root 451 Aug 5 11:15 rsa_public.pem
-rw-r--r--. 1 root root 32 Aug 5 11:19 temp_aes_key
-rw-r--r--. 1 root root 32 Aug 5 11:19 target_aes_key
```

6. Wrap the temporary AES key with the wrapping public key using the CKM_RSA_PKCS_OAEP algorithm. For example:

```
openssl pkeyutl -encrypt -pubin -inkey rsa_public.pem -in temp_aes_key -out
wrapped_aes_key -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha1
```

7. List the files again. For example:

```
[root@machine-name-10-1-228-132 import_key_sample2]# ls -lrt
total 12
-rw-r--r--. 1 root root 451 Aug 5 11:15 rsa_public.pem
-rw-r--r--. 1 root root 32 Aug 5 11:19 temp_aes_key
-rw-r--r--. 1 root root 32 Aug 5 11:19 target_aes_key
-rw-r--r--. 1 root root 296 Aug 5 11:22 wrapped_aes_key
```

8. Wrap the target key with the temporary AES key using the CKM_AES_KEY_WRAP_PAD algorithm, and append it to the wrapped key. For example:

```
openssl enc -id-aes256-wrap-pad -iv A65959A6 -K $( hexdump -v -e '/1 "%02x"' <
temp_aes_key ) -in target_aes_key >> wrapped_aes_key
```

9. List the files again. For example:

```
[root@machine-name-10-1-228-132 import_key_sample2]# ls -lrt
total 16
-rw-r--r--. 1 root root 451 Aug 5 11:15 rsa_public.pem
-rw-r--r--. 1 root root 32 Aug 5 11:19 temp_aes_key
-rw-r--r--. 1 root root 32 Aug 5 11:19 target_aes_key
-rw-r--r--. 1 root root 296 Aug 5 11:22 wrapped_aes_key
```

10. Base64-encode the wrapped AES key. For example:

```
[root@machine-name-10-1-228-132 import_key_sample2]# openssl enc -base64 -A -in
wrapped_aes_key

M65ZDVmHPMnT/bFE8idDaJnMeS+Pb/LB+vlJIsBCInnAI05UDtK0E7it6FoxAy0F
dQsYmJYqJJuOVjkMGX/Uid8N6vDhpHaX2NAQcJsVZMas2sW03gUaeqXcrlOcDKzb
CgAXbCovBMWEC46HZwqpiIZD8pqqRlxuMqb3m95/7TomPtZh7BYRbtWboJFtq1MA
ljzjwLTvUdcDZuMf03wHZhPZEaxrZKS68By2KLcHGS/oFvgSvAFH54doBJBRS2jP
tir5hxo/lma4BQuKwCebRyf9ugOKlGjEJt2DEmTAPAWZ257TxXCinY9ooLTouGY4
cdqBHimmTDVjgyg28u76poyqMZkUq9ZywVUf8onvEsaNSBERva3DbuoKEZSdbt/1
MHg/L1031Rg=
```

11. Copy the base64-encoded key into a file. This will be the key material used during the upload.

> ⚠ Remove any newline characters so the key is on a single line.

Importing a wrapped key using the API

Send the following POST request to import a wrapped key.

```
https://<VAULT_IP_or_FQDN>/token/1.0/key_import/
```

Use a request payload like the following.

```
{
  "cipher": "RSA-2048",
  "description": "Signing key",
  "key_material":
"MIHuAgEAMBAGByqGSM49AgEGBSuBBAAjBIHWMIHTAgEBBEIBJ2oatGhkdy1W6pS9xygCo8cEbnV/...iE55Z
A==",
  "keyset_guid": "b4e6b2a8-a693-40ab-9cb3-5f34cbf2227e",
  "name": "key1",
  "sha256": true,
  "wrapping_key_guid": "9b1f5a14-1f5f-4167-b3aa-257a8ce2944c"
}
```

See below for each parameter.

Parameter	Value
cipher	The cipher of the key. Only RSA-2048 is supported
description	The optional description of the key
key_material	The key material of the key that was used for wrapping
keyset_guid	The GUID (Globally Unique Identifier) of the key set where the key will be imported

Parameter	Value
name	The name of the key to be imported
sha256	`true` to use sha256to wrap the key; false to use `sha1`
wrapping_key_guid	The GUID of the key used for wrapping

Importing a wrapped key in the web GUI

See below for importing a wrapping key using the web GUI.

To import a key using the web GUI

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Manage > Keys**.
3. On the Keys page, select **Actions > Import Key**.
4. On the Import Key page, complete the following:

Field	Description
Name	Enter the name for the key.
Description	Enter the optional description for the key.
Algorithm	Select AES.
Key Length	Select 256.
Key Material	Select the wrapped AES key that you created and saved as a single line during the wrapping process
Wrapping Key	Select the RSA-2048 wrapping key that you created.
Wrapping Key Version	Select the wrapping key version.
Hashing Algorithm	Select SHA1 or SHA256.

5. Click **Import**.

Creating keys

See below for instructions on creating a key.

To create a key

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Manage > Keys**.
3. Click the **Create** icon.
4. In the Create Key dialog box, complete the following:
    - Name
    - Description
    - Algorithm
    - Key Length
5. Click **Create**.

Name

The name of the key

Description

An optional description for the key

Algorithm

Select the algorithm to use for the key. This can be one of the following:

- AES
- ARIA
- RSA
- DES
- DESede
- SEED
- HMAC
- EC
- ML-DSA (PQ algorithm)
- SLH-DSA (PQ algorithm)

⚠ If you want to use a key with a tokenization policy, it must be an AES key.

Key Length

Select the key length.

ℹ The EC algorithm uses a key curve instead of a key length.

Viewing key details

See below to view a key's details.

To view the details of a key

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Manage > Keys**.
3. On the **Manage Keys** page, click on the Name link for the key that you want to view.
4. In the **Details** tab of the **Key Details** page, check the following information:
    - Name
    - Status
    - Description

- Version
- Source
- Cipher
- Type
- Creation date

5. In the **Versions** tab of the Key Details page, check all versions of the key.

> The current version is enabled and depicted with a star. All other versions are disabled.

Editing keys

See below to change the status of an existing key or update its description.

To edit a key

1. Log in to the Vault web GUI.
2. From the Home tab, select **Manage > Keys**.
3. On the **Manage Keys** page, select the key that you want to edit.
4. Click the **Edit** icon.
5. Change the key status or update the description.
6. Click **Apply**.

Rotating keys

See below for rotating a key.

To rotate a key

1. Log in to the web GUI.
2. From the **Home** tab, select **Manage > Keys**.
3. On the **Manage Keys** page, select the key that you want to rotate.
4. Select **Actions > Rotate Key**.
5. On the confirmation screen, click **Rotate**.

Programming key deletion

See below for programming the deletion of a key.

> Deleting a key will not take effect immediately. However, applications will no longer be able to use the key.

To delete a key

1. Log in to the webGUI.
2. From the **Home** tab, select **Manage > Keys**.
3. On the **Manage Keys** page, select the key that you want to delete.
4. Click the **Delete** icon.
5. In the **Delete Key** dialog box, select the number of days after which the key should be permanently deleted.
6. Click **Delete Key**.

Canceling key deletion

See below for canceling the programmed deletion of a key.

To cancel the deletion of a key

1. Log in to the web GUI.
2. From the Home tab, select **Manage > Keys**.
3. On the **Manage Keys** page, select a key with the status of **Pending Deletion**.
4. Select **Actions > Cancel Deletion**.
5. In the confirmation window, click **Cancel Delete**.
6. Re-enable the key as explained in Editing keys.

Permanently deleting keys

See below to permanently delete a key programmed for deletion.

To permanently delete a key

1. Log in to the web GUI.
2. From the **Home** tab, select **Manage > Keys**.
3. On the **Manage Keys** page, select the key that you want to delete. The status should be **Pending Deletion**.
4. Click the **Delete** icon.
5. In the **Permanently Delete Key** dialog box, click **Permanently Delete Key**.

Setting the password policy for users

The password policy allows you to set the expiration date for all Vault users.

To set the password policy

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. In the top-right corner of the vault page, click the Settings icon.
3. On the Settings page, click the Password Policy tab.
4. Complete the following:

Option	Description
Password Expiration	The expiration value that you want to use for the password in months or days.
Minimum Length	The minimum length for the password.
Minimum Numbers	The minimum amount of numbers required in the password.
Minimum Lowercase Characters	The minimum amount of lowercase characters that must be included in the password.
Minimum Uppercase Characters	The minimum number of uppercase characters that must be included in the password.
Minimum Special Characters	The minimum number of special characters that must be included in the password.

5. Click **Save**.

Managing access policies and users

Add the required users and configure access policies to define who can access the vault, their role, and access level.

- The system creates a default admin policy. You can add users to this default policy. This is the only admin policy available for tokenization vaults.
- You create additional policies for users and add the required users to each policy.

See below for the roles granted to the Administrator and User access policies.

Role	Administrator	User
Access all tokenization policies	✓	✓
Create tokenization policies	✓	✓
Edit tokenization policies	✓	✗
Delete tokenization policies	✓	✗
Create local users	✓	✗
Manage all access policies to determine user access and roles	✓	✗
Manage the vault, including authentication and HSM configuration	✓	✗
View the audit log	✓	✓

See below for how to manage policies and users.

- Creating an access policy
- Editing an access policy
- Deleting an access policy
- Adding Cryptographic APIs users
- Editing Cryptographic APIs users
- Deleting Cryptographic APIs Users

If the vault is configured for Active Directory authentication, the Users tab does not appear, and you add AD users and groups directly in the access policy.

Creating an access policy

You create access policies and add users to policies to give them appropriate roles and access.

- The system creates a default admin policy for you. You can add users to the default admin policy. This is the only admin policy available for tokenization vaults.

- You create additional policies for users and add the required users to each policy.

To create an access policy

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Security > Access Policies**.
3. On the Manage Access Policies page, click the Create icon.
4. On the About tab of the Create Access Policy dialog box, complete the following:

Field	Description
Name	Enter the policy name.
Description	Optionally enter a description for the policy.
Role	Set this to User for all policies other than the admin policy.
Client Certificate for mTLS	To use mTLS with this policy, select the client certificate. Otherwise, leave this blank.
Users	Select the required users to be added to the policy. If the vault is configured for Active Directory authentication, select User or Group and search for the required AD user or AD group.

5. Click **Continue**.
6. On the Permissions tab of the Create Access Policy dialog box, select whether to grant All Permissions or Specific Permissions to the users.
7. If you selected Specific Permissions, check the checkboxes for each permission that you want to assign.
8. Click **Apply**.

Editing an access policy

You can edit an access policy to add or remove users, or update their permissions.

There must be a rescue user, and that user must be an administrator.

To edit an access policy

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Security > Access Policies**.
3. On the Manage Access Policies page, select the access policy that you want to edit.
4. In the About tab of the Edit Access Policy dialog box, you can update the following:

Field	Description
Description	Click Browse and select the Certificate Signing Request.
Client Certificate for mTLS	You can remove any assigned client certificates.

Field	Description
Users	Add and remove users from the policy as required. • For user access policies, you can add or remove users. • For the admin access policy, you can add or remove users from the policy and also the rescue user list.

5. Click the **Permissions** tab.
6. Select whether to grant **All Permissions** or **Specific Permissions** to the users.
7. If you selected **Specific Permissions**, check the checkboxes for each permission that you want to assign.
8. Click **Save** to save the policy but leave the window open, or click **Save and Close** to save the policy and close the window.

Deleting an access policy

You can delete an access policy if it is no longer required and no users or applications use it.

⚠ You cannot delete the default admin policy.

To delete an access policy

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. From the Home tab, select **Security > Access Policies**.
3. On the Manage Access Policies page, select the access policy you want to delete, then click the Delete icon.
4. On the confirmation screen, click **Delete**.

Adding Cryptographic APIs users

If the vault is configured for local authentication, you add users as described below to give them access to the vault. Users must also be added to policies as these determine their role and level of access.

If the vault is configured for Active Directory authentication, the Users tab does not appear, and you add AD users/groups directly in the access policy.

To add a Cryptographic APIs user

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs web GUI.
2. On the Home tab, select **Security > Users**.
3. On the **Manage Users** page, click the **Create** icon to add a user.
4. On the **Add User** dialog, enter the user's details:

Field	Description
Status	By default, the user account is enabled. If you do not want to activate the user account, set the status to DISABLED.
User Name	Enter a user name.
Full Name	Enter the user's full name.

Field	Description
Email	Enter the user's email address. The user will be notified about their account using this email address.
Password	Enter a password for the user.
Password Expiration	Enter the expiry date for the user's password.

5. Click **Add**. The user can't access the vault unless you add them to a policy. You can:
    - Add the user to an existing policy
    - Create a new policy
    - Select **Not Now** and add the user to a policy later

Editing Cryptographic APIs users

See below for editing Cryptographic API users.

To edit a Cryptographic API user

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs web GUI.
2. On the Home tab, select **Security > Users**.
3. On the **Manage Users** page, select a user and click the Edit icon.
4. On the **Edit User** dialog box, update the user's details as necessary.
5. Click **Apply**.

Deleting Cryptographic APIs Users

See below for deleting a Cryptographic APIs user.

> ⚠ You cannot delete a user that is part of an access policy. Update the access policy to remove the user before you delete them.

To delete a Cryptographic APIs user

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. On the Home tab, select **Security > Users**.
3. On the Manage Users page, select a user and click the Delete icon.
4. On the confirmation page, click **Delete**.

Managing Authentication for Vault for Cryptographic APIs

By default each vault is configured for local authentication. You can change the authentication method as required. In the current release, you can choose between local authentication, Active Directory, OpenID Connect (OIDC) with AD, or OIDC without AD.

> ℹ You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users.

For details on configuring each authentication option, see:

- Configuring local authentication for Vault for Cryptographic APIs
- Configuring Active Directory for the Vault for Cryptographic APIs
- Configuring OIDC with Active Directory for Vault for Cryptographic APIs
- Configuring OIDC for Vault for Cryptographic APIs
- Managing two-factor authentication in Vault for Cryptographic APIs

Configuring local authentication for Vault for Cryptographic APIs

Local authentication is enabled by default when you create a vault. If using local authentication, no further authentication configuration is required. The next step is to configure your access policies and users.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users

Configuring Active Directory for the Vault for Cryptographic APIs

See below for configuring Active Directory for the Vault for Cryptographic APIs.

> By default, the vault uses local authentication. You can change the authentication method as required.

To configure Active Directory

1. Log in to the CSP Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. On the Authentication page, select **LDAP** as the Authentication Type.
5. On the **Domain** tab, enter:
    - Domain Name—Enter the domain name for the service account.
    - Directory Service Type—Select **Microsoft AD** if you plan to use Microsoft AD directory services, or **OpenLDAP** for all non-Microsoft AD directory services.
    - Service Account Name—Enter the name of the service account for the given domain (for example, Administrator).

      > The service account needs read-only access to users and groups on the domain and any subdomain used.

    - Service Account Password —Enter the password for the service account.
    - UID Attribute—Enter the Security Manager Account Name (sAMAccountName) for the user.

      > This is the attribute of the user or group object that would be queried during search.

6. Click **Apply** to save the changes.
7. Click the **Domain Controllers** tab.
8. Click **+**
9. Add the following details in the **Add Domain Controller** window.
    - Server URL
    - STARTTLS
    - CA Certificate
    - User Search Context (Base DN)
    - Group Search Context (Base DN)

- Timeout

10. Click **Save and Close**.

Server URL

Select LDAP or LDAPS and enter the domain name or IP address. To include a port number, use the following syntax:

```
<ip>:<port>
```

STARTTLS

If you selected LDAP, check the checkbox if you want to use LDAP over TLS.

CA Certificate

The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller.

- The CA certificate must be in Base64-encoded PEM format.
- If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates.

Click Load File to select the CA certificate that you want to use.

User Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the user search should start. For performance reasons, make the base DN as specific as possible. For example:

```
dc=ldapserver,dc=com
```

This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP.

Group Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the search for Security groups should start.

This option applies to AD Security groups being associated with an admin group.

Timeout

Set the timeout in seconds before connecting to an alternate domain controller.

- If multiple domain controllers are specified, this is how long the Cryptographic Security Platform Vault waits for a response before re-sending the request to another domain controller.
- If the DNS server is down, Cryptographic Security Platform Vault may take longer than the time specified here before it fails over to the next domain controller in the list or considers the authentication request failed.

This option only applies to the TCP/LDAP request. It does not apply to the DNS request before the LDAP server has been successfully contacted.

Configuring OIDC with Active Directory for Vault for Cryptographic APIs

By default, the vault uses local authentication. You can change the authentication method as required, and you can have multiple authentication modes active at the same time. However, OIDC without Active Directory cannot be used with Active Directory, and OIDC with Active Directory cannot be used without Active Directory.

You cannot disable OIDC authentication once it is configured. After you enable OIDC, you can no longer sign in with AD credentials. However, you can sign in using local authentication credentials without any issues.

To configure OIDC

1. Log in to the Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. In the **Choose Authentication Type** drop-down menu, select:
    - **OpenID Connect** to configure OIDC without Active Directory
    - **OpenID Connect (with AD)** to configure OIDC with Active Directory
5. Click the **Learn more about configuring the OIDC Provider** link to view the OIDC provider's login redirect URL and logout redirect URL.
6. Specify the OpenID Connect Configuration settings:
    - Name
    - Client ID
    - Client Secret
    - Base URL
7. Optionally, click **Load File** to upload the CA certificate in base64-encoded PEM format.
8. Click **Apply**.
9. Select **Verify and Enable**. After verification, a message appears confirming OpenID Connect has been successfully enabled. Vault is set for OIDC authentication.
10. Sign out from the vault and sign in to the vault as an OIDC user by selecting **Sign in with IDAAS** and entering your OIDC credentials.

Name

A user-defined name for the OpenID Connect provider.

Cryptographic Security Platform Vault displays this name on the button in the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

⚠ This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Configuring OIDC for Vault for Cryptographic APIs

By default, the KeyControl Vault Management application is configured for local authentication. You can change the authentication method as required, but you can use only one type of authentication per vault at a time.

- If you want to use OIDC without AD, you can only change to that mode from the local authentication mode.
- If you have configured AD or OIDC with AD, you cannot change to OIDC without AD. You must rescue the vault, which returns the vault to **Local Authentication** mode. Then remove any additional users and policies, and configure OIDC without AD.

Each vault can be configured with a separate OIDC server or a separate application from same server.

⚠ OIDC without AD is the recommended mode of OIDC authentication method where the OIDC provider independently manages identity and authentication. For new OIDC setups, this is the preferred option.

To configure OIDC

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Choose Authentication Type** drop-down list, select **OpenID Connect**.
6. Specify the OpenID Connect Configuration settings:
   - Name
   - Client ID
   - Client Secret
   - Base URL
7. Optional. Click **Browse** to upload the CA Certificate.

   ℹ The certificate needs to be in base64 encoded pem format.
8. Enter the Admin Name and Admin Email for OIDC user. This user will be created and will act as the Vault Administrator. They will be assigned to the admin policy and receive the email with the registration URL.
9. Click **Apply**. The OpenID Connect Configuration window appears showing the current configuration.
10. Click **Verify and Enable**. The OpenID Connect Successfully Configured window displays the new login URL.
11. Copy the URL, and click **Log Out and Sign in with IDP**.
12. After you are logged out, paste the URL into the browser window.
13. Log in to the Identity Provider using the name and password that you created.

Name

A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

> ⚠ This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Managing two-factor authentication in Vault for Cryptographic APIs

Two-factor authentication requires you to enter two forms of identification before you can access your CSP Vault.

- The first form is your standard username and password combination,
- The second is a one-time password (OTP) generated by an authorization app. The OTP is appended to your existing password.

See below for how to enable and manage it.

- Requirements for enabling two-factor authentication in Vault for Cryptographic APIs
- Enforcing two-factor authentication in Vault for Cryptographic APIs
- Disabling two-factor authentication in Vault for Cryptographic APIs

> ℹ Two-factor authentication is supported with local authentication only. If you want to use two-factor authentication for non-local users, we recommend enabling it in your remote authentication provider.

Requirements for enabling two-factor authentication in Vault for Cryptographic APIs

Make sure you have access to an authentication app that can generate HOTP or TOTP passwords. For example:

- For TOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. These applications continuously generate passwords valid for 30 seconds. If the current password expires before you can submit the login request, you must wait for it to generate a new password, then use that to log in.
- For HOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. A password generated through the application is valid from the time you create it until you use it to log in. To log in again, click **Next** in the app to generate a new password.

Enforcing two-factor authentication in Vault for Cryptographic APIs

See below for enforcing two-factor authentication in Vault for Cryptographic APIs.

- Enforcing two-factor authentication for the current user
- Enforcing two-factor authentication for all users

Enforcing two-factor authentication for the current user

See below for enforcing two-factor authentication for the current user.

To enforce two-factor authentication for the current user

1. Log in to the Cryptographic Security Platform Vault for Cryptographic APIs webGUI.
2. In the top menu bar, click **Settings**.
3. In the **Two-Factor Authentication** field, click **Set up Two-Factor Authentication**.
4. In the **Enable Two-Factor** dialog box, select the HOTP or TOTP radio button.
5. Scan the generated barcode with your authorization app.
6. Enter the six-digit verification code from your app in the dialog box.
7. Click **Continue**. Cryptographic Security Platform Vault verifies the code and displays a message indicating success or failure. If the code is not correct, re-enter it.
8. After the code has been accepted, click **Done**.
9. When you log into the Vault web GUI:
    - Enter a valid OTP along with your standard account password on the login page. Do not add any characters or spaces between your account password and the one-time password generated by your authorization app. For example, if your password is `XyZ123$`, and your OTP is `32325`, you enter `XyZ123$32325` in the password field.
    - If you use TOTP, make sure your password doesn't expire before you submit the login request.

Enforcing two-factor authentication for all users

See below for enforcing two-factor authentication for all Vault users

To enforce two-factor authentication for all users

1. Log into the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the **Two-Factor Authentication Settings** page, select **ENFORCED**.
5. Click **Apply**.

Disabling two-factor authentication in Vault for Cryptographic APIs

See below for disabling two-factor authentication in Vault for Cryptographic APIs.

- Disabling two-factor authentication for a user
- Disabling two-factor authentication for all users

Disabling two-factor authentication for a user

See below to disable two-factor authentication for a single Vault user.

To disable two-factor authentication

1. Log in to the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Security**.
3. Select the **Users** tab
4. Select the user for whom you want to disable two-factor authentication.

5. In the **Details** tab below the table, click the **Enabled** link for the **Two-Factor Authentication** row.
6. In the **Disable Two-Factor Authentication** window, click **Proceed**.

Disabling two-factor authentication for all users

See below to disable two-factor authentication for all Vault users.

To disable two-factor authentication for all users

1. Log into the Cryptographic Security Platform Vault for Cryptographic APIs webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the Two-Factor Authentication Settings page, select **NOT ENFORCED**.
5. Click **Apply**.

CSP Vault for Databases

The CSP Vault for Databases lets you integrate KeyControl with external databases, such as Microsoft SQL Server, Oracle, MariaDB, and PostgreSQL. This lets you manage keys and encrypt sensitive data using Transparent Data Encryption (TDE).

- Databases supported by Vault for Databases
- CSP Vault for Databases with EnterpriseDB
- CSP Vault for databases with OpenSource PostgreSQL
- CSP Vault for Databases with MariaDB TDE
- Setting up Data Guard with Scripts
- Scripted Installation and Configuration for Oracle TDE
- CSP Vault with Oracle TDE
- CSP Vault as EKM Provider for Microsoft SQL Server
- Creating a Cloud VM Set for the CSP Vault for Databases
- Changing a Cluster Node Mapping for CSP Vault for Databases
- Creating a Cluster Node Mapping for CSP Vault for Databases
- Disabling a CloudKey or All CloudKey Versions
- Creating a CloudKey for TDE
- Creating a Key Set for TDE
- Managing Authentication for Vault for Databases

Databases supported by Vault for Databases

CSP Vault for Databases supports the following databases

- MariaDB
- Microsoft SQL Server
- Oracle TDE
- OpenSource PostgreSQL
- EnterpriseDB

MariaDB

The CSP Vault for Databases supports the following MariaDB versions:

- MariaDB 11.8 (LTS), 11.8.6 (latest)
- MariaDB 11.4 (LTS), 11.4.10 (latest)
- MariaDB 10.11 (LTS), 10.11.16 (latest)

- MariaDB 10.6 (LTS), 10.6.25 (latest)

On the following Linux (x86_64) platforms:

- RHEL 9.6
- Ubuntu 24.04

Microsoft SQL Server

The CSP Vault for Databases supports the following Microsoft SQL Server versions.

- Microsoft 2025 UEFI only
- Microsoft 2022 Enterprise Edition
- Microsoft 2022 Developer and Standard Editions
- Microsoft 2019 Enterprise Edition with Cumulative Update Package 18
- Microsoft 2019 Developer and Standard Editions
- Microsoft 2016 Enterprise Edition
- Microsoft SQL Server Management Studio versions 18.8 - 22

On the Windows Server platforms.

> On Windows 2025, installing the Policy Agent is only supported on the UEFI version of Windows.

Oracle TDE

The CSP Vault for Databases supports the following Oracle databases.

- Oracle 19C Single Node
- Oracle 19C RAC (supported for Oracle Linux only)
- Oracle 19C with Data Guard

On the following platforms:

- Oracle Linux (x86_64)
- AIX 7.3

OpenSource PostgreSQL

The CSP Vault for Databases supports the following OpenSource PostgreSQL versions.

- PostgreSQL 16
- PostgreSQL 17

On the following Linux (x86_64) platform:

- Ubuntu 22.04

EnterpriseDB

The CSP Vault for Databases supports the following EnterpriseDB versions.

- EDB 16.11.0

On the following Linux (x86_64) platforms

- Ubuntu 22.04

CSP Vault for Databases with EnterpriseDB

Cryptographic Security Platform Vault for Databases supports EnterpriseDB (EDB) PostgreSQL Advanced Server for column-level encryption. This allows you to encrypt specific columns in your database that contain sensitive information.

- Manually installing and registering the policy agent for EDB PostgreSQL
- Enabling TDE on EDB PostgreSQL database server
- Creating a key set for EDB PostgreSQL database server
- Creating a CloudKey for EDB PostgreSQL database server
- Configuring the EDB PostgreSQL database connector
- Configuring a cryptographic provider on the EDB PostgreSQL server
- Configuring the EDB PostgreSQL server for encryption
- Rotating EDB PostgreSQL keys
- Backing up and restoring EDB PostgreSQL
- Configuring EDB PostgreSQL scripted installation

Manually installing and registering the policy agent for EDB PostgreSQL

See below to manually install and register the policy agent for EDB PostgreSQL.

To manually install and register the Policy Agent:

1. Log in to the web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Download Policy Agent**.
4. Install the Policy Agent on your PostgreSQL Server VM.
5. Return to the web GUI and click **Workloads** in the top menu bar.
6. Select **Actions > Create New Cloud VM Set**.
7. On the **VM Set** tab, enter a name for the Cloud VM Set.
8. Select the group to which this set should belong.
9. Optionally enter a description for the set.
10. If you want to use the BoundaryControl feature, select the CloudControl app server link that you want to use.
11. After you finish specifying the Cloud VM Set options, click **Create**.
12. When you see the **Cloud VM Set Successfully Created** message, click **Close**.
13. Register the EDB PostgreSQL Server VM with Vault by running the following command:

```
hcl register -a <Cryptographic Security Platform Vault IP Address>
```

14. When prompted, enter the vault ID, username, and password for the Cryptographic Security Platform Vault.
15. The EDB PostgreSQL Server will display the available Cloud VM Sets. Select the Cloud VM Set that you want to use, and confirm your selection.

Enabling TDE on EDB PostgreSQL database server

Before you can use the EDB PostgreSQL Database Server VM for TDE, enable it.

To enable TDE

1. Log in to the command prompt on the PostgreSQL Database Server VM.
2. Run the following command:

```
hcl tde enable -y
```

Creating a key set for EDB PostgreSQL database server

See below for creating a key set for the EDB PostgreSQL Database Server.

To create a key set

1. Log in to the Cryptographic Security Platform Vault for Databases webGUI.
2. In the top menu bar, click **CloudKeys**.
3. Select **Actions > Create Key Set**.
4. On the **Details** tab of the **Create Key Set** dialog box, ensure that you select **PostgreSQL Database Server** for the Database type.
5. If you have an HSM, set the HSM properties.
6. Set the CloudKey rotation schedule.
7. Click **Apply**.

Creating a CloudKey for EDB PostgreSQL database server

See below for creating a CloudKey for an EDB PostgreSQL Database Server.

> Only keys created in the Cryptographic Security Platform Vault for Databases are supported.

To create a CloudKey

1. Log in to the Vault web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab and select the key set with which the CloudKey will be associated.
4. Select **Actions > Create CloudKey**.
5. On the **Details** tab of the **Create CloudKey** dialog box, enter the following:
    - Name—Enter the name for the CloudKey
    - Description—Enter the optional description for the CloudKey
    - Cipher—Select AES-256
6. Click **Continue**.
7. On the **Schedule** tab, determine the rotation schedule for the CloudKey. This can be one of the following:
    - Inherit from Key Set—The CloudKey will use the Key Set's default schedule. If the Key Set schedule changes after you create the CloudKey, the CloudKey schedule will not update.
    - Never—The CloudKey will never be rotated.
    - Once a year—The CloudKey will be rotated once a year.
    - Every 6 months—The CloudKey will rotate every 6 months.
    - Every 30 days—The CloudKey will rotate every 30 days.
    - Other—The CloudKey will be rotated at the interval you select.
8. Choose when this CloudKey version should expire. The per-version expiration can be one of the following:
    - Never—The CloudKey version will never expire.
    - Fixed Date—All CloudKey versions will expire on the date that you set.
    - Relative Expiry—Each CloudKey version will expire after the number of days that you set.
9. Choose when the CloudKey should expire. This can be **Never**, or you can choose a specific date.
10. If you selected an expiration date, choose the Expire Action to define what happens to the CloudKey when it expires. This can be one of the following:
    - Disable—The key will remain in the cloud, but is disabled and cannot be used by any applications.
    - Delete—The key is disabled in the cloud and cannot be used by any applications. You can set the date for permanent deletion.
11. Click **Apply**.

Configuring the EDB PostgreSQL database connector

See below for configuring the EDB PostgreSQL database connector.

To configure a database connector

1. Log in to the Vault web GUI.
2. In the top menu bar, click **CloudKeys**.
3. Select the PostgreSQL Key Set that you created
4. Click the **Database Connectors** tab in the bottom half of the screen.
5. Select **Actions > Create Connector**.
6. In the **Create Database Connector** dialog box, enter the following:

Field	Description
VM Name	Enter the name for the PostgreSQL Database Server VM.
Connector Name	Enter the name to use for the database connector.
Expiration	Select Never (the database connector will never expire) or Choose a date (the database connector will expire on the selected date)

7. Click **Create**. If the database connector is created correctly, you will see it listed in the table beneath the **Database Connectors** tab as **ENABLED**.
8. Select the database connector that you just created
9. Select **Actions > Generate Access Token**.
10. On the **Generate Access Token** window, the new access token is created and displays both an identity and a secret. Copy these to use when configuring the cryptographic provider.

Configuring a cryptographic provider on the EDB PostgreSQL server

See below for configuring a cryptographic provider on the EDB PostgreSQL server.

> ⚠ You must have created a database connector and an access connector before you can configure the cryptographic provider.

To configure a cryptographic provider

1. In your EDB PostgreSQL Server VM, navigate to the directory where you installed the Policy Agent.
2. Create the following configuration file:

```
opt/hcs/etc/edb-psql.conf
```

3. In this file, paste the text from the Access Token (**Identity** and **Secret**). The file should be in JSON format similar to the following:

```
{
    "identity" : "postgres_connector",
    "secret" : "S3XsZJe/EPNVf2D/YufOUS2HuOsLfKJBKjp3Zx...CExetFk="
```

```
}
```

Alternatively, you can directly provide the copied Access Token to the `open_session()` function.

Configuring the EDB PostgreSQL server for encryption

See below for configuring the EDB PostgreSQL server for encryption.

- Logging in to the EDB PostgreSQL server
- Exporting the wrapping variables
- Enabling encryption
- Starting the server
- Verifying encryption

Logging in to the EDB PostgreSQL server

Log in to the EDB PostgreSQL server as the EDB user:

```
su - enterprisedb
```

Exporting the wrapping variables

Export the variables needed to wrap and unwrap the EDB Data Encryption Key.

```
export PGDATAKEYWRAPCMD='/opt/hcs/bin/htkey encrypt --config-file <config-file-path>
--key-name <key-name> --out-file "%p"'
export PGDATAKEYUNWRAPCMD='/opt/hcs/bin/htkey decrypt --config-file <config-file-
path> --in-file "%p"'
```

Where:

- `<config-file-path>` is the absolute path of the Access Token file previously created.
- `<key-name>` is the CloudKey previously created.

Enabling encryption

Enable database encryption.

```
/usr/lib/edb-as/16/bin/initdb -D <data> --data-encryption
```

Where <data> is the path of an empty data directory. For example:

```
/var/lib/edb-as/16/main
```

The command may fail with the following error:

```
sh: 1: /opt/hcs/bin/htkey: not found
```

If this happens, you will need to convert the htkey file to UNIX format using the following command:

```
dos2unix /opt/hcs/bin/htkey
```

Starting the server

Run the following command to start the server.

```
/usr/lib/edb-as/16/bin/pg_ctl start -D /var/lib/edb-as/16/main
```

Verifying encryption

Verify that encryption is enabled.

```
select data_encryption_version from pg_control_init();
```

Rotating EDB PostgreSQL keys

For EDB PostgreSQL, we highly recommend rotating keys only manually because key rotation in EDB will not change the Data Encryption Key (DEK). Only the wrapping key rotates.

- Manually rotating the CloudKey wrapping
- Manually rotating the key in EDB PostgreSQL
- Rewrapping the data encryption key

Manually rotating the CloudKey wrapping

See below for manually rotating the CloudKey wrapping

To rotate the CloudKey wrapping

1. Log in to the Vault web GUI.
2. In the top menu bar, click **CloudKeys**.
3. Select the **CloudKeys** tab, and then select the appropriate Key Set.
4. Select the specific CloudKey you want to apply scheduled key rotation to.
5. Select the Details tab and then click **Rotate Now** in the Rotation Schedule row.
6. Click **Save**.

Manually rotating the key in EDB PostgreSQL

After you have rotated the CloudKey, run the following:

```
cd $PGDATA/pg_encryption/
/opt/hcs/bin/htkey decrypt --config-file <config-file-path> --in-file key.bin | /opt/
hcs/bin/htkey encrypt --config-file <config-file-path> --key-name <key-name> --out-
file key.bin.new
```

```
mv key.bin.new key.bin
```

Where:

- `<config-file-path>` is the absolute path of the Access Token file.
- `<key-name>` is the CloudKey that you just rotated.

Rewrapping the data encryption key

After you rotate the wrapping key, you will need to rewrap the DEK (Data Encryption Key) located at the following path.

```
$PGDATA/pg_encryption/key.bin
```

Backing up and restoring EDB PostgreSQL

See below to back up and restore an EDB PostgreSQL database on the same virtual machine.

- Requirements to restore an EDB PostgreSQL database
- Logging into the virtual machine
- Starting EDB PostgreSQL
- Creating a database in EDB PostgreSQL
- Verifying the database name
- Backing up the EDB PostgreSQL database
- Restarting the EDB PostgreSQL database
- Restoring the EDB PostgreSQL backup

⚠ To restore your EDB PostgreSQL database on a different virtual machine, we recommend using the scripted version.

Requirements to restore an EDB PostgreSQL database

You must have the following:

- Access to the VM as the enterprisedb user.
- PostgreSQL EDB (version 16) installed at:

  ```
  /usr/lib/edb-as/16/
  ```

- Encryption keys configured and accessible via the database vault.

Logging into the virtual machine

Run the following commands to log into the virtual machine with the `<vm-ip>` hostname or IP address.

```
ssh root@<vm-ip>
su - enterprisedb
```

Starting EDB PostgreSQL

Run the following command to start the EDB PostgreSQL database.

```
/usr/lib/edb-as/16/bin/pg_ctl start -D /var/lib/edb-as/16/main
```

Creating a database in EDB PostgreSQL

Create a database and a table. For example:

```
psql -U enterprisedb
CREATE DATABASE mydb;
\c mydb
CREATE TABLE test_table (id INT, name TEXT);
INSERT INTO test_table VALUES (1, 'Alice'), (2, 'Bob');
```

In this example:

- `mydb` is the specific database name
- `test_table` is the specific table name

Verifying the database name

Run the following command to verify the database name.

```
psql -U enterprisedb -l
```

Backing up the EDB PostgreSQL database

Generate an encrypted backup of the EDB PostgreSQL database

```
pg_dumpall -U enterprisedb -f <backup>.sql
```

Where `<backup>.sql` is the backup file name.

Restarting the EDB PostgreSQL database

Restart the database if needed:

```
/usr/lib/edb-as/16/bin/pg_ctl restart -D /var/lib/edb-as/16/main
```

Restoring the EDB PostgreSQL backup

Run the following command to restore the backup:

```
psql -U enterprisedb -d mydb -f <backup>.sql
```

Where `<backup>.sql` is the name of the backup file.

Configuring EDB PostgreSQL scripted installation

You can now use scripts to install and configure EDB PostgreSQL TDE on the Cryptographic Security Platform Vault for Databases. This simplifies the setup process.

- Downloading the TDE script bundle for EDB PostgreSQL
- Setting up the Entrust client using scripts for EDB

Downloading the TDE script bundle for EDB PostgreSQL

See below to download the TDE (Transparent Data Encryption) script bundle for EDB PostgreSQL.

> ⚠ Before you download the TDE script bundle, make sure you've created a Cryptographic Security Platform Vault for Databases and can log in to the webGUI.

To download the TDE script bundle

1. Log in to the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Download TDE script bundle**.
4. On the Download TDE script bundle dialog box, complete the following:

Field	Description
Name	Select a name to identify this database. This name will be used for the .zip bundle you download, and also as a prefix for related assets such as the KeySet and the Cloud VM Set.
Database Type	Select PostgreSQL Database Server.
Enable HSM	If you have an HSM configured, check the Enable HSM checkbox to protect your TDE master keys with the HSM. You will need to verify the HSM connection before you can proceed.
CSP Nodes Mapping	Optionally select the name of your Node Mapping.

5. **Click Continue**.
6. On the TDE Script Bundle Details dialog box, review your choices and click **Download**.

Setting up the Entrust client using scripts for EDB

See below to set up the Entrust client application using the EDB (EnterpriseDB) PostgreSQL scripts.

- Copying the scripts to the first node
- Configuring the script execution
- Running the setup script on the first node

- Running the setup script on the second node

Copying the scripts to the first node

Copy the script bundle to the first EDB PostgreSQL Server node. Extract the bundle contents on a folder.

File	Description
entrust.conf	Configuration file with some pre-populated values
setup.sh	Bash script signed with the Entrust signature. Do not modify

Configuring the script execution

Add the path of the `pg_config` PostgreSQL utility program path to the PATH variable. For example, for Ubuntu 22.04:

```
export PATH="/usr/edb/as-common/bin/:$PATH"
```

Ensure that `pg_config` is accessible from the shell:

```
pg_config --version
```

Running the setup script on the first node

Run the setup.sh script as follows:

```
./setup.sh first entrust.conf
```

Where:

- `first` is the node you are updating. This can be either first or other.
- `entrust.conf` is the name of the configuration file that you downloaded.

If setup is successful, it prints the path of the Access Token file.

⚠ Please note this path, as you'll use it later.

Running the setup script on the second node

If you have a second PostgreSQL server node in your cluster:

1. Copy the script bundle to the second node
2. Extract the bundle contents.
3. Run the setup script as follows:

```
./setup.sh other entrust.conf
```

CSP Vault for databases with OpenSource PostgreSQL

Cryptographic Security Platform Vault for Databases supports PostgreSQL for column-level encryption. This allows you to encrypt specific columns in your database that contain sensitive information.

- Configuring Vault Authentication for CSP Vault for Databases
- Backup and Restore
- Key Rotation
- Functions provided by the Entrust PostgreSQL Extension
- Encrypting and Decrypting Data using the PostgreSQL Server
- Configuring the PostgreSQL Database Server
- Configuring a Cryptographic Provider on the PostgreSQL Server
- Configuring the PostgreSQL Database Connector
- Creating a CloudKey for PostgreSQL Database Server
- Creating a Key Set for PostgreSQL Database Server
- Enable TDE on PostgreSQL Database Server
- Manually Installing and Registering the Policy Agent for PostgreSQL
- Installing PostgreSQL

Configuring Vault Authentication for CSP Vault for Databases

By default each vault is configured for local authentication. You can change the authentication method as required. In the current release, you can choose between local authentication, Active Directory, OpenID Connect (OIDC) with AD, or OIDC without AD.

> Note: You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users.

For details on configuring each authentication option, see:

- Configuring Active Directory for the CSP Vault for Databases
- Configuring Local Authentication for CSP Vault for Databases
- Configuring OIDC for the CSP Vault for Databases

Configuring Active Directory for the CSP Vault for Databases

By default the vault is configured for local authentication. You can change the authentication method as required.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. On the Authentication page, select **LDAP** as the Authentication Type.
5. On the Domain tab, enter:

Field	Description
Domain Name	Enter the domain name for the service account.
Directory Service Type	If you plan to use Microsoft AD directory services, select Microsoft AD. Select OpenLDAP for all non-Microsoft AD directory services.

Field	Description
Service Account Name	Enter the name of the service account for given domain. For example: Administrator. The service account needs read-only access for users and groups on the domain and any subdomain that is used. Note: The service account name and password is required.
Service Account Password	Enter the password for the service account.
UID Attribute	Enter the Security Manager Account Name (sAMAccountName) for the user. This is the attribute of the user or group object that would be queried during search.

6. Click **Apply** to save the changes.
7. Click the Domain Controllers tab.
   To add a controller, select **+**. The Add Domain Controller window appears.
   Add the following details:

Field	Description
Server URL	Select LDAP:// or LDAPS://, then enter the domain name or IP address. To include a port number, enter `<ip-address>:<port>`.
STARTTLS	If you selected LDAP, check the checkbox if you want to use LDAP over TLS. Note: This is not available if you selected LDAPS.
CA Certificate	The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller. The CA certificate must be in Base64-encoded pem format. If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates. Click Load File to select the CA certificate that you want to use.

Field	Description
User Search Context (Base DN)	Enter the Distinguished Name (DN) of the node where the search for users should start. This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP. For performance reasons, the base DN should be as specific as possible. For example, `dc=ldapserver,dc=com`.
Group Search Context (Base DN)	Enter the Distinguished Name (DN) of the node where the search for Security groups should start. This option applies to AD Security groups being associated with a Cloud Admin Group.
Timeout	Set the timeout in seconds before connecting to an alternate domain controller. If multiple domain controllers are specified, this is the amount of time Cryptographic Security Platform Vault waits for a response before it re-sends the request to another domain controller. This option only applies to the TCP/LDAP request. It does not apply to the DNS request before the LDAP server has been successfully contacted. If the DNS server is down, Cryptographic Security Platform Vault may take longer than the length of time specified here before it fails over to the next domain controller in the list or it considers the authentication request to have failed.

8. Click **Save and Close**.

If you want to add an Active Directory Group, complete the following:

1. From the Cryptographic Security Platform Vault for Databases webGUI, in the top menu bar, click **Security**.
2. Click the Groups tab.
3. Select **Actions > Create Group**.
4. On the Group tab, enter the name of the group and click **Next**.
5. On the Active Directory Groups tab, type the first three letters of the group to fetch the group name from the AD server.
6. Click **Next**.
7. On the KeyControl Managed User Members tab, select the managed users that you want to assign and click the right arrow icon.
8. Click **Create**.

For information on using Cloud Admin groups with this Cryptographic Security Platform Vault, see Cloud Admin Groups and CSP Vault User Accounts.

Configuring Local Authentication for CSP Vault for Databases

Local authentication is enabled by default when you create a vault. If using local authentication, no further authentication configuration is required. The next step is to configure your access policies and users..

> Note: You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users.

Configuring OIDC for the CSP Vault for Databases

By default the vault is configured for local authentication. You can change the authentication method as required, and you can have multiple authentication modes active at the same time. However, OIDC without Active Directory cannot be used with Active Directory or OIDC with Active Directory.

> Note: If you want to use OIDC without AD, you can only change to that mode from the local authentication mode. If you have configured AD or OIDC with AD, you cannot change to OIDC without AD.

Each vault can be configured with a separate OIDC server or a separate application from same server.

For an example of how to configure an OIDC provider, see Example: Configuring Entrust Identity as a Service. If you are using a cluster, even though you configure OIDC for only one node, you will need to enter the Callback URIs (the Login Redirect URIs and Logout Redirect URIs) for all nodes in the cluster.

Important: OIDC without AD is the recommended mode of OIDC authentication method where the OIDC provider independently manages identity and authentication. For new OIDC setups, this is the preferred option.

Procedure

1. Log into the Cryptographic Security Platform Vault for Databases webGUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. In the Choose Authentication Type drop-down menu, select **OpenID Connect**.
   Click the **Learn more about configuring the OIDC Provider** link to view the login redirect URL and the logout redirect URL for the OIDC provider.
5. Specify the OpenID Connect Configuration settings:

Field	Description
Client ID	The organizational identity assigned by the OpenID Connect provider when you sign up for the service.
Client Secret	A cryptographic component used to secure the organization's access to the OpenID Connect provider. Important: This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.
Base URL	The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Field	Description
Name	A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.

6. Optional. Click **Load File** to upload the CA certificate.
   Note: The certificate needs to be in base64 encoded pem format.
7. Click **Apply**.
   A dialog box displays the configuration.
8. Select **Verify and Enable**.
   After the verification, a message appears confirming OpenID Connect has been successfully enabled. The vault is now set for OIDC authentication.
9. Sign out from the vault and sign in to the vault as an OIDC user.
   To sign in as an OIDC user, select **Sign in with IDAAS** and enter your OIDC credentials.
   Important: You cannot disable OIDC authentication once it is configured. After OIDC is enabled you cannot sign in using AD credentials. However, you can sign in using local authentication credentials without any issues.

Backup and Restore

he simplest way to back up and restore a PostgreSQL database us by using pg_dump for backup and pg_restore for restoration. For more information, see https://www.postgresql.org/docs/8.1/backup.html.

Backup your PostgreSQL Database

Backup your PostgreSQL database by running the following command:

Copy

```
pg_dump -U <your_username> -d <your_database> -F c -f backup.dump
```

Where:

- **-U <your_username>** specifies the PostgreSQL user.
- **-d <your_database>** specifies the name of the database to back up.
- **-F -c** specifies the format (c for custom, t for tar, p for plain text).
- **-f backup.dump** specifies the output file.

Restoring your PostgreSQL Database on a Same VM

1. Restore the backup and exit from the PostgreSQL console:
   Copy
   ```
   pg_restore -U <your_username> -d <your_database> -F c backup.dump
   ```
2. Restart PostgreSQL:
   Copy
   ```
   systemctl restart postgresql
   ```
3. Login to the PostgreSQL server:
   Copy
   ```
   sudo -u postgresql psql
   ```
4. Ensure the Entrust PSQL extension is created:
   Copy

```
CREATE EXTENSION IF NOT EXISTS entrust_psql_extension;
```

Restoring your PostgreSQL Database on a Different VM

1. After the backup is complete, share the folder to the new backup location.
   Copy
   ```
   scp backup.dump user@destination_host:/tmp/backup.dump
   ```
   Where user@destination_host is the new location for the backup.
2. Install the Policy Agent in the new directory and configure it. For more information, see Manually Installing and Registering the Policy Agent for PostgreSQL.
3. Enable TDE. For more information, see Enable TDE on PostgreSQL Database Server.
4. Create the database connector in the same Key Set that was used to encrypt the backed up data, then generate the access token and store it in a file. For more information, see:
   - Configuring the PostgreSQL Database Connector
   - Configuring a Cryptographic Provider on the PostgreSQL Server
5. Restore your database:
   Copy
   ```
   pg_restore -U <your_username> -d <your_database> -F c /tmp/backup.dump
   ```
6. Restart PostgreSQL:
   Copy
   ```
   systemctl restart postgresql
   ```
   Login to the PostgreSQL server:
   Copy
   ```
   sudo -u postgresql psql
   ```
7. Ensure the Entrust PSQL extension is created:
   Copy
   ```
   CREATE EXTENSION IF NOT EXISTS entrust_psql_extension;
   ```

Key Rotation

Key rotation in PostgreSQL involves updating the encryption key used to secure data. When a key rotation occurs, it's important to manage sessions and data encryption carefully to ensure security and consistency.

After key rotation, any open sessions should be closed. This ensures that the old key is no longer in use. Once the sessions are closed, open a new session and use the get_key() function to fetch the latest key version. This new key version will be used to encrypt any new data.

It's important to note that after key rotation, older data remains encrypted with the previous key version. Only new data will be encrypted with the latest key version. If you need to re-encrypt older data with the new key, you must first decrypt the data using the old key and then encrypt it again using the new key version.

Scheduled Key Rotation

You can set up scheduled key rotation either on the Key Set or on the CloudKey.

Scheduled rotation on the Key Set:

1. Log into the Cryptographic Security Platform Vault for Databases webGUI.
2. In the top menu bar, click **CloudKeys**.
3. Select the **Key Sets** tab, and then select the specific Key Set on which you want to apply scheduled key rotation.
4. Select the Details tab and update the Default Rotation Schedule.

If there are existing CloudKeys in the Key Set, you can update the rotation schedule of the CloudKeys to align with your new Key Set rotation schedule by checking the Apply to all CloudKeys checkbox.

5. Click **Save**.

Scheduled rotation on the CloudKey:

1. Log into the Cryptographic Security Platform Vault for Databases webGUI.
2. In the top menu bar, click **CloudKeys**.
3. Select the **CloudKeys** tab, and then select the appropriate Key Set.
4. Select the specific CloudKey on which you want to apply scheduled key rotation.
5. Select the Details tab and update the Rotation Schedule.
6. Click **Save**.

Manually Rotating a CloudKey

1. Log into the Cryptographic Security Platform Vault for Databases webGUI.
2. In the top menu bar, click **CloudKeys**.
3. Select the **CloudKeys** tab, and then select the appropriate Key Set.
4. Select the specific CloudKey on which you want to apply scheduled key rotation.
5. Select the Details tab and then click **Rotate Now** in the Rotation Schedule row.
6. Click **Save**.

Functions provided by the Entrust PostgreSQL Extension

1. open_session()
   Copy
   ```
   open_session(access token file path) returns void
   ```

   ```
   open_session(access token) returns void
   ```

   The open_session() function is responsible for creating a session. It reads the access token either from a file or directly as a parameter. Once the access token is obtained, the function stores it in cache for subsequent use.
   For example:
   Copy
   ```
   select open_session('file:///opt/hcs/etc/psql.conf');
   ```

2. close_session()
   Copy
   ```
   close_session() returns void
   ```

   The close_session() function is used to close a session. This function will remove the access token and keys from the cache.
   For example:
   Copy
   ```
   select close_session();
   ```

3. get_key()
   Copy
   ```
   get_key(keyname) returns key handle (INTEGER)
   ```

   The get_key() function is used to fetch a key from the Cryptographic Security Platform Vault for Databases. It stores the key in the cache and returns the key handle.
   For example:
   Copy

```
select get_key('master-key1') as handle \gset
```

4. encrypt_data(text, key_handle)
   Copy
   ```
   encrypt_data(data TEXT, keyhandle INTEGER) returns TEXT
   ```
   The encrypt_data() function is used to encrypt the provided TEXT type data. It has two parameters: data and key_handle. The key_handle is returned by the get_key() function. It returns encrypted TEXT data.
   For example:
   Copy
   ```
   insert into users (name, credit_card_details) values ('John', encrypt_data('my_details', :handle));
   ```
5. decrypt_data()
   Copy
   ```
   decrypt_data(encrypted_data TEXT) returns TEXT
   ```
   The decrypt_data() function is used to decrypt TEXT type data. It also verifies the integrity of the data during decryption. It returns decrypted TEXT data.
   For example:
   Copy
   ```
   select name, decrypt_data(credit_card_details) from users;
   ```
6. encrypt_data_bytea()
   Copy
   ```
   encrypt_data_bytea(data BYTEA, keyhandle INTEGER) returns BYTEA
   ```
   The encrypt_data_bytea() function is used to encrypt the provided BYTEA type data. It has two parameters: data and key_handle. The key_handle is returned by the get_key() function. It returns encrypted BYTEA data.
   For example:
   Copy
   ```
   insert into users (name, bytea_details) values ('John', encrypt_data_bytea(E'\\xDEADBEEF', :handle));
   ```
7. decrypt_data_bytea()
   Copy
   ```
   decrypt_data_bytea(encrypted_data BYTEA) returns BYTEA
   ```
   The decrypt_data_bytea() function is used to decrypt BYTEA data. It also verifies the integrity of the data during decryption. It returns decrypted BYTEA data.
   For example:
   Copy
   ```
   select name, decrypt_data_bytea(bytea_details) from users;
   ```

Encrypting and Decrypting Data using the PostgreSQL Server

Before you can encrypt and decrypt data using the PostgreSQL server, you must create the Entrust PSQL Extension. For more information on the functions included in the extension, see Functions provided by the Entrust PostgreSQL Extension.

1. Log in to the PostgreSQL server using the following command:
   Copy
   ```
   sudo -u postgres psql
   ```
2. Create the Entrust PSQL Extension using the following command:
   Copy

```
CREATE EXTENSION IF NOT EXISTS entrust_psql_extension;
```

Perform Encryption and Decryption

To encrypt and decrypt data on a PostgreSQL Server using the Entrust PostgreSQL Extension functions, follow these steps:

1. Open Session—This will read the access token and store it in memory using the open_session() function.
2. Fetch Key—Use the get_key() function to fetch the key and store it in cache. This function returns a key handle that will be used to encrypt the data.
3. Encrypt Data—Pass the data and key handle to the encryption function.
4. Decrypt Data—Provide the encrypted data to the decryption function. This function will return the plaintext data.
5. Close Session—Use close_session() to close the current session and clean the key cache.

Example

1. Create a table.
   Copy
   ```
   create table users (name VARCHAR(100), credit_card_details text);
   ```
2. Open the session using the Access Token file path.
   Copy
   ```
   select open_session('file:///opt/hcs/etc/psql.conf');
   ```
3. Fetch the key. refers to the CloudKey that you created. See Creating a CloudKey for PostgreSQL Database Server.
   Copy
   ```
   select get_key('master-key1') as handle \gset
   ```
4. Encrypt and insert the encrypted data into the table.
   Copy
   ```
   insert into users (name, credit_card_details) values ('John', encrypt_data('my_details', :handle));
   ```
5. Decrypt the data.
   Copy
   ```
   select name, decrypt_data(credit_card_details) from users;
   ```
6. Close the session.
   Copy
   ```
   select close_session();
   ```

Configuring the PostgreSQL Database Server

You will need to log into the PostgreSQL database server to configure it.

1. Create a symbolic link of the extension file entrust_psql_extension_{posgresql_version}.so to the PostgreSQL Server VM lib directory, where {postgresql_version} is the major version of PostgreSQL. For example:
   Copy
   ```
   ln -s </pa_installation_directory_path/lib/entrust_psql_extension_{postgresql_version}.so </
   path_of_postgresql_extension_directory/entrust_psql_extension_{postgresql_version}.so
   ```
   To find your PostgresSQL version, run the following:
   Copy

```
postgres=# select version();
version
------------------------------------------------------------------------------------------------------------------------
PostgreSQL 16.8 (Ubuntu 16.8-1.pgdg24.04+1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu
13.3.0-6ubuntu2~24.04) 13.3.0, 64-bit
```

Note: The lib/extension directory may be different depending on the Linux distribution. For Ubuntu it is /usr/lib/postgresql/16/lib/.

2. Create a symbolic link of the sql and control file to the share/extension directory of PostgreSQL Server VM. The share/extension directory may be different depending on the Linux distribution. For example, for Ubuntu it is /usr/share/postgresql/16/extension/.
   SQL example:
   Copy
   ```
   ln -s </pa_installation_directory_path/postgresql/entrust_psql_extension--1.0.sql </
   path_of_postgresql_extension_share_directory/entrust_psql_extension--1.0.sql
   ```
   Control file example:
   Copy
   ```
   ln -s </pa_installation_directory_path/postgresql/entrust_psql_extension.control </
   path_of_postgresql_extension_share_directory/entrust_psql_extension.control
   ```
3. Log in to PostgreSQL. For example:
   Copy
   ```
   sudo -u postgres psql
   ```
4. Run the PostgreSQL query to create the extension. For example:
   Copy
   ```
   CREATE EXTENSION entrust_psql_extension;
   ```

Configuring a Cryptographic Provider on the PostgreSQL Server

You must have created a database connector and an access connector before you can configure the cryptographic provider.

1. In your PostgreSQL Server VM, navigate to the directory where you installed the Policy Agent.
2. Create a config file **psql.conf** inside the /etc directory using the text from the Access Token (**Identity** and **Secret**). The file should be in json format similar to the following:

```
{
   "identity" : "postgres_connector", "secret" :
   "S3XsZJe/EPNVf2D/YufOUS2HuOsLfKJBKjp3Zx/
JIrODqWYRQaYiFWnqet4lPsW0VcvGSvH7yB9BUZIxGi7CaM68cZFtw6yY5IvaCl
   wD3344MFy28U9zjc0ayFRoHQi/
Dv25xTZ8a2JLlxJRyavO2VNGaCPUZfFsPN4lZg3EZwJ3fNKa7Owfpk0AuHmWmcqcYsxNnUxPuc+VY
   qXZk17omHzYP/sA86RCv6+825t0EvuQhDHF7PxSiHjn+VShCYKNb+RxAvLgllP/eVx0k/HWWI6/
bZPpxwjFtw3tqnJ/8toqPD+f+ZUl

YT0mFRuE7BExGFf5LBCaVwf5FXKcOeXdaAg8zvaq0ynUjSB9JVw5FP6ZtFrY22hUcFcYDPlTpjMzUzs
X9d5BM8BhyTLmoPkj4lMyrSh
   3/nwGlJqPLj92EylmKsSOtOP6irpN22A2omvTsXUP/
pajuGrtUsKqzDdhAj+qmR2IDkSdOQMoSSvAgWylAuS6q8WdMvm8SVCVUZpQrL
```

vm226NvfvGCHKKNZaQCdxvL4XIgKI/tCt+F+Xx0Pk/
bkPgLby90IM5NtktRkroxakhGkgSnoyDj2KovGvIwrHLpFpvDJkCwxbBce+Op
cOjxR2tZ3nDM2zoZraSviT0P+V2hh7Z0jAWd4YrRdooxtQc3VPjTOrdOBldCExetFk="
}

Alternatively, you can directly provide the copied Access Token to the open_session() function.

Configuring the PostgreSQL Database Connector

Before creating the Database Connector, you must ensure you have enabled TDE on the PostgreSQL Database Server VM. See Enable TDE on PostgreSQL Database Server . After you create the connector, you can generate an access token to be used to configure the cryptographic provider.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI.
2. In the top menu bar, click **CloudKeys**.
3. Select the PostgreSQL Key Set that you created, and click the **Database Connectors** tab in the bottom half of the screen.
4. Select **Actions > Create Connector**.
5. In the Create Database Connector dialog box, enter the following:

Field	Description
VM Name	Enter the name for the PostgreSQL Database Server VM.
Connector Name	Enter the name to use for the database connector.
Expiration	Select one of the following: • Never—The database connector will never expire. • Choose a date—The database connector will expire on the selected date.

6. Click **Create**.
   If the database connector is created correctly, you will see it listed in the table beneath the Database Connectors tab as ENABLED.
7. Select the database connector that you just created, and select **Actions > Generate Access Token**.
   On the Generate Access Token window, the new access token is created and displays both an identity and a secret. You will need to copy these to use when configuring the cryptographic provider.

Creating a CloudKey for PostgreSQL Database Server

Only keys created in the Cryptographic Security Platform Vault for Databases are supported.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the CloudKeys tab and select the Key Set with which the CloudKey will be associated.
4. Select **Actions > Create CloudKey**.
5. On the Details tab of the Create CloudKey dialog box, enter the following:

Field	Description
Name	Enter the name for the CloudKey.
Description	Enter the optional description for the CloudKey.
Cipher	Select AES-256.

6. Click **Continue**.
7. On the Schedule tab, determine the rotation schedule for the CloudKey. This can be one of the following:
   - Inherit from Key Set—The CloudKey will use the default schedule from the Key Set. If the Key Set schedule changes after the CloudKey is created, the CloudKey schedule will not be updated.
   - Never—The CloudKey will never be rotated.
   - Once a year—The CloudKey will be rotated once a year.
   - Every 6 months—The CloudKey will be rotated once every 6 months.
   - Every 30 days—The CloudKey will be rotated once every 30 days.
   - Other—The CloudKey will be rotated at the interval you select.
8. Choose when this version of the CloudKey should expire. The per version expiration can be one of the following:
   - Never—The CloudKey version will never expire.
   - Fixed Date—All CloudKey versions will expire on the date that you set.
   - Relative Expiry—Each CloudKey version will expire after the number of days that you set.
9. Choose when the CloudKey as a whole should expire. This can be Never, or you can choose a specific date.
10. If you selected an expiration date, choose the Expire Action to define what happens to the CloudKey when it expires. This can be one of the following:
    - Disable—The key will remain in the cloud, but is disabled and cannot be used by any applications.
    - Delete—The key is disabled in the cloud and cannot be used by any applications. You can set the date when the key is permanently deleted.

    Note: When the CloudKey expires, the selected Expire Action is performed on the key. The Cryptographic Security Platform Vault handles the expiry date and expire action. The expire date is not set in the cloud service provider.
11. Click **Apply**.

Creating a Key Set for PostgreSQL Database Server

Only keys created in the Cryptographic Security Platform Vault for Databases are supported.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the CloudKeys tab and select the Key Set with which the CloudKey will be associated.
4. Select **Actions > Create CloudKey**.
5. On the Details tab of the Create CloudKey dialog box, enter the following:

Field	Description
Name	Enter the name for the CloudKey.
Description	Enter the optional description for the CloudKey.

Field	Description
Cipher	Select AES-256.

6. Click **Continue**.
7. On the Schedule tab, determine the rotation schedule for the CloudKey. This can be one of the following:
    - Inherit from Key Set—The CloudKey will use the default schedule from the Key Set. If the Key Set schedule changes after the CloudKey is created, the CloudKey schedule will not be updated.
    - Never—The CloudKey will never be rotated.
    - Once a year—The CloudKey will be rotated once a year.
    - Every 6 months—The CloudKey will be rotated once every 6 months.
    - Every 30 days—The CloudKey will be rotated once every 30 days.
    - Other—The CloudKey will be rotated at the interval you select.
8. Choose when this version of the CloudKey should expire. The per version expiration can be one of the following:
    - Never—The CloudKey version will never expire.
    - Fixed Date—All CloudKey versions will expire on the date that you set.
    - Relative Expiry—Each CloudKey version will expire after the number of days that you set.
9. Choose when the CloudKey as a whole should expire. This can be Never, or you can choose a specific date.
10. If you selected an expiration date, choose the Expire Action to define what happens to the CloudKey when it expires. This can be one of the following:
    - Disable—The key will remain in the cloud, but is disabled and cannot be used by any applications.
    - Delete—The key is disabled in the cloud and cannot be used by any applications. You can set the date when the key is permanently deleted.

    Note: When the CloudKey expires, the selected Expire Action is performed on the key. The Cryptographic Security Platform Vault handles the expiry date and expire action. The expire date is not set in the cloud service provider.
11. Click **Apply**.

Enable TDE on PostgreSQL Database Server

Before the PostgreSQL Database Server VM can be used for TDE, you need to enable TDE.

1. Log in to the command prompt PostgreSQL Database Server VM.
2. Run the following command: `hcl tde enable -y`

Manually Installing and Registering the Policy Agent for PostgreSQL

To manually install and register the Policy Agent:

1. Log in to the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Download Policy Agent**.
4. Install the Policy Agent on your PostgreSQL Server VM. For details, see the installation and administration guide at https://api.managed.entrust.com/vault/latest
5. Return to the Cryptographic Security Platform Vault for Databases webGUI and click **Workloads** in the top menu bar.
6. Select **Actions > Create New Cloud VM Set** and complete the following:
    a. On the VM Set tab, enter a name for the Cloud VM Set.
    b. Select the group to which this set should belong.
    c. Optionally enter a description for the set.

d. If you want to use the BoundaryControl feature, select the CloudControl app server link that you want to use.
e. To specify additional options, see Creating a Cloud VM Set for the CSP Vault for VM Encryption for the descriptions.
f. After you finish specifying the Cloud VM Set options, click **Create**.
g. When you see the **Cloud VM Set Successfully Created** message, click **Close**.

7. Register the PostgreSQL Server VM with Cryptographic Security Platform Vault by running the following command:

```
hcl register -a <Cryptographic Security Platform Vault IP Address>
```

When prompted, enter the vault ID, username, and password for the Cryptographic Security Platform Vault. The PostgreSQL Server will display the available Cloud VM Sets. Select the Cloud VM Set that you want to use, and confirm your selection.

Installing PostgreSQL

You can either use the PostgreSQL that is included with your Ubuntu, or use the PostgreSQL Advanced Packaging Tool (APT) Repository. For the list of supported versions, see Database Vault Overview.

The supported algorithm is AES-256.

Installing PostgreSQL in Ubuntu:

PostgreSQL is included automatically with Ubuntu. You can install it by using the following APT command:

Copy

```
apt install postgresql
```

Using the PostgreSQL APT Repository

If the PostgreSQL version included in your version of Ubuntu is not the one that you want to use, you can use the PostgreSQL APT Repository. The PostgreSQL APT Repository supports the following versions of Ubuntu:

- noble (24.04, LTS)
- mantic (23.10, non-LTS)
- jammy (22.04, LTS)
- focal (20.04, LTS)

To automatically install and configure the PostgreSQL APT Repository, use the following APT commands:

Copy

```
sudo apt install -y postgresql-common
sudo /usr/share/postgresql-common/pgdg/apt.postgresql.org.sh
```

To manually install and configure the PostgreSQL APT Repository, perform the following:

1. Import the repository signing key. For example:
   Copy
   ```
   sudo apt install curl ca-certificates
   sudo install -d /usr/share/postgresql-common/pgdg
   sudo curl -o /usr/share/postgresql-common/pgdg/apt.postgresql.org.asc --fail https://www.postgresql.org/media/keys/ACCC4CF8.asc
   ```
2. Create the repository confirmation file. For example:

Copy

```
sudo sh -c 'echo "deb [signed-by=/usr/share/postgresql-common/pgdg/apt.postgresql.org.asc] https://
apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" > /etc/apt/sources.list.d/pgdg.list'
```

3. Update the package lists. For example:
   Copy
   ```
   sudo apt update
   ```
4. Install the latest version of PostgreSQL. For example:
   Copy
   ```
   sudo apt -y install postgresql
   ```

   Note: If you want to use a particular version of PostgreSQL, enter that instead of 'postgresql'. For example, use 'postgresql-16'.

CSP Vault for Databases with MariaDB TDE

Cryptographic Security Platform Vault for Databases supports MariaDB TDE as an external key provider. You can encrypt your keys using the AES-256 key cipher, and also rotate the keys, which creates a new version of the encryption key.

- Common MariaDB Queries for Manual or Scripted Installation
- Manual Installation and Configuration for Maria DB
- Scripted Installation and Configuration1

Common MariaDB Queries for Manual or Scripted Installation

The following queries can help with your MariaDB TDE installation:

Query	Description
SHOW DATABASES;	Lists all MariaDB databases in the server.
CREATE DATABASE my_database;	Creates a new database.
USE my_database;	Specifies the database to use.
INSTALL SONAME 'entrust_key_management';	Installs the entrust_key_management plugin.
SHOW TABLES	Lists all tables inside a database.

Query	Description
CREATE TABLE table1 (i int)	Creates a table "table1" that contains one column "i" which is in format integer.
CREATE TABLE table1 (i int) ENGINE=InnoDB ENCRYPTED=YES;	Creates an encrypted table "table1" using the default storage engine InnoDB, with one column "i" which is in format integer. This table will use key ID 1 by default as no key ID was specified.
CREATE TABLE table1 (i int) ENGINE=InnoDB ENCRYPTED=YES ENCRYPTION_KEY_ID=2;	Creates the encrypted table described above using key ID 2.
CREATE TABLE table2 (i int); ALTER TABLE table2 ENCRYPTED=YES encryption_key_id=2;	Creates the unencrypted table "table2" with one column "i" which is in format integer. The ALTER command encrypts the table using key ID 2.
ALTER TABLE table4 ENCRYPTED=NO	Disables the encryption on table "table4".
SELECT * FROM information_schema.innodb_tablespaces_encryption G;	Displays the encryption table details.

Manual Installation and Configuration for Maria DB

This section explains how to manually install and configure Cryptographic Security Platform Vault and Maria DB.

Scripted Installation and Configuration1

You can now use PowerShell-based scripts to install and configure MariaDB TDE on the Cryptographic Security Platform Vault for Databases. This allows you to simplify the setup process.

- Common MariaDBQueries for Manual or Scripted Installation

- Downloading the TDE Script Bundle for MariaDB
- Encrypting Tables on MariaDB Server
- Setting up the Entrust Client on MariaDB Using Scripts

Common MariaDBQueries for Manual or Scripted Installation

The following queries can help with your MariaDB TDE installation:

Query	Description
SHOW DATABASES;	Lists all MariaDB databases in the server.
CREATE DATABASE my_database;	Creates a new database.
USE my_database;	Specifies the database to use.
INSTALL SONAME 'entrust_key_management';	Installs the entrust_key_management plugin.
SHOW TABLES	Lists all tables inside a database.
CREATE TABLE table1 (i int)	Creates a table "table1" that contains one column "i" which is in format integer.
CREATE TABLE table1 (i int) ENGINE=InnoDB ENCRYPTED=YES;	Creates an encrypted table "table1" using the default storage engine InnoDB, with one column "i" which is in format integer. This table will use key ID 1 by default as no key ID was specified.
CREATE TABLE table1 (i int) ENGINE=InnoDB ENCRYPTED=YES ENCRYPTION_KEY_ID=2;	Creates the encrypted table described above using key ID 2.

Query	Description
CREATE TABLE table2 (i int); ALTER TABLE table2 ENCRYPTED=YES encryption_key_id=2;	Creates the unencrypted table "table2" with one column "i" which is in format integer. The ALTER command encrypts the table using key ID 2.
ALTER TABLE table4 ENCRYPTED=NO	Disables the encryption on table "table4".
SELECT * FROM information_schema.innodb_tablespaces_encryption G;	Displays the encryption table details.

Downloading the TDE Script Bundle for MariaDB

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Download TDE script bundle**.
4. On the Download TDE script bundle dialog box, complete the following:

Field	Description
Name	Select a name to identify this database. This name will be used for the .zip bundle you download, and also as a prefix for related assets such as the KeySet and the Cloud VM Set. For example, if you choose mariadb as the name, then the script will create mariadb_keyset and mariadb_cvmset.
Database Type	Select MariaDB Database Server.
Enable HSM	If an HSM is configured, check the Enable HSM checkbox to protect your TDE master keys with the HSM. You will need to verify the HSM connection before you can proceed.
CSP Nodes Mapping	Optionally select the name of your Node Mapping.

5. **Click Continue**.
6. On the TDE Script Bundle Details dialog box, review your choices and click **Download**.

The <name>.zip bundle is automatically downloaded.

Encrypting Tables on MariaDB Server

1. Login to MariaDB using the following command: `mariadb`
   Note: If you want to log in using a specific user, use the following command: `mariadb -u <user_name> -p`
2. Install the Entrust encryption plugin.
   Copy
   ```
   INSTALL SONAME 'entrust_key_management';
   ```
3. Encrypting the tables.
   To encrypt the new table, you have to provide the following options while creating the table:

Option	Description
ENCRYPTED=YES	This option is used to encrypt the table.
ENCRYPTION_KEY_ID=1	This option is used to provide the master key ID. If you include ENCRYPTED=YES and do not include the encryption key ID, then MariaDB will use ENCRYPTION_KEY_ID=1 as the default.

   For example:
   Copy
   ```
   CREATE TABLE table1 (i int) ENGINE=InnoDB ENCRYPTED=YES ENCRYPTION_KEY_ID=1;
   ```
   To encrypt an existing table, use ALTER TABLE and provide the following options:

Option	Description
ENCRYPTED=YES	This option is used to encrypt the table.
ENCRYPTION_KEY_ID=1	This option is used to provide the master key ID. If you include ENCRYPTED=YES and do not include the encryption key ID, then MariaDB will use ENCRYPTION_KEY_ID=1 as the default.

   For example:
   Copy
   ```
   ALTER TABLE table2 ENCRYPTED=YES ENCRYPTION_KEY_ID=2;
   ```
4. Retrieve encryption details.
   To retrieve encryption details such as the key ID, and key version, run the following query:
   Copy
   ```
   SELECT * FROM information_schema.innodb_tablespaces_encryption G;
   ```

Note: We recommend that you run the shutdown command (SHUTDOWN;) before you exit MariaDB to ensure that your encrypted tables are synchronized correctly. The shutdown command forces MariaDB to write the encrypted data to disk.

Setting up the Entrust Client on MariaDB Using Scripts

1. Copy the script bundle to the first MariaDB node.

2. Create a folder and extract the bundle. The bundle contains the following files:
   - entrust.conf—The configuration file with some pre-populated values. You can modify these values if necessary.
   - setup.sh—A bash script signed with the Entrust signature. Do not modify.

   Run the setup.sh script as follows:
   bash> ./setup.sh first entrust.conf
   Where:
   - first is the node you are updating. This can be either first or other.
   - entrust.conf is the name of the configuration file that you downloaded.

3. If you have a second MariaDB node in your cluster, copy the script bundle to the second node and extract it.
4. Run the setup.sh script as follows:
   bash> ./setup.sh other entrust.conf

Setting up Data Guard with Scripts

Data Guard is set up with a primary node and a standby node. The primary node is set up using the same process as the first Oracle Server node. For details, see the following:

- Prerequisites for Scripted Oracle TDE
- Downloading the TDE Script Bundle for Oracle
- Setting up the Entrust Client Using Scripts for Oracle

If your Oracle environment is set up with Data Guard for disaster recovery, then you will need to make the keys accessible to any standby VMs as well as the primary. To ensure that the same keys are accessible to the standby nodes, all of the VMs must be connected to the same Key Set on the Cryptographic Security Platform Vault for Databases as well.

Setting up the Entrust Client on the Standby Oracle VMs:

- Copy the bundle that you downloaded to the standby node.
- Create a directory and extract the bundle.
- Copy the modified entrust.conf file from the first Oracle server node and overwrite the config file from the bundle.
- Run the setup.sh script using bash as the ROOT user:
  ```
  bash> sudo ./setup.sh other entrust.conf
  ```
  Where:
  - other is the node you are updating.
  - entrust.conf is the name of the configuration file that you downloaded.

Oracle Server Setup:

Important:

Data Guard mandates that the DB_UNIQUE_NAME for primary and standby servers should be different. Oracle derives the application name (CKA_APPLICATION) from the DB_UNIQUE_NAME, so the application name on standby is also different. The keys created by primary are marked with primary's application name. This causes v$encryption_keys view to return empty list.

The Entrust library and scripts have been designed to look for DB_UNIQUE_NAME of both primary and standby servers. This ensures that the v$encryption_keys view shows the keys correctly.

Set Environment:

The oracle administrator must provide the following parameters to set the context. Note that the database unique name here is orcls which is different from the same on primary.

The script provides the "default" parameter value in the brackets, if you want to use that, then just press enter to accept it.

Copy

```
[oracle@oracle19cn1 ~]$ ./encrypt.sh setenv
Using configuration file: ./entrust.conf
Using environment file: ./oracle.env
ORACLE_BASE (/u01/app/oracle) ?
ORACLE_HOME (/u01/app/oracle/product/19c/db_1) ?
Software Wallet Password (**********) ?
Database Unique Name (orcls) ?
Database SID (orcl) ?
Access token file (/opt/oracle/entrust/oracle.conf) ?
Successfully set environment variables for TDE scripts in ./oracle.env
Updated env cache ./oracle.tab
```

Initial setup of standby server:

Copy

```
./encrypt.sh standby setup
```

Check the status:

Copy

```
./encrypt.sh status
```

Configuring Auto-login for the Keystore on the Standby Node

You can enable auto login on the standby server.

1. Setup the auto-login:
   `./encrypt.sh standby setup_auto_login`
2. Check the status:
   `./encrypt.sh status`

Migrating from Software Wallet with Data Guard

If the database is already encrypted with a software keystore, then you need to use the migration process.

Oracle requires both the software keystore and CSP Vault-based wallet are open when transitioning from software wallet to the CSP Vault-based keystore. Because both keystores cannot be opened at the same time, Oracle uses Auto Login Wallet to open both keystores during the migration. This applies to both the Primary as well as Standby servers / clusters.

1. On the Standby server, stop the Managed Recovery process (redo log apply):
   Copy
   ```
   ./encrypt.sh standby stop_redo_log_apply
   ```
2. Migrate the Primary server to a CSP Vault-based keystore and setup auto login wallet:
   Copy

```
./encrypt.sh migrate
./encrypt.sh setup_auto_login
```

3. Copy the wallet files from the Primary wallet to the Standby wallet. The WALLET_ROOT can be seen in the output of the command:
   Copy
   ```
   ./encrypt.sh status
   scp $WALLET_ROOT/tde/* oracle@standby:$WALLET_ROOT/tde
   ```
4. Resync the standby server:
   This command will stop and restart the database as well as restart the Manged Recovery process (redo log apply).
   Copy
   ```
   ./encrypt.sh standby resync
   ```
5. Check the status.
   Copy
   ```
   ./encrypt.sh status
   ```

Primary Key Rotation with Data Guard

If the master key has to be rotated while there is an active Data Guard managed standby, you must stop the redo log apply on the standby node to temporarily prevent synchronization with the Primary database.

1. Stop the redo log apply on the standby node.
   Copy
   ```
   ./encrypt.sh standby stop_redo_log_apply
   ```
2. Rotate the key on the Primary node.
   Copy
   ```
   ./encrypt.sh rotate_key
   ```
3. After the key has been successfully rotated, restart the redo log apply on the standby.
   Copy
   ```
   ./encrypt.sh standby restart_redo_log_apply
   ```
4. Check the status of the Managed Recovery Process (MRP) to ensure that the new key has been synchronized. If the MRP has not started, then wait for a few seconds then restart it again.
   Copy
   ```
   ./encrypt.sh standby restart_redo_log_apply
   ```
5. Check the status.
   Copy
   ```
   ./encrypt.sh status
   ```

Switch Standby Node to Primary with Data Guard

After a failover, the Primary node becomes the standby, and the original standby node becomes the new Primary. When this occurs, you must setup the old Primary node as the new standby node.

1. Perform the failover using your company's best practices.
2. Run the following command on the old primary node to convert it to the new standby node:
   Copy

```
./encrypt.sh standby setup
```

3. Check the status.
   Copy
   ```
   ./encrypt.sh status
   ```

Scripted Installation and Configuration for Oracle TDE

You can use scripts to install and configure Oracle TDE on the Cryptographic Security Platform Vault for Databases. This allows you to simplify the setup process. You should be familiar with Oracle database before using the scripts.

This section contains example commands that use parameter values specific to the Entrust lab environment. Before executing these commands in your own setup, ensure that you replace these parameters with values appropriate to your environment. For example:

- `/opt/oracle/entrust/oracle.conf` is the config file created by the `setup.sh` script.
- `orcl` is the ORACLE_SID.

Note: Every script that you run collects debug trace. The name of the trace file is auto-generated and displayed at the beginning of the script run. For example:

```
./encrypt.sh rotate_key

Logging debug trace and output to: ./trace/encrypt_99.trc
```

This section includes:

- Scripted Backup and Restore with Oracle TDE
- Viewing TDE Reports for Oracle Database
- Remove Entrust Software from Oracle with Scripts
- Rotating the TDE Key using Scripts
- Reverse Migrate to Software Wallet using Scripts
- Configuring Auto-login for the Keystore using Scripts
- Migrating from Software Wallet using Scripts
- Encrypting Multiple Oracle Databases with one Command
- Scripted Database Encryption with TDE Keys
- Enabling TDE on a Non-Encrypted Oracle Database using Scripts
- Setting up the Entrust Client Using Scripts for Oracle
- Downloading the TDE Script Bundle for Oracle
- Prerequisites for Scripted Oracle TDE

Scripted Backup and Restore with Oracle TDE

Administrators usually use "rman" for backup and restore with Oracle server. However, if the database is encrypted with TDE using Cryptographic Security Platform Vault for Databases as the master key provider, then the administrator must first open the HSM keystore on the node where you plan to restore. This document describes the simplest backup and restore method to be used when integrated with the CSP Vault for Databases.

This process has been tested on Oracle Database 19c.

- Backing Up Oracle TDE on an Encrypted Database
- Restoring Oracle TDE Using Scripts

Backing Up Oracle TDE on an Encrypted Database

1. If Oracle is not running, login as sysdba and run the startup.
   Copy
   ```
   su - oracle
   sqlplus / as sysdba
   sql> startup;
   ```
2. If the database is running in NOARCHIVELOG mode, change it to ARCHIVELOG mode.
   Copy
   ```
   sql> shutdown immediate;
   sql> startup mount;
   sql> alter database archivelog;
   sql> alter database open;
   ```
3. Exit the sqlplus session and connect to the rman session.

   Copy
   ```
   rman target /
   ```
4. List any existing backup files.
   Copy
   ```
   rman> list backup;
   ```
5. If there are any backup files, optionally delete them.
   Copy
   ```
   rman> delete backup;
   ```
6. Display the default configuration for rman.
   Copy
   ```
   rman> show all;
   ```
7. Set the backup and configuration file location and the file name format of the backup files. If the path doesn't exist, create it using the following: `mkdir -p /u02/backup/ORCL/`
   Copy
   ```
   rman> CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT '/u02/backup/ORCL/ORCL_BKP_%U';
   rman> CONFIGURE controlfile autobackup on;
   ```
8. Create the backup with archive logs.
   Copy
   ```
   rman> BACKUP DATABASE PLUS ARCHIVELOG;
   ```
9. Create the init file using the pfile.
   Copy
   ```
   cd $ORACLE_HOME/dbs/
   sqlplus / as sysdba

   sql> create pfile from spfile;
   ```
10. After the backup is completed, identify the encryption key using the following query as sysdba on the source machine.

Copy

```
sqlplus / as sysdba
startup;
select KEY_ID,KEY_USE from V$ENCRYPTION_KEYS;
```

Search for the section called "Current database master encryption key/s in use".

Restoring Oracle TDE Using Scripts

To restore the backup on an alternate Oracle Server VM, you will need to perform the same setup process as you did to prepare a secondary node. For more information, see Scripted Installation and Configuration for Oracle TDE.

Note: If the Oracle server node is already connected to the CSP Vault for Databases, you can skip the setup steps.

1. Copy the bundle file to the Oracle server node where you want to restore the database.
2. Create a directory and extract the bundle.
3. Copy the modified entrust.conf from the first Oracle server node and overwrite the configuration file from the bundle.
4. Run the setup.sh script using bash as the ROOT user.
   Copy
   ```
   sudo ./setup.sh other entrust.conf
   ```
   Note: Because this is an additional node, the value of the node parameter must be 'other'.
5. Retrieve the access token for accessing the backup key.
   The Oracle server node where you want to restore can now access keys in the Key Set to which it is connected. However, the backup might have been taken with a key in a different Key Set. To ensure that you have the correct key, you will need to retrieve the master key ID of the key which is associated with the backup. It can be seen in the output of command "./encrypt.sh status" on Oracle server node where the backup was taken
   a. Run the following script on the Oracle server node where the backup was taken.
      Copy
      ```
      ./encrypt.sh status
      ```
      The output displays the master key ID.
   b. Run the following script to get the access token for accessing the appropriate Key Set.
      Copy
      ```
      ./get_token.sh <Master key ID>
      ```
      This command prints the path of the access token file you will need to open the keystore for accessing the keys. For example:
      Copy
      ```
      $ get_token.sh 0684299E32808C4F5ABF40262B20AF86D7
      ...
      Key with Key ID 0684299E32808C4F5ABF40262B20AF86D7 found in KeySet named poc_keyset
      ...
      ...
      Successfully created access token file "/opt/oracle/entrust/poc_keyset.conf"
      ```
6. Set the environment variables. In this example, the access token file is located at /opt/oracle/entrust/poc_keyset.conf.
   Copy

```
[oracle@oracle19cn1 ~]$ ./encrypt.sh setenv


Using configuration file: ./entrust.conf
Using environment file: ./oracle.env

ORACLE_BASE (/u01/app/oracle) ?
ORACLE_HOME (/u01/app/oracle/product/19c/db_1) ?
Software Wallet Password (************) ?
Database Unique Name (orcl) ?
Database SID (orcl) ?

Access token file (/opt/oracle/entrust/oracle.conf) ? /opt/oracle/entrust/poc_keyset.conf

Successfully set environment variables for TDE scripts in ./oracle.env
Updated env cache ./oracle.tab
```

7. Copy the backup and control file from the source server to the same location on the destination server.
8. Copy the `initorcl.ora` and `orapworcl` files to the destination server at $ORACLE_HOME/dbs.

   Note: If you are using Oracle RAC, the file is called `orapw`, not `orapworcl`.

   The following files need to be copied into the locations on the destination server:

File	Location
init<SID>.ora For example, initorcl.ora	$ORACLE_HOME/dbs
orapw<SID> or orapw (RAC)	$ORACLE_HOME/dbs
Control files, for example: c-1730471087-20250602-00 /u02/oracle/oradata/ORCL/control01.ctl /u02/oracle/FRA/ORCL/control02.ctl	grep control $ORACLE_HOME/dbs/init<SID>.ora
Redo log files, for example: /u02/oracle/oradata/ORCL/redo0*	SQL> SELECT GROUP#, STATUS, MEMBER FROM V$LOGFILE;

File	Location
Backup files	Backup directory. For example: /u02/backup/ORCL
Autobackup files for controlfile	For example: /u01/app/oracle/oradata/fra/ORCLP/autobackup

9. Delete any older backup files on the destination server.
   Copy
   ```
   rman target /

   rman> list backup;
   rman> delete backup;
   ```
   If you have another database with the same name, you will need to delete that database using the dbca command.
10. Create a dummy entry in /etc/oratab file in the format $ORACLE_SID:$ORACLE_HOME:<N|Y>
    Where $ORACLE_SID is the system identifier, $ORACLE_HOME is the home directory of the database, and Y/N indicates whether or not to start the database after reboot or startup. For example:
    Copy
    ```
    orcl:/u01/app/oracle/product/19c/db_1:N
    ```
11. Optionally run the following command to get information on the control file path and learn where the control file will be restored.
    Copy
    ```
    cat $ORACLE_HOME/dbs/initorcl.ora | grep control

    # it will display output in this format
    *.control_files='/u02/oracle/oradata/ORCL/control01.ctl','/u02/oracle/FRA/ORCL/control02.ctl'
    ```
12. Ensure that the path exists for both files. Create them if needed.
    Copy
    ```
    mkdir -p /u02/oracle/oradata/ORCL/
    mkdir -p /u02/oracle/FRA/ORCL/
    ```
13. Create the audit dump directory in each node of the RAC cluster.
    Copy
    ```
    mkdir -p $ORACLE_BASE/admin/$ORACLE_SID/adump
    ```
14. Startup the database in nomount mode.
    Copy
    ```
    cd $ORACLE_HOME/dbs/
    sqlplus / as sysdba

    sql> startup nomount pfile=$ORACLE_HOME/dbs/initorcl.ora
    ```

15. Connect to rman and restore the control file. If you do not know the control file location, run "list backup;" on the source server.
    Copy
    ```
    rman target /
    rman> restore controlfile from '/u02/oracle/oradata/ORCL/control01.ctl';
    OR
    rman> restore controlfile from autobackup;
    ```
16. Start the database in nomount mode.
    Copy
    ```
    rman> alter database mount;
    ```
17. Crosscheck the backup.
    Copy
    ```
    rman> crosscheck backup;
    ```
18. Optionally catalog the old control file.
    Copy
    ```
    rman> catalog start with '/u02/backup/ORCL/' noprompt;
    ```
19. Restore the database.
    Copy
    ```
    rman> restore database ;
    rman> ALTER DATABASE FLASHBACK OFF;
    ```
20. Exit rman.
21. Open the wallet.
    Copy
    ```
    ./encrypt.sh open_hsm_keystore
    ```
22. When the wallet is open, start rman and finish the recovery process.
    Copy
    ```
    rman target /
    rman> recover database ;
    ```
    Note: If you see a media recovery error, you can safely ignore it.
23. If you see a failure, open the database with resetlogs.
    Copy
    ```
    alter database open resetlogs;
    ```
24. If no failures are seen, open the database normally.
    Copy
    ```
    alter database open;
    ```
25. Ensure the database mode is set to Read, Write.
    Copy
    ```
    select name, open_mode from v$database;
    ```
26. Add the database to the cluster and add the RAC instances.
    Copy
    ```
    srvctl add database -d orcl -o $ORACLE_HOME
    srvctl add instance -d orcl -i orcl1 -n oracle19cn1
    ```

```
srvctl add instance -d orcl -i orcl2 -n oracle19cn2
srvctl config database -d orcl -a
```

27. If required, set the key ID in sqlpls using the following:
    Copy
    ```
    ADMINISTER KEY MANAGEMENT USE KEY '0684299E32808C4F5ABF40262B20AF86D7' IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf";
    ```
28. Crosscheck any other encrypted table data or tables in the encrypted table space using select query by login as the Key Management (syskm) user.

Viewing TDE Reports for Oracle Database

If you used scripted installation, configuration, and encryption, you can download TDE reports from the CSP Vault for Databases webGUI for a specific VM.

> Note: If you have upgraded your CSP Vault for Databases from a previous version, then you will need to download the latest TDE script bundle and run at least the key rotation command before you can access any reports. For more information, see Downloading the TDE Script Bundle for Oracle and Rotating the TDE Key using Scripts.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab.
4. Select the VM for which you want to view TDE reports.
5. In the Details section, click the **TDE Reports** tab.
   The CSP Vault for Databases webGUI displays the list of reports for the VM that you specified. You can click the download icon to download the report in plain text, or the eyeball icon to view the report in the vault. When viewing the report, you can also download or copy the text.
   You can also search for a specific report if you know the report ID.

Remove Entrust Software from Oracle with Scripts

If necessary, you can remove the Entrust CSP Vault software from your Oracle server.

1. Run the Reverse Migrate command. For more information, see Reverse Migrate to Software Wallet using Scripts.
   Copy
   ```
   ./encrypt.sh reverse_migrate
   ```
2. Verify that your data is accessible.
   At this point, it should be encrypted with the software wallet and password protected.
3. Unregister each Oracle node by running the following command on the Oracle Server VM.
   Copy
   ```
   hcl unregister -y
   ```
4. Log into the Cryptographic Security Platform Vault for Databases webGUI and remove the following:
   - The database connector that you created
   - All Oracle TDE keys
   - The Key Set used for Oracle TDE
   - The Cloud VM Set used for Oracle TDE

Rotating the TDE Key using Scripts

The Rekey operation is initiated in the Oracle server. The Oracle server deactivates the existing master key and creates a new master key. The data encryption key is then rewrapped using the new master key.

Note: The older key is deactivated but not destroyed.

1. Rotate the key:
   `./encrypt.sh rotate_key`
2. Check the status:
   `./encrypt.sh status`

Reverse Migrate to Software Wallet using Scripts

You can reverse migrate the Oracle database from a CSP Vault-based TDE master key to a software wallet.

1. Migrate the database:
   `./encrypt.sh reverse_migrate`
2. Check the status:
   `./encrypt.sh status`

Configuring Auto-login for the Keystore using Scripts

After enabling encryption with CSP Vault, the administrator can setup an auto-login wallet which opens the keystore automatically when the database restarts.

1. Setup the auto-login:
   `./encrypt.sh setup_auto_login`
2. Check the status:
   `./encrypt.sh status`

Migrating from Software Wallet using Scripts

If the database is already encrypted with a software keystore then use the following command to migrate to a CSP Vault-based HSM keystore:

1. Migrate the database:
   `./encrypt.sh migrate`
2. Check the status:
   `./encrypt.sh status`

Encrypting Multiple Oracle Databases with one Command

You can now prepare multiple databases for encryption and encrypt all of them using one command. Before you begin, please review Enabling TDE on a Non-Encrypted Oracle Database using Scripts.

Most of the commands in this section use the following options:

Option	Description
`[-all]`	Apply the operation to all databases.

Option	Description
`[-dblist <dblist_file>]`	Apply the operations to all databases listed in the dblist file. The dblist file should contain a newline-separated list of database SIDs.

Procedure

1. List the available databases using the following command:
   Copy
   ```
   ./encrypt.sh listdatabases
   ```
   Note: If the Oracle server does not have Clusterware set up, you will be prompted to provide the path to the Oracle Home directory ($ORACLE_HOME). If you have multiple ORACLE_HOME directories, you will need to run the command for each ORACLE_HOME directory.
2. Prepare to encrypt the databases using the following command:
   Copy
   ```
   ./encrypt.sh setenv -all
   ```
   This is an interactive process that will prompt for the necessary information, such as the software wallet password. If you do not want to encrypt all of the databases, use the -dblist <dblist_file> option.
3. If your databases are NOT encrypted with a software keystore, use the following command to encrypt all the prepared databases:
   Copy
   ```
   ./encrypt.sh encrypt -all
   ```
   Note: If you do not want to encrypt all of the databases, use the -dblist <dblist_file> option.
4. If your databases are already encrypted with a software keystore, use the following command to migrate all the prepared databases to CSP Vault-based encryption:
   Copy
   ```
   ./encrypt.sh migrate -all
   ```
   Note: If you do not want to encrypt all of the databases, use the -dblist <dblist_file> option.
5. Optionally check the encryption or migration status of the prepared databases using the following command:
   Copy
   ```
   ./encrypt.sh status -all
   ```
6. Set up auto login for all the CSP Vault-based encrypted databases using the following command:
   Copy
   ```
   ./encrypt.sh setup_auto_login -all
   ```
7. If you are using Data Guard, and your databases are not yet encrypted, do the following:
   a. Ensure that you have encrypted the databases (Step 3).
   b. Set up the standby server using the following command:
      Copy
      ```
      ./encrypt.sh standby setup -all
      ```
8. If you are using Data Guard, and your databases are encrypted using software wallet, do the following:
   a. Ensure that you have migrated the databases on the primary to CSP Vault-based encryption (Step 4) and set up auto login (step 6).
   b. Copy all the wallet files from the primary to the standby server.
   c. Resync the standby server using the following command:

Copy

```
./encrypt.sh standby resync -all
```

Scripted Database Encryption with TDE Keys

You can use column level encryption and tablespace level encryption.

Column Encryption

Option 1: Encrypt plaintext table

Create a plaintext table.

Copy

```
CREATE TABLE CUSTOMERS (ID NUMBER(5), NAME VARCHAR(42), CREDIT_LIMIT NUMBER(10));
```

Add data to the table.

Copy

```
INSERT INTO CUSTOMERS VALUES (001, 'Rakesh Sharma', 10000);
INSERT INTO CUSTOMERS VALUES (002, 'Betty John', 20000);
INSERT INTO CUSTOMERS VALUES (003, 'T Ramchandran', 30000);
INSERT INTO CUSTOMERS VALUES (004, 'Amir Khan', 40000);
```

Encrypt a column.

Copy

```
ALTER TABLE CUSTOMERS MODIFY (CREDIT_LIMIT ENCRYPT);
```

List the encrypted columns.

Copy

```
SELECT * FROM DBA_ENCRYPTED_COLUMNS;
```

Option 2: Create a table with encrypted column

Copy

```
CREATE TABLE CUSTOMERS (ID NUMBER(5), NAME VARCHAR(42), CREDIT_LIMIT NUMBER(10) ENCRYPT );
```

Tablespace Encryption

Data encryption keys are managed by Oracle. They are created when tablespaces are encrypted. The DEKs are wrapped with the master key and the wrapped keys are stored with the data. Oracle communicates with Cryptographic Security Platform Vault for Databases to wrap and unwrap these data keys.

Option 1: Online Encryption of Tablespace

If the tablespace is already created without enabling encryption, then the encryption can be enabled later. For example:

Copy

```
ALTER  TABLESPACE plaintext_tablespace encryption online using 'AES192' encrypt ;
```

Option 2: Create encrypted tablespace

Create an encrypted tablespace. For example using the AES256 algorithm:

Copy

```
CREATE TABLESPACE SECURESPACE
DATAFILE '/u01/app/oracle/oradata/orcl/SECURE01.DBF' SIZE 150M
ENCRYPTION using 'AES256'
DEFAULT STORAGE (ENCRYPT);
```

Create a table in the encrypted tablespace.

Copy

```
CREATE TABLE EMPLOYEE (ID NUMBER(5),NAME VARCHAR(42),SALARY NUMBER(10)) TABLESPACE
SECURESPACE;
```

Insert data.

Copy

```
INSERT INTO EMPLOYEE VALUES (001,'JOHN LENON',100000);
INSERT INTO EMPLOYEE VALUES (002,'MARTINA HINGIS',200000);
INSERT INTO EMPLOYEE VALUES (003,'R ATTENBOROUGH',350000);
COMMIT;
```

Display the data.

Copy

```
SELECT * FROM EMPLOYEE;
```

Display the tablespaces.

Copy

```
COLUMN tablespace_name heading "Tablespace Name" format a20
COLUMN encryption_algorithm heading "Encryption Algorithm" format a21
SELECT
t.name AS tablespace_name,
e.encryptionalg AS encryption_algorithm,
masterkeyid AS "Master Key ID"
FROM
v$tablespace t
JOIN
v$encrypted_tablespaces e
ON
t.ts# = e.ts#;
```

Copy

```
#-------- output is like this ------->>

Tablespace Name     Encryption Algorithm  Master Key ID
-------------------- --------------------- ------------------------------
```

```
SECURESPACE        AES256          17639D6AEE554F27BFB9DD2F3738E145
SECURESPACE2       AES128          17639D6AEE554F27BFB9DD2F3738E145
```

Verification

This verification process works the same for the column and tablespace encryption.

Retrieve the encrypted data.

Copy

```
SELECT CREDIT_LIMIT FROM CUSTOMERS;
```

Close the wallet.

Copy

```
ADMINISTER KEY MANAGEMENT SET KEYSTORE CLOSE IDENTIFIED BY "file:/opt/oracle/entrust/oracle.conf"
CONTAINER = ALL;
```

Retrieve the data again. It should fail because the wallet is closed.

Copy

```
SELECT CREDIT_LIMIT FROM CUSTOMERS;
ERROR at line 1:
ORA-28365: wallet is not open
```

Open the key store and retrieve the data again. It should work properly this time.

Copy

```
ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY "file:/opt/oracle/entrust/oracle.conf"
CONTAINER = ALL;
SELECT CREDIT_LIMIT FROM CUSTOMERS;
```

Enabling TDE on a Non-Encrypted Oracle Database using Scripts

This section describes how to enable TDE if the database is not previously encrypted. If your database is already encrypted using software wallet, then see Migrating from Software Wallet using Scripts.

The script encrypt.sh that you downloaded with the TDE script bundle is used to enable encryption of the Oracle database. This script must be run as the Oracle user.

Usage: encrypt.sh {command} [<config file>]

```
Commands:
   help:                    Show this help message

   getenv:                   Get environment variables for TDE scripts
   setenv:                   Set environment variables for TDE scripts
   setsid <ORACLE_SID>:            Select environment variables for ORACLE_SID
   status:                  Show current TDE status and configuration
   bounce:                   Restart the database
   report:                  Show TDE report for all databases on this server

   encrypt:                  Enable TDE with KeyControl
```

```
rotate_key:                  Rotate TDE master key using KeyControl
migrate:                     Migrate from Software Wallet to KeyControl
reverse_migrate:             Reverse migration from KeyControl to Software Wallet
setup_auto_login:            Configure auto login for KeyControl
remove_auto_login:           Remove auto login wallet
open_hsm_keystore:           Open HSM (KeyControl) KeyStore
close_hsm_keystore:          Close HSM (KeyControl) KeyStore
open_hsm_keystore_and_db:    Open HSM (KeyControl) KeyStore and database

standby setup:               Setup TDE parameters on Data Guard standby server
standby setup_auto_login:    Configure auto login on Data Guard standby server
standby remove_auto_login:   Remove auto login wallet on Data Guard standby server
standby open_hsm_keystore:   Open HSM (KeyControl) KeyStore on Data Guard standby server
standby close_hsm_keystore:  Close HSM (KeyControl) KeyStore on Data Guard standby server
standby open_hsm_keystore_and_db:  Open HSM (KeyControl) KeyStore and database
standby stop_redo_log_apply  Stop managed recovery process
standby restart_redo_log_apply  Restart managed recovery process
standby redo_log_status      Check status of managed recovery process

<config file>:               Path to the configuration file (default: entrust.conf)
```

To enable TDE:

1. Set the environment.
   The Oracle administrator needs to provide the following parameters to set the environment. This operation creates a file called <dbset_name>.env in the script's directory. The actual name will usually be oracle.env.
   ./encrypt.sh setenv
   For example:
   ```
   [oracle@oracle19cn1 ~]$ ./encrypt.sh setenv

   Using configuration file: ./entrust.conf
   Using environment file: ./oracle.env

   ORACLE_BASE (/u01/app/oracle) ?
   ORACLE_HOME (/u01/app/oracle/product/19c/db_1_rac) ?
   Software Wallet Password (**********) ?
   Database Unique Name (orcl) ?
   Database SID (orcl1) ?

   Successfully set environment variables for TDE scripts in ./oracle.env
   ```
2. Check the database status.
   After setting the environment variables, the administrator should check the status to view the current state of the Oracle database server.
   ./encrypt.sh status
3. Encrypt the database.
   Run the following command to encrypt the database set that you specified.
   ./encrypt.sh encrypt
4. Check the database status again.
   The administrator should recheck the status to ensure that the database is encrypted.
   ./encrypt.sh status

Example:

```
[oracle@oracle19cn1 ~]$ ./encrypt.sh status

Using configuration file: ./entrust.conf
Using environment file: ./oracle.env
Using access token file: /opt/oracle/entrust/oracle.conf


Database orcl is already running
Instance orcl1 is running on node oracle19cn1
Instance orcl2 is running on node oracle19cn2b

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Database Role: PRIMARY

db_unique_name         ------- orcl
Multitenant database    ------- YES
Database type          ------- Oracle RAC
Number of instances     ------- 2
Active instances       ------- 2

tde_configuration       ------- KEYSTORE_CONFIGURATION=HSM|FILE
db_create_file_dest     ------- +DATA
Current wallet_root     ------- +DATA/ORCL/wallet
Calculated wallet_root  ------- +DATA/ORCL/wallet

Database encryption wallet  ------- HSM
Auto Login enabled         ------- YES

Database state
------------------------
Database Name   OPEN_MODE          DATABASE_ROLE      Switchover Status
--------------- ------------------- ----------------   ------------------------
ORCL          READ WRITE         PRIMARY           NOT ALLOWED


SHOW PDBs
------------------------
PDB Name       CON_ID OPEN_MODE  RES
-------------- ------ ---------- ---
PDB$SEED          2 READ ONLY  NO
PDB               3 MOUNTED
PDB2              4 MOUNTED

Encryption Wallets
------------------------
Encryption Wallets for instance: 1

PDB Name   Status            WRL_TYPE   WALLET_OR Wallet Type  KEYSTORE WRL_PARAMETER
---------- ------------------- ---------- --------- ------------ -------- ----------------------------------------
CDB$ROOT   OPEN              HSM       PRIMARY   HSM         NONE
PDB        OPEN              HSM       PRIMARY   HSM         UNITED
PDB2       OPEN              HSM       PRIMARY   HSM         UNITED
CDB$ROOT   OPEN              ASM       SECONDARY AUTOLOGIN    NONE     +DATA/ORCL/wallet/tde/
```

```
PDB       OPEN            ASM       SECONDARY AUTOLOGIN    UNITED
PDB2      OPEN            ASM       SECONDARY AUTOLOGIN    UNITED
PDB$SEED  OPEN            ASM       SINGLE    AUTOLOGIN    UNITED
PDB$SEED  OPEN            HSM       SINGLE    HSM          UNITED

Encryption Wallets for instance: 2

PDB Name   Status            WRL_TYPE   WALLET_OR Wallet Type  KEYSTORE WRL_PARAMETER
---------- ------------------ ---------- --------- ----------- -------- ------------------------------------
CDB$ROOT   OPEN              HSM        PRIMARY   HSM         NONE
PDB        OPEN              HSM        PRIMARY   HSM         UNITED
PDB2       OPEN              HSM        PRIMARY   HSM         UNITED
CDB$ROOT   OPEN              ASM        SECONDARY AUTOLOGIN    NONE     +DATA/ORCL/wallet/tde/
PDB        OPEN              ASM        SECONDARY AUTOLOGIN    UNITED
PDB2       OPEN              ASM        SECONDARY AUTOLOGIN    UNITED
PDB$SEED   OPEN              ASM        SINGLE    AUTOLOGIN    UNITED
PDB$SEED   OPEN              HSM        SINGLE    HSM          UNITED


Database master encryption keys
------------------------
PDB Name        Master Key ID                    MKID base64
--------------- -------------------------------- ------------------------
CDB$ROOT        5915AFE732974FDCBF67BB1628974E84    AVkVr+cyl0/cv2e7FiiXToQ=
PDB$SEED        00000000000000000000000000000000    AQAAAAAAAAAAAAAAAAAAAA=
PDB             6ACD2A03E83A4F3BBFDC2F6EA1FADC49    AWrNKgPoOk87v9wvbqH63Ek=
PDB2            2AAF9C18FC2E4F62BF9DF8786C58E724    ASqvnBj8Lk9iv534eGxY5yQ=


TDE Master keys in open wallets
------------------------------
PDB Name        Master Key ID                    TAG                  CON_ID Keystore Type      Origin     Key Creation
Time  Activation Time
--------------- -------------------------------- -------------------- ---------- ------------------ ----------
------------------ ----------------
PDB2            062AAF9C18FC2E4F62BF9DF8786C58E724   ORCL_082025062919           4 SOFTWARE
KEYSTORE  LOCAL     08/20/2025 06:31   08/20/2025 06:31
CDB$ROOT        065915AFE732974FDCBF67BB1628974E84   ORCL_082025062919           1 SOFTWARE
KEYSTORE  LOCAL     08/20/2025 06:30   08/20/2025 06:30
PDB             066ACD2A03E83A4F3BBFDC2F6EA1FADC49   ORCL_082025062919           3 SOFTWARE
KEYSTORE  LOCAL     08/20/2025 06:30   08/20/2025 06:30
CDB$ROOT        062C19E6EDB47C4F8EBF86920158C81FD0                    1 HSM             LOCAL
08/20/2025 06:06   08/20/2025 06:06
PDB             06CB0E514DC64C4F43BF29FE846D8CB92D                    3 HSM             LOCAL
08/20/2025 06:06   08/20/2025 06:06
PDB2            0669595E41E8734F64BF239BD19297A849                    4 HSM             LOCAL
08/20/2025 06:06   08/20/2025 06:06


Services
------------------------
orclXDB
```

```
pdb
pdb2
SYS$BACKGROUND
SYS$USERS
orcl.db.com


Datafiles
------------------------
+DATA/ORCL/DATAFILE/system.289.1205374577
+DATA/ORCL/DATAFILE/sysaux.290.1205374611
+DATA/ORCL/DATAFILE/undotbs1.291.1205374637
+DATA/ORCL/86B637B62FE07A65E053F706E80A27CA/DATAFILE/system.302.1205375527
+DATA/ORCL/86B637B62FE07A65E053F706E80A27CA/DATAFILE/sysaux.303.1205375527
+DATA/ORCL/DATAFILE/users.292.1205374637
+DATA/ORCL/86B637B62FE07A65E053F706E80A27CA/DATAFILE/undotbs1.304.1205375527
+DATA/ORCL/38F0B2B59DDE65C9E06333E5010AD3FB/DATAFILE/system.308.1205378809
+DATA/ORCL/38F0B2B59DDE65C9E06333E5010AD3FB/DATAFILE/sysaux.309.1205378809
+DATA/ORCL/38F0B2B59DDE65C9E06333E5010AD3FB/DATAFILE/users.311.1205378823
+DATA/ORCL/DATAFILE/undotbs2.315.1205453085
+DATA/ORCL/38F0B2B59DDE65C9E06333E5010AD3FB/DATAFILE/undo_2.317.1205454319
+DATA/ORCL/DATAFILE/my_ts.367.1207804451


Wallet files
------------------------
+DATA/ORCL/wallet/tde/cwallet.sso
+DATA/ORCL/wallet/tde/cwallet_072925082421.sso
+DATA/ORCL/wallet/tde/ewallet.p12
+DATA/ORCL/wallet/tde/ewallet_2025072914472796.p12
+DATA/ORCL/wallet/tde/ewallet_2025072914500471_tde_backup.p12


ASM disk group
------------------------
DATA

ASM check
------------------------
orcl is using ASM disk group DATA
```

Setting up the Entrust Client Using Scripts for Oracle

Important: If you add the vault user password to the entrust.conf file, then it can be seen in trace log files. We recommend that you do not include the password and let the vault user type it in manually when they are prompted when running the script.

1. Copy the script bundle to the first Oracle Server node.
    a.
    As the Oracle user, create a folder and extract the bundle. The bundle contains the following files:
        - entrust.conf—The configuration file with some pre-populated values.
        - setup.sh—A bash script signed with the Entrust signature. Do not modify. This should be run as the ROOT user.

- encrypt.sh—This should be run as the Oracle user.

b. Open the entrust_conf file and update the following parameters:
- oracle_user—The name of the Oracle database admin user. Typically the value is "oracle".
- oracle_user_group—The group to which the oracle_user belongs. Typically the value is "oinstall".

c. After editing the entrust_conf file, save your changes.

- Run the setup.sh script using bash as the ROOT user:

```
bash> sudo ./setup.sh first entrust.conf
```

Where:
- first is the node you are updating. This can be either first or other.
- entrust.conf is the name of the configuration file that you downloaded.

If setup is successful, it prints the path of the Access Token file as follows:

```
Saving access token in file /opt/oracle/entrust/oracle.conf
```

Please make a note of this path, as it will be used later to open the wallet.
- If you have an additional Oracle RAC node, Oracle Data Guard, or any alternate restore node, copy the script bundle to this node and extract it.
- Copy the modified entrust.conf file from the first node and overwrite the config file from the bundle.
- **Important:** If you are using Oracle Data Guard, you will need to run a different script to set up the standby nodes. See Setting up Data Guard with Scripts.
- Run the setup.sh script using bash as the ROOT user:

```
bash> sudo ./setup.sh other entrust.conf
```

Where:
- other is the node you are updating. This can be either first or other.
- entrust.conf is the name of the configuration file that you downloaded.

Downloading the TDE Script Bundle for Oracle

Before you download the TDE script bundle, please ensure that you have already created a Cryptographic Security Platform Vault for Databases and can log in to the webGUI.

If you plan to use Node Mapping, please create the mapping before you download the scripts, as you will be prompted for the information. For more information, see Creating a Cluster Node Mapping.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Download TDE script bundle**.
4. On the Download TDE script bundle dialog box, complete the following:

Field	Description
Name	Select a name to identify this database. This name will be used for the .zip bundle you download, and also as a prefix for related assets such as the KeySet and the Cloud VM Set.
Database Type	Select Oracle Database Server.

Field	Description
Enable HSM	If an HSM is configured, check the Enable HSM checkbox to protect your TDE master keys with the HSM. You will need to verify the HSM connection before you can proceed.
CSP Nodes Mapping	Optionally select the name of your Node Mapping.

5. **Click Continue**.
6. On the TDE Script Bundle Details dialog box, review your choices and click **Download**.

The <name>.zip bundle is automatically downloaded.

Prerequisites for Scripted Oracle TDE

Using Scripted Oracle TDE requires the following:

- OpenSSL
- Python3 and the following python modules and packages: json, shutil, base64, requests
- Device-mapper and dmsetup
- Curl

If you are using RAC, please ensure that your Oracle RAC setup is working correctly before you start the setup. You can check the cluster and database status using the following commands:

- `crsctl stat res -t`
- `srvctl status database -db <database name>`

Your Oracle database must be open before you attempt to encrypt it.

CSP Vault with Oracle TDE

The following topics explain how to configure Cryptographic Security Platform Vault as an external key provider with Oracle TDE.

Important: Oracle TDE (both single node and RAC) is only supported in the VMware environment.

- Migrating from Software Keystore to CSP Vault
- Migrating from Software Wallet to CSP Vault
- Configuring Auto-Login with Oracle RAC for the CSP Vault Keystore on ASM Wallet
- Configuring Auto-Login for the CSP Vault Keystore
- Oracle TDE Key Rotation
- Oracle TDE Keys in Cryptographic Security Platform Vault
- Creating a Key Set for Oracle Database Server TDE
- Oracle RAC Cluster Setup
- Oracle Single Node Setup
- Manual Installation and Configuration for Oracle TDE

Migrating from Software Keystore to CSP Vault

The following procedure applies when the target database is multitenant, and you are already using a software wallet with TDE encryption. If your target database is non-multitenant, see Migrating from Software Wallet to CSP Vault.

Repeat the following procedure for each software keystore from which you want to migrate. Each container database (CDB) can use its own Entrust key protection method (credential) if required. However, once a Entrust key protection method has been activated for a particular database instance (CDB), then you must continue to use that same credential for any further keys you want to protect for that instance.

Use the `WALLET_ROOT` and `TDE_CONFIGURATION` parameters.

In the following steps, use the `orcl.conf` file to utilize the access credentials for the Cryptographic Security Platform Vault for Databases.

1. Back up your software keystore before attempting key migration to Cryptographic Security Platform Vault:
   Copy
   ```
   CONNECT sysdba@CDB<n>
   ADMINISTER KEY MANAGEMENT BACKUP KEYSTORE USING '<PreMigrationBackupString>' IDENTIFIED BY
   "<keystorepassphrase>";
   ```
2. Prepare for key migration by running the following SQL script:
   Copy
   ```
   CONNECT sysdba@CDB1ROOT
   ALTER SYSTEM SET TDE_CONFIGURATION = "KEYSTORE_CONFIGURATION=HSM|FILE" SCOPE=BOTH
   SID='*';
   ```
3. Migrate from the keystore to Cryptographic Security Platform Vault:
   Copy
   ```
   CONNECT sysdba@CDB1ROOT
   ALTER SESSION SET CONTAINER = CDB$ROOT;
   SHOW con_name;
   --Open all the PDBs.
   ALTER PLUGGABLE DATABASE ALL OPEN;
   ADMINISTER KEY MANAGEMENT SET ENCRYPTION KEY IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf"
   MIGRATE
   USING <keystore-passphrase> WITH BACKUP;
   ```
4. For Oracle 21c Database, you must open PDB$SEED with read write permissions to successfully bounce the database after migrating from the keystore to Cryptographic Security Platform Vault:
   Copy
   ```
   CONNECT sysdba@CDB1ROOT
   ALTER SESSION SET CONTAINER = CDB$ROOT;
   SHOW con_name;
   --Open all the PDBs.
   ALTER PLUGGABLE DATABASE ALL OPEN;
   -- open PDB$SEED with read write perm show pdbs;
   alter pluggable database pdb$seed close;
   alter pluggable database pdb$seed open read write;
   show pdbs;
   ADMINISTER KEY MANAGEMENT SET ENCRYPTION KEY IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf"
   ```

```
MIGRATE
USING <keystore-passphrase> WITH BACKUP;
```

5. Return to the Oracle Server in the SQL database and run the `select CON_ID,WRL_TYPE,STATUS from V$ENCRYPTION_WALLET;` command.
   For example:
   Copy

```
SQL> select CON_ID,WRL_TYPE,STATUS from V$ENCRYPTION_WALLET;
 CON_ID WRL_TYPE STATUS
---------- -------------------- ------------------------------
 1 HSM OPEN
 2 HSM OPEN
 3 HSM OPEN
 4 HSM OPEN
```

Migrating from Software Wallet to CSP Vault

The following procedure applies when the target database is non-multitenant, and you are already using a software wallet with TDE encryption. If your target database is multitenant, see Migrating from Software Keystore to CSP Vault .

Entrust strongly recommends you back up your software wallet as an independent operation before attempting migration to KeyControl. Keep the backup folder in a safe place separated from the associated database files. Only users with authorization should be able to access the backup folder.

Repeat the following procedure for each database software wallet from which you want to migrate. Each independent database instance can use its own Entrust key protection method or credential if required.

Once an Entrust key protection method has been activated for a particular database instance, then you must continue to use that same credential for any further keys you want to protect for that instance.

Use the `WALLET_ROOT` and `TDE_CONFIGURATION` parameters. The `WALLET_ROOT` parameter should have already been set for Oracle keystore use.

In the following steps, use the `orcl.conf` file to utilize the access credentials for the Cryptographic Security Platform Vault for Databases:

1. Prepare for key migration by running the following SQL script:
   Copy

```
CONNECT sysdba@DB
ALTER SYSTEM SET TDE_CONFIGURATION = "KEYSTORE_CONFIGURATION=HSM|FILE" SCOPE=BOTH
SID='*';
```

2. Migrate from the keystore to Cryptographic Security Platform Vault:
   Copy

```
CONNECT sysdba@DB
ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf" MIGRATE USING
<keystorepassphrase>;
```

   The cloud key is created.
3. Return to the Oracle Server in the SQL database and run the `select CON_ID,WRL_TYPE,STATUS from V$ENCRYPTION_WALLET;` command.

For example:

```
Copy
SQL> select CON_ID,WRL_TYPE,STATUS from V$ENCRYPTION_WALLET;

CON_ID WRL_TYPE STATUS
---------- -------------------- ------------------------------
0 HSM OPEN
```

Configuring Auto-Login with Oracle RAC for the CSP Vault Keystore on ASM Wallet

When you configure auto-login with an Oracle RAC cluster, you will need to create an ASM wallet so that it is accessible to all nodes in the cluster.

Before You Begin

Replace the following values according to your setup:

Script Value	Actual Value
/opt/oracle/entrust/orcl.conf	Replace with the actual path of your configuration file.
ASMDIR	Replace with your ASM storage directory name.
Database Name	Replace with the name of your database.
software_keystore_password	Replace with the password that you want to use.
backup_identifier	Replace with a tag of your choice to identify the backup.

Procedure

1. Close the hardware keystore if it is opened using the following command:

```
Copy
connect / as sysdba;
ADMINISTER KEY MANAGEMENT SET KEYSTORE CLOSE IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf"
CONTAINER = ALL;
```

2. Create a wallet in ASM using the `asmcmd` command.
   For example, +ASMDIR/<Database name>/wallet/tde
3. Set parameters for software keystore using the following commands:

```
Copy
ALTER SYSTEM SET WALLET_ROOT="+ASMDIR/<Database name>/wallet" scope=spfile sid='*';
shutdown immediate;
startup;
ALTER SYSTEM SET TDE_CONFIGURATION="KEYSTORE_CONFIGURATION=FILE" SCOPE=both sid='*';
```

```
shutdown immediate;
startup;
```

4. Create and open the software keystore.
   Copy
   ```
   ADMINISTER KEY MANAGEMENT CREATE KEYSTORE IDENTIFIED BY <software_keystore_password>;
   ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY <software_keystore_password>;
   ```
5. Add the config file as secret for a client HSM_PASSWORD.
   Copy
   ```
   ADMINISTER KEY MANAGEMENT ADD SECRET 'file:/opt/oracle/entrust/orcl.conf' FOR CLIENT
   'HSM_PASSWORD' IDENTIFIED BY <software_keystore_password> WITH BACKUP USING <backup_identifier>;
   ```
6. Close the software keystore.
   Copy
   ```
   ADMINISTER KEY MANAGEMENT SET KEYSTORE CLOSE IDENTIFIED BY <software_keystore_password>;
   ```
7. Create Auto-login keystore.
   Copy
   ```
   ADMINISTER KEY MANAGEMENT CREATE AUTO_LOGIN KEYSTORE FROM KEYSTORE IDENTIFIED BY
   <software_keystore_password>;
   ```
8. Set parameters for software to hardware keystore configuration.
   Copy
   ```
   ALTER SYSTEM SET TDE_CONFIGURATION="KEYSTORE_CONFIGURATION=HSM|FILE" SCOPE=both;
   shutdown immediate;
   startup;
   SELECT * FROM V$ENCRYPTION_WALLET;
   ```

After this configuration, when the database starts, the hardware keystore is opened automatically.

Configuring Auto-Login for the CSP Vault Keystore

When you configure auto-login, replace the following values according to your setup:

Script Value	Actual Value
/opt/oracle/entrust/orcl.conf	Replace with the actual path of your configuration file.
ASMDIR	Replace with your ASM storage directory name.
Database Name	Replace with the name of your database.
software_keystore_password	Replace with the password that you want to use.
back_identifier	Replace with a tag of your choice.

Procedure

1. Close the hardware keystore if it is opened using the following command:

```
connect / as sysdba;
ADMINISTER KEY MANAGEMENT SET KEYSTORE CLOSE IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf"
CONTAINER = ALL;
```

2. Set parameters for software keystore using the following commands:

```
startup;
ALTER SYSTEM SET WALLET_ROOT="/opt/oracle/admin/orcl/wallet" scope=spfile;
shutdown immediate;
startup;
ALTER SYSTEM SET TDE_CONFIGURATION="KEYSTORE_CONFIGURATION=FILE" SCOPE=both;
shutdown immediate;
startup;
```

3. Create and open the software keystore.

```
ADMINISTER KEY MANAGEMENT CREATE KEYSTORE IDENTIFIED BY <software_keystore_password>;
ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY <software_keystore_password>;
```

4. Add the config file as secret for a client HSM_PASSWORD.

```
ADMINISTER KEY MANAGEMENT ADD SECRET 'file:/opt/oracle/entrust/orcl.conf' FOR CLIENT
'HSM_PASSWORD' IDENTIFIED BY <software_keystore_password> WITH BACKUP USING <backup_identifier>;
```

5. Create Auto-login keystore.

```
ADMINISTER KEY MANAGEMENT CREATE AUTO_LOGIN KEYSTORE FROM KEYSTORE IDENTIFIED BY
<software_keystore_password>;
```

6. Set parameters for software to hardware keystore configuration.

```
ALTER SYSTEM SET TDE_CONFIGURATION="KEYSTORE_CONFIGURATION=HSM|FILE" SCOPE=both;
shutdown immediate;
startup;
SELECT * FROM V$ENCRYPTION_WALLET;
```

After this configuration, when the database starts, the hardware keystore is opened automatically.

Oracle TDE Key Rotation

The rekey operation is initiated in Oracle Server. The Oracle Server deactivates the existing key and creates a new master key. The encryption key is then wrapped using the new master key.

Important: You cannot rotate the Oracle TDE Key from the Cryptographic Security Platform Vault for Databases.

1. Ensure that the hardware wallet is open.
2. Run the following command:

```
ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf" CONTAINER = ALL;
```

Note: If you want to use the force option, run the following command:

```
ADMINISTER KEY MANAGEMENT SET KEY FORCE IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf" CONTAINER = ALL;
```

Oracle TDE Keys in Cryptographic Security Platform Vault

You create the Oracle TDE keys in Oracle Server using the PKCS11 API.

You can view the TDE keys in Cryptographic Security Platform Vault.

Creating a Key Set for Oracle Database Server TDE

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Cloud Keys**.
3. Select **Actions > Create Key Set**.
4. On the Details tab of the Create Key Set dialog box, ensure that you select **Oracle Database Server** for the Database type.
5. If you have an HSM, ensure that you set the properties for the HSM.

For more information, see Creating a Key Set for TDE.

Oracle RAC Cluster Setup

This section describes how to configure Oracle TDE on a Oracle Real Application Clusters (RAC) cluster.

Before you begin, you must have completed the topics in Oracle Single Node Setup. After that, you can perform these tasks on the secondary nodes in Oracle RAC.

Oracle RAC is only supported in the VMware environment.

- Configuring CSP Vault for Oracle TDE on the Second Node
- Configuring the Oracle Server Database on the Second Node
- Configuring the Oracle Server Cryptographic Library on the Second Node
- Installing the CSP Vault Linux Policy Agent for Oracle TDE on the Second Node

Configuring CSP Vault for Oracle TDE on the Second Node

This section explains how to configure Cryptographic Security Platform Vault for Oracle TDE.

Important: Use the same Cryptographic Security Platform Vault Key Set for Oracle TDE that was used for the first node.

Enable TDE on Oracle Server

Before creating the Cryptographic Security Platform Vault Database Connector, you must enable TDE on the Oracle Server VM.

To enable TDE, run the following command on the Oracle Server VM: `hcl tde enable -y`

Configure Cryptographic Security Platform Vault Database Connector

To create the Cryptographic Security Platform Vault Database Connector.

1. Create a Database Connector for this KeySet and the Oracle Server VM.

This is the VM registered during installation.
Navigate to the KeySet and select the **Database Connectors** tab. Select **Create Connector Now**.
2. Enter the VM Name and Connector Name.
3. Check the database connector is created correctly.

Configuring the Oracle Server Database on the Second Node

This section explains how to configure the Oracle Server database.

Export Oracle Variables

On the Oracle Server, export the Oracle variables as follows:

```
export ORACLE_SID=orcl
export ORACLE_BASE=/opt/oracle
export ORACLE_HOME=$ORACLE_BASE/product/<oracle_db_version>/dbhome_1
export PATH=$PATH:$ORACLE_HOME/bin
export TNS_ADMIN=$ORACLE_HOME/network/admin
```

Where ORACLE_BASE is the Oracle installation directory. This is usually `/opt/oracle` or `/u01/app/oracle`.

Link pkcs11 library

To configure the Oracle PKCS#11 library folder to use the Entrust KeyControl PKCS#11 API.

1. On the Oracle Server, create the following directory path for the Entrust API library as the **oracle** user. Configure ownership and permissions on the directory as: **owner=oracle; group=oinstall; permissions=775**.
```
sudo chown -R oracle:oinstall /opt/oracle/
sudo chmod -R 775 /opt/oracle/
mkdir -p /opt/oracle/extapi/64/hsm/entrust
chown oracle:oinstall /opt/oracle/extapi/64/hsm/entrust
chmod 775 /opt/oracle/extapi/64/hsm/entrust
```
2. Link the PKCS#11 library into the directory as the **oracle** user.
```
ln -s /opt/hcs/lib/libpkcs11.so /opt/oracle/extapi/64/hsm/entrust/libpkcs11.so
```
Important: The link must be created in /opt/oracle/extapi/64/hsm/entrust/libpkcs11.so or the connection between the Oracle DB and Cryptographic Security Platform Vault will not work.

Bounce the Database

```
sqlplus / as sysdba
```

```
sql> shutdown immediate;
```

```
sql> startup
```

Configuring the Oracle Server Cryptographic Library on the Second Node

This section explains how to configure the cryptographic library on Oracle Server.

1. Navigate to the Cryptographic Security Platform Vault database connector (configured here Configuring CSP Vault for Oracle TDE on the Second Node).
2. Select the database connector and from the **Action** menu, select **Generate Access Token**.
3. Copy the access token to the Oracle Server and create the **Cryptographic Config file**.
4. Create a config file using the copied Access Token (**Identity** and **Secret**) in your Oracle Server that will be used by the database administrators.
Important: You must use the same path for the config file as you used for the first node.
The file should be in json format similar to the following:

```
# cat /opt/oracle/entrust/orcl.conf
{
   "identity" : "tde_connect1",
   "secret" : "S3XsZJe/EPNVf2D/YufOUS2HuOsLfKJBKjp3Zx/
JIrODqWYRQaYiFWnqet4lPsW0VcvGSvH7yB9BUZI
      xGi7CaM68cZFtw6yY5IvaClwD3344MFy28U9zjc0ayFRoHQi/
Dv25xTZ8a2JLlxJRyavO2VNGaCPUZfF
      sPN4lZg3EZwJ3fNKa7Owfpk0AuHmWmcqcYsxNnUxPuc+VYqXZk17omHzYP/
sA86RCv6+825t0EvuQhDH
      F7PxSiHjn+VShCYKNb+RxAvLglIP/eVx0k/HWWI6/bZPpxwjFtw3tqnJ/
8toqPD+f+ZUlYT0mFRuE7BE

xGFf5LBCaVwf5FXKcOeXdaAg8zvaq0ynUjSB9JVw5FP6ZtFrY22hUcFcYDPlTpjMzUzsX9d5BM8BhyT
L
      moPkj4lMyrSh3/nwGlJqPLj92EylmKsSOtOP6irpN22A2omvTsXUP/
pajuGrtUsKqzDdhAj+qmR2IDkS
      dOQMoSSvAgWylAuS6q8WdMvm8SVCVUZpQrLvm226NvfvGCHKKNZaQCdxvL4XIgKI/
tCt+F+Xx0Pk/bkP

gLby90IM5NtktRkroxakhGkgSnoyDj2KovGvIwrHLpFpvDJkCwxbBce+OpcOjxR2tZ3nDM2zoZraSviT
      0P+V2hh7Z0jAWd4YrRdooxtQc3VPjTOrdOBldCExetFk="
}
```

Installing the CSP Vault Linux Policy Agent for Oracle TDE on the Second Node

To install and set up the Cryptographic Security Platform Vault on an Oracle Server. You will need to:

- Install the Policy Agent on the Oracle Server VM
  Important: Only virtual machines are supported.
- Use the same VM Set in the Cryptographic Security Platform Vault for Databases that was used to register the first node.
  Important: You must use the same VM Set or Oracle RAC will not work correctly.
- Register the Oracle Server VM on the Cryptographic Security Platform Vault VM Set.

To install and register the Policy Agent on the Oracle Server:

1. Log in to the Cryptographic Security Platform Vault for Databases webGUI.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Download** Policy Agent.
4. Install the Policy Agent on the Oracle Server VM. For details, see the installation and administration guide at https://api.managed.entrust.com/vault/latest
5. Register the Oracle Server VM with the Cryptographic Security Platform Vault.

Oracle Single Node Setup

This section describes how to configure Oracle TDE on a single node.

- Configuring CSP Vault for Oracle TDE
- Configuring the Oracle Server Cryptographic Library
- Configuring the Oracle Server Database
- Configuring the Oracle Server Database Encryption with TDE Key
- Installing the Cryptographic Security Platform Vault Linux Policy Agent for Oracle TDE

Configuring CSP Vault for Oracle TDE

This section explains how to configure Cryptographic Security Platform Vault for Oracle TDE.

Create Cryptographic Security Platform Vault Key Set for Oracle TDE

> Note: If you have an HSM configured with Cryptographic Security Platform Vault, you can create a keyset with HSM support enabled.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Cloud Keys**.
3. From the Key Sets tab, select **Actions > Create Key Set**.
4. On the Details tab of the Create Key Set dialog box, ensure that you select Oracle Database Server for the Database type.

For more information, see Creating a Key Set for TDE.

Enable TDE on Oracle Server

Before creating the Cryptographic Security Platform Vault Database Connector, you must enable TDE on the Oracle Server VM.

To enable TDE, run the following command on the Oracle Server VM: `hcl tde enable -y`

Configure Cryptographic Security Platform Vault Database Connector

To create the Cryptographic Security Platform Vault Database Connector.

1. Create a Database Connector for this KeySet and the Oracle Server VM.
   This is the VM registered during installation.
   Navigate to the KeySet and select the **Database Connectors** tab. Select **Create Connector Now**.
2. Enter the VM Name and Connector Name.
3. Check the database connector is created correctly.

Configuring the Oracle Server Cryptographic Library

This section explains how to configure the cryptographic library on Oracle Server.

1. Navigate to the Cryptographic Security Platform Vault database connector (configured here Configuring CSP Vault for Oracle TDE).
2. Select the database connector and from the **Action** menu, select **Generate Access Token**.
3. Copy the access token to the Oracle Server and create the **Cryptographic Config file**.
4. Create a config file using the copied Access Token (**Identity** and **Secret**) in your Oracle Server that will be used by the database administrators. The file should be in json format similar to the following:

```
# cat /opt/oracle/entrust/orcl.conf
{
   "identity" : "tde_connect1",
   "secret" : "S3XsZJe/EPNVf2D/YufOUS2HuOsLfKJBKjp3Zx/
JIrODqWYRQaYiFWnqet4lPsW0VcvGSvH7yB9BUZI
      xGi7CaM68cZFtw6yY5IvaClwD3344MFy28U9zjc0ayFRoHQi/
Dv25xTZ8a2JLlxJRyavO2VNGaCPUZfF
      sPN4lZg3EZwJ3fNKa7Owfpk0AuHmWmcqcYsxNnUxPuc+VYqXZk17omHzYP/
sA86RCv6+825t0EvuQhDH
      F7PxSiHjn+VShCYKNb+RxAvLgIIP/eVx0k/HWWI6/bZPpxwjFtw3tqnJ/
8toqPD+f+ZUlYT0mFRuE7BE

xGFf5LBCaVwf5FXKcOeXdaAg8zvaq0ynUjSB9JVw5FP6ZtFrY22hUcFcYDPITpjMzUzsX9d5BM8BhyT
L
```

```
        moPkj4IMyrSh3/nwGlJqPLj92EyImKsSOtOP6irpN22A2omvTsXUP/
pajuGrtUsKqzDdhAj+qmR2IDkS
        dOQMoSSvAgWyIAuS6q8WdMvm8SVCVUZpQrLvm226NvfvGCHKKNZaQCdxvL4XIgKI/
tCt+F+Xx0Pk/bkP

gLby90IM5NtktRkroxakhGkgSnoyDj2KovGvIwrHLpFpvDJkCwxbBce+OpcOjxR2tZ3nDM2zoZraSviT
        0P+V2hh7Z0jAWd4YrRdooxtQc3VPjTOrdOBldCExetFk="
}
```

Configuring the Oracle Server Database

This section explains how to configure the Oracle Server database.

Export Oracle Variables

On the Oracle Server, export the Oracle variables as follows:

```
export ORACLE_SID=orcl
export ORACLE_BASE=/opt/oracle
export ORACLE_HOME=$ORACLE_BASE/product/<oracle_db_version>/dbhome_1
export PATH=$PATH:$ORACLE_HOME/bin
export TNS_ADMIN=$ORACLE_HOME/network/admin
```

Where ORACLE_BASE is the Oracle installation directory. This is usually `/opt/oracle` or `/u01/app/oracle`.

Link pkcs11 library

To configure the Oracle PKCS#11 library folder to use the Entrust KeyControl PKCS#11 API.

1. On the Oracle Server, create the following directory path for the Entrust API library as the **oracle** user. Configure ownership and permissions on the directory as: **owner=oracle; group=oinstall; permissions=775**.
   ```
   sudo chown -R oracle:oinstall /opt/oracle/
   sudo chmod -R 775 /opt/oracle/
   mkdir -p /opt/oracle/extapi/64/hsm/entrust
   chown oracle:oinstall /opt/oracle/extapi/64/hsm/entrust
   chmod 775 /opt/oracle/extapi/64/hsm/entrust
   ```
2. Link the PKCS#11 library into the directory as the **oracle** user.
   ```
   ln -s /opt/hcs/lib/libpkcs11.so /opt/oracle/extapi/64/hsm/entrust/libpkcs11.so
   ```
   Important: The link must be created in /opt/oracle/extapi/64/hsm/entrust/libpkcs11.so or the connection between the Oracle DB and Cryptographic Security Platform Vault will not work.

Handling Timeout issues

1. If you expect network latency in the communication channel between Entrust KeyControl and Oracle Server, increase the fault tolerance of the database by setting the below as **sysdba**.
   ```
   ALTER SYSTEM SET "_heartbeat_period_multiplier"=<N> SCOPE=SPFILE;
   ALTER SYSTEM SET "_heartbeat_config"=AUTOCONNECT SCOPE=SPFILE;
   ```
2. Oracle Event 28420 determines the number of HSM heartbeats that can fail before the Oracle wallet is closed. Because the HSM heartbeat fires every 3 seconds, a very short network outage may result in wallet closure. Similarly, if a session is left idle for a period of approximately 15 minutes, HSM heartbeats can stop, and the Oracle wallet is closed. Therefore, Entrust recommends increasing the number of possible HSM heartbeat failures before the wallet closes. To make this a default setting execute
   ```
   ALTER SYSTEM SET EVENT='28420 trace name context <quantity> level <timeout_count>'
   COMMENT='HSM heartbeat attempts' SCOPE=SPFILE;
   ```

Set WALLET ROOT

Set the Oracle wallet location. Even though the HSM Wallet does not reside on a local disk, this step is required for TDE.

```
startup;
ALTER SYSTEM SET WALLET_ROOT="/opt/oracle/admin/orcl/wallet" scope=spfile;
shutdown immediate;
startup;
```

Set Hardware Keystore Type

Set the wallet type to HSM.

```
startup;
ALTER SYSTEM SET TDE_CONFIGURATION="KEYSTORE_CONFIGURATION=HSM" scope=both;
shutdown immediate;
startup;
```

Show wallet and keystore parameters

```
show parameter wallet
show parameter tde
```

Configure Oracle to generate the master encryption key

1. Grant the ADMINISTER KEY MANAGEMENT privilege to SYSTEM and any additional users that require access.
   ```
   GRANT ADMINISTER KEY MANAGEMENT TO SYSTEM;
   commit;
   exit;
   ```
2. Connect to the database as **System user**.
   ```
   $ sqlplus / as system
   ```
   Or from within `sqlplus` command.
   ```
   connect / as system/<password>
   ```
3. Open the HSM keystore.
   ```
   ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY "file:/opt/oracle/entrust/
   orcl.conf" CONTAINER = ALL;
   ```
4. Show keystore state.
   ```
   select CON_ID,WRL_TYPE,STATUS from V$ENCRYPTION_WALLET;
   ```

Generate the master encryption key

Create a TDE master encryption key that is stored inside the Entrust KeyControl. Oracle Database uses the TDE master encryption key to encrypt or decrypt TDE table keys and tablespace keys.

```
ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf" CONTAINER =
ALL;
```

This command performs two actions:

- **Create** key in KeyControl.
- **Use** the created key in Oracle as master encryption key.

Create the master encryption key for later use

The CREATE KEY clause of the ADMINISTER KEY MANAGEMENT statement can create a TDE master encryption key which can be activated later.

```
ADMINISTER KEY MANAGEMENT CREATE KsEY IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf"
CONTAINER = ALL;
```

Use pre-created master encryption key

List all encryption keys.

SELECT KEY_ID,KEY_USE FROM V$ENCRYPTION_KEYS;

Use the key from this list.

ADMINISTER KEY MANAGEMENT USE KEY 'key_identifier' IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf" CONTAINER = ALL;

Identify KeyID in use

SELECT KEY_ID FROM V$ENCRYPTION_KEYS WHERE ACTIVATION_TIME = (SELECT MAX(ACTIVATION_TIME) FROM V$ENCRYPTION_KEYS WHERE ACTIVATING_DBID = (SELECT DBID FROM V$DATABASE));

Configuring the Oracle Server Database Encryption with TDE Key

This section explains how to configure the Oracle Server database encryption using the TDE key.

Column Encryption

1. Create a table.
   Copy
   ```
   CREATE TABLE CUSTOMERS (ID NUMBER(5), NAME VARCHAR(42), CREDIT_LIMIT NUMBER(10));
   ```
2. Add data to the table.
   Copy
   ```
   INSERT INTO CUSTOMERS VALUES (001, 'Rakesh Sharma', 10000);
   INSERT INTO CUSTOMERS VALUES (002, 'Betty John', 20000);
   INSERT INTO CUSTOMERS VALUES (003, 'T Ramchandran', 30000);
   INSERT INTO CUSTOMERS VALUES (004, 'Amir Khan', 40000);
   ```
3. Encrypt a column.
   Copy
   ```
   ALTER TABLE CUSTOMERS MODIFY (CREDIT_LIMIT ENCRYPT);
   ```
4. List encrypted columns.
   Copy
   ```
   SELECT * FROM DBA_ENCRYPTED_COLUMNS;
   ```

Verification

To verify the column encryption.

1. Retrieve the encrypted data.
   Copy
   ```
   SELECT CREDIT_LIMIT FROM CUSTOMERS;
   ```
2. Close the wallet.
   Copy
   ```
   ADMINISTER KEY MANAGEMENT SET KEYSTORE CLOSE IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf"
   CONTAINER = ALL;
   ```
3. After closing the wallet, data retrieval should fail.
   Copy

```
ADMINISTER KEY MANAGEMENT SET KEYSTORE CLOSE IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf"
CONTAINER = ALL;
```

4. Data retrieval works again after opening the key store.
   Copy
   ```
   ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY "file:/opt/oracle/entrust/orcl.conf"
   CONTAINER = ALL;
   SELECT CREDIT_LIMIT FROM CUSTOMERS;
   ```

Tablespace Encryption

1. Create encrypted tablespace.
   Copy
   ```
   CREATE TABLESPACE SECURESPACE DATAFILE '/opt/oracle/oradata/orcl/SECURE01.DBF' SIZE 150M
   ENCRYPTION DEFAULT STORAGE (ENCRYPT);
   ```
2. Create a table in encrypted tablespace.
   Copy
   ```
   CREATE TABLE EMPLOYEE (ID NUMBER(5),NAME VARCHAR(42),SALARY NUMBER(10)) TABLESPACE
   SECURESPACE;
   ```
3. Insert data.
   Copy
   ```
   SELECT * FROM EMPLOYEE;
   ```

Verification: Verifying tablespace encryption is the same as for Column Encryption. See Verification.

Installing the Cryptographic Security Platform Vault Linux Policy Agent for Oracle TDE

To install and set up the Cryptographic Security Platform Vault on an Oracle Server. You will need to:

- Install the Policy Agent on the Oracle Server VM
  Important: Only virtual machines are supported.
- Create a VM Set in the Cryptographic Security Platform Vault for Databases.
- Register the Oracle Server VM on the Cryptographic Security Platform Vault VM Set.

⚠ When using Oracle TDE, the Cryptographic Security Platform Vault for Databases supports Oracle Database version 19c on Oracle Linux, RHEL, and SUSE.

To install and register the Policy Agent on the Oracle Server

1. Log in to the Cryptographic Security Platform Vault for Databases webGUI.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Download** Policy Agent.
4. Install the Policy Agent on the Oracle Server VM. For details, see the installation and administration guide at https://api.managed.entrust.com/vault/latest
5. Return to the Cryptographic Security Platform Vault for Databases web GUI and click **Workloads** in the top menu bar.
6. Select **Actions > Create New Cloud VM Set**. For more information, see Creating a Cloud VM Set for the CSP Vault for Databases.
7. Register the Oracle Server VM with the Cryptographic Security Platform Vault.

Manual Installation and Configuration for Oracle TDE

This section explains how to manually install and configure Cryptographic Security Platform Vault and Oracle TDE.

CSP Vault as EKM Provider for Microsoft SQL Server

The following topics explain how to configure Cryptographic Security Platform Vault as an EKM provider with Microsoft SQL Server.

- Cell-Level Encryption (CLE)
- Database Backup and Restore
- Encryption and Keys
- Introduction of Microsoft SQL Server
- Microsoft SQL Server Manual Installation and Configuration
- Removing Microsoft SQL Server TDE from the CSP Vault for Databases
- Rotating Microsoft SQL Server Keys
- Scripted Installation and Configuration
- Setting Up a Microsoft SQL Server Cluster for TDE
- Transparent Data Encryption (TDE)
- T-SQL Shortcuts and Tips
- Viewing TDE Reports for Microsoft SQL Server

Cell-Level Encryption (CLE)

In CLE separate data fields in the same table can be encrypted under different keys. These keys can be protected by different credentials. Unlike TDE protection, the user will need to obtain keys from the Cryptographic Security Platform Vault SQLEKM provider, and must have the correct credential to authorize and load the key(s) for the specific encrypted data they wish to access. Non-encrypted data is not affected by this and is visible to any authorized user.

> Note: This release of Cryptographic Security Platform Vault as an EKM for Microsoft SQL Server does not support key caching and this might impact CLE performance.

Cell-level encryption will only work on data stored in the database as VARBINARY type. You must provide any necessary type conversions so that data is in VARBINARY form before encryption is performed. Decryption will return the data to its original VARBINARY structure. It may then be necessary to reconvert to its original type for viewing in human-readable form.

> Note: Database backup files that use the VARBINARY type are not human-readable. Therefore, the previous inspection method, as used for TDE to directly check if data has been encrypted on disk, cannot be used for cell-level encryption.

If you have not already created the following keys and made them available in your current database copy, then create them now.

Symmetric key

Copy

```
USE TestDatabase
CREATE SYMMETRIC KEY dbAES256Key
FROM PROVIDER SQLEKM
WITH PROVIDER_KEY_NAME='ekmAES256Key',
IDENTITY_VALUE='Rg7n*9mnf29xl4',
```

```
CREATION_DISPOSITION = CREATE_NEW, ALGORITHM=AES_256;
GO
```

Asymmetric key

Copy

```
USE TestDatabase
CREATE ASYMMETRIC KEY dbRSA2048Key FROM PROVIDER SQLEKM
WITH PROVIDER_KEY_NAME='ekmRSA2048Key',
CREATION_DISPOSITION = CREATE_NEW, ALGORITHM=RSA_2048;
GO
```

Encrypting and decrypting a single cell of data

Before you start, make sure you have a fresh version of the 'TestTable' that is unencrypted.

> Note: In the example below, the encrypted and decrypted data is stored separately. Normally, the original data would be overwritten with the processed data.

1. View 'TestTable' by running the following query:

   Copy

   ```
   SELECT TOP 10 [FirstName]
   ,[LastName]
   ,CAST(NationalIdNumber AS decimal(16,0)) AS [NationalIDNumber]
   ,(NationalIdNumber) AS VarBinNationalIdNumber
   ,[EncryptedNationalIdNumber]
   ,[DecryptedNationalIdNumber]
   FROM [TestDatabase].[dbo].[TestTable]
   ```

   You will see the column NationalIdNumber in its original decimal form, and the column VarBinNationalIdNumber which shows the same number in its VARBINARY form (as stored in the database), and in which it will be encrypted.
   The columns EncryptedNationalIdNumber and DecryptedNationalIdNumber should contain NULL.
2. To encrypt a single cell in the 'TestTable', run the following query:

   Copy

   ```
   USE TestDatabase
   UPDATE TestTable
   SET EncryptedNationalIDNumber = EncryptByKey(Key_GUID('dbAES256Key'),
   NationalIDNumber)
   WHERE FirstName = 'Kate' AND LastName = 'Austin';
   GO
   ```

   This query encrypts the 'NationalIdNumber' for Kate Austin using the symmetric key 'dbAES256Key', and stores the result in the column 'EncryptedNationalIDNumber'.
   If encrypting using an asymmetric key, run the following query:

   Copy

   ```
   USE TestDatabase
   UPDATE TestTable
   ```

```
SET EncryptedNationalIDNumber =
ENCRYPTBYASYMKEY(ASYMKEY_ID('dbRSA2048Key'), NationalIDNumber)
WHERE FirstName = 'Kate' AND LastName = 'Austin';
GO
```

3. Run the previous 'View Table' query. The 'EncryptedNationalIdNumber' will now contain the encrypted value against the name Kate Austin.
4. Run the following query to decrypt the information:

Copy

```
USE TestDatabase
UPDATE TestTable
SET DecryptedNationalIDNumber = DecryptByKey(EncryptedNationalIDNumber)
WHERE FirstName = 'Kate' AND LastName = 'Austin';
GO
```

If decrypting using an asymmetric key, run the following query:

Copy

```
USE TestDatabase
UPDATE TestTable
SET DecryptedNationalIDNumber =
DECRYPTBYASYMKEY(ASYMKEY_ID('dbRSA2048Key'), EncryptedNationalIDNumber)
WHERE FirstName = 'Kate' AND LastName = 'Austin';
GO
```

5. Run the previous 'View Table' query. The 'DecryptedNationalIdNumber' will now contain the decrypted value against the name Kate Austin. Ensure that this value matches the corresponding value in the 'VarBinNationalIdNumber' column. If the values match, then the decryption worked successfully.
6. To view the decrypted value in its original decimal form, run the following query:

Copy

```
SELECT TOP 10 [FirstName]
,[LastName]
,CAST(NationalIdNumber AS decimal(16,0)) AS [NationalIDNumber]
,(NationalIdNumber) AS VarBinNationalIdNumber
,[EncryptedNationalIdNumber]
,CAST(DecryptedNationalIdNumber AS decimal(16,0)) AS
[DecryptedNationalIdNumber]
FROM [TestDatabase].[dbo].[TestTable]
```

1. Reset the 'EncryptedNationalIdNumber' and 'DecryptedNationalIdNumber' columns by running the following query:

Copy

```
USE TestDatabase
UPDATE TestTable
SET EncryptedNationalIDNumber = NULL, DecryptedNationalIDNumber = NULL;
GO
```

Encrypting and decrypting columns of data

Before you start, make sure you have a fresh version of the 'TestTable' that is unencrypted.

> Note: In the example below, the encrypted and decrypted data is stored separately. Normally, the original data would be overwritten with the processed data.

Perform the same steps as shown in Cell-Level Encryption (CLE) , but in this case where encryption or decryption occurs, replace with the following queries.

- Encrypt an existing column of data using the symmetric key:
  Copy
  ```
  USE TestDatabase
  UPDATE TestTable
  SET EncryptedNationalIDNumber = EncryptByKey(Key_GUID('dbAES256Key'),
  NationalIDNumber);
  GO
  ```
- Decrypt an existing column of data using the symmetric key:
  Copy
  ```
  USE TestDatabase
  UPDATE TestTable
  SET DecryptedNationalIDNumber = DecryptByKey(EncryptedNationalIDNumber);
  GO
  ```
- Encrypt an existing column of data using the asymmetric key:
  Copy
  ```
  USE TestDatabase
  UPDATE TestTable
  SET EncryptedNationalIDNumber = ENCRYPTBYASYMKEY(ASYMKEY_ID('dbRSA2048Key'), NationalIDNumber);
  GO
  ```
- Decrypt an existing column of data using the asymmetric key:
  Copy
  ```
  USE TestDatabase
  UPDATE TestTable
  SET DecryptedNationalIDNumber = DECRYPTBYASYMKEY(ASYMKEY_ID('dbRSA2048Key'),
  EncryptedNationalIDNumber);
  GO
  ```

Creating a new table and inserting cells of encrypted data

The following assumes you have available 'TestDatabase' and the keys 'dbAES256Key', 'dbRSA2048Key' as created previously.

Create a table with an encrypted field:

To create a new database table 'Customers', where individual cells of data held in the third column ('CardNumber') will be encrypted, execute the following query:

Copy

```
USE TestDatabase
GO
CREATE TABLE Customers (FirstName varchar(MAX), SecondName varchar(MAX), CardNumber varbinary (MAX));
GO
```

Insert encrypted data with the symmetric key:

The following query allows the user to enter the sensitive data ('CardNumber') via the keyboard and then immediately encrypt using a symmetric key, sending the 'CardNumber' directly into memory (and database) in an encrypted state.

Copy

```
USE TestDatabase
INSERT INTO Customers (FirstName, SecondName, CardNumber) VALUES ('Joe', 'Blogg',
ENCRYPTBYKEY(KEY_GUID('dbAES256Key'), CAST('<16 digit card number>' AS VARBINARY)));
INSERT INTO Customers (FirstName, SecondName, CardNumber) VALUES ('Iain', 'Hood',
ENCRYPTBYKEY(KEY_GUID('dbAES256Key'), CAST('<16 digit card number>' AS VARBINARY)));
INSERT INTO Customers (FirstName, SecondName, CardNumber) VALUES ('Joe', 'Smith',
ENCRYPTBYKEY(KEY_GUID('dbAES256Key'), CAST('<16 digit card number>' AS VARBINARY)));
GO
```

where *<16 digit card number>* is a 16-digit payment card number to be encrypted.

View data encrypted with the symmetric key in plain text:

The following query allows the user to view, in plain text on screen, the sensitive data ('CardNumber') for customers named 'Joe'. The data remains encrypted in memory and (database).

Copy

```
USE TestDatabase
SELECT [FirstName], [SecondName],
CAST(DecryptByKey(CardNumber) AS varchar) AS 'Decrypted card number'
FROM Customers WHERE [FirstName] LIKE ('%Joe%');
GO
```

If an asymmetric key ('dbRSA2048Key') is used, similar actions can be achieved using the following queries.

Insert encrypted data with the asymmetric key:

Copy

```
USE TestDatabase
INSERT INTO Customers (FirstName, SecondName, CardNumber)
VALUES ('Joe', 'Connor', ENCRYPTBYASYMKEY(ASYMKEY_ID('dbRSA2048Key'), CAST('<16 digit card number>' AS VARBINARY)));
INSERT INTO Customers (FirstName, SecondName, CardNumber)
VALUES ('Richard', 'Taylor', ENCRYPTBYASYMKEY(ASYMKEY_ID('dbRSA2048Key'), CAST('<16 digit card number>' AS VARBINARY)));
INSERT INTO Customers (FirstName, SecondName, CardNumber)
VALUES ('Joe', 'Croft', ENCRYPTBYASYMKEY(ASYMKEY_ID('dbRSA2048Key'), CAST('<16 digit card number>' AS VARBINARY)));
GO
```

where *<16 digit card number>* is a 16-digit payment card number to be encrypted.

View data encrypted with the asymmetric key in plain text:

Copy

```
USE TestDatabase
SELECT [FirstName], [SecondName],
CAST(DECRYPTBYASYMKEY(ASYMKEY_ID('dbRSA2048Key'),CardNumber) AS varchar) AS 'Decrypted card number'
FROM Customers WHERE [FirstName] LIKE ('%Joe%');
GO
```

> Note: It is possible to encrypt separate table cells using different keys. When decrypting with a particular key, it should not be possible to see data that was encrypted using another key.

Database Backup and Restore

To back up and restore the TDE encrypted database, the TDE EKM access must be available to the same Keys from the SQL Server VM where you are trying to restore the database.

- Backing up the TDE Encrypted Database
- Restoring the TDE Encrypted Database
- Restoring the TDE Encrypted Database on an Alternate (Failover) VM

Backing up the TDE Encrypted Database

If you are backing up a database that uses cell encryption keys, you should ensure that all sensitive data is encrypted first before back-up commences. Before back-up, remove the cell encryption key references from the database itself. If key references are not removed from the database, they will be stored within the database back-up. This should be avoided from a security point of view. If you are backing up a database that is both cell and TDE encrypted, perform the above instructions for the cell encryption keys before continuing with the following instructions for backing up a TDE encrypted database.

When backing up a TDE encrypted database, you must have the TDE credential and database wrapping key (TDEKEK) present.

Your backup will include data content of your selected database, but may not include backups of SQL Server logins or credentials. For further details, see the Microsoft SQL Server documentation.

Important:

If you plan to restore this backup to an alternate database, we recommend that you retrieve the thumbprint of the master key before the backup. This will be required when you restore the backup. Because administrators usually rotate the master key after creating a backup, you will not be able to fetch the thumbprint at that time.

Use the following SQL statements to get the thumbprint:

Copy

```
use master
GO

SELECT DB_NAME(database_id) AS DatabaseName,encryption_state,percent_complete,encryptor_thumbprint,
encryptor_type FROM sys.dm_database_encryption_keys
GO

Select * from sys.dm_database_encryption_keys
Select * from sys.asymmetric_keys
GO
```

Use the following SQL statement to backup the encrypted database:

Copy

```
BACKUP DATABASE [testdb] TO  DISK = N'D:\testdb.bak'
```

Restoring the TDE Encrypted Database

On the same SQL Server VM, you can restore the backup using the following SQL statements:

Copy

```
USE [master]
RESTORE DATABASE testdb FROM DISK = N'D:\testdb.bak' WITH FILE = 1, NOUNLOAD, STATS = 5
```

To open old versions of the TDE key with its thumbprint, you will need to specify the key name starting with @ followed by the thumbprint of the key. For example:

Copy

```
USE master;
CREATE ASYMMETRIC KEY TDE_KEY_v1 -- Give the master key version a name in SQL Server
FROM PROVIDER EKM_Prov WITH
PROVIDER_KEY_NAME = '@E5196A7752214754934DF7BD479B6F7E',   -- master key thumbprint
CREATION_DISPOSITION = OPEN_EXISTING;
GO
```

Restoring the TDE Encrypted Database on an Alternate (Failover) VM

Before You Begin

- You must connect to the same CSP Vault cluster that the primary SQL Server VM is connected to.
- The user group must be the same as the primary VM. The default user group is Cloud Admin Group.
- You have to make the keys accessible on this VM in addition to the original VM.

Note: To restore a TDE encrypted database on the same VM, see Restoring the TDE Encrypted Database .

Procedure

1. Copy the bundle that you downloaded in Downloading the TDE Script Bundle for Microsoft SQL Server.
2. Extract the bundle on the new VM and copy the modified entrust.conf from the primary and overwrite the configuration file that you just extracted.
3. Run the following PowerShell script to set up the new client:
   PS> .\setup.ps1 -node other -config .\entrust.conf
   Note: The `-node` parameter must be `other`.
4. Edit the entrust.conf file and update the following parameters:

Parameter	Description
db_server_name	The name of the SQL server instance where you are restoring the backup.
sysadmin_user	If you are using SQL server authentication, then set its value to the correct sysadmin user for the node that you are restoring. If you are using Windows authentication, keep this line commented out.
sysadmin_password	If you are using SQL Server authentication, you can either write the password here or keep this line commented out to be prompted for the password. If you are using Windows authentication, keep this line commented out.

5. Fetch the thumbprint of the master key. This can be done using one of the following ways:
   - If you retrieved the master key thumbprint immediately before running the backup, you can skip this section.
   - If you attempt to restore the backup without the thumbprint, the thumbprint is printed in the failure message.
     Microsoft SQL Server Management Studio example:

Encryption and Keys

This section provides more detail regarding encryption and key management, together with examples showing how to encrypt and decrypt data.

When you have configured the CSP Vault SQLEKM provider, and you have a suitable credential associated with your login, you can use the provider to:

- Manage keys.
- Encrypt or decrypt entire databases, or fields within tables, within SQL Server using TDE or cell-level encryption, or both at the same time.

Keys can be created in the Cryptographic Security Platform Vault for Databases and referenced by the appropriate database as required for use. When a reference of a key is no longer required for active use in the database, it should be deleted from the database while retaining the original copy of the key in the provider, which also acts as a secure backup. Storing original copies of keys in Cryptographic Security Platform Vault for Databases is more secure than leaving key references and associated data together in the database. As long as the key is not deleted from Cryptographic Security Platform Vault for Databases, its reference can be restored when next required for active use in the database.

Note: Copying and deletion of keys does not apply to a TDE Database Encryption Key (TDEDEK), which is created as an integral part of a user database. On the other hand, this can apply to the wrapping key (TDEKEK) which is used to protect the TDEDEK. See Encryption and Keys .

It is recommended to regularly re-encrypt your data using fresh keys so that any persistent attempts to decipher or compromise your encrypted data are impeded.

Examples

To run the examples included in this section, open SQL Server Management Studio and connect to a SQL Server instance, then open a query window to execute a query.

In the example T-SQL statements, the names used for keys (such as 'dbAES256Key') and databases (such as 'TestDatabase') are example names only.

The exception is 'master' database, which is a real database.

Note: You must have a SQL Server login and appropriate permissions to configure or access Microsoft SQL Server or the CSP Vault SQLEKM provider.

Key naming, tracking and other identity issues

Keys held in the database are really references to actual keys held in the Cryptographic Security Platform Vault. For the purpose of key tracking, it is suggested that you use the same name for both the database and the provider version of a key. Use a suffix or prefix to distinguish between the database and provider versions.

In a database there can be only one key with a specific name at any one time.

If you have a significant number of keys, you may wish to implement a key naming convention that helps you track which keys encrypt which data, backed up with some form of secure documentation.

To use the examples in this document you will first need to create 'TestDatabase' and 'TestTable' as shown in Creating a database and Creating a table Otherwise, provide your own database and table to perform encryption operations and adapt the examples accordingly. Refer to Encryption and Keys before adapting any examples.

Note: Keys created under a login that is mapped to a particular credential will be protected by that credential.

Supported cryptographic algorithms

The CSP Vault SQLEKM provider supports the following algorithms: 'AES_256', 'RSA_ 2048', 'RSA_3072' and 'RSA_4096'.

Introduction of Microsoft SQL Server

The CSP Vault for Databases can be integrated with Microsoft SQL Server, Extensible Key Management (EKM), to manage the keys and provide data-at-rest encryption for sensitive information held by Microsoft SQL Server. This gives you a high quality SQL Extensible Key Management (SQLEKM) provider, integrating with your Microsoft SQL Server database infrastructure with minimal disruption.

The following Microsoft SQL Server types are supported:

- Single node MSSQL server
- MSSQL Failover cluster
- MSSQL always on cluster

There are no limitations while using TDE with Microsoft SQL Server database.

The integration supports Transparent Data Encryption (TDE) and Cell-Level Encryption (CLE), and the concurrent use of both TDE and CLE.

For a list of tested versions, see CSP Database Vault Overview.

Extensible Key Management (EKM)

The Extensible Key Management (EKM) API, as provided for Microsoft SQL Server, can be used to protect databases when using Entrust Cryptographic Security Platform Vault.

> Note: Encryption should be part of a wider scheme of security practices to protect your database assets that should take into account any regulatory or legal requirements for data protection. Administration and management of encryption within any organization is a serious issue that requires appropriate training and resources.

A Microsoft SQL Server service permits the creation of one or more databases. When a client request is made to the SQL Server, it determines which of the databases are the subject of the query, and loads data that is the subject of the query into available memory from disk storage.

From a security perspective, the Microsoft SQL Server supports the use of keys to protect its databases. These keys can be used to perform two levels of encryption.

- **Transparent Data Encryption (TDE)** is used to encrypt an entire database in a way that does not require changes to existing queries and applications. A database encrypted with TDE is automatically decrypted when SQL Server loads it into memory from disk storage, which means that a client can query the database within the server environment without having to perform any decryption operations. The database is encrypted again when saved to disk storage. When using TDE, data is not protected by encryption whilst in memory. Only one key at a time per database can be used for TDE.
- To use **Cell-Level Encryption (CLE)**, you must specify the data to be encrypted and the key(s) with which to encrypt it. CLE uses one or more keys to encrypt individual cells or columns. It gives the ability to apply fine-grained access policies to the most sensitive data in a database. Only the specified data is encrypted: other data remains unencrypted. This mode of encryption can minimize data exposure within the database server and client applications. You can apply CLE to database tables that are also encrypted using TDE. Note that when using CLE, data is only decrypted in memory when required for use. Separate data can be encrypted using different keys within the same data table.

There may be performance trade-offs between speed and security, regarding use of TDE or CLE, but these issues are beyond the scope of this document.

Cryptographic Security Platform Vault supports the generation and management of these keys. Authorized access to the secure environment and the keys under its protection, is controlled by a protection domain. To use a protection domain, you must first set up a database credential.

To read from or write to an encrypted database, a user must have all of the following:

- An authorized database login, with password, that maps to an appropriate database credential.
- Knowledge of the correct protection domain(s) and associated passphrase(s).
- For CLE, knowledge of the keys in use, and their passwords (if any).
- Knowledge of the appropriate encrypted database to read or write to.

If keys are lost, they can be securely recovered from a backup as authorized through secure administrative means. It is important to maintain an up-to date backup of your data.

> Note: When use of keys is legitimately made available to the database, the continuing security of data protected by those keys becomes dependent on access offered through SQL Server in accordance with your organization's security policies.

For more information about configuring the Entrust CSP Vault SQLEKM provider to perform encryption, see Microsoft SQL Server Manual Installation and Configuration.

Querying encrypted data

When the client sends a query to SQL Server, the Entrust CSP Vault SQLEKM provider checks the level of encryption on the database that is the subject of the query. If SQL Server uses a database that employs TDE, the process of loading the assigned keys and encrypting the database when it is stored is done automatically. The reverse decryption operation is also automatic when a TDE encrypted database needs to be used and is loaded into memory. If a database is encrypted using TDE only, this is transparent to the client or user who does not need to be aware of the encryption status or specify any encryption or decryption operations when querying the database. Backup and transaction logs are similarly encrypted.

CLE can be used with or without TDE. In either case, when using CLE the target data must be explicitly encrypted in memory before being stored, or explicitly decrypted after being loaded into memory from storage. You must specify:

- The fields to be encrypted or decrypted.
- The (correct) key to be used.

CLE is not automatic. If you use it, you must be aware of the encryption or decryption process.

Note that if TDE is used in combination with CLE, then after the CLE has been performed, the encrypted cells will be additionally encrypted by the TDE process when the data is stored. When the TDE process decrypts, the cells are returned to memory in their original encrypted form and must be decrypted a second time using the appropriate cell-level key. The database-level TDE processes remain automatic.

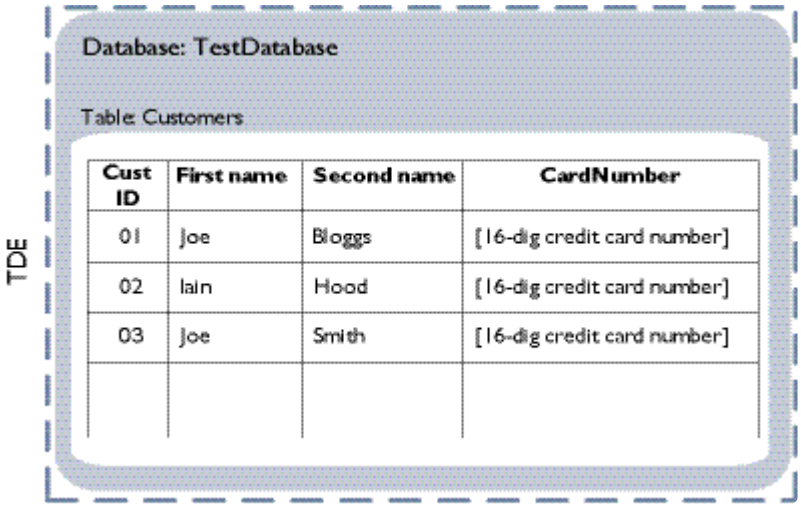
Example queries

The following example queries use a database table of customer information that includes first names, second names and payment card numbers. The queries concern the details of customers whose first names are Joe.

The database is decrypted when it is loaded into memory from disk storage. As this happens before the query is performed, the query does not have to specify any decryption operation:

Example 1: TDE encryption/decryption only

In this example, the entire database is encrypted with TDE.



The database is decrypted when it is loaded into memory from disk storage.

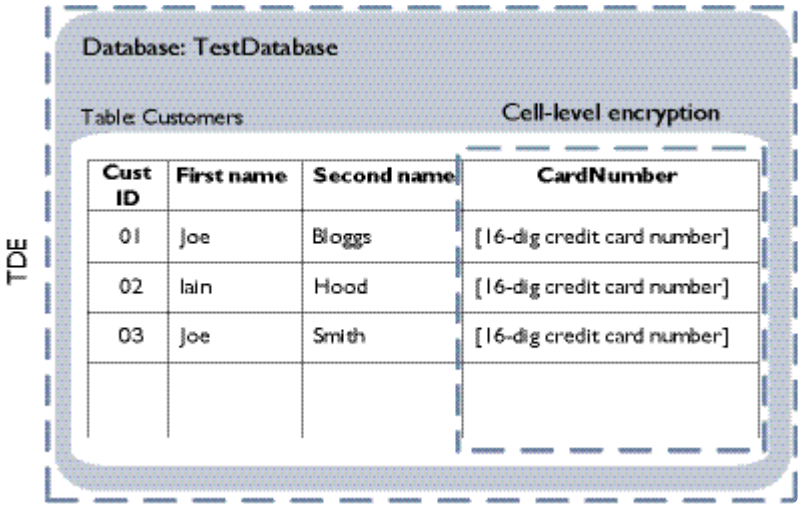
As this happens before the query is performed, the query does not have to specify any decryption operation:

Copy

```
USE TestDatabase
SELECT * FROM Customers WHERE
FirstName LIKE ('%Joe%');
```

Example 2: TDE combined with CLE/decryption

In this example, the database is encrypted with TDE, and the column of credit card numbers in the table of customers is additionally protected with CLE.



The query does not have to take account of TDE on the database because it is automatically decrypted on loading into memory from disk storage before the query is performed. However, the query must specify the (cell-level) decryption of the column of credit card numbers before the details of customers called 'Joe' can be returned.

Copy

```
USE TestDatabase
SELECT [FirstName], [SecondName], CAST(DecryptByKey(CardNumber) AS VARCHAR)
AS 'Decrypted card number'
FROM Customers WHERE [FirstName] LIKE ('%Joe%');
```

Microsoft SQL Server Manual Installation and Configuration

This section explains how to manually install and configure Cryptographic Security Platform Vault and Microsoft SQL Server for TDE.

- Configuring a CSP Vault Database Connector
- Configuring Microsoft SQL Server for EKM
- Creating a Cloud VM Set for Microsoft SQL Server TDE
- Creating a Key Set for Microsoft SQL Server TDE

- Enable TDE on SQL Server
- Installation Requirements for Microsoft SQL Server TDE
- Installing and Registering the Policy Agent for SQL Server

Configuring a CSP Vault Database Connector

Before creating the Cryptographic Security Platform Vault Database Connector, you must ensure you have enabled TDE on the SQL Server VM. See Installation Requirements for Microsoft SQL Server TDE . After you create the connector, you can generate an access token to be used to configure the cryptographic provider.

1. Create a Database Connector for this Key Set and the SQL Server VM.
   This is the VM that you registered when you installed the Policy Agent. See Installing and Registering the Policy Agent for SQL Server.
2. Select the Key Set that you want to use and then scroll down to select the **Database Connectors** tab.
3. Select **Actions > Create Connector**.
   If there are no database connectors created, you can also click **Create Connector Now**.
4. In the Create Database Connector dialog box, enter the VM Name and Connector Name, then select the Expiration.
5. Click **Create**.
   If the database connector is created correctly, you will see it listed in the table beneath the Database Connectors tab as ENABLED.
6. Select the database connector that you just created, and select Actions > **Generate Access Token**.
   On the Generate Access Token window, the new access token is created and displays both an identity and a secret. You will need to copy these to use when configuring the cryptographic provider.

Configuring Microsoft SQL Server for EKM

This section explains how to configure Microsoft SQL Server for Extensible Key Management (EKM).

You must have configured the Cryptographic Security Platform Vault Database Connector before you configure EKM. See Configuring a CSP Vault Database Connector .

Configure EKM on the SQL Server

1. Start a connection with the SQL Server database engine.
2. Run the following commands to enable Extensible Key Management:

```
sp_configure 'show advanced', 1
GO
RECONFIGURE
GO

sp_configure 'EKM provider enabled', 1
GO
RECONFIGURE
GO
```

3. Run the following command to create the Cryptographic Provider:

```
CREATE CRYPTOGRAPHIC PROVIDER EKM_Prov
FROM FILE = 'c:\program files\hcs\bin\htsqlekm_provider.dll';
GO
```

Configure the Cryptographic Provider on SQL Server

1. Using the identity and secret that you copied when you generated the access token, create a credential file in json format. This file should be named something easily identifiable, and located where it is accessible to SQL Server, for example, C:\Users\Administrator\sqlcred.conf. Please make sure that Windows did not add an extra .txt extension to the filename.
   For SQL server clusters, the file path and name should be the same on all nodes.
   Copy
   ```
   {
     "identity"    : "<the identity copied from the access token>",
     "secret"      : "<the secret copied from the access token>"
   }
   ```
2. Create a credential in your Microsoft SQL Server VM that includes the credential file path for the identity and secret file that you created.
   Important: The parameter SECRET is mandatory for the CREATE CREDENTIAL statement in EKM, but is not used here because both the identity and secret are contained in the sqlcred.conf file. You can assign it any value because the provider will ignore it.
   Copy
   ```
   CREATE CREDENTIAL sa_ekm_tde_cred
   WITH IDENTITY = 'file:C:\Users\Administrator\sqlcred.conf',
   SECRET = 'ignore'
   FOR CRYPTOGRAPHIC PROVIDER EKM_Prov ;
   GO
   ```

   Important: We recommend using the file method instead of simply copying the actual identity and secret because it is required for SQL Server clusters.
   If you do not plan to use a SQL Server cluster, and would rather use the identity and secret values, enter it as follows:
   Copy
   ```
   CREATE CREDENTIAL sa_ekm_tde_cred
   WITH IDENTITY = '<Connector name>',
   SECRET = '<Secret Access Key>'
   FOR CRYPTOGRAPHIC PROVIDER EKM_Prov ;
   GO
   ```
3. Add the credential to a privileged user with domain login in the format [DOMAIN\login].
   Copy
   ```
   ALTER LOGIN [DOMAIN\login]
   ADD CREDENTIAL "sa_ekm_tde_cred";
   GO
   ```

Creating a Cloud VM Set for Microsoft SQL Server TDE

Before you install the Policy Agent, you must create a Cloud VM Set.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Create New Cloud VM Set**.

4. On the **VM Set** tab:
    a. Enter a name for the Cloud VM Set.
    b. Select the group to which this set should belong, or accept the default.
    c. Optionally enter a description for the set.
5. Click **Create**, or see Creating a Cloud VM Set for the CSP Vault for Databases for descriptions of additional properties that you can set.

Creating a Key Set for Microsoft SQL Server TDE

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Cloud Keys**.
3. Select **Actions > Create Key Set**.
4. On the Details tab of the Create Key Set dialog box, ensure that you select **Microsoft SQL Server** for the Database type.
5. If you have an HSM, ensure that you set the properties for the HSM.

For more information, see Creating a Key Set for TDE.

Enable TDE on SQL Server

Before the Microsoft SQL Server VM can be used for TDE, you need to enable TDE.

1. Log in to the command prompt or power-shell for the Microsoft SQL Server VM.
2. Run the following command: `hcl tde enable -y`
3. Enter `y` at the confirmation prompt.

Installation Requirements for Microsoft SQL Server TDE

Entrust recommends you install the following:

- Microsoft SQL Server
  Important: Only virtual machines are supported.
  If you are using a SQL Server cluster, these installation steps should be repeated for each node in the cluster.
- Ensure you apply all the latest service packs, updates and hotfixes for Microsoft SQL Server software.
- SQL Server credentials and appropriate permissions are required for all users to install and configure SQL EKM.
- Install Microsoft SQL Server Management Studio
- Install Microsoft SQLCmd Utility

Installing and Registering the Policy Agent for SQL Server

To install and register the Policy Agent on the SQL Server:

1. Log in to the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Download Policy Agent**.
4. Install the Policy Agent on your SQL Server VM. For details, see the installation and administration guide at https://api.managed.entrust.com/vault/latest
5. Locate the Cloud VM Set that you created on the **WORKLOADS** tab.
6. Register the SQL Server VM with Cryptographic Security Platform Vault. For details, see the installation and administration guide at https://api.managed.entrust.com/vault/latest
7. Select the database connector that you just created, and select **Actions > Generate Access Token**.
   On the Generate Access Token window, the new access token is created and displays both an identity and a secret. Copy these to use when configuring the cryptographic provider.

Removing Microsoft SQL Server TDE from the CSP Vault for Databases

This section explains how to uninstall the Cryptographic Security Platform Vault Policy Agent and the VM for Microsoft SQL Server TDE.

Note:

- If you delete a provider login credential you will no longer be able to use it for the Cryptographic Security Platform Vault SQLEKM provider.
- If you delete an associated Cryptographic Security Platform Vault database connector you will no longer be able to use it to access the SQL Server or the Cryptographic Security Platform Vault SQLEKM provider.
- If you unregister, uninstall or destroy the Cryptographic Security Platform Vault Policy Agent client, you will no longer be able to access the data on SQL Server.

Turning off TDE and removing TDE setup

You must turn off TDE on all your databases and remove the TDE setup before uninstalling Cryptographic Security Platform Vault SQLEKM. Otherwise, you will not be able to decrypt any databases encrypted with TDE.

Before disabling and removing TDE encryption you are advised to back up the encrypted database. For more information, see Restoring the TDE Encrypted Database .

1. In SQL Server Management Studio, navigate to **Databases > TestDatabase**.
2. Right-click **TestDatabase**, then select **Tasks > Manage Database Encryption...**.
3. Ensure **Set Database Encryption On** is deselected, then click **OK**.
4. Wait for the decryption process to finish. Check this by referring to Microsoft SQL Server Manual Installation and Configuration .
5. When the database has completed decryption, drop the encryption key using the following T-SQL query:
   Copy
   ```
   USE TestDatabase
   DROP DATABASE ENCRYPTION KEY;
   GO
   ```
6. Restart the database instance. If you are using a database failover cluster, you may have to do this directly on the active server. In SQL Server Management Studio right click on the instance and select **Restart**.
7. In SQL Server Management Studio, navigate to **Security > Logins**, and select the TDE login you wish to remove (for example, **tdeLogin**). Right-click on the selected login and select **Properties**.
8. Ensure the associated credential (for example, **tdeCredential**) is highlighted then choose **Remove**. Untick the box **Map to credential**. Click **OK**.
9. In SQL Server Management Studio, navigate to **Security > Credentials**, and select the same credential you previously removed from the login (for example, **tdeCredential**). Right-click on the credential and select **Delete**. In the following screen, select **OK**.
10. In SQL Server Management Studio, navigate to **Security > Logins**, and select the TDE login you wish to remove (for example, **tdeLogin**). Right-click on the selected login and select **Delete**. In the following screen, select **OK**.
11. In SQL Server Management Studio, navigate to **Databases > System Databases > master >Security > Asymmetric keys**. Select the key you wish to remove (for example, **dbAsymWrappingKey**). Right click on the key and select **Delete**. Alternatively, you can use the following query:
    Copy
    ```
    USE master
    DROP ASYMMETRIC KEY dbAsymWrappingKey REMOVE PROVIDER KEY;
    GO
    ```

Rotating Microsoft SQL Server Keys

Rotating Keys using the webGUI:

1. Log in to the CSP Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, select **CloudKeys**.
3. Click the **CloudKeys** tab and then select the key that you want to rotate.
4. In the Details section, in the Rotation Schedule row, click **Rotate Now**.

Rotating Keys using Microsoft SQL Server:

Copy

```
USE master;
CREATE ASYMMETRIC KEY TDE_KEY_v2 -- Give the NEW KEK version a name in SQL Server
FROM PROVIDER EKM_Prov
WITH PROVIDER_KEY_NAME = '<Cloud Key>', -- master_key1 created in CSP Vault
CREATION_DISPOSITION = OPEN_EXISTING;
GO

CREATE CREDENTIAL tde_ekm_cred_v2
WITH IDENTITY = 'tde_connect1',
SECRET = 'xdZ5TCNRLcldfeCr8SDZyu+TJF1kH5MGMZgaj2vZeUgP3Nf2xBh/
lWicDzhvaWZCN3w3A5gVlkgG05AnfdllYafP6HE+zSqsGX
Ay4Fx7deZYqTbOcz3HOYmu99IE81fATfG58C1qukmzY9UW3z04p3TaAM2xho30Slhm2hs1iupsXADGBuSVYSxi5C8aH2
6jrXZFl 6hlilnwK8F3GF3MQSWksRmgruAOSBLfnh+iasM1vqkZ/BHZ/
3vRcsZZTrC3DycHXGrZqwcVxZaPsQlok2vC0cRw6m7afBCJI76y
854klGEflOCvQugGxxyEBpPOOuLrCEQo0y5jr9x2dYgWlr4X24qTnW9+BVMlMqGh2oOmqBqqNFBVUBEUjSIjHZuE/4xo/
lH6akn
Ru0PHP2JDhvDGpouRfCaJ7/5q1dygiEl1OcSoANemqu44GUaVyAS1esIM182T6rNbbmRgRJsyqznrdTLx02oUPbtbUXRUd
h7hgY GPBB+uvid2YYT+NOsXM2nR0XdkxJ59x2RbFErjTGuf6mj756qE2RBzV9eeIEjMQgiajfTUNWz/
NTk+Ca5z6Rdznig8VTCLR0Q3i HxF6zb5jSYkLeo0pbeUuuSLtlPX7kkrzFt07j2dj8q3V2lkcvYLOMdgtzzW/
ILGjS0jEyZBbyROxK+48WSQ244EVhs='
FOR CRYPTOGRAPHIC PROVIDER EKM_Prov ;
GO

CREATE LOGIN TDE_Login_v2
FROM ASYMMETRIC KEY TDE_KEY_v2 ;
GO

ALTER LOGIN TDE_Login_v2
ADD CREDENTIAL tde_ekm_cred_v2
GO

use testdb
```

```
GO

ALTER DATABASE ENCRYPTION KEY
ENCRYPTION BY SERVER ASYMMETRIC KEY TDE_KEY_v2;
GO
```

Check the thumbprint of the TDE key used to encrypt the database key:

Check the “encryptor thumbprint” to know the version of key used to encrypt the database key.

Copy

```
use master
GO
SELECT DB_NAME(database_id) AS DatabaseName,encryption_state,percent_complete,encryptor_thumbprint,
encryptor_type
FROM sys.dm_database_encryption_keys
GO
```

Scripted Installation and Configuration

You can use PowerShell-based scripts to install and configure Microsoft SQL Server TDE on the Cryptographic Security Platform Vault for Databases. This allows you to simplify the setup process.

- Checking your Microsoft SQL Server Connections
- Downloading the TDE Script Bundle for Microsoft SQL Server
- Encrypting the Database on the Active SQL Server Node
- Rotating the Master Key on the Active SQL Server Node
- Setting up the Entrust Client Using Scripts

Checking your Microsoft SQL Server Connections

It is highly recommended that you check the connections with each SQL Server node after you run the setup.ps1 command. If the connection test fails due to an invalid TDE connector, then you should manually create a new TDE connector and access token, and copy them to the access token file.

You can check the connection between the SQL Server VM and CSP Vault for Databases using the following commands:

- PS> hcl status
  This command shows if the VM is able to communicate with the CSP Vault for Databases. It also shows if the VM is properly authenticated and has a regular heartbeat with the CSP Vault for Databases.
- PS> check-connection <Access Token File Path>
  This command creates a test RSA-2048 key on the CSP Vault for Databases. The name of the key is _rsa_2048_test_key_. CSP Vault uses this key to test encrypt and decrypt operations and then destroys the key.
  This command executes all the tasks using the TDE library installed by the Entrust Policy Agent. The TDE library can be found in the Policy Agentinstallation directory, for example, in C:\Program Files\hcs\bin\htsqlekm_provider.dll

Downloading the TDE Script Bundle for Microsoft SQL Server

Important: To extract the TDE Script Bundle ZIP file on Windows, use the PowerShell Expand-Archive command instead of the Windows ZIP tool to prevent signing warnings.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Download TDE script bundle**.
4. On the Download TDE script bundle dialog box, complete the following:

Field	Description
Name	Select a name to identify this database. This name will be used for the .zip bundle you download, and also as a prefix for related assets such as the KeySet and the Cloud VM Set.
Database Type	Select Microsoft SQL Server.
Enable HSM	If an HSM is configured, check the Enable HSM checkbox to protect your TDE master keys with the HSM. You will need to verify the HSM connection before you can proceed.
CSP Nodes Mapping	Optionally select the name of your Node Mapping.

5. **Click Continue**.
6. On the TDE Script Bundle Details dialog box, review your choices and click **Download**.

The <name>.zip bundle is automatically downloaded.

Important: To extract the TDE Script Bundle ZIP file on Windows, use the PowerShell Expand-Archive command instead of the Windows ZIP tool to prevent signing warnings.

Encrypting the Database on the Active SQL Server Node

1. Ensure that you are running on the active node for the database that you intend to encrypt. You can do this by checking the Windows Failover Cluster Manager or the SQL Server Management Studio.
2. Encrypt the database using the following script:
   PS> .\encryptclust.ps1 -database <my_test_db> -config .\entrust.conf
   Where -database is the name of the database to be encrypted and -config is the configuration file.
3. Check the keys and the encryption state of the database as follows:

```
Copy
use master
GO

SELECT DB_NAME(database_id) AS DatabaseName,encryption_state,percent_complete,encryptor_thumbprint,
encryptor_type FROM sys.dm_database_encryption_keys
GO

Select * from sys.dm_database_encryption_keys
Select * from sys.asymmetric_keys
GO
```

Note: The SQL key thumbprint is the same as the Cryptographic Security Platform Vault KEY ID.

Rotating the Master Key on the Active SQL Server Node

1. Ensure that you are running on the active node for the database that you intend to encrypt. You can do this by checking the Windows Failover Cluster Manager or the SQL Server Management Studio.
2. Rotate the master key using the following script:
   PS> .\encryptclust.ps1 -database <my_test_db> -config .\entrust.conf -rotate
   Where:
   - -database is the name of the database.
   - -config is the name of the configuration file that you updated.
   - -rotate provides the information that the database is already encrypted and the key needs to be rotated.

Setting up the Entrust Client Using Scripts

Important: If you add the vault user password to the entrust.conf file, then it can be seen in trace log files. We recommend that you do not include the password and let the vault user type it in manually when they are prompted when running the script.

1. Copy the script bundle to the first SQL Server node.
2. Create a folder and extract the bundle. The bundle contains the following files:
   - entrust.conf—The configuration file with some pre-populated values.
   - setup.ps1—A PowerShell script signed with the Entrust signature. Do not modify.
   - encryptclust.ps1—A PowerShell script signed with the Entrust signature. Do not modify.

   Note: The scripts use Windows authentication by default, and are executed in the context of the user who is logged in to the SQL Server VM.
3. Edit the entrust.conf file and update the following parameters:
   - db_server_name—The name of the database server which contains the database to be encrypted.
   - sysadmin_user—Optional. If this parameter is set, then the SQL commands are run as this user instead of the user who is logged in to the SQL server VM
   - sysadmin_password—Optional. If you set the sysadmin_user, you can add the password for that user. If left blank, the user will be prompted for the password when you run the scripts.
     Note: You can also modify any pre-populated files if needed.
4. Save the entrust.conf file.
5. Run the setup.ps1 script as follows:
   PS> .\setup.ps1 -node first -config .\entrust.conf
   Where:
   - -node is the node you are updating. This can be either first or other. This should be pre-populated with first.
   - -config is the name of the configuration file that you updated.If you have a second SQL Server node in your cluster, copy the script bundle to the second node and extract it.
   - This script displays the location of the Access Token file. You will need this to check the status of your connection.
6. Copy your modified configuration file from the first node and overwrite the configuration file from the bundle.
7. Run the setup.ps1 script as follows:

   PS> .\setup.ps1 -node other -config .\entrust.conf

   Please ensure that the -node parameter is set to other.

Setting Up a Microsoft SQL Server Cluster for TDE

When you set up a failover cluster, you will share the same Key Set and Cloud VM Set that you created for the primary VM.

1. Ensure that you have completed all of the previous steps to create and configure the primary VM of your SQL Server cluster.
   Important: The credential for your primary VM must include the credential file path for the identity and secret file. This file path and name must be the same for all nodes in the SQL Server cluster.
   For example:
   Copy
   ```
   C:\Users\Administrator\sqlcred.conf


   {
     "identity"    : "<the identity copied from the access token>"
     "secret"      : "<the secret copied from the access token>"
   }
   ```
   See Configuring Microsoft SQL Server for EKM.
2. Install and register the Policy Agent on your failover SQL Server VM.
   Note: The failover VM must be registered to the same Cloud VM Set that you created for the primary VM. Ensure that the VM name indicates that this is a failover VM.
   See Installing and Registering the Policy Agent for SQL Server.
3. Enable TDE on the failover SQL Server VM.
   See Enable TDE on SQL Server.
4. Create a database connector for the failover SQL Server VM on the same Key Set that you used for the primary SQL Server VM. Ensure that the connector name indicates that this is the failover VM.
   See Configuring a CSP Vault Database Connector.
5. Select the database connector that you just created, and select **Actions > Generate Access Token**.
   On the Generate Access Token window, the new access token is created and displays both an identity and a secret. You will need to copy these to use when configuring the cryptographic provider.
6. Using the identity and secret that you copied when you generated the access token, create a credential file in json format.
   Important: This file should have the same name and path that you used for the Primary SQL Server, for example, C:\Users\Administrator\sqlcred.conf.
   Please make sure that Windows did not add an extra .txt extension to the filename.
   Copy
   ```
   {
     "identity"    : "<the identity copied from the access token>",
     "secret"      : "<the secret copied from the access token>"
   }
   ```
7. Use your preferred method to failover to the new failover VM.
8. Enter the following command to ensure that the TDE Key that you created is visible:
   Copy
   ```
   USE master;
   select name,thumbprint,algorithm_desc from sys.asymmetric_keys
   GO
   ```

Transparent Data Encryption (TDE)

These examples assume that both the 'TestDatabase' and 'TestTable' as described in T-SQL Shortcuts and Tips have been created, and are not currently encrypted.

When TDE encryption has been correctly set up and switched on, the database it is protecting will appear as normal to any user who has been granted suitable permissions to use the database. The user does not require a Cryptographic Security Platform Vault SQLEKM provider credential to access or modify TDE protected data.

Note that the person setting up or managing the TDE encryption keys must use the same protection domain for their login credential as used for the 'tdeCredential' below.

The TDE Database Encryption Key (TDEDEK) is a symmetric key that is used to perform the actual encryption of the database. It is created by SQL Server and cannot be exported from the database meaning that it cannot be created or directly protected by the Cryptographic Security Platform Vault SQLEKM provider. In order to protect the TDEDEK within the database it may in turn be encrypted by a wrapping key. The wrapping key is called the TDE Key Encryption Key (TDEKEK). In this case, the Cryptographic Security Platform Vault SQLEKM provider can create and protect the TDEKEK.

Before running the following examples, you should create a backup copy of the unencrypted database. See Restoring the TDE Encrypted Database . Alternatively, you may prefer to adapt the T-SQL query shown in Making a database backup . Save the backup as '<Drive>:\<Backup_directory_path>\TestDatabase_TDE_Unencrypted.bak`.

Note: If you are using a shared disk cluster, TDE should be configured on the active node.

Note: In this document TDE key refers to TDE Key Encryption Key(TDEKEK)

There are two ways to create TDE keys:

- Create key in Cryptographic Security Platform Vault and open in MS SQL Server
- Create key directly in Microsoft SQL Server using SQL script

Create TDE Key in Cryptographic Security Platform Vault

1. Navigate to **CLOUD KEYS > CloudKeys** and select the Key Set that you created.
2. Select **Actions > Create CloudKey**.
3. On the Details tab of the Create CloudKey dialog box, enter the following:

Field	Description
Name	Enter the name for the CloudKey. For this example, use master_key1.
Description	Enter the optional description for the CloudKey.
Cipher	Select RSA-2018.

4. Click **Continue**.
5. On the Schedule tab, determine the rotation schedule for the CloudKey. This can be one of the following:
   - Inherit from Key Set—The CloudKey will use the default schedule from the Key Set. If the Key Set schedule changes after the CloudKey is created, the CloudKey schedule will not be updated.
   - Never—The CloudKey will never be rotated.
   - Once a year—The CloudKey will be rotated once a year.
   - Every 6 months—The CloudKey will be rotated once every 6 months.
   - Every 30 days—The CloudKey will be rotated once every 30 days.
   - Other—The CloudKey will be rotated at the interval you select.
6. Choose when this version of the CloudKey should expire. The per version expiration can be one of the following:
   - Never—The CloudKey version will never expire.

- Fixed Date—All CloudKey versions will expire on the date that you set.
- Relative Expiry—Each CloudKey version will expire after the number of days that you set.

7. Choose when the CloudKey as a whole should expire. This can be Never, or you can choose a specific date.
8. If you selected an expiration date, choose the Expire Action to define what happens to the CloudKey when it expires. This can be one of the following:
   - Disable—The key will remain in the cloud, but is disabled and cannot be used by any applications.
   - Delete—The key is disabled in the cloud and cannot be used by any applications. You can set the date when the key is permanently deleted.

   Note: When the CloudKey expires, the selected Expire Action is performed on the key. The Cryptographic Security Platform Vault handles the expiry date and expire action. The expire date is not set in the cloud service provider.
9. Click **Apply.**
10. Navigate to the details page of the CloudKey, and select the Key ID for the keyset.
11. To configure the TDE key in Microsoft SQL Server, create an asymmetric key stored inside the EKM provider. Login again on the **SQL Server** and create a master key (**KEK**) using the name of the key generated in the previous step and the provider created earlier (see Configuring Microsoft SQL Server for EKM).

```
USE master;
CREATE ASYMMETRIC KEY TDE_KEY      -- Give the KEK a name in SQL Server
FROM PROVIDER EKM_Prov WITH
PROVIDER_KEY_NAME = '<Cloud Key>',   -- master_key1 created in last Step
CREATION_DISPOSITION = OPEN_EXISTING;
GO
```

Creating TDE key using Microsoft SQL Server

To create a TDE Key programmatically using SQL script directly in MS SQL Server:

```
USE master
CREATE ASYMMETRIC KEY dbAsymWrappingKey
FROM PROVIDER <provider name>
WITH PROVIDER_KEY_NAME='ekmAsymWrappingKey',
CREATION_DISPOSITION = CREATE_NEW, ALGORITHM = RSA_2048;
GO
```

Where *<provider name>* is the name that is used to refer to the Cryptographic Security Platform Vault SQLEKM provider. The TDE Key is the only key you must create in the 'master' database.

Note: The key thumbprint in SQL Server is same as the keyid in Cryptographic Security Platform Vault.

Check the key is created and has correct key thumbprint.

Copy

```
USE master;
SELECT name,thumbprint,algorithm_desc FROM sys.asymmetric_keys
GO
```

To check the TDEKEK, in SQL Server Management Studio navigate to Databases > System Databases > Master > Security > Asymmetric Keys. If necessary, right-click and select Refresh.

Create credential and login for TDE

Create another credential and a login for TDE. Add the credential to the login.

Setting up TDE login programmatically

Copy

```
CREATE CREDENTIAL tde_ekm_cred
WITH IDENTITY = 'tde_connect1',
SECRET = 'xdZ5TCNRLcldfeCr8SDZyu+TJF1kH5MGMZgaj2vZeUgP3Nf2xBh/
lWicDzhvaWZCN3w3A5gVlkgG05AnfdlIYafP6HE+z
SqsGXAy4Fx7deZYqTbOcz3HOYmu99lE81fATfG58C1qukmzY9UW3z04p3TaAM2xho30SIhm2hs1iupsXADGBuSVYSxi5
C8 aH26jrXZFl6hIiInwK8F3GF3MQSWksRmgruAOSBLfnh+iasM1vqkZ/BHZ/
3vRcsZZTrC3DycHXGrZqwcVxZaPsQlok2vC0
cRw6m7afBCJI76y854klGEflOCvQugGxxyEBpPOOuLrCEQo0y5jr9x2dYgWIr4X24qTnW9+BVMlMqGh2oOmqBqqNFBV
UBE UjSIjHZuE/4xo/
lH6aknRu0PHP2JDhvDGpouRfCaJ7/5q1dygiEl1OcSoANemqu44GUaVyAS1esIM182T6rNbbmRgRJsyq
znrdTLx02oUPbtbUXRUdh7hgYGPBB+uvid2YYT+NOsXM2nR0XdkxJ59x2RbFErjTGuf6mj756qE2RBzV9eeIEjMQgiajfT
UNWz/NTk+Ca5z6Rdznig8VTCLR0Q3iHxF6zb5jSYkLeo0pbeUuuSLtlPX7kkrzFt07j2dj8q3V2lkcvYLOMdgtzzW/ILGj
S0jEyZBbyROxK+48WSQ244EVhs='
FOR CRYPTOGRAPHIC PROVIDER EKM_Prov ;
GO

CREATE LOGIN TDE_Login
FROM ASYMMETRIC KEY TDE_KEY ;
GO

ALTER LOGIN TDE_Login
ADD CREDENTIAL tde_ekm_cred
GO
```

Setting up TDE login and credential in SQL Server Management Studio

1. In SQL Server Management Studio, navigate to **Security > Credentials**.
2. Right-click **Credentials**, then select **New Credential**.
3. Set **Credential name** to **tdeCredential** (for example).
4. Set **Identity** to *<protection domain id>*, where *<protection domain id>* matches the id of the protection domain. This must be the same key protector as that used to protect the 'ekmAsymWrappingKey' created above.
5. Set **Password** to *<passphrase>*, where *<passphrase>* matches the passphrase of the protection domain.
6. Set **se Encryption Provider** to *<provider name>*, where *<provider name>* is the name of the provider you are using. Click **OK**.
7. In SQL Server Management Studio, navigate to **Security > Logins**.
8. Right-click **Logins**, then select **New Login**.
9. Set **Login name** to **tdeLogin** (for example).

Check credential is created correctly

1. Ensure **Mapped to asymmetric key** is selected, then select **'dbAsymWrappingKey'** (the TDEKEK created previously) from the drop down list.
2. Ensure **Map to Credential** is selected, then select **tdeCredential** from the drop down list. Click **dd**, then click **OK**.
3. In SQL Server Management Studio, check that the **tdeCredential** exists by navigating to **Security > Credentials**. If necessary, right-click and select **Refresh**. You should see the credential name listed.
4. In SQL Server Management Studio, check that the **tdeLogin** exists by navigating to **Security > Logins**. If necessary, right-click and select **Refresh**. You should see the login name listed.

Configuring Microsoft SQL Server Database Encryption with TDE Key

This section explains how to configure Microsoft SQL Server database encryption with TDE key.

Database Encryption with TDE key

To create the database encryption with TDE key.

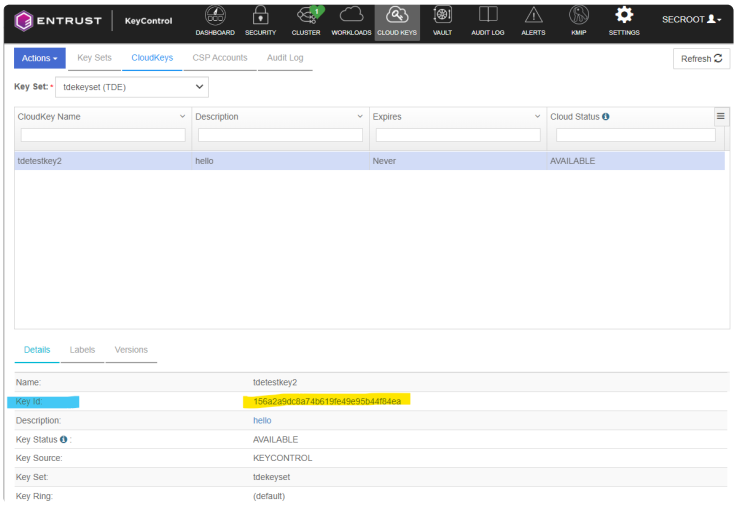
1. Use the TDE_KEY to create a database encryption key.

   In this example, we used a test database “testdb” and "TDE_KEY" to create database encryption key.

```
use testdb
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM  = AES_256
ENCRYPTION BY SERVER ASYMMETRIC KEY TDE_KEY;
GO

ALTER DATABASE testdb
SET ENCRYPTION ON ;
GO
```

2. Check created encryption keys and progress of encryption. There are fields like “encryption_state” and “percent_complete” which show relevant information. Also check the “**encryptor thumbprint**” to know the version of key used to encrypt the database key.
   Note: The key **key thumbprint** in SQL server is same as the **Key Id** in Cryptographic Security Platform Vault. To find the Key ID:



You can list all the asymmetric keys and database encryption keys using following SQL statements.

```
use master
GO
Select * from sys.dm_database_encryption_keys
Select * from sys.asymmetric_keys
GO
```

For more information regarding these options and fields, see https://learn.microsoft.com/en-us/sql/relational-databases/system-dynamic-management-views/sys-dm-database-encryption-keys-transact-sql?view=sql-server-ver15.

For more information on how to monitor and manage Transparent Data Encryption (TDE) in SQL Server, see https://www.sqlshack.com/how-to-monitor-and-manage-transparent-data-encryption-tde-in-sql-server/.

Switching on encryption using SQL Server Management Studio

Only one TDEDEK per database can be used at a time.

To create the TDEDEK using the 'dbAsymWrappingKey' (TDEKEK) created above for database encryption, and enable TDE on the database ('TestDatabase'):

1. In SQL Server Management Studio, navigate to **Databases > TestDatabase**.
2. Right-click **'TestDatabase'**, then select **Tasks > Manage Database Encryption...**.
3. Set **Encryption Algorithm** to the desired algorithm.
4. Ensure that **Use server asymmetric key** is selected, then select **'dbAsymWrappingKey'** from the drop down list.
5. Ensure **Set Database Encryption On** is selected, then click **OK**.

After successfully setting up the TDE encryption, the person performing the set up no longer needs to use the same protection domain for their login credential as used for the 'tdeCredential'.

Verifying by inspection that TDE has occurred on disk

Note that the inspection method will only work for data that can be backed up in the database (on disk) as human-readable character strings.

To check the encryption state of the database, refer to How to check the TDE encryption/decryption state of a database .

If the TDE has been successful, then an 'Encrypted' state should be indicated.

Querying the 'TestTable' or database contents will not indicate whether the table was encrypted on disk, because it will be automatically decrypted when loaded into memory.

TDE encryption on disk can be verified by inspecting backup copies of the 'TestDatabase' from before and after the TDE encryption.

After TDE encryption has been set up and checked to be functioning, make a backup copy of the encrypted 'TestDatabase'. For more detail, see Database Backup and Restore .

You should now have the following unencrypted and encrypted backup copies of the 'TestDatabase':

- '<Drive>:\<Backup_directory_path>\TestDatabase_TDE_Unencrypted.bak'
- '<Drive>:\<Backup_directory_path>\TestDatabase_TDE_Encrypted.bak'

These backup files can be inspected using a text editor, provided you have appropriate access permissions.

1. Open 'TestDatabase_TDE_Unencrypted.bak' in a text editor and search for a known value. It should be possible to find the plaintext 'FirstName' or else 'LastName' of anyone mentioned in the original and unencrypted 'TestTable'.
2. Open 'TestDatabase_TDE_Encrypted.bak' in a text editor and search for the same value. It should not be possible to find any plaintext names or other values in the encrypted file.

The backup files circumvent the automatic TDE decryption of the database, allowing direct inspection of the contents as stored on disk. Although this inspection has been carried out on backup files, these should contain information similar enough to the actual database disk contents to demonstrate whether the TDE encryption is working on disk or not.

To replace the TDE Key (TDEKEK)

1. Follow the procedure Configuring Microsoft SQL Server Database Encryption with TDE Key to create a new asymmetric TDEKEK called 'dbAnotherAsymWrappingKey'.
2. Create a new credential called 'anotherTdeCredential'.
3. Create a new TDE login called 'anotherTdeLogin'. Map it to 'dbAnotherAsymWrappingKey' and the new 'anotherTdeCredential'.
4. In SQL Server Management Studio, navigate to **Databases > TestDatabase**.
5. Right-click TestDatabase, then select **Tasks > Manage Database Encryption...**.
6. Select **Re-Encrypt Database Encryption Key** and **Use server asymmetric**. Select **'dbAnotherAsymWrappingKey'** from the drop down list.
7. Ensure **Regenerate Database Encryption Key** is not selected.
8. Ensure **Set Database Encryption On** is selected, then click **OK**.

To replace the TDE Key (TDEDEK)

1. In SQL Server Management Studio, navigate to **Databases > TestDatabase**.
2. Right-click **TestDatabase**, then select **Tasks > Manage Database Encryption...**.
3. Ensure **Re-Encrypt Database Encryption Key** is not selected.
4. Ensure **Regenerate Database Encryption Key** is selected, then select **AES 256** from the drop down list.
5. Ensure **Set Database Encryption On** is selected, then click **OK**.

How to check the TDE encryption/decryption state of a database

Note: The following 'encryption_state' information applies to TDE encryption only.

You can use the following T-SQL queries to find the current encryption state of a database. This can be particularly useful where large amounts of data have to be processed and you wish to check progress before attempting any further operations on the database.

First, find the database ID from the database name by using the following query:

Copy

```
SELECT DB_ID('<Database name>') AS [Database ID];
GO
SELECT * FROM sys.dm_database_encryption_keys
GO
```

Where *<Database name>* is the name of the database you are interested in.

The above query provides a table output that includes columns titled 'database_id' and 'encryption_state'. Find the database ID you are interested in and look at the corresponding value for the encryption state.

Alternatively, you can use the composite query:

Copy

```
SELECT db_name(database_id), encryption_state FROM sys.dm_database_encryption_keys
GO
```

Where *<database_id>* is the ID number of the database you are interested in.

Values of 'encryption_state' are as follows:

Value of 'encryption_state'	Meaning of value
0	Encryption disabled (or no encryption key)
1	Unencrypted or Decrypted
2	Encryption in progress
3	Encrypted
4	Key change in progress
5	Decryption in progress
6	Protection change in progress (The certificate or asymmetric key that is encrypting the database encryption key is being changed.)

Viewing Tables and Checking Keys

Viewing tables

Using SQL Server Management Studio

To check that data in a table was either encrypted or decrypted successfully, complete the following steps with SQL Server Management Studio:

1. Go to **Databases > TestDatabase > Tables**.
2. Right-click the table name and select **Select Top 1000 Rows** to view the encrypted or decrypted data.

Using SQL Query

To check that data in a table was either encrypted or decrypted successfully, execute the following SQL query:

Copy

```
Use TestDatabase
SELECT * FROM <table_name>
```

Checking keys

The following queries show how you can check the attributes of keys in your database and the Cryptographic Security Platform Vault SQLEKM provider.

- To view the symmetric keys in a database:
  Copy
  ```
  Use TestDatabase
  SELECT * FROM sys.symmetric_keys
  ```
- To view the asymmetric keys in a database:
  Copy
  ```
  Use TestDatabase
  SELECT * FROM sys.asymmetric_keys
  ```
- To list all the Cryptographic Security Platform Vault SQLEKM provider keys that are associated with the current credential:
  Copy
  ```
  DECLARE @ProviderId int;
  SET @ProviderId = (SELECT TOP(1) provider_id
  FROM sys.dm_cryptographic_provider_properties
  WHERE friendly_name LIKE '<provider friendly_name>');
  SELECT * FROM sys.dm_cryptographic_provider_keys(@ProviderId);
  GO
  ```

Where *<provider friendly_name>* can be found as shown in Viewing Tables and Checking Keys .

- To correlate symmetric keys between the database and the Cryptographic Security Platform Vault SQLEKM provider:
  Copy
  ```
  DECLARE @ProviderId int;
  SET @ProviderId = (SELECT TOP(1) provider_id FROM sys.dm_cryptographic_provider_properties WHERE
  friendly_name LIKE '<provider friendly_name>');
  SELECT * FROM sys.dm_cryptographic_provider_keys(@ProviderId) FULL OUTER JOIN sys.symmetric_keys
  ON sys.symmetric_keys.key_thumbprint = sys.dm_cryptographic_provider_keys.key_thumbprint WHERE
  sys.dm_cryptographic_provider_keys.key_type = 'SYMMETRIC KEY'
  GO
  ```
  where *<provider friendly_name>* can be found as shown in Viewing Tables and Checking Keys .
- To correlate asymmetric keys between the database and the Cryptographic Security Platform Vault SQLEKM provider:
  Copy

```
DECLARE @ProviderId int;
SET @ProviderId = (SELECT TOP(1) provider_id FROM sys.dm_cryptographic_provider_properties
WHERE friendly_name LIKE '<provider friendly_name>');
SELECT * FROM sys.dm_cryptographic_provider_keys(@ProviderId)
FULL OUTER JOIN sys.asymmetric_keys
ON sys.asymmetric_keys.thumbprint = sys.dm_cryptographic_provider_keys.key_thumbprint
WHERE sys.dm_cryptographic_provider_keys.key_type = 'ASYMMETRIC KEY'
GO
```

where *<provider friendly_name>* can be found as shown in Viewing Tables and Checking Keys .

- To correlate all keys (symmetric and asymmetric) between the database and cryptographic provider:

Copy

```
DECLARE @ProviderId int;
SET @ProviderId = (SELECT TOP(1) provider_id FROM sys.dm_cryptographic_provider_properties
WHERE friendly_name LIKE '<provider friendly_name>');
SELECT * FROM sys.dm_cryptographic_provider_keys(@ProviderId)
FULL OUTER JOIN sys.symmetric_keys
ON sys.symmetric_keys.key_thumbprint = sys.dm_cryptographic_provider_keys.key_thumbprint
FULL OUTER JOIN sys.asymmetric_keys
ON sys.asymmetric_keys.thumbprint = sys.dm_cryptographic_provider_keys.key_thumbprint
GO
```

where *<provider friendly_name>* can be found as shown in Viewing Tables and Checking Keys .
The 'key_thumbprint' returned by the T-SQL queries, maps to the 'key ID' when listing keys with the REST API.

T-SQL Shortcuts and Tips

The following Transact-SQL queries provide assistance or alternative methods to perform some of the examples shown in this document.

Creating a database

To create a database called `TestDatabase` :

```
USE master
GO
CREATE DATABASE TestDatabase;
GO
```

Creating a table

To create the following example table called `TestTable` within a previously created database:

```
USE TestDatabase
GO
CREATE TABLE TestTable (FirstName varchar(MAX), LastName varchar(MAX), NationalIdNumber varbinary(MAX),
EncryptedNationalIdNumber varbinary(MAX), DecryptedNationalIdNumber varbinary(MAX));
```

```
GO
INSERT INTO TestTable (FirstName, LastName, NationalIdNumber) VALUES ('Jack', 'Shepard', 156587454525658);
INSERT INTO TestTable (FirstName, LastName, NationalIdNumber) VALUES ('John', 'Locke', 2365232154589565);
INSERT INTO TestTable (FirstName, LastName, NationalIdNumber) VALUES ('Kate', 'Austin', 332652021154256);
INSERT INTO TestTable (FirstName, LastName, NationalIdNumber) VALUES ('James', 'Ford', 465885875456985);
INSERT INTO TestTable (FirstName, LastName, NationalIdNumber) VALUES ('Ben', 'Linus', 5236566698545856);
INSERT INTO TestTable (FirstName, LastName, NationalIdNumber) VALUES ('Desmond', 'Hume', 6202366652125898);
INSERT INTO TestTable (FirstName, LastName, NationalIdNumber) VALUES ('Daniel', 'Faraday', 7202225698785652);
INSERT INTO TestTable (FirstName, LastName, NationalIdNumber) VALUES ('Sayid', 'Jarrah', 8365587412148741);
INSERT INTO TestTable (FirstName, LastName, NationalIdNumber) VALUES ('Richard', 'Alpert', 2365698652321459);
INSERT INTO TestTable (FirstName, LastName, NationalIdNumber) VALUES ('Jacob', 'Smith', 12545254587850);
GO
```

Viewing a table

To view the previously created `TestTable`:

```
SELECT TOP 10 [FirstName]
,[LastName]
,[NationalIDNumber]
,[EncryptedNationalIdNumber]
,[DecryptedNationalIdNumber]
FROM [TestDatabase].[dbo].[TestTable]
```

To view the previously created `TestTable` with the `NationalIDNumber` in the original decimal form:

```
SELECT TOP 10 [FirstName]
,[LastName]
,CAST(NationalIdNumber AS decimal(16,0)) AS [NationalIDNumber]
,[EncryptedNationalIdNumber]
,[DecryptedNationalIdNumber]
FROM [TestDatabase].[dbo].[TestTable]
```

To view the previously created `TestTable` with the `NationalIDNumber` in the original decimal form, and also show the `NationalIdNumber` in `VarBinary` form:

```
SELECT TOP 10 [FirstName]
,[LastName]
,CAST(NationalIdNumber AS decimal(16,0)) AS [NationalIDNumber]
,(NationalIdNumber) AS VarBinNationalIdNumber
,[EncryptedNationalIdNumber]
,[DecryptedNationalIdNumber]
FROM [TestDatabase].[dbo].[TestTable]
```

Making a database backup

To make a database backup:

```
USE TestDatabase;
GO
BACKUP DATABASE TestDatabase
TO DISK = '<Drive>:\<Backup_directory>\TestDatabase_SomeState.bak'
WITH NOFORMAT,
INIT,
NAME = TestDatabase_SomeState Backup',
SKIP,
NOREWIND,
NOUNLOAD,
STATS = 10
GO
```

Where: *<Drive>:\<Backup_directory>* is the path to the directory to store the backup.

Adding a credential

To add a credential to the database:

```
CREATE CREDENTIAL <credential name> WITH IDENTITY = '<protection domain id>',
SECRET = '<protection domain passphrase>' FOR CRYPTOGRAPHIC PROVIDER <provider name>;
ALTER LOGIN "<domain>\<login name>" ADD CREDENTIAL <credential name>;
```

Where;

- *<credential name>* is the name you wish to provide for the credential.
- *<protection domain id>* matches the id of the protection domain.
- *<protection domain passphrase>* matches the passphrase of the protection domain.
- *<provider name>* is the name of the provider you are using.
- *<domain>* is the relevant login domain.
- *<login name>* is the relevant login name (to the database host).

Removing a credential

To remove a credential from the database:

```
ALTER LOGIN "<domain>\<login name>" DROP CREDENTIAL <credential name>;
DROP CREDENTIAL <credential name>;
```

Creating a TDEDEK

To create a TDEDEK using `TestDatabase` and `dbAsymWrappingKey` as an example:

```
USE TestDatabase;
CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER ASYMMETRIC KEY dbAsymWrappingKey;
GO
```

Removing a TDEDEK

To remove a TDEDEK using TestDatabase as an example:

```
USE TestDatabase
DROP DATABASE ENCRYPTION KEY;
```

Switching on TDE

To switch on TDE using TestDatabase as an example:

```
ALTER DATABASE TestDatabase SET ENCRYPTION ON;
```

Switching off TDE

To switch off TDE using TestDatabase as an example:

```
ALTER DATABASE TestDatabase SET ENCRYPTION OFF;
```

Dropping a provider

To drop an existing provider:

```
DROP CRYPTOGRAPHIC PROVIDER <provider name>
```

Where:

- *<provider name>* is the name of an existing provider.

Disabling existing providers

To disable all existing providers:

```
sp_configure 'show advanced options', 1; RECONFIGURE;
GO
sp_configure 'EKM provider enabled', 0; RECONFIGURE;
GO
```

Checking encryption state

To check the encryption state of your databases:

```
SELECT DB_NAME(e.database_id) AS DatabaseName, e.database_id, e.encryption_state, CASE e.encryption_state
WHEN 0 THEN 'No database encryption key present, no encryption'
WHEN 1 THEN 'Unencrypted'
WHEN 2 THEN 'Encryption in progress'
WHEN 3 THEN 'Encrypted'
WHEN 4 THEN 'Key change in progress'
WHEN 5 THEN 'Decryption in progress'
END AS encryption_state_desc, c.name, e.percent_complete FROM sys.dm_database_encryption_keys AS e
LEFT JOIN master.sys.certificates AS c ON e.encryptor_thumbprint = c.thumbprint
```

Viewing TDE Reports for Microsoft SQL Server

If you used scripted versions for installation, configuration, and encryption, you can download TDE reports from the CSP Vault for Databases webGUI for a specific VM.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.

3. Click the **VMs** tab.
4. Select the VM for which you want to view TDE reports.
5. In the Details section, click the **TDE Reports** tab.
   The CSP Vault for Databases webGUI displays the list of reports for the VM that you specified. You can click the download icon to download the report in plain text, or the eyeball icon to view the report in the vault. When viewing the report, you can also download or copy the text.
   You can also search for a specific report if you know the report ID.

Creating a Cloud VM Set for the CSP Vault for Databases

A VM must be part of a Cloud VM Set before it can be used for Transparent Data Encryption (TDE) in a database.

Before You Begin

- If you want to use a Key Encryption Key (KEK) with the Cloud VM Set, Cryptographic Security Platform Vault for Databases must have access to a hardware security module (HSM) in which it can store the KEK. For more information, see KEKs with Cloud VM Sets

Procedure

1. Log in to the Cryptographic Security Platform Vault for Databases web GUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Create New Cloud VM Set**.
4. On the **VM Set** tab:
   a. Enter a name for the Cloud VM Set.
   b. Select the group to which this set should belong, or accept the default.
   c. Optionally enter a description for the set.
5. If you want to specify additional options, click the **Additional Properties** tab and specify the options you want to use.
6. To specify when VMs in the Cloud VM Set need to be re-authenticated, click the Reauthentication Settings tab and choose the options you want to use.

Option	Description
Reauthentication on IP Change	Whether a VM in the set must be re-authenticated when the VM's IP address changes. The default is No. If your system configuration uses DHCP or multiple NICs, do *not* set this option to Yes. If you do so, the VMs in the set may go into a reboot loop if their boot partitions are encrypted and any encrypted drives may be detached.

Option	Description
Reauthentication on H/W Signature Change	Whether a VM in the set must be re-authenticated if its MAC address or UUID changes. The options are: • **Yes**—If *either* the MAC address *or* the UUID changes, the VM requires reauthentication. This is the default. We recommend that you do not change this option. • **Permissive**—Both the MAC address *and* the UUID must change before the VM requires reauthentication. You can use this option if your system administrators are performing maintenance on the VMs in this Cloud VM Set that require changes to the network cards and hence to the MAC addresses of the VMs in the set. We recommend you reset this value to **Yes** once maintenance is finished. • **No**—The Cryptographic Security Platform Vault for Databases does not require reauthentication if VM's MAC address or UUID changes. We strongly recommend that you do **not** select this option. If you do, a cloned or misconfigured VM could gain access to the keys associated with the original VM. If you do select this option, you must confirm the selection before you can proceed. If Cryptographic Security Platform Vault for Databases detects multiple VMs with the same MAC address and UUID combination when hardware validation is off, Cryptographic Security Platform Vault for Databases generates an alert every 8 hours until the cloned VMs stop heartbeating or hardware authentication is set to **Yes** or **Permissive**. In addition, Cryptographic Security Platform Vault for Databases generates an alert when client operations, such as key access or device registration, occur on the cloned VMs.
Reauthentication on Reboot	Whether a VM in the set must be re-authenticated every time it reboots. The default is No. Setting this value to Yes is similar to requiring a boot-time password before the VM can come up completely.

7. If you want to specify a key encryption key (KEK), click the **Key Encryption Key** tab, choose the type of Key Encryption Key Association, and then specify the required information.
   A KEK provides an extra layer of security by encrypting the individual data encryption keys on the VMs associated with this Cloud VM Set. It also controls the expiration and revocation of those data encryption keys. To protect the KEK, Cryptographic Security Platform Vault requires that the KEK be stored in the hardware security module (HSM) associated with this Cryptographic Security Platform Vault cluster. For more information, see KEKs with Cloud VM Sets.
   You can add the KEK during Cloud VM Set creation or at a later time.
   a. Determine whether Cryptographic Security Platform Vault for Databases creates a KEK for this Cloud VM Set. To use a KEK, select **Use KEK** from the drop-down list and click **Save** to view the KEK properties.
      If you do not make a selection, then the default value is **No KEK Association** is used, and the tab is not populated. If you decide you want to use a KEK, you can add the KEK to the Cloud VM Set later.
   b. If you selected USE KEK, complete the following:

Option	Description
Key Expiration Period	The length of time for which the KEK and all data encryption keys on the VMs will be valid. To indicate that the KEK should never expire, set this field to 0 (zero). This is the default. If you change the Key Expiration Period, the new expiration period begins from the day you make the change, not from the day the Cloud VM Set was created. When this time period expires: • All disks on all VMs in the Cloud VM Set are automatically detached. What happens to the keys depends on the setting in the **Key Expiration Action** field. • Any attempt to register a new VM with the Cloud VM Set will fail. • Any encrypt or decrypt operation on any of the associated VMs will fail. To change the expiration period, click the existing value and enter a new value in the text field, then select days/weeks/months/years from the drop-down list. When you are finished, click Save. Note: If the Key Expiration Option field is set to Change, you can shorten the expiration period but you cannot lengthen it beyond the original date.
Key Expiration Action	The options are: • **No Use**—The KEK and all data encryption keys are deactivated but retained. The keys can be reactivated and the expiration date extended if the **Key Expiration Option** field is set to **Extend**. This is the default. • **Shred**—The KEK and all data encryption keys are destroyed and cannot be retrieved. In addition, all VMs in the set are removed from Cryptographic Security Platform Vault for Databases and the Cloud VM Set itself is deleted. **Shred** is a destructive action that cannot be undone. Make sure you have set the correct **Key Expiration Period** when using this option.
Key Expiration Option	The options are: • **No Change**—The KEK expiration options cannot be changed after the Cloud VM Set has been created. This is the default. Selecting this option means that once the top-level key expires it cannot be reactivated and all VMs will be automatically detached from Cryptographic Security Platform Vault for Databases when the expiration date is reached. • **Change**—The KEK expiration options can be changed after the Cloud VM Set has been created, but the **Key Expiration Period** cannot be extended beyond the original date. This is the default. • **Extend**—All KEK expiration options can be changed after the Cloud VM Set has been created.

8. When you have finished specifying the Cloud VM Set options, click **Create**.
9. When you see the **Cloud VM Set Successfully Created** message, click **Close**.

What to Do Next

Install the Policy Agent on the VM(s) where you want to use TDE and register it with Cryptographic Security Platform Vault. For details, see the installation and administration guide at:

https://api.managed.entrust.com/vault/latest

Changing a Cluster Node Mapping for CSP Vault for Databases

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **Mappings** tab.
4. Select the Node Mapping you want to change in the list.
5. If you want to change the Node Mapping name, associated Cloud Admin Group, or description, do the following:
    a. In the Details tab below the table, click the text in the field you want to change.
    b. Make your changes and click **Save**.
6. If you want to change the Cryptographic Security Platform Vault for Databases nodes in the Node Mapping or the order of the node in the Node Mapping, do the following:
    a. Select **Actions > Edit Mapping**.
    b. If you want to add a new IP address, click the **+** (Plus sign) on the right-hand side of the dialog box to add a new row, then enter the following information:

Field	Description
External IP	The externally-visible hostname or IP address to which this node should be mapped. Each node in the cluster can be associated with one and only one externally-visible IP address. Note: If the VMs will be communicating with the Cryptographic Security Platform Vault for Databases node through a firewall or in an environment like Amazon Web Services or Microsoft Azure, the externally-visible IP address may not be the same as the internal Cryptographic Security Platform Vault for Databases node IP address. Make sure that all VMs that will use this Node Mapping can communicate with the Cryptographic Security Platform Vault for Databases node via the specified IP address/port number combination.
Port	The port number for the specified Hostname or IP address. The default is 443.
Cryptographic Security Platform Vault Server	Select the appropriate Cryptographic Security Platform Vault for Databases node in the drop-down list. You can only have one entry for each Cryptographic Security Platform Vault for Databases node.
State	Select Enabled if the node is available to the VMs associated with this Cluster Node Mapping. If you want to use this as a placeholder until you bring the node online, select Disabled. The default is Enabled.

Field	Description
Description	Enter a description for this node that lets you distinguish it from other nodes in the Cluster Node Mapping.

c. If you want to delete an existing entry, click the **–** (Minus sign) at the end of the row you want to delete.
d. When you are done changing the list of nodes, make sure that the order is correct because the order of the IP addresses in the list determines the order of precedence. The first node in a Cluster Node Mapping is considered the preferred node, and all VMs will use that node as long as it is available. If the preferred node is offline when a VM heartbeats, the VM will try the other IP addresses in the Node Mapping, starting with the second IP address in the list and working downwards. Once the VM finds an available Cryptographic Security Platform Vault for Databases node, it will use that node to complete the current heartbeat, and it will continue to use that node until the cluster returns to a healthy state. After the cluster becomes healthy, the VM will resume using the preferred node at its next heartbeat.
If you need to change the order, click and hold on the arrow icon at the beginning of the line to drag the entry to the proper position. Release the mouse to drop the entry in the new location.
You can view the Preferred Node in the Details section of the selected mapping.
e. When you are done, click **Update**. Cryptographic Security Platform Vault for Databases communicates the changes to the associated VMs on their next heartbeat.

Creating a Cluster Node Mapping for CSP Vault for Databases

Cluster Node Mapping lets you create a list of Cryptographic Security Platform Vault for Databases IP addresses that you maintain in the Cryptographic Security Platform Vault for Databases. Each node in the Node Mapping is associated with an externally-visible IP address or hostname that the VMs can use to access that Cryptographic Security Platform Vault for Databases node. If you ever change the list of Cryptographic Security Platform Vault for Databases nodes in the Node Mapping, Cryptographic Security Platform Vault for Databases automatically disseminates the changes to the each associated VM at its next heartbeat.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **Mappings** tab.
4. Select **Actions > Create Mapping**.
5. On the **Mapping** dialog box, specify the options you want to use.

Field	Description
Name	Enter the name for this Cluster Node Mapping. You can use - (hyphen) and _ (underscore) as well as any alphanumeric characters.
Cloud Admin Group drop-down list	Select the Cloud Admin Group associated with this Node Mapping. The Node Mapping will be available to all VMs that are registered with the Cloud VM Sets assigned to the selected Cloud Admin Group.

Field	Description
Description	Enter a description for the Cluster Node Mapping. This description will be displayed on the VMs when they are associated with the Cluster Node Mapping.

6. When you are done, click **Next**.
7. On the **Servers** tab, create an entry for the first Cryptographic Security Platform Vault for Databases node by specifying the options you want to use.

Field	Description
External IP	The externally-visible hostname or IP address to which this node should be mapped. Each node in the cluster can be associated with one and only one externally-visible IP address. Note: If the VMs will be communicating with the Cryptographic Security Platform Vault for Databases node through a firewall or in an environment like Amazon Web Services or Microsoft Azure, the externally-visible IP address may not be the same as the internal Cryptographic Security Platform Vault for Databases node IP address. Make sure that all VMs that will use this Node Mapping can communicate with the Cryptographic Security Platform Vault for Databases node via the specified IP address/port number combination.
Port	The port number for the specified Hostname or IP address. The default is 443.
Cryptographic Security Platform Vault Server	Select the appropriate Cryptographic Security Platform Vault for Databases node in the drop-down list. You can only have one entry for each Cryptographic Security Platform Vault for Databases node.
State	Select Enabled if the node is available to the VMs associated with this Cluster Node Mapping. If you want to use this as a placeholder until you bring the node online, select Disabled. The default is Enabled.
Description	Enter a description for this node that lets you distinguish it from other nodes in the Cluster Node Mapping.

8. To add another node, click the **+** button and enter the appropriate information.
9. When you are done adding nodes, make sure that the order is correct because the order of the IP addresses in the list determines the order of precedence. The first node in a Cluster Node Mapping is considered the preferred node, and all VMs will use that node as long as it is available. If the preferred node is offline when a VM heartbeats, the VM will try the other IP addresses in the Node Mapping, starting with the second IP address in the list and working downwards. Once the VM finds an available Cryptographic Security Platform Vault for Databases node, it will use that node to complete the current heartbeat, and it will continue to use that node until the cluster returns to a healthy state. After the cluster becomes healthy, the VM will resume using the preferred node at its next heartbeat.

To change the order, click and hold the arrow icon at the beginning of the line, then drag the entry to the correct position. Release the mouse to drop the entry in the new location.

10. When you include all nodes and the order is correct, click **Create**.
11. At the Mapping Successfully Created message, click **Close**.
12. If you want to associate the Cluster Node Mapping with an existing VM that already has the Policy Agent installed:
    a. Log into the VM as an administrator.
    b. Enter the command `hcl updatekc -a` and enter the credentials for a Cryptographic Security Platform Vault for Databases user account with Cloud Admin privileges at the prompt. Cryptographic Security Platform Vault for Databases displays a list of available Cluster Node Mappings that you can use with the VM.
    c. Select the Cluster Node Mapping you want to use from the list. Cryptographic Security Platform Vault for Databases echoes the IP addresses in the list for confirmation.
    Example:

```
# hcl updatekc -a
Getting Mapping information
Please provide the login details
username: cloudadmin
password: ********

This VM can be added to one of the following Mappings
-----------------------------------------------------
1 : San Francisco Datacenter
2 : AWS VMs
-----------------------------------------------------
Please select Mapping (0 to skip): 1

Mapping
server description KC-1, ip 192.168.140.151, port 443
server description KC-2, ip 192.168.140.152, port 443
Updated list with nodes 192.168.140.151:443,192.168.140.152:443
```

Note: For details about specifying a Cluster Node Mapping when you install the Policy Agent, see the installation and administration guide at https://api.managed.entrust.com/vault/latest

Disabling a CloudKey or All CloudKey Versions

When you disable a CloudKey for TDE, you can disable all existing CloudKey versions at the same time. The key versions will remain in the cloud, but cannot be used by any applications.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab.
4. Select the CloudKey that you want to disable.
5. Click Actions > **Disable CloudKey**.
6. In the Disable CloudKey window, if you want to disable all versions of the CloudKey, check the Disable All Key Versions checkbox.
   Note: This option is not available if there is only one version of the CloudKey.
7. Click **Disable**.

Creating a CloudKey for TDE

Before you can create a CloudKey, you must have created a Key Set. See Creating a Key Set for TDE.

Note: For Oracle TDE, you cannot create a CloudKey in the Cryptographic Security Platform Vault for Databases.

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Click the **CloudKeys** tab and then select the Key Set with which the CloudKey will be associated.
4. Select **Actions > Create CloudKey**.
5. On the Details tab of the Create CloudKey dialog box, enter the following:

Field	Description
Name	Enter the name for the CloudKey. Not applicable for SFDC.
Description	Enter the optional description for the CloudKey Not applicable for SFDC.
Cipher	Select AES-256.

6. Click **Continue**.
7. On the Schedule tab, determine the rotation schedule for the CloudKey. This can be one of the following:
   - Inherit from Key Set—The CloudKey will use the default schedule from the Key Set. If the Key Set schedule changes after the CloudKey is created, the CloudKey schedule will not be updated.
   - Never—The CloudKey will never be rotated.
   - Once a year—The CloudKey will be rotated once a year.
   - Every 6 months—The CloudKey will be rotated once every 6 months.
   - Every 30 days—The CloudKey will be rotated once every 30 days.
   - Other—The CloudKey will be rotated at the interval you select.
8. Choose when this version of the CloudKey should expire. The per version expiration can be one of the following:
   - Never—The CloudKey version will never expire.
   - Fixed Date—All CloudKey versions will expire on the date that you set.
   - Relative Expiry—Each CloudKey version will expire after the number of days that you set.
9. Choose when the CloudKey as a whole should expire. This can be Never, or you can choose a specific date.
10. If you selected an expiration date, choose the Expire Action to define what happens to the CloudKey when it expires. This can be one of the following:
    - Disable—The key will remain in the CSP Vault for Databases, but is disabled and cannot be used by any databases.
    - Delete—The key is disabled in the CSP Vault for Databases and cannot be used by any databases. You can set the date when the key is permanently deleted.

    Note: When the CloudKey expires, the selected Expire Action is performed on the key. The Cryptographic Security Platform Vault handles the expiry date and expire action.
11. Click **Apply**.

Creating a Key Set for TDE

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **CloudKeys**.
3. Select **Actions > Create Key Set**.
4. On the **Details** tab of the **Create Key Set** dialog box, enter the following:

Field	Description
Name	Enter the name for the Key Set.
Description	Enter the optional description for the Key Set.
Admin Group	Select the Admin Group.
Database Type	Select the database type that you are going to use. This can be one of the following: • Microsoft SQL Server • Oracle Database Server • MariaDB Database Server • PostgreSQL Database Server
Allow automatic key creation from MariaDB	For MariaDB only. If set to Yes, when MaraDB attempts to fetch a key with a keyID that is not present in this vault, the Cryptographic Security Platform Vault for Databaseswill automatically create a key with that keyID and send it to MariaDB.

5. Click **Continue**.
6. On the HSM tab, if an HSM exists, complete the following tasks:
   a. Check the **Enable HSM** checkbox if you plan to use an HSM to create CloudKeys that can be uploaded to the cloud.
   b. Choose the **Yes** radio button if you want to allow key caching. This caches the key in the Cryptographic Security Platform Vault for Databases, where it is protected by the key set local root key.
   c. If you selected Enable HSM, click **Verify HSM connection** to test the connectivity and suitability of the configured HSM. Cryptographic Security Platform Vault checks if the HSM is accessible and if it supports the creation and export of relevant keys.
   Note: Some HSM servers with older versions of firmware do not support key creation and wrapping. If the connection test fails, check the firmware version of the HSM server. If it is old, update it to the latest version.

   Note: You can enable an HSM after creation from the Key Set Details page.
7. For MariaDB and PostgreSQL only. Click **Continue**.
8. For MariaDB and PostgreSQL only. On the Schedule tab, determine the default rotation schedule for the CloudKeys created in this Key Set. This can be one of the following:
   - Never—The CloudKey will never be rotated.
   - Once a year—The CloudKey will be rotated once a year.
   - Every 6 months—The CloudKey will be rotated once every 6 months.
   - Every 30 days—The CloudKey will be rotated once every 30 days.

- Other—The CloudKey will be rotated at the interval you select.

Note: This rotation schedule is applied to all CloudKeys created in the Key Set, unless a different value is explicitly chosen. If there are existing CloudKeys in the Key Set, you can update the rotation schedule of the CloudKeys to align with your selected rotation schedule by checking **Apply to all CloudKeys**.

9. Click **Apply**.

Managing Authentication for Vault for Databases

By default each vault is configured for local authentication. You can change the authentication method as required. In the current release, you can choose between local authentication, Active Directory, OpenID Connect (OIDC) with AD, or OIDC without AD.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users.

For details on configuring each authentication option, see:

- Configuring local authentication for Vault for Databases
- Configuring Active Directory for the Vault for Databases
- Configuring OIDC with Active Directory for Vault for Databases
- Configuring OIDC for Vault for Databases
- Managing two-factor authentication in Vault for Databases

Configuring local authentication for Vault for Databases

Local authentication is enabled by default when you create a vault. If using local authentication, no further authentication configuration is required. The next step is to configure your access policies and users.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users

Configuring Active Directory for the Vault for Databases

See below for configuring Active Directory for the Vault for Databases.

> By default, the vault uses local authentication. You can change the authentication method as required.

To configure Active Directory

1. Log in to the CSP Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. On the Authentication page, select **LDAP** as the Authentication Type.
5. On the **Domain** tab, enter:
   - Domain Name—Enter the domain name for the service account.
   - Directory Service Type—Select **Microsoft AD** if you plan to use Microsoft AD directory services, or **OpenLDAP** for all non-Microsoft AD directory services.
   - Service Account Name—Enter the name of the service account for the given domain (for example, Administrator).

> The service account needs read-only access to users and groups on the domain and any subdomain used.

- Service Account Password —Enter the password for the service account.
- UID Attribute—Enter the Security Manager Account Name (sAMAccountName) for the user.

> This is the attribute of the user or group object that would be queried during search.

6. Click **Apply** to save the changes.
7. Click the **Domain Controllers** tab.
8. Click **+**
9. Add the following details in the **Add Domain Controller** window.
    - Server URL
    - STARTTLS
    - CA Certificate
    - User Search Context (Base DN)
    - Group Search Context (Base DN)
    - Timeout
10. Click **Save and Close**.

Server URL

Select LDAP or LDAPS and enter the domain name or IP address. To include a port number, use the following syntax:

```
<ip>:<port>
```

STARTTLS

If you selected LDAP, check the checkbox if you want to use LDAP over TLS.

CA Certificate

The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller.

- The CA certificate must be in Base64-encoded PEM format.
- If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates.

Click Load File to select the CA certificate that you want to use.

User Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the user search should start. For performance reasons, make the base DN as specific as possible. For example:

```
dc=ldapserver,dc=com
```

This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP.

Group Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the search for Security groups should start.

This option applies to AD Security groups being associated with an admin group.

Timeout

Set the timeout in seconds before connecting to an alternate domain controller.

- If multiple domain controllers are specified, this is how long the Cryptographic Security Platform Vault waits for a response before re-sending the request to another domain controller.
- If the DNS server is down, Cryptographic Security Platform Vault may take longer than the time specified here before it fails over to the next domain controller in the list or considers the authentication request failed.

This option only applies to the TCP/LDAP request. It does not apply to the DNS request before the LDAP server has been successfully contacted.

Configuring OIDC with Active Directory for Vault for Databases

By default, the vault uses local authentication. You can change the authentication method as required, and you can have multiple authentication modes active at the same time. However, OIDC without Active Directory cannot be used with Active Directory, and OIDC with Active Directory cannot be used without Active Directory.

You cannot disable OIDC authentication once it is configured. After you enable OIDC, you can no longer sign in with AD credentials. However, you can sign in using local authentication credentials without any issues.

To configure OIDC

1. Log in to the Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. In the **Choose Authentication Type** drop-down menu, select:
    - **OpenID Connect** to configure OIDC without Active Directory
    - **OpenID Connect (with AD)** to configure OIDC with Active Directory
5. Click the **Learn more about configuring the OIDC Provider** link to view the OIDC provider's login redirect URL and logout redirect URL.
6. Specify the OpenID Connect Configuration settings:
    - Name
    - Client ID
    - Client Secret
    - Base URL
7. Optionally, click **Load File** to upload the CA certificate in base64-encoded PEM format.
8. Click **Apply**.

9. Select **Verify and Enable**. After verification, a message appears confirming OpenID Connect has been successfully enabled. Vault is set for OIDC authentication.
10. Sign out from the vault and sign in to the vault as an OIDC user by selecting **Sign in with IDAAS** and entering your OIDC credentials.

Name

A user-defined name for the OpenID Connect provider.

> Cryptographic Security Platform Vault displays this name on the button in the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

> This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Configuring OIDC for Vault for Databases

By default, the KeyControl Vault Management application is configured for local authentication. You can change the authentication method as required, but you can use only one type of authentication per vault at a time.

- If you want to use OIDC without AD, you can only change to that mode from the local authentication mode.
- If you have configured AD or OIDC with AD, you cannot change to OIDC without AD.

Each vault can be configured with a separate OIDC server or a separate application from same server.

> OIDC without AD is the recommended mode of OIDC authentication method where the OIDC provider independently manages identity and authentication. For new OIDC setups, this is the preferred option.

To configure OIDC

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Choose Authentication Type** drop-down list, select **OpenID Connect**.
6. Specify the OpenID Connect Configuration settings:
    - Name
    - Client ID
    - Client Secret

- Base URL

7. Optional. Click **Browse** to upload the CA Certificate.

   The certificate needs to be in base64 encoded pem format.

8. Enter the Admin Name and Admin Email for OIDC user. This user will be created and will act as the Vault Administrator. They will be assigned to the admin policy and receive the email with the registration URL.
9. Click **Apply**. The OpenID Connect Configuration window appears showing the current configuration.
10. Click **Verify and Enable**. The OpenID Connect Successfully Configured window displays the new login URL.
11. Copy the URL, and click **Log Out and Sign in with IDP**.
12. After you are logged out, paste the URL into the browser window.
13. Log in to the Identity Provider using the name and password that you created.

Name

A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Managing two-factor authentication in Vault for Databases

Two-factor authentication requires you to enter two forms of identification before you can access your CSP Vault.

- The first form is your standard username and password combination,
- The second is a one-time password (OTP) generated by an authorization app. The OTP is appended to your existing password.

See below for how to enable and manage it.

- Requirements for enabling two-factor authentication in Vault for Databases
- Enforcing two-factor authentication in Vault for Databases
- Disabling two-factor authentication in Vault for Databases

Two-factor authentication is supported with local authentication only. If you want to use two-factor authentication for non-local users, we recommend enabling it in your remote authentication provider.

Requirements for enabling two-factor authentication in Vault for Databases

Make sure you have access to an authentication app that can generate HOTP or TOTP passwords. For example:

- For TOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. These applications continuously generate passwords valid for 30 seconds. If the current password expires before you can submit the login request, you must wait for it to generate a new password, then use that to log in.
- For HOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. A password generated through the application is valid from the time you create it until you use it to log in. To log in again, click **Next** in the app to generate a new password.

Enforcing two-factor authentication in Vault for Databases

See below for enforcing two-factor authentication in Vault for Databases.

- Enforcing two-factor authentication for the current user
- Enforcing two-factor authentication for all users

Enforcing two-factor authentication for the current user

See below for enforcing two-factor authentication for the current user.

To enforce two-factor authentication for the current user

1. Log in to the Cryptographic Security Platform Vault for Databases webGUI.
2. In the top menu bar, click **Settings**.
3. In the **Two-Factor Authentication** field, click **Set up Two-Factor Authentication**.
4. In the **Enable Two-Factor** dialog box, select the HOTP or TOTP radio button.
5. Scan the generated barcode with your authorization app.
6. Enter the six-digit verification code from your app in the dialog box.
7. Click **Continue**. Cryptographic Security Platform Vault verifies the code and displays a message indicating success or failure. If the code is not correct, re-enter it.
8. After the code has been accepted, click **Done**.
9. When you log into the Vault web GUI:
    - Enter a valid OTP along with your standard account password on the login page. Do not add any characters or spaces between your account password and the one-time password generated by your authorization app. For example, if your password is `XyZ123$`, and your OTP is `32325`, you enter `XyZ123$32325` in the password field.
    - If you use TOTP, make sure your password doesn't expire before you submit the login request.

Enforcing two-factor authentication for all users

See below for enforcing two-factor authentication for all Vault users

To enforce two-factor authentication for all users

1. Log into the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the **Two-Factor Authentication Settings** page, select **ENFORCED**.
5. Click **Apply**.

Disabling two-factor authentication in Vault for Databases

See below for disabling two-factor authentication in Vault for Databases.

- Disabling two-factor authentication for a user
- Disabling two-factor authentication for all users

Disabling two-factor authentication for a user

See below to disable two-factor authentication for a single Vault user.

To disable two-factor authentication

1. Log in to the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Security**.
3. Select the **Users** tab
4. Select the user for whom you want to disable two-factor authentication.
5. In the **Details** tab below the table, click the **Enabled** link for the **Two-Factor Authentication** row.
6. In the **Disable Two-Factor Authentication** window, click **Proceed**.

Disabling two-factor authentication for all users

See below to disable two-factor authentication for all Vault users.

To disable two-factor authentication for all users

1. Log into the Cryptographic Security Platform Vault for Databases webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the Two-Factor Authentication Settings page, select **NOT ENFORCED**.
5. Click **Apply**.

CSP Vault for KMIP

- CSP Vault for KMIP KMIPCLI
- Resetting KMIP Vaults
- Rekeying KMIP Objects in the CSP Vault for KMIP webGUI
- KEK with a KMIP Vault
- Viewing CSP Vault for KMIP Audit Logs
- Managing KMIP Objects in the CSP Vault for KMIP webGUI
- Managing KMIP Client Certificates
- Creating a KMIP Client Certificate
- CSP Vault for KMIP Access Policies
- KMIP Cluster Considerations
- Configuring a new KMIP Server
- Post Quantum Support in the CSP Vault for KMIP
- KMIP Vault Overview
- Managing Authentication for Vault for KMIP

CSP Vault for KMIP KMIPCLI

- Accessing the KMIPCLI
- Change-AD Domain Command
- Completion Command
- Configure-HSM-KEK Command
- Create-Client-Cert Command
- Create-Local User Command
- Create-Policy Command

- Delete-Client-Cert Command
- Delete-Local User Command
- Delete-Policy-Command
- Disable-KMIP-KEK Command
- Download Audit Command
- Download-Client-Cert Command
- Get-AD Group Command
- Get-AD Settings Command
- Get-AD User Command
- Get-Audit-Message Template Command
- Get-Audit Settings Command
- Get-Client-Cert Command
- Get-HSM Info Command
- Get-KEK-Setting Command
- Get-KMIP-Object Command
- Get-KMIP-Object-Count Command
- Get-Local User Command
- Get-Personal-Access-Token Command
- Get-Platform Info Command
- Get-Policy-Command
- Get-Vault-Info Command
- Get-Vault-Settings Command
- KMIPCLI Examples
- KMIPCLI Overview
- List-AD Settings Command
- List-Audit Messages Command
- List-Audit-Message Templates Command
- List-Client-Certs Command
- List-KMIP-Objects Command
- List-Local-Users Command
- List-Personal-Access-Tokens Command
- List-Policies Command
- List-Policy Versions Command
- Locate-Root-Key Command
- Login-Command
- Rekey-KMIP-KEK Command
- Renew-Command
- Set-Policy Version Command
- Update-AD Settings Command
- Update-Audit Settings Command
- Update-KMIP-Object Command
- Update-Local-User Command
- Update-Personal-Access-Token Command
- Update-Policy Command
- Update-Vault-Auth-Method-to-AD Command
- Update-Vault-Settings Command
- Version-Command

Accessing the KMIPCLI

To access the KMIPCLI, you will need the following:

- The Cryptographic Security Platform Vault for the KMIP CA Certificate.

- The login URL of the vault. This is listed as the API URL on the **Details** page.

KMIPCLI is supported on Linux VMs with Python installed. It is not supported on Windows. You can download the KMIPCLI here: https://github.com/EntrustCorporation/kmipcli.

You can use the CLI commands in the KMIPCLI only after a vault has been created. In all commands in this section, the KMIPCLI application is located in the same directory as the downloaded Cryptographic Security Platform Vault for the KMIP CA certificate.

Change-AD Domain Command

Use the KMIPCLI change-ad-domain command to change your Active Directory domain.

Syntax

kmipcli change-ad-domain [*options*]

Option	Description
-d, --domain-name string	The Active Directory Domain Name. Strings must be enclosed in double quotes.
-h or --help	Displays usage text.
-n or --netbios-name string	The Active Directory NetBIOS name. Strings must be enclosed in double quotes.

Option	Description

-j, --servers-json-file string	The Active Directory Domain Controller List JSON File. This is an array of JSON objects, each object representing a Domain Controller. Strings must be enclosed in double quotes.
	The following keys are supported:
	• server_url - the (mandatory) full url of the Domain Controller
	• cacert (optional) - the path to the CA Certificate to verify with
	• user_base_dn (optional) - the user base DN
	• group_base_dn (optional) - the group base DN
	• timeout (optional) - the connection timeout in seconds. The default is 5 seconds.
	• tls (optional) - whether to enable StartTLS or not. The default is false.
	Example:
	[
	{
	"server_url": "ldaps://
	dc1.mycompany.eng.com",
	"cacert": "/root/cacert.pem",
	"user_base_dn":
	"DC=mycompany,DC=eng,DC=com",
	"group_base_dn":
	"DC=mycompany,DC=eng,DC=com",
	"timeout": 10,
	"tls": false,
	}
	]

-p, --service-password string	The Active Directory service account user password. Strings must be enclosed in double quotes.
-s, --service-account string	The Active Directory service account user name. Strings must be enclosed in double quotes. To clear, set it to "unset".
-t, --type string	The domain type.
-u, --uid-attribute string	The Active Directory UID Attribute. Strings must be enclosed in double quotes.

Completion Command

Use the KMIPCLI completion command to generate the KMIPCLI versions of scripts for bath, fish, powershell, and zsh.

Syntax

kmipcli completion [command]

Option	Description
-h or --help	Displays usage text.
bash	Generates the autocompletion script for bash.
fish	Generates the autocompletion script for fish.
powershell	Generates the autocompletion script for powershell.
zsh	Generates the autocompletion script for zsh.

Configure-HSM-KEK Command

Use the KMIPCLI configure-hsm-kek command to configure encrypting KMIP objects using a KEK stored in a system HSM.

Syntax

kmipcli configure-hsm-kek [*options*]

Option	Description
-h or --help	Displays usage text.
-s, --hsm_type string	The HSM type that is configured on the system. This can be NCIPHER or LUNA. NCIPHER is the default.

Option	Description
-t, --kek_cache_timeout int	For KMIP Key wrapping, this is the cache timeout for the KEK. Because connecting frequently to the System HSM to fetch the KEK and encrypt the object can affect performance, you can select how long you would like to keep the KEK cached in the Cryptographic Security Platform Vault for KMIP. When the timeout period ends, the KEK is deleted from the cache. The default value is 1800 seconds. Set to 0 to disable KEK cache timeout.
-R, --revision int	Enter the current revision number of the HSM KEK. If you do not know the revision number, run the `get-kek-setting` command.
-l, --rootkey_label string	The identifier to identify the root key on the HSM that is used to wrap and unwrap keys. If the root key label already exists, it will be used. If it does not exist, the Cryptographic Security Platform Vault for KMIP creates a new one. The root key label must meet the following requirements: • At least 8 characters • No more than 31 characters • Can include uppercase, lowercase, numbers, and special characters • No space or tab character At this point, all existing KMIP objects and all new Key creation requests will be encrypted using the key.

Create-Client-Cert Command

Use the KMIPCLI create-client-cert command to create the certificate to be used for the KMIP Client.

Syntax

```
kmipcli create-client-cert [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-t, --cert string	The certificate to be used for the KMIP Client. Strings must be enclosed in double quotes. This field is only visible if the custom_cacert_use_to_verify_kmip_client_cert option is enabled in hicli. If enabled, you must provide the location to upload a custom certificate. If no certificate is uploaded, then you will see an error saying that the certificate was not provided.
-c, --csr string	The certificate signing request to be used to generate the KMIP Client Certificate. Strings must be enclosed in double quotes.
-e, --expiry-days int	The number of days before the KMIP Client Certificate expires.
-n, --name string	The name to be used for the Client Certificate.
-p, --passphrase string	The passphrase to be used if the KMIP Client Certificate is encrypted.

Create-Local User Command

Use the KMIPCLI create-local-user command to create a local user.

Syntax

```
kmipcli create-local-user [options]
```

Option	Description
-h or --help	Displays usage text.
-e, --email string	The email address for the local user.
-n, --name string	The full name of the local user.

Create-Policy Command

Use the KMIPCLI create-policy command to create a KMIP policy.

Syntax

```
kmipcli create-policy [options]
```

Option	Description
-h or --help	Displays usage text.
-g, --ad-group stringArray	The ||-separated string containing the DN and display name of AD groups to be added as principals.
-L, --ad-logon-name stringArray	The login name of AD users to be added as principals. This option is repeatable.
-u, --ad-upn stringArray	The UPN of AD users to be added as principals. This option is repeatable.
-d, --description string	Short description for the policy.
-l, --local-user stringArray	Reserved for future use.
-n, --name string	The name of the policy.
-r, --role string	The role of the user.
-t, --tagkey stringArray	The tag key to associate with the policy. This option is repeatable.
-v, --tagvalue stringArray	The tag value to associate with the policy. This option is repeatable.

Delete-Client-Cert Command

Use the KMIPCLI delete-client-cert command to delete the certificate used for the KMIP Client.

Syntax

```
kmipcli delete-client-cert [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-c, --certid string	The ID or name of the KMIP Client Certificate that you want to delete.

Delete-Local User Command

Use the KMIPCLI delete-local-user command to delete a local user.

Syntax

```
kmipcli delete-local-user [options]
```

Option	Description
-h or --help	Displays usage text.
-u, --user string	The name of the user to be deleted.

Delete-Policy-Command

Use the KMIPCLI delete-policy command to delete a KMIP policy.

Syntax

```
kmipcli delete-policy [options]
```

Option	Description
-h or --help	Displays usage text.
-p, --policyid string	The ID or name of the policy to be deleted.

Disable-KMIP-KEK Command

Use the KMIPCLI disable-kmip-kek command to disable encrypting KMIP objects using a KEK.

Syntax

```
kmipcli disable-kmip-kek [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-R, --revision int	Enter the current revision number of the HSM KEK. If you do not know the revision number, run the `get-kek-setting` command.

Download Audit Command

Use the KMIPCLI download-audit command to download the audit log bundle.

Syntax

```
kmipcli download-audit [options]
```

Option	Description
-h or --help	Displays usage text.

Download-Client-Cert Command

Use the KMIPCLI download-client-cert command to download your KMIP client certificate.

Syntax

```
kmipcli download-client-cert [options]
```

Option	Description
-h or --help	Displays usage text.

Get-AD Group Command

Use the KMIPCLI get-ad-group command to search for a specific AD group.

Syntax

```
kmipcli get-ad-group [options]
```

Option	Description
-h or --help	Displays usage text.
-n, --name string	The prefix for the AD group name that you are searching for.

Get-AD Settings Command

Use the KMIPCLI get-ad-settings command to fetch the specified AD settings.

Syntax

```
kmipcli get-ad-settings [options]
```

Option	Description
-h or --help	Displays usage text.
-a, --ad-setting-id string	The ID or name of the AD setting to fetch. Strings must be enclosed in double quotes.

Get-AD User Command

Use the KMIPCLI get-ad-user command to search for a specific AD user.

Syntax

```
kmipcli get-ad-user [options]
```

Option	Description
-h or --help	Displays usage text.
-n, --name string	The prefix of the username to search for.

Get-Audit-Message Template Command

Use the KMIPCLI get-audit-message-template command to fetch an audit message template with a specific message ID.

Syntax

```
kmipcli get-audit-message-template [options]
```

Option	Description
-h or --help	Displays usage text.
-m, --msgid int	The message ID of the audit message template to fetch.

Get-Audit Settings Command

Use the KMIPCLI get-audit-settings command to fetch the current audit settings.

Syntax

```
kmipcli get-audit-settings [options]
```

Option	Description
-h or --help	Displays usage text.

Get-Client-Cert Command

Use the KMIPCLI get-client-cert command to fetch the details of the specified KMIP client certificate.

Syntax

```
kmipcli get-client-cert [options]
```

Option	Description
-h or --help	Displays usage text.
-c, --certid string	The ID or name of the KMIP Client certificate to fetch.

Get-HSM Info Command

Use the KMIPCLI get-hsm-info command to fetch the configuration details of your system HSM.

Syntax

```
kmipcli get-hsm-info [options]
```

Option	Description
-h or --help	Displays usage text.

Get-KEK-Setting Command

Use the KMIPCLI get-kek-setting command to fetch the KMIP KEK setting information.

Syntax

```
kmipcli get-kek-setting [options]
```

Option	Description
-h or --help	Displays usage text.

Get-KMIP-Object Command

Use the KMIPCLI get-kmip-object command to fetch all attributes of the specified KMIP object.

Syntax

```
kmipcli get-kmip-object [options]
```

Option	Description
-h or --help	Displays usage text.
-u, --uuid string	The UUID of the KMIP object to fetch.

Get-KMIP-Object-Count Command

Use the KMIPCLI get-kmip-object-count command to fetch the count of KMIP objects.

Syntax

```
kmipcli get-kmip-object-count [options]
```

Option	Description
-h or --help	Displays usage text.
-f, --filter stringArray	The fields to be filtered on in a ||-separated list. For example: `-f ["name", "Smith" || "group", "operations" || "ID", "e72b2cd1-f722-4f4c-a919-b440feb7e88a"]` .

Get-Local User Command

Use the KMIPCLI get-local-user command to get details about the specified local user.

Syntax

```
kmipcli get-local-user [options]
```

Option	Description
-h or --help	Displays usage text.
-u, --user string	The username that you want to search for.

Get-Personal-Access-Token Command

Use the KMIPCLI get-personal-access-token command to fetch details about the specified personal access token.

Syntax

```
kmipcli get-personal-access-token [options]
```

Option	Description
-h or --help	Displays usage text.
--n, --name string	The name of the personal access token.

Get-Platform Info Command

Use the KMIPCLI get-platform-info command to fetch information about the platform.

Syntax

```
kmipcli get-platform-info [options]
```

Option	Description
-h or --help	Displays usage text.

Get-Policy-Command

Use the KMIPCLI get-policy command to fetch the specified policy.

Syntax

```
kmipcli get-policy [options]
```

Option	Description
-h or --help	Displays usage text.
-p, --policyid string	The ID or name of the policy to fetch.
-v, --version int	The version of the policy to fetch. If not specified, this command fetches the current version.

Get-Vault-Info Command

Use the KMIPCLI get-vault-info command to fetch information about the Cryptographic Security Platform Vault for KMIP.

Important: If you are using an older version of KMIPCLI, this command may be called `get-tenant-info`.

Syntax

```
kmipcli get-vault-info [options]
```

Option	Description
-h or --help	Displays usage text.

Get-Vault-Settings Command

Use the KMIPCLI get-vault-settings command to fetch the settings for the Cryptographic Security Platform Vault for KMIP.

Important: If you are using an older version of KMIPCLI, this command may be called `get-tenant-settings`.

Syntax

```
kmipcli get-vault-settings [options]
```

Option	Description
-h or --help	Displays usage text.

KMIPCLI Examples

Login to the Cryptographic Security Platform Vault for KMIP:

$./kmipcli login -u "username" -p "password" --login-URL <VAULT_API_URL> --cacert ca.cert

Create the KMIP client certificate:

$./kmipcli create-client-cert --name "client-cert-name" --expiry-days "expiry_days_in_int"

Get the KMIP client certificate details:

$./kmipcli get-client-cert -c "client-cert-name"

Download the KMIP client certificate:

$./kmipcli download-client-cert -c "client-cert-name"

Delete the KMIP client certificate:

$./kmipcli delete-client-cert -c "client-cert-name"

List all Cryptographic Security Platform Vault for KMIP local users:

$./kmipcli list-local-users

Get the total count of all objects in the Cryptographic Security Platform Vault for KMIP:

$./kmipcli get-kmip-object-count

```
//response
 {
   "total": 1
 }
```

Get Cryptographic Security Platform Vault for KMIP access policy details:

$./kmipcli list-policies

Update the state of an existing key to archived:

$./kmipcli update-kmip-object -a archive -u c2b0d10f-4255-46cb-9ef0-1ab5de5c7428

Fetch the full details including custom attributes of a key:

$ ./kmipcli get-kmip-object -u c2b0d10f-4255-46cb-9ef0-1ab5de5c7428

```
//response
 {
   "activationDate": "2025-06-30T08:07:46Z",
    "archive_date": "2025-06-30T08:28:58Z",
    "cryptographic_algorithm": "3DES",
    "cryptographic_length": 128,
    "cryptographic_usage_mask": "Encrypt,Decrypt",
    "initial_date": "2025-06-30T08:07:46Z",
    "key_format_type": "Raw",
    "last_change_date": "2025-06-30T08:28:58Z",
    "object_type": "Symmetric Key",
    "Operation Policy Name": "default",
    "state": "Active",
    "x-NETAPP-ClusterId": "50b7a51c-6f12-11e4-88de-123478563412",
    "x-NETAPP-KeyId":
"000000000000000002000000000000500f6296053dd1df233554eaf8f3665d2ce0000000000000000"
,
    "x-NETAPP-KeyType": "AES",
    "x-NETAPP-Product": "Data ONTAP",
    "x-NETAPP-VserverId": "48",
    "kek_encrypted": false
 }
```

KMIPCLI Overview

With KMIPCLI, you can manage your Cryptographic Security Platform Vault for KMIP with a shell script. All vault management operations, including user management, KMIP key operations, HSM Management, and KMIP Client certificate management can be performed with KMIPCLI.

Important: KMIPCLI is supported on Linux VMs with python installed. It is not supported on Windows.

Before using KMIPCLI, ensure the following:

- The Cryptographic Security Platform Vault for KMIP must be created by the Cryptographic Security Platform Vault Administrator.
- The KMIPCLI user must be an administrator for the Cryptographic Security Platform Vault for KMIP and must have the login API URL for that vault.
  The API URL is located in the Cryptographic Security Platform Vault Management application, in the Details section for the Cryptographic Security Platform Vault for KMIP.

- If the KMIPCLI is not executable, ensure that you run the `chmod +x kmipcli` command to make it executable.
- You must download the CA Certificate to log in to the Cryptographic Security Platform Vault for KMIP. To do so, do one of the following:
  - Enter the following command: `$wget https://<kcv ip>/v4/ca_certificate/ --no-check-certificate -O ca.cert`.
  - Log into the Cryptographic Security Platform Vault Management webGUI and select **? > Download CA Certificate**.

List-AD Settings Command

Use the KMIPCLI list-ad-settings command to list all of your AD settings in the Cryptographic Security Platform Vault for KMIP.

Syntax

```
kmipcli list-ad-settings [options]
```

Option	Description
-h or --help	Displays usage text.
-f, --field stringArray	Enter the AD setting fields to include in the response.
-l, --filters string	Enter the conditional expression to filter AD settings.
-m, --max-items int	Enter the maximum number of items to include in response.
-n, --next-token string	The token from which subsequent AD settings would be listed.
-p, --prefix string	List only those AD settings that use this string as a prefix.

List-Audit Messages Command

Use the KMIPCLI list-audit-messages command to list all available audit messages.

Syntax

```
kmipcli list-audit-messages [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-f, --field stringArray	The audit message fields to include in the response
-l, --filters string	Conditional filter expression to apply
-i, --include-info	Show additional information if available.
-j, --json-output	Show JSON-formatted audit messages.
-t, --local-time	Convert the audit message timestamp to local time.
-m, --max-items int	The maximum number of items to include in the response.
-n, --next-token string	The token from which subsequent audit messages would be listed.

List-Audit-Message Templates Command

Use the KMIPCLI list-audit-message-templates command to list all audit message templates that match the query.

Syntax

```
kmipcli list-audit-message-templates [options]
```

Option	Description
-h or --help	Displays usage text.
-m, --max-items int	The maximum number of items to include in the response.
-n, --next-token string	The token from which subsequent audit messages would be listed.

List-Client-Certs Command

Use the KMIPCLI list-client-certs command to list all KMIP client certificates.

Syntax

```
kmipcli list-client-certs [options]
```

Option	Description
-h or --help	Displays usage text.
-f, --field stringArray	The KMIP client certificate field to include in the response.
-l, --filters string	The conditional expression to list the filtered KMIP client certificates.
-m, --max-items int	The maximum number of items to include in the response.
-n, --next-token string	The token from which subsequent KMIP client certificates would be listed.
-p, --prefix string	The prefix to list all KMIP client certificates with.

List-KMIP-Objects Command

Use the KMIPCLI list-kmip-objects command to fetch all KMIP objects that match your requirements.

Syntax

```
kmipcli list-kmip-objects [options]
```

Option	Description
-h or --help	Displays usage text.
-f, --filter stringArray	The fields to be filtered on in a ||-separated list. For example: `-f ["name", "Smith" || "group", "operations" || "ID", "e72b2cd1-f722-4f4c-a919-b440feb7e88a"]` .
-m, --max-items int	The maximum number of items to include in the response.
-s, --sort-by string	How the list of items should be sorted.

Option	Description
-o, --start-offset int	The index of the first object to retrieve in the list. If you specify 0 (zero) for this parameter, the command starts at the top of the list.

List-Local-Users Command

Use the KMIPCLI list-local-users command to list all local users.

Syntax

```
kmipcli list-local-users [options]
```

Option	Description
-h or --help	Displays usage text.
-f, --fields stringArray	The fields to include in the response.
-l, --filters string	The conditional expression to list filtered users.
-m, --max-items int	The maximum number of items to include in the response.
-n, --next-token string	The token from which subsequent users would be listed
-p, --prefix string	The prefix to list users with.

List-Personal-Access-Tokens Command

Use the KMIPCLI list-personal-access-tokens command to fetch details about all personal access tokens.

Syntax

```
kmipcli list-personal-access-tokens [options]
```

Option	Description
-h or --help	Displays usage text.

List-Policies Command

Use the KMIPCLI list-policies command to list all specified access policies.

Syntax

```
kmipcli list-policies [options]
```

Option	Description
-h or --help	Displays usage text.
-f, --field stringArray	The policy field to include in the response.
-l, --filters string	The conditional expression to list filtered policies.
-m, --max-items int	The maximum number of items to include in the response.
-n, --next-token string	The token from which subsequent policies would be listed.
-p, --prefix string	The prefix with which to list policies.

List-Policy Versions Command

Use the KMIPCLI list-policy-versions command to list all of the versions of the specified policy.

Syntax

```
kmipcli list-policy-versions [options]
```

Option	Description
-h or --help	Displays usage text.
-p, --policyid string	The ID or name of the policy.

Locate-Root-Key Command

Use the KMIPCLI locate-root-key command to locate the KMIP KEK root key.

Syntax

```
kmipcli locate-root-key [options]
```

Option	Description
-h or --help	Displays usage text.

Login-Command

Use the KMIPCLI login command to log in to the Cryptographic Security Platform Vault for KMIP.

Syntax

```
kmipcli login [options]
```

Option	Description
-h or --help	Displays usage text.
-C, --cacert string	The CA certificate to verify your login.
-l, --login-URL string	The login URL for the Cryptographic Security Platform Vault for KMIP.
-u, --username string	The login username. You will be prompted to enter if it is not provided.
-p, --password string	The login password. You will be prompted to enter if it is not provided.

Rekey-KMIP-KEK Command

Use the KMIPCLI rekey-kmip-kek command to rekey KMIP objects with a new KEK.

Syntax

```
kmipcli rekey-kmip-kek [options]
```

Option	Description
-h or --help	Displays usage text.
-R, --revision int	Enter the current revision number of the KEK. If you do not know the revision number, run the `get-kek-setting` command.

Renew-Command

Use the KMIPCLI renew command to renew the access token.

Syntax

```
kmipcli renew [options]
```

Option	Description
-h or --help	Displays usage text.

Set-Policy Version Command

Use the KMIPCLI set-policy-version command to set a specific version of the policy to be the current policy.

Syntax

```
kmipcli set-policy-version [options]
```

Option	Description
-h or --help	Displays usage text.
-p, --policyid string	The ID or name of the policy.
-v, --version int	The version of the policy to be set as current.

Update-AD Settings Command

Use the KMIPCLI update-ad-settings command to update your Active Directory settings.

Syntax

```
kmipcli update-ad-settings [options]
```

Option	Description
-h or --help	Displays usage text.
-a, --ad-setting-id string	The Active Directory setting ID or name.
-n, --netbios-name string	The Active Direcotry NetBIOS name.
-r, --revision int	The Active Directory setting current revision.

Option	Description
-j, --servers-json-file string	Active Directory Domain Controller List JSON File. This is to be a array of JSON objects, each object representing a Domain Controller. Following keys are supported, server_url (mandatory) full url of the Domain Controller cacert (optional) path to CA Certificiate to verify with user_base_dn (optional) user base DN group_base_dn (optional) group base DN timeout (optional) connection timeout in seconds, defaults to 5 seconds tls (optional) enable StartTLS or not, defaults to false Example: [{ "server_url": "ldaps://dc1.mycompany.eng.com", "cacert": "/root/cacert.pem", "user_base_dn": "DC=mycompany,DC=eng,DC=com", "group_base_dn": "DC=mycompany,DC=eng,DC=com", "timeout": 10, "tls": false, }]
-s, --service-account string	The Active Directory service account user name. To clear this value, set it to "unset".
-p, --service-password string	The Active Directory service account password.
-t, --type string	The domain type.
-u, --uid-attribute string	The Active Directory UID attribute.

Update-Audit Settings Command

Use the KMIPCLI update-audit-settings command to update your audit log settings.

Syntax

```
kmipcli update-audit-settings [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-m, --max-logs-size int	The maximum size for the audit logs in bytes. Set 0 for no limit.
-r, --retention-days int32	The number of days to retain the audit logs. Choose a value between 30 and 365 days. Set to 0 to retain all audit logs.

Update-KMIP-Object Command

Use the KMIPCLI update-kmip-object command to update a KMIP object.

Syntax

```
kmipcli update-kmip-object [options]
```

Option	Description
-h or --help	Displays usage text.
-a, --action string	The action to perform on the KMIP object. This can be one of the following: • archive • revoke • destroy
-c, --revcode string	The revocation code if the action is set to revoke.
-m, --revmsg string	The revocation message if the action is set to revoke.
-u, --uuid string	The UUID of the KMIP object to update.

Update-Local-User Command

Use the KMIPCLI update-local-user command to update the specified local user.

Syntax

```
kmipcli update-local-user [options]
```

Option	Description
-h or --help	Displays usage text.
-s, --account-status string	The account status of the user.
-n, --name string	The full name of the user.
-R, --revision int	The revision number of the user.
-u, --user string	The username of the user to update.

Update-Personal-Access-Token Command

Use the KMIPCLI update-personal-access-token command to update a personal access token.

Syntax

```
kmipcli update-personal-access-token [options]
```

Option	Description
-h or --help	Displays usage text.
-d, --description string	The description of the personal access token.
-e, --expiry string	The date the personal access token expires in yyyy-mm-dd format.
-n, --name string	The name of the personal access token.
-r, --revoked	Set to True if you want to revoke this token.

Update-Policy Command

Use the KMIPCLI update-policy command to update the specified KMIP policy.

Syntax

```
kmipcli update-policy [options]
```

Option	Description
-h or --help	Displays usage text.
-g, --ad-group stringArray	The || separated string containing the DN and display name of AD groups to be added as principals.
-L, --ad-logon-name stringArray	The login name of AD users to be added as principals. This option is repeatable.
-u, --ad-upn stringArray	The UPN of AD users to be added as principals. This option is repeatable.
-d, --description string	Short description for the policy.
-l, --local-user stringArray	Reserved for future use.
-p, --policyid string	The ID or name of the policy to update.
-R, --revision int	The revision number of the policy.
-r, --role string	The role of the user.
-t, --tagkey stringArray	The tag key to associate with the policy. This option is repeatable.
-v, --tagvalue stringArray	The tag value to associate with the policy. This option is repeatable.

Update-Vault-Auth-Method-to-AD Command

Use the KMIPCLI update-vault-auth-method-to-ad command to update the authentication method to Active Directory.

Important: If you are using an older version of KMIPCLI, this command may be called `update-tenant-auth-method-to-ad`.

Syntax

```
kmipcli update-vault-auth-method-to-ad [options]
```

Option	Description
-h or --help	Displays usage text.
-a, --ad-domain-name string	The Active Directory name.
-t, --ad-domain-type string	The Active Directory domain type. This can be one of the following: • Microsoft_AD • openLDAP

-j	The Active Directory Domain Controller List JSON File. This is an array of JSON objects, each object representing a Domain Controller. Strings must be enclosed in double quotes.
	The following keys are supported:
	• server_url - the (mandatory) full url of the Domain Controller
	• cacert (optional) - the path to the CA Certificate to verify with
	• user_base_dn (optional) - the user base DN
	• group_base_dn (optional) - the group base DN
	• timeout (optional) - the connection timeout in seconds. The default is 5 seconds.
	• tls (optional) - whether to enable StartTLS or not. The default is false.
	Example:
	[
	{
	"server_url": "ldaps://
	dc1.mycompany.eng.com",
	"cacert": "/root/cacert.pem",
	"user_base_dn":
	"DC=mycompany,DC=eng,DC=com",
	"group_base_dn":
	"DC=mycompany,DC=eng,DC=com",
	"timeout": 10,
	"tls": false,
	}
	]

Option	Description
-p, --ad-service-account-pw string	The Active Directory service account user password. Strings must be enclosed in double quotes. You can enter the value either through the console or by using a flag.
-s, --ad-service_account_name string	The Active Directory service account user name. Strings must be enclosed in double quotes. To clear, set it to "unset". You can enter the value either through the console or by using a flag.
--u, --ad-uid string	The Active Directory UID attribute. Strings must be enclosed in double quotes.
-k, --initial-ad-member-cn string	The initial Active Directory member CN.
-d, --initial-ad-member-distinguished-name string	The initial Active Directory member distinguished name.
-m, --initial-ad-member-mail string	The initial Active Directory member email address.
-o, --initial-ad-member-upn string	The initial Active Directory member UPN.
-n, --name string	The name of the vault to be updated.

Update-Vault-Settings Command

Use the KMIPCLI update-vault-settings command to update the KMIP vault settings.

Important: If you are using an older version of KMIPCLI, this command may be called `update-tenant-settings`.

Syntax

```
kmipcli update-vault-settings [options]
```

Option	Description
-h or --help	Displays usage text.

Option	Description
-d, --degraded-mode-availability string	The degraded mode availability flag. Accepts enable or disable.
-o, --oidc-enabled string	The OIDC enabled flag. Accepts enable or disable.
-R, --revision int	The current revision number of the vault settings.

Version-Command

Use the KMIPCLI version command to display the version of the Entrust KMIP Vault Portal CLI.

Syntax

```
kmipcli version [options]
```

Option	Description
-h or --help	Displays usage text.

Resetting KMIP Vaults

Warning: The following procedure destroys all current KMIP user accounts, KMIP objects and client certificates, including any encryption keys that may be stored in the KMIP vault. This operation is not reversible.

Before You Begin

- If this KMIP vault is used as a KMS server for vSphere Key Management Server, make sure that you decrypt all workloads whose keys are stored in the KMIP server. Those keys will be destroyed when the KMIP server is reset. For more information, the *Entrust Cryptographic Security Platform Vault with VMware VSAN and vSphere VM Encryption* guide.
- If this KMIP vault is used as an External Key Server for one or more Cryptographic Security Platform Vault clusters, download the Admin keys for those clusters in case you need to restore those clusters. All objects, including Cryptographic Security Platform Vault Admin keys, will be destroyed when you reset the server.

Procedure

1. Log in to the Cryptographic Security Platform Vault for KMIP webGUI.
2. Click the gear icon on the right top corner to view **Settings**.
3. On the Settings page, click **Advanced**.
4. Click **Reset**.

Rekeying KMIP Objects in the CSP Vault for KMIP webGUI

On rekey, all existing KMIP objects and any new KMIP objects are encrypted using a new Key Encryption Key (KEK). The HSM must be available before you can rekey. KMIP clients continue to be able to access KMIP objects when the rekey is in progress.

Procedure

1. Log in to the Cryptographic Security Platform Vault for KMIP webGUI.
2. Click **Objects**.
3. On the Objects page, select **Actions > Rekey All Objects**.
4. At the prompt, click **Rekey** to re-encrypt KMIP objects using a new KEK.

When the encryption of all KMIP objects completed, an audit log is generated.

KEK with a KMIP Vault

KMIP vaults can be configured with a Key Encryption Key (KEK) that provides an extra layer of security by encrypting individual KMIP objects.

When KEK wrapping is enabled, the KMIP object data is protected not only by Cryptographic Security Platform Vault object store encryption but also by a KEK stored in an HSM. KMIP vaults can use the system HSM configured on Cryptographic Security Platform Vault to generate and store KEK.

> The system HSM server configuration is shared by all Cryptographic Security Platform Vault for KMIPs.

To configure KEK

1. Log in to the Cryptographic Security Platform Vault for KMIP web GUI.
2. Click the gear icon in the top-right corner to view Settings.
3. On the Settings page, click **HSM**.
4. In the KMIP Key Wrapping window, select the options you want.
   - Server
   - HSM Root Key Label
   - KEK Cache Timeout
5. When you are finished, click **Enable**.
6. The Cryptographic Security Platform Vault contacts the HSM to create a root key specified by the root key label (if it doesn't already exist) and uses it to derive a KEK. The system then encrypts each KMIP object with a unique key derived from the KEK. The system encrypts all existing KMIP objects in the background and generates an audit log.
7. To disable KEK wrapping, set the status button to **Disabled**. The system decrypts all existing KMIP objects in the background and generates an audit log.

Server

Select System HSM. This allows you to use the HSM configured to work with KeyControl. This can be either the Luna SA HSM, Luna Cloud HSM, or nShield Connect HSM. You must configure the HSM before it will display here.

HSM Root Key Label

The identifier used to identify the root key on the HSM that is used to wrap and unwrap keys. If the root key label already exists, it will be used. If it does not exist, Cryptographic Security Platform Vault creates a new one.

The root key label must meet the following requirements:

- At least 8 characters
- No more than 31 characters
- Can include uppercase, lowercase, numbers, and special characters

- No space or tab characters

At this point, all existing KMIP objects and all new Key creation requests will be encrypted using the key.

KEK Cache Timeout

For KMIP Key wrapping, this is the cache timeout for the KEK. Because frequently connecting to the System HSM to fetch the KEK and encrypt the object can affect performance, you can choose how long to keep the KEK cached in Cryptographic Security Platform Vault. When the timeout period ends, the Cryptographic Security Platform Vault deletes the KEK from its cache. The default value is 30 minutes. Set 0 to disable KEK cache timeout.

Viewing CSP Vault for KMIP Audit Logs

The KMIP Vault audit logs page tracks all activity for the KMIP vault. The audit logs are view only.

Audit logs generated by the KMIP vault can be accessed both in the Cryptographic Security Platform Vault for KMIP webGUI.

Procedure

1. Log in to the Cryptographic Security Platform Vault for KMIP webGUI.
2. Click Audit Logs.
   The Audit Logs page shows the following information for each audit log:

Field	Description
Time	Time when the audit message is posted.
Type	Type of the audit message.
User	User or KMIP client whose action generated the audit log.
Message	Audit message content.

   Tip: You can filter the objects based on these fields.
3. Optionally click the **Download** button in the top-right corner of the Audit Logs page to download the log file.

Managing KMIP Objects in the CSP Vault for KMIP webGUI

KMIP objects include certificates and symmetric or asymmetric keys. External KMIP clients create them as needed, and those clients can then fetch them. You can use the Cryptographic Security Platform Vault for KMIP webGUI to view and manipulate all objects created by all KMIP users in the system.

> The Cryptographic Security Platform Vault for KMIP does not support RSA keys of length 512 and 1024.

If this KMIP server is being used as a KMS for VMware, the number of KMIP objects may exceed the number of encrypted VMs because:

- The KMIP objects created when a VM is encrypted are not removed when that VM is decrypted or deleted.
- Cloned VMs may share the same key if they have the same UUID.

- vCenter creates a KMIP object for each ESXi host when you enable encryption for that host.
- Stale keys for an ESXi host are not removed unless you detach, reboot, and then reattach the ESXi host.

To manage KMIP objects

1. Log in to the Cryptographic Security Platform Vault for KMIP webGUI.
2. From the Cryptographic Security Platform Vault for KMIP webGUI, select the following options.
    - Objects
    - Actions

Objects

The Objects tab shows the following information for each object:

- **UUID**—The Universally Unique Identifier associated with the KMIP object.
- **Initial Date**—When the object was created.
- **Last Change Date**—When the object was last modified.
- **Object Type**—The object type.
- **Archived**—Whether the object has been archived. You can recover archived objects if needed.
- **State**—The state of the KMIP object. This can be one of the following:
    - Pre-Active—The object has been created, but it is not yet available for use.
    - Active—The object is fully operational and available for use.
    - Deactivated/Archived—The object is temporarily unavailable, but can be reactivated.
    - Compromised—The object is suspected or confirmed to be compromised.
    - Destroyed—The object has been permanently deleted and is unrecoverable.
    - Destroyed Compromised—The object was compromised before being destroyed.

To filter the object based on any of the fields:

1. Click the text box next to the Filter tab
2. Select Filter by
3. Enter the filter value

Click any object in the list to view additional attributes for that object. The OASIS KMIP standard defines all attributes.

Actions

The Actions menu in the right corner allows you to perform any of the following actions on the selected object. All actions, except Rekey All Objects, follow the KMIP standard. Some actions require the object to be in a specific state. For details, see the OASIS KMIP standard.

- **Activate**—By default, objects are created in the PreActive state. Click **Activate** to enable more transitions for the object. **Note**: Many KMIP clients change objects to Active state as part of the creation process.
- **Archive**—Objects will no longer return keys, but they remain in the system. You can use the **Recover** command to return an archived object to active state and retrieve its keys.
- **Destroy**—This operation will destroy the object and change the object's state to “Destroyed”. Destroyed objects cannot be retrieved, but the object metadata will continue to appear on the KMIP objects page.
- **Recover**—Restores an Archived object to the active state so that its keys can be retrieved.
- **Revoke**—Revocation is permanent. Objects that are revoked cannot be moved back to Active, but the client can still retrieve any key material. Revocation prompts for a revocation reason, which can be any string. Revocation also prompts for a Reason Code, which is one of the following KMIP standard codes.

```
1–Unspecified
2–Key Compromise
```

```
3—CA Compromise
4—Affiliation Changed
5—Superseded
6—Cessation of Operation
7—Privilege Withdrawn
```

Any unrecognized value will be considered the same as "1—Unspecified."

- **Rekey KMIP Objects** - This option allows you to rekey all existing KMIP objects using a new KEK if KMIP KEK wrapping is enabled. See KEK with a KMIP Vault.

Managing KMIP Client Certificates

When you navigate to the Client Certificates page, you can create KMIP Client certificates, view the contents of a KMIP Client certificate, download the KMIP Client certificate bundled with the CA Certificate, or delete an existing KMIP Client certificate.

1. Log into the Cryptographic Security Platform Vault for KMIP webGUI.
2. From the Cryptographic Security Platform Vault for KMIP webGUI, select **Security > Client Certificates**. The Manage Client Certificate page displays the name of the certificate, the date the certificate is valid from, the expiration date, whether the certificate was generated from a external CSR, and
3. Perform one of the following tasks:
    - To download a KMIP Client certificate bundle:
      Select the certificate that you want to download, and click **Download**.
    - To view the contents of the KMIP Client certificate:
      Click the certificate that you want to view. The Certificate Details window has the following tabs:
        - Details—Displays the details of the certificate.
        - Client Certificate—Displays the text of the KMIP Client certificate. Click **Download** to download the bundle containing the KMIP Client certificate and the CA certificate.
        - CA Certificate—Displays the text of the CA certificate.
    - To delete a KMIP Client certificate:
      Select the certificate that you want to delete, and click the **Delete** icon.

Creating a KMIP Client Certificate

Each KMIP Client that you want to connect to the Cryptographic Security Platform Vault KMIP server must use a client certificate/key `pem` file and optionally a server (cacert) certificate `pem` file generated by the KMIP server.

Note: When the KMIP client certificate expiration date is approaching, the alert will be generated in the Cryptographic Security Platform Vault Appliance webGUI.

The client certificate can be created using one of the following:

- Username and password
- Certificate name

Note: You can either use the user name and password or the certificate name. Whichever name you choose is not case-sensitive and will be displayed in lowercase letters only.

You can download an existing certificate bundle at any time. One or more KMIP clients can then use the certificates in the bundle when contacting the KMIP server.

Note: If you are creating a KMIP user account to use with VMware vSphere Encryption.

Procedure

1. Log in to the Cryptographic Security Platform Vault for KMIP webGUI.
2. From the Cryptographic Security Platform Vault for KMIP webGUI, select **Security > Client Certificates**.
3. Select **Actions > Create Certificate**.
4. On the Manage Client Certificate page, click the **+** icon to create a new client certificate.
5. In the **Create Client Certificate** dialog box, complete the appropriate sections:
   - If you check the **Add Authentication for Certificate** checkbox, complete the following:

Field	Description
User name on Certificate	Enter the user name for the certificate. This is the user name used to authorize this certificate. The user name is not case-sensitive.
User password on the Certificate	Enter the user password for the certificate. This password authorizes this certificate.

   - If you do not want to use authentication, complete the following:

Field	Description
Certificate Name	Enter the user-defined name for this bundle. If you create multiple KMIP certificate bundles, make this name descriptive enough to tell the bundles apart. The name must start and end with an alphanumeric character. The only other characters allowed are hyphens (-) and underscores (_). You cannot change the name after you create the bundle. The certificate name is not case-sensitive.

   - Complete the rest of the fields as necessary:

Field	Description
Certificate Expiration	The date on which the certificates in the bundle will expire. If the certificates expire, communication between the Cryptographic Security Platform Vault KMIP server and the client will be disrupted until you upload a new certificate bundle to the client.
Certificate Signing Request (CSR)	To use an external CSR, click Load File and upload the CSR you want to use. The custom CSR must: • Be in PKCS#10 format. • Have a non-empty Common Name. • If keyUsage is specified, it must include 'digitalSignature'. If you do not specify an external CSR, Cryptographic Security Platform Vault uses an internally-generated CSR to create the certificate.

Field	Description
Encryption Password/ Confirm Encryption Password	Check the Encrypt Certificate Bundle checkbox to encrypt the certificates in the bundle, then enter and re-enter the encryption password. Whether the certificates need to be encrypted depends on how your security is configured and the implementation you are using. Not all third-party KMIP clients can accept encrypted certificates. For example, if you are integrating Cryptographic Security Platform Vault with VMware vSphere Encryption, you *cannot* specify a certificate passphrase because of vSphere limitations.

6. Click **Create**.
7. On the Manage Client Certificate page, select the certificate bundle that you just created and click **Download**.
   The webGUI downloads a bundle containing one of the following:
   - `<username_datetimestamp>.zip`
     This bundle contains a user certification/key file called *username*.pem and a CA certificate called cacert.pem .
   - `<certificatename_datetimestamp>`.zip
     This bundle contains a user certification/key file called *certificatename*.pem and a CA certificate called cacert.pem .

   You can now upload the certificates on the KMIP client. You can use standard API calls to interact with the KMIP server.

Important: You cannot renew client certificates in the Cryptographic Security Platform Vault for KMIP webGUI. If the client certificate used by a KMIP client has expired, a new client certificate has to be created, and the KMIP client needs to be reconfigured with the new certificate.

CSP Vault for KMIP Access Policies

The Cryptographic Security Platform Vault for KMIP supports Role-based Access Control (RBAC) Policies. Access to KMIP objects is denied by default, and must be explicitly granted through Access Control Policies.

Roles

Roles define actions or operations that can be performed on the KMIP Cryptographic Security Platform Vault for KMIP and KMIP objects. The following pre-defined roles are supported:

- **KMIP Administrators** have full access to all aspects of the Cryptographic Security Platform Vault for KMIP. This access includes:
  - KMIP objects—Can view and perform actions on KMIP objects.
  - Client certificates—Can create and manage KMIP client certificates that will be used by KMIP clients to create or access the KMIP objects.
  - Policy management—Can create role-based access control policies to allow users or applications the ability to access the Cryptographic Security Platform Vault for KMIP webGUI.
  - Audit logs—Can view audit logs.
  - Settings—Can view and modify Active Directory, KEK wrapping, and other settings.

- **Audit Administrators** have minimal access and can only view audit logs.

Policies

KMIP Administrators can create and manage access control policies that manage access to the KMIP objects. Policies consist of the following:

- Security principle—The list of users and groups governed by this policy. This can be an individual Local User, AD user or a group.
- Security principle—The list of users and groups governed by this policy. This can be an individual AD user or a group.
- Role—The permissions or a list of actions and operations that are granted to the user. The role can be KMIP Administrator or Audit Administrator.

Default Admin Policy

Cryptographic Security Platform Vault creates a default admin policy that grants the KMIP administrator role to the Local User, AD user or group that is set as the first KMIP administrator. This policy can be edited to add and remove AD groups or users but cannot be deleted.

KMIP Cluster Considerations

The Master node of a Cryptographic Security Platform Vault cluster must be available to access or create KMIP keys to encrypt or rekey your data. You can determine which node of your cluster is the Master node by logging into the Cryptographic Security Platform Vault Management webGUI, clicking Switch to Appliance Management, and then selecting Cluster > Servers. A yellow star appears before the server name of the node designated as the KMIP database master node. The master is the first node in the cluster list. The other nodes in the cluster are replica nodes.

All KMIP requests are forwarded to the master node for processing. When the master node's database is updated, all replica nodes receive the updates synchronously. When the master node is down, it may take approximately 1 minute before the other nodes start servicing READ requests.

If your Master node is going to be unavailable for a long time, for example, if there is a network outage, you can log into any other node of the cluster and remove the Master node. When you remove the former Master node, the second node in the cluster list will become the Master. Because the new Master node will update or create KMIP keys, which are replicated only to nodes participating in the cluster, we highly recommend that you immediately shut down the removed node VM to prevent communication with external applications. Once the crisis is averted, you can rejoin the former Master to the cluster, but it will no longer be the Master node.

If you have a strong reason to return the former-Master node to be the Master node after it has been rejoined, you would need to log in to the former Master and, one at a time, remove all nodes from the cluster. At that point, the former Master node will become the new Master node. You can then rejoin the removed nodes to the cluster.

Configuring a new KMIP Server

Any KMIP client can connect to the Cryptographic Security Platform Vault KMIP server and perform all standard KMIP operations with the following restrictions:

- The Cryptographic Security Platform Vault KMIP server supports KMIP versions 1.0, 1.1, 1.2, 1.3, 1.4, 2.0, 2.1, and 3.0. The KMIP server protocol version is configured automatically and set between 1.0 to 3.0, as requested by the client.
- The object count (for example, keys) is limited to 1 million KMIP objects per KeyControl Vault cluster. This limit includes all of the Cryptographic Security Platform Vault for KMIP instances in that cluster. If you

exceed this limit, the KMIP server will still create and maintain the objects, but the Cryptographic Security Platform Vault for KMIP webGUI may not display those objects correctly.

⚠ Cryptographic Security Platform Vault includes a component for creating a Root Certificate Authority (CA) that can generate digital certificates. When you install the first Cryptographic Security Platform Vault node, it creates a Public CA and stores it in the Cryptographic Security Platform Vault object store.

By default, the KMIP server uses a default certificate signed by the CA inside Cryptographic Security Platform Vault. You can change this by installing a custom SSL certificate for the KMIP server. To generate a custom SSL certificate, you can use a CSR created from Cryptographic Security Platform Vault for the KMIP server, or you can use your own CSR. If you use your own CSR, you must upload a private key for that custom certificate.

For details about the standard KMIP operations and configuration settings, see

- https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip
- https://en.wikipedia.org/wiki/Key_Management_Interoperability_Protocol

Other considerations:

- When a KMIP client connects to the Cryptographic Security Platform Vault for KMIP server, the client must use the certificates associated with a KMIP server user account. The KMIP server does not support username/password login credentials. For details about downloading a user account certificate bundle, see Creating a KMIP Client Certificate.
- If you are configuring a KMIP server for VMware vSphere encryption or VSAN encryption, see the *Entrust KeyControl with VMware VSAN and vSphere VM Encryption* guide.
- If you are using a KMIP server with KEK enabled, please ensure that the KEK cache timeout is enabled. Set the value to anything other than 0.

To configure a new KMIP Server

1. Log in to the Cryptographic Security Platform Vault Management webGUI.
2. Select the Settings icon at the top right of the vault page.
3. On the KMIP Vault Settings page, complete the following.
    - State
    - Port
    - Verify
    - Log Level
    - TLS
    - Timeout
    - KMIP Locate Operation: Maximum Items Default
    - SSL/TSL Ciphers
    - Certificate Types
4. Click **Apply** and confirm your changes when prompted.

State

The KMIP server status. Enable for clients to connect to the server.

Port

The server port number. Defaults to 5696.

Verify

Yes to verify the KMIP client identity before the server handles its request; No otherwise.

Log Level

The lowest level of log messages saved in the audit log.

Level	Logged events
All	All requests to the KMIP server and responses from the KMIP server.
Create-Modify	Object creation, object modification requests, and object deletion requests and responses. This is the default level.
Create-Get	Object creation messages, object fetch requests, and object fetch responses.
Creat	Object creation request and response messages.
Get	Object fetch and object locate requests and responses.
Off	None

TLS

The supported TLS version. For example, select TLS 1.3 for all clients to connect to the KMIP server using TLS 1.3. Defaults to supporting both TLS 1.2 and TLS 1.3.

> This setting applies to the KMIP server only and affects the entire cluster.

Timeout

The number of minutes after which a client request will time out. You can:

- Select **Yes** and enter 1 to 60 minutes.
- Select **NO** (default value) for client requests never to time out.

KMIP Locate Operation: Maximum Items Default

The maximum number of items to be returned from the KMIP server `Locate` operation.

> The KMIP client allows you to set an offset items value (the record number the return starts with) and a maximum items value (how many items are returned) when you run the KMIP locate operation.

The maximum number of items depends on both the choice that you set in the webGUI and the value that you set in the KMIP Client. For example:

- If you choose the default value in the webGUI, and you DO set a max value in the KMIP Client, it returns up to 1000 UUIDs.
- If you choose the default value in the webGUI, and you do NOT set a max value in the KMIP Client, it returns up to 100 UUIDs.
- If you choose the maximum items value from the KMIP Client in the webGUI and DO set a max value, it returns the maximum number of UUIDs set in the KMIP Client.
- If you choose the maximum items value from the KMIP Client in the webGUI and do NOT set a max value, it returns all UUIDs found in the locate operation.

For more information on the KMIP `Locate` command, see https://docs.oasis-open.org/kmip/kmip-spec/.

SSL/TSL Ciphers

Enter the SSL ciphers in a comma-separated list that you want the KMIP server to use.

> The following ciphers are not supported: DHE-DSS-AES128-256 and DHE-DSS-AES128-SHA256.

Certificate Types

The certificate type. Select:

- **Default** for the KMIP server to use a default certificate.
- **Custom** to use a custom SSL certificate generated from Cryptographic Security Platform Vault or from your own CSR. You will need to provide the following:
  - **SSL Certificate**: Upload the SSL certificate file in Base64-encoded PEM format. It must function as a server certificate.
  - **CA Certificate**: Upload the certificate for the CA that signed the custom SSL certificate in Base64-encoded PEM format. If you want to use the CA certificate to verify the KMIP client certificate, select **Yes** and upload a KMIP client certificate for every Cryptographic Security Platform Vault for KMIP.
  - **Private Key**: Optionally upload the private key file in Base64-encoded PEM format. This is required if you used your own CSR and not the CSR generated on the KMIP page.
  - **Password**: Optionally enter the password for the custom certificate.

Post Quantum Support in the CSP Vault for KMIP

Beginning in version 10.5.3, we now offer the following KMIP Post Quantum (PQ) features:

- PQ object creation—You can create the following KMIP objects that are considered PQ-safe.
  - ML-KEM
  - ML-DSA
  - SLH-DSA
- PQ operations—The following KMIP operations are considered PQ-safe:
  - Encapsulation (ML-KEM)
  - DecapSulation (ML-KEM)
  - Sign (ML-DSA, SLH-DSA)
  - Verify (ML-DSA, SLH-DSA)

  Note: When the KMIP client supports OpenSSL 3.5.4, the channel between the KMIP client and the KMIP server uses PQ-TLS to protect data against harvest now, decrypt later.

KMIP Vault Overview

You manage your KMIP configuration in the Cryptographic Security Platform Vault.

KMIP (Key Management Interoperability Protocol) enables the secure creation and storage of keys and other security objects on a key management server. Cryptographic Security Platform Vault includes a fully functional KMIP server that you can use to serve requests from external KMIP clients. The KMIP server is required if you want to use Cryptographic Security Platform Vault with servers encrypted by vSphere.

You can use KMIP with multiple vaults. This allows security administrators to isolate different KMIP environments for security and compliance.

- Each KMIP vault has its own KMIP objects, client certificates, access policies, audit logs, Local User Accounts, Active Directory settings, and HSM root key label for KEK wrapping.
- Each KMIP vault has access to its own Cryptographic Security Platform Vault for KMIP webGUI. Cryptographic Security Platform Vault-managed user accounts and Cryptographic Security Platform Vault Security Administrators do not have access to the Cryptographic Security Platform Vault for KMIP webGUI.
- The KMIP vault supports Local User Authentication and Managed Authentication. If you create the vault with Local User Authentication, the Cryptographic Security Platform Vault stores all user usernames and passwords, and you can manage users in the Cryptographic Security Platform Vault for KMIP webGUI. With Managed Authentication, you can use an external authentication service such as Active Directory, OpenLDAP, or OIDC.

  Note: The Cryptographic Security Platform Vault for KMIP webGUI has an automatic timeout value of 15 minutes.

Managing Authentication for Vault for KMIP

By default each vault is configured for local authentication. You can change the authentication method as required. In the current release, you can choose between local authentication, Active Directory, OpenID Connect (OIDC) with AD, or OIDC without AD.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users.

For details on configuring each authentication option, see:

- Configuring local authentication for Vault for KMIP
- Configuring Active Directory for the Vault for KMIP
- Configuring OIDC with Active Directory for Vault for KMIP
- Configuring OIDC for Vault for KMIP
- Managing two-factor authentication in Vault for KMIP

Configuring local authentication for Vault for KMIP

Local authentication is enabled by default when you create a vault. If using local authentication, no further authentication configuration is required. The next step is to configure your access policies and users.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users

Configuring Active Directory for the Vault for KMIP

See below for configuring Active Directory for the Vault for KMIP.

> By default, the vault uses local authentication. You can change the authentication method as required.

To configure Active Directory

1. Log in to the CSP Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. On the Authentication page, select **LDAP** as the Authentication Type.
5. On the **Domain** tab, enter:
    - Domain Name—Enter the domain name for the service account.
    - Directory Service Type—Select **Microsoft AD** if you plan to use Microsoft AD directory services, or **OpenLDAP** for all non-Microsoft AD directory services.
    - Service Account Name—Enter the name of the service account for the given domain (for example, Administrator).

      > The service account needs read-only access to users and groups on the domain and any subdomain used.

    - Service Account Password —Enter the password for the service account.
    - UID Attribute—Enter the Security Manager Account Name (sAMAccountName) for the user.

      > This is the attribute of the user or group object that would be queried during search.

6. Click **Apply** to save the changes.
7. Click the **Domain Controllers** tab.
8. Click **+**
9. Add the following details in the **Add Domain Controller** window.
    - Server URL
    - STARTTLS
    - CA Certificate
    - User Search Context (Base DN)
    - Group Search Context (Base DN)
    - Timeout
10. Click **Save and Close**.

Server URL

Select LDAP or LDAPS and enter the domain name or IP address. To include a port number, use the following syntax:

```
<ip>:<port>
```

STARTTLS

If you selected LDAP, check the checkbox if you want to use LDAP over TLS.

CA Certificate

The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller.

- The CA certificate must be in Base64-encoded PEM format.
- If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates.

Click Load File to select the CA certificate that you want to use.

User Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the user search should start. For performance reasons, make the base DN as specific as possible. For example:

```
dc=ldapserver,dc=com
```

This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP.

Group Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the search for Security groups should start.

This option applies to AD Security groups being associated with an admin group.

Timeout

Set the timeout in seconds before connecting to an alternate domain controller.

- If multiple domain controllers are specified, this is how long the Cryptographic Security Platform Vault waits for a response before re-sending the request to another domain controller.
- If the DNS server is down, Cryptographic Security Platform Vault may take longer than the time specified here before it fails over to the next domain controller in the list or considers the authentication request failed.

This option only applies to the TCP/LDAP request. It does not apply to the DNS request before the LDAP server has been successfully contacted.

Configuring OIDC with Active Directory for Vault for KMIP

By default, the vault uses local authentication. You can change the authentication method as required, and you can have multiple authentication modes active at the same time. However, OIDC without Active Directory cannot be used with Active Directory, and OIDC with Active Directory cannot be used without Active Directory.

You cannot disable OIDC authentication once it is configured. After you enable OIDC, you can no longer sign in with AD credentials. However, you can sign in using local authentication credentials without any issues.

To configure OIDC

1. Log in to the Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. In the **Choose Authentication Type** drop-down menu, select:
   - **OpenID Connect** to configure OIDC without Active Directory
   - **OpenID Connect (with AD)** to configure OIDC with Active Directory
5. Click the **Learn more about configuring the OIDC Provider** link to view the OIDC provider's login redirect URL and logout redirect URL.
6. Specify the OpenID Connect Configuration settings:
   - Name
   - Client ID
   - Client Secret
   - Base URL
7. Optionally, click **Load File** to upload the CA certificate in base64-encoded PEM format.
8. Click **Apply**.
9. Select **Verify and Enable**. After verification, a message appears confirming OpenID Connect has been successfully enabled. Vault is set for OIDC authentication.
10. Sign out from the vault and sign in to the vault as an OIDC user by selecting **Sign in with IDAAS** and entering your OIDC credentials.

Name

A user-defined name for the OpenID Connect provider.

> Cryptographic Security Platform Vault displays this name on the button in the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

> This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Configuring OIDC for Vault for KMIP

By default, the KeyControl Vault Management application is configured for local authentication. You can change the authentication method as required, but you can use only one type of authentication per vault at a time.

- If you want to use OIDC without AD, you can only change to that mode from the local authentication mode.
- If you have configured AD or OIDC with AD, you cannot change to OIDC without AD.

Each vault can be configured with a separate OIDC server or a separate application from same server.

⚠ OIDC without AD is the recommended mode of OIDC authentication method where the OIDC provider independently manages identity and authentication. For new OIDC setups, this is the preferred option.

To configure OIDC

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Choose Authentication Type** drop-down list, select **OpenID Connect**.
6. Specify the OpenID Connect Configuration settings:
   - Name
   - Client ID
   - Client Secret
   - Base URL
7. Optional. Click **Browse** to upload the CA Certificate.

   ℹ The certificate needs to be in base64 encoded pem format.
8. Enter the Admin Name and Admin Email for OIDC user. This user will be created and will act as the Vault Administrator. They will be assigned to the admin policy and receive the email with the registration URL.
9. Click **Apply**. The OpenID Connect Configuration window appears showing the current configuration.
10. Click **Verify and Enable**. The OpenID Connect Successfully Configured window displays the new login URL.
11. Copy the URL, and click **Log Out and Sign in with IDP**.
12. After you are logged out, paste the URL into the browser window.
13. Log in to the Identity Provider using the name and password that you created.

Name

A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

⚠ This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Managing two-factor authentication in Vault for KMIP

Two-factor authentication requires you to enter two forms of identification before you can access your CSP Vault.

- The first form is your standard username and password combination,
- The second is a one-time password (OTP) generated by an authorization app. The OTP is appended to your existing password.

See below for how to enable and manage it.

- Requirements for enabling two-factor authentication in Vault for KMIP
- Enforcing two-factor authentication in Vault for KMIP
- Disabling two-factor authentication in Vault for KMIP

> Two-factor authentication is supported with local authentication only. If you want to use two-factor authentication for non-local users, we recommend enabling it in your remote authentication provider.

Requirements for enabling two-factor authentication in Vault for KMIP

Make sure you have access to an authentication app that can generate HOTP or TOTP passwords. For example:

- For TOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. These applications continuously generate passwords valid for 30 seconds. If the current password expires before you can submit the login request, you must wait for it to generate a new password, then use that to log in.
- For HOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. A password generated through the application is valid from the time you create it until you use it to log in. To log in again, click **Next** in the app to generate a new password.

Enforcing two-factor authentication in Vault for KMIP

See below for enforcing two-factor authentication in Vault for KMIP.

- Enforcing two-factor authentication for the current user
- Enforcing two-factor authentication for all users

Enforcing two-factor authentication for the current user

See below for enforcing two-factor authentication for the current user.

To enforce two-factor authentication for the current user

1. Log in to the Cryptographic Security Platform Vault for KMIP webGUI.
2. In the top menu bar, click **Settings**.
3. In the **Two-Factor Authentication** field, click **Set up Two-Factor Authentication**.
4. In the **Enable Two-Factor** dialog box, select the HOTP or TOTP radio button.
5. Scan the generated barcode with your authorization app.
6. Enter the six-digit verification code from your app in the dialog box.
7. Click **Continue**. Cryptographic Security Platform Vault verifies the code and displays a message indicating success or failure. If the code is not correct, re-enter it.
8. After the code has been accepted, click **Done**.
9. When you log into the Vault web GUI:
    - Enter a valid OTP along with your standard account password on the login page. Do not add any characters or spaces between your account password and the one-time password generated by your

authorization app. For example, if your password is `XyZ123` $, and your OTP is `32325` , you enter `XyZ123$32325` in the password field.

- If you use TOTP, make sure your password doesn't expire before you submit the login request.

Enforcing two-factor authentication for all users

See below for enforcing two-factor authentication for all Vault users

To enforce two-factor authentication for all users

1. Log into the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the **Two-Factor Authentication Settings** page, select **ENFORCED**.
5. Click **Apply**.

Disabling two-factor authentication in Vault for KMIP

See below for disabling two-factor authentication in Vault for KMIP.

- Disabling two-factor authentication for a user
- Disabling two-factor authentication for all users

Disabling two-factor authentication for a user

See below to disable two-factor authentication for a single Vault user.

To disable two-factor authentication

1. Log in to the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Security**.
3. Select the **Users** tab
4. Select the user for whom you want to disable two-factor authentication.
5. In the **Details** tab below the table, click the **Enabled** link for the **Two-Factor Authentication** row.
6. In the **Disable Two-Factor Authentication** window, click **Proceed**.

Disabling two-factor authentication for all users

See below to disable two-factor authentication for all Vault users.

To disable two-factor authentication for all users

1. Log into the Cryptographic Security Platform Vault for KMIP webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the Two-Factor Authentication Settings page, select **NOT ENFORCED**.
5. Click **Apply**.

CSP Vault for PKCS#11

CSP Vault for PKCS#11 provides a PKCS#11 interface for applications that use keys and cryptographic operations managed by a CSP Vault and backed by an nShield HSM. The client communicates securely with the Vault server using mutual TLS (mTLS).

- PKCS#11 is a public standard that defines an API for interacting with hardware security modules (HSMs). CSP Vault for PKCS#11 includes a lightweight client that communicates with the nShield HSMs used by the CSP

Vault cluster. The PKCS#11 client implements https://docs.oasis-open.org/pkcs11/pkcs11-spec/v3.2/pkcs11-spec-v3.2.html
- CSP Vault includes a PKCS#11 server that listens for secure client connections. Client libraries are available for Linux and Windows on x86-64 platforms. The client establishes a mutually authenticated TLS (mTLS) connection to the PKCS#11 server and must use a client certificate issued by CSP Vault.
- The client serializes PKCS#11 function calls and their parameters and sends them to the PKCS#11 server running in the CSP Vault cluster. The server passes the requests to the nShield `libcknfast.so` library, which communicates with the HSMs and returns the results to the client. See https://nshielddocs.entrust.com/security-world-docs/api-pkcs11/intro.html for details.
- Release 10.6.1 supports module protection and softcard protection. Data used by CSP Vault for PKCS#11 is isolated from data used by other CSP Vault service.

See below for the configuration steps.

- Setting up the PKCS#11 Vault
- Using the client
- Capabilities
- Logging
- Managing Authentication for Vault for PKCS#11

Setting up the PKCS#11 Vault

This section explains how to set up the PKCS#11 Vault.

- Requirements to set up the PKCS#11 vault
- Creating a PKCS#11 Vault
- Logging in to the PKCS#11 Vault
- Configuring a port
- Adding a Softcard
- Configuring service log level
- Generating a private key and a CSR
- Creating a PKCS#11 client certificate
- Configuring the PKCS#11 Vault client

Requirements to set up the PKCS#11 vault

Before you begin, make sure you have configured and enabled an Entrust nShield Hardware Security Module (HSM) for the Cryptographic Security Platform (CSP) Vault cluster. For more information, see: Hardware Security Modules with CSP Vault.

Creating a PKCS#11 Vault

Creating a PKCS#11 vault enables secure storage and management of cryptographic objects through the PKCS#11 interface.

To create a PKCS#11 Vault

1. Log in to the Cryptographic Security Platform Vault.
2. On the **Vaults** page, click **+ Create Vault**. The **Create Vault** form appears.
3. Complete the following fields:
    a. From the **Type** dropdown list, select **PKCS11**.
    b. In the **Name** field, enter a name for the vault.
    c. In the **Admin Name** field, enter the admin name.
    d. In the **Admin Email** field, enter the admin email.

4. Click **Create Vault**. A **Vault Successfully Created** notification with the Vault URL, username, and temporary password appears.

   > Remember the Vault URL, username, and temporary password. You will need this information to complete Logging in to the PKCS#11 Vault.

5. Click **Close**.

Logging in to the PKCS#11 Vault

Logging in to the PKCS#11 vault lets you manage vault settings, certificates, softcards, and cryptographic objects. When you log in to the PKCS#11 vault for the first time, you must set a new password.

To log in to the PKCS#11 Vault

1. Click the Vault URL in the **To Create a PKCS#11 Vault** field.
2. Complete the following fields in the **Expired Password** window.
   a. **New Password:** Enter a desired password.
   b. **Re-enter New Password:** Re-enter the password.
3. Click **Change**. The **Cryptographic Security Platform Vault for PCKS #11** login screen appears.
4. Enter your **User Name** and **Password**.
5. Click **Login**.

Configuring a port

Configuring a port enables PKCS#11 clients to connect to the vault.

To configure a port

1. Log in to the Cryptographic Security Platform Vault for PKCS#11 webGUI.
2. From the left menu, select **HSM**. The **HSM** page appears.
3. In the **Port** section, click the pencil icon. The **Edit Port** page appears.
4. In the **Port** field, enter a port number based on your requirements.
5. Click **Save**.

Adding a Softcard

Adding a softcard enables PKCS#11 clients to log in to a PKCS#11 slot and access cryptographic objects in the Vault.

To add a Softcard

1. Log in to the Cryptographic Security Platform Vault web GUI.
2. From the left menu, select **HSM**.
3. Click **+ Add Softcard o**n the **HSM** page.
4. Complete the following fields on the **Add Softcard** page.
   a. **Label**: Enter a label for the softcard.
   b. **Password**: Enter a password for the softcard.
   c. **Re-Enter Password**: Re-enter the password.
5. Click **Save**. The softcard you created appears under the **SOFTCARDS** section on the **HSM** page.

Configuring service log level

Configuring the log level enables collection of diagnostic information for monitoring and troubleshooting.

The `DEBUG` log level and `debug_level 7` or higher includes sensitive information in log files.

To configure the log level

1. Log in to the Cryptographic Security Platform Vault for PKCS#11 webGUI.
2. From the left menu, select **Settings**. The **Settings** page appears.
3. From the right menu, select **Debug Log Levels**. The **Debug Log Levels** page appears.
4. From the **Debug Level** dropdown list, select the level based on your requirements.
5. From the **Log Level** dropdown list, select the level based on your requirements.
6. Click **Apply**.

Generating a private key and a CSR

Generating a private key and certificate signing request (CSR) lets you create a client certificate for secure communication with the vault.

The following example uses OpenSSL commands to generate an RSA private key and CSR:

```
openssl genrsa -out client_key.pem 4096

openssl req -out client.csr -new -key client_key.pem
```

Creating a PKCS#11 client certificate

Creating a PKCS#11 client certificate enables a PKCS#11 client to authenticate and establish a secure connection to the vault.

To create a PKCS#11 client certificate

1. Log in to the Vault web GUI.
2. From the left menu, select **Security**.
3. Click **+ Create Certificate** on the **Security** page.
4. Complete the following fields on the **Create Client Certificate** page.
   - **Name**: Enter a name for the certificate.
   - **Create For**: Specify the owner of the certificate.
   - **Expiration**: Select an expiration date based on your requirements.

     The expiration date must be within three years.

   - **Certificate Signing Request (CSR)**: Click **Browse** to select the CSR you generated in Generating a Private Key and a CSR.
5. Click **Create**. The client certificate you just created appears under the Client Certificates table on the **Security** page.
6. In the row of the created certificate, click **More Actions** (vertical ellipsis icon) on the right.
7. Select **Download to download a** bundle that contains
   - A PEM user certificate and key file
   - A PEM CA certificate
8. Extract the bundle contents file.
9. Save the user certificate and key files and the CA certificate to the same folder as the key and the CSR you generated in Generating a Private Key and a CSR.

> You will need the user certificate and key files and the CA certificate to complete Configuring the PKCS#11 Vault client.

Configuring the PKCS#11 Vault client

This page explains how to configure and verify the Entrust CSP PKCS#11 Vault client.

- Prerequisites
- Creating a client configuration file
- Setting a custom configuration path
- Using the client library
- Verifying the configuration
- Troubleshooting
- Security requirements

> A Vault administrator must complete Vault creation, Vault service configuration, softcard management, and client-certificate issuance. Ask the Vault administrator for the connection details and certificate files required on this page.

Prerequisites

Before configuring the client, make sure you have completed the following tasks:

- Obtain the following information from the Vault administrator:
  - Vault service hostname or IP address
  - Vault service port
  - CA certificate in PEM format
  - Client certificate in PEM format
  - Any required PKCS#11 login or token credentials
- Ensure the private key corresponding to the CSR provided to the Vault administrator is available in PEM format.
- Install the CSP PKCS#11 Vault client using the Windows installer or the Linux tarball supplied with the product. The installation includes the PKCS#11 library, header files, and a configuration-file template.

Creating a client configuration file

The library reads its configuration from the following location:

Linux

```
/etc/cspp11/config.txt
```

Windows

```
<PROGRAMDATA>\\Entrust\\cspp11\\config.txt
```

This can be overridden by setting the `CSPP11CONFIG_PATH` environment variable to the full path to the configuration file.

1. Copy the configuration template to the default location, or choose a different location for the file.
2. Set `CSPP11_CONFIG_PATH` to the custom file path when using a non-default location.
3. Uncomment the required settings in the configuration file.
4. Replace the example values with the values the Vault administrator supplies.
5. Verify that the client certificate, private key, and CA certificate are readable by the application account.
6. Protect the private-key file using the operating-system permissions appropriate for your environment.

The settings are:

Setting	Description	Mandatory
port	Port used by the Vault service	✅
server_ip	Hostname or IP address of the CSP Vault node	✅
ca_cert_path	Path to the PEM-encoded CA certificate provided by the Vault	✅
client_cert_path	Path to the PEM-encoded client certificate provided by the Vault	✅
client_key_path	Path to the PEM-encoded private key corresponding to the client certificate	✅
log_file_path	Path to the client log file. If omitted, the client uses the platform-specific default	❌
log_level	The logging level: • DEBUG (includes sensitive information in log files) • INFO • WARN (default) • ERROR • FATAL	❌

See below for a configuration example:

```
# Entrust CSP PKCS#11 Vault client configuration

port=10000
server_ip=vault.example.com
ca_cert_path=/path/to/vault_cacert.pem
client_cert_path=/path/to/vault_client_cert.pem
client_key_path=/path/to/vault_client_key.pem

# Optional settings
# log_file_path=/path/to/client.log
```

```
# log_level=INFO
```

Use Windows paths when configuring the client on Windows. For example:

```
ca_cert_path=C:\ProgramData\Entrust\cspp11\vault_cacert.pem
client_cert_path=C:\ProgramData\Entrust\cspp11\vault_client_cert.pem
client_key_path=C:\ProgramData\Entrust\cspp11\vault_client_key.pem
```

Setting a custom configuration path

Set the variable before starting the PKCS#11 application. To make the setting persistent, configure it using the operating system's environment-variable settings.

Linux

```
export CSPP11_CONFIG_PATH=/opt/entrust/cspp11/config.txt
```

Using the client library

Configure the application to load the CSP PKCS#11 library installed with the client. The library filename and installation path depend on the operating system and installation package.

Applications using the PKCS#11 standard can then initialize the library, enumerate available slots, open a session, and authenticate using the credentials provided by the Vault administrator. Application-specific configuration and login procedures are outside the scope of this guide.

If you are using a test or diagnostic program that supports dynamic library loading, provide the path to the CSP PKCS#11 library with that program's library option. For example:

```
ckinfo-dynamic --library /opt/entrust/cspp11/lib/libcspp11.so
```

Verifying the configuration

After configuring the client:

1. Confirm that the Vault hostname or IP address and port are reachable from the client host.
2. Confirm that all certificate and key paths are correct.
3. Confirm that the private key corresponds to the client certificate.
4. Start a PKCS#11 application or diagnostic tool.
5. Verify that the application can initialize the library and enumerate the expected slot or token.
6. Review the client log if the connection or initialization fails.

Troubleshooting

Issue	Solution
The configuration file is not found	Verify that the file exists at the default path or that `CSPP11_CONFIG_PATH` points to the correct file. Check the environment variable's spelling and capitalization.
The client cannot connect to the Vault	Verify the server hostname or IP address, port, firewall rules, and network route. Review the client log for additional details.
Certificate or key errors occur	Verify that the files are PEM-encoded, readable by the application account, and specified with the correct paths. Ask the Vault administrator to confirm the client certificate is valid and that the configured private key matches that certificate.
No slot or token is displayed	Verify that the PKCS#11 library loaded successfully and that the Vault service is available. If authentication is required, verify that the application is using the credentials or token PIN supplied by the Vault administrator.

Security requirements

- Do not share the client private key or token credentials.
- Do not place private keys or credentials in source code or command history.
- Restrict access to the configuration file and certificate files according to your organization's security policy.
- Use `DEBUG` logging only for troubleshooting and return to `WARN` or the approved production level afterward.
- Contact the Vault administrator when certificates expire, are revoked, or need replacement.

Using the client

This page is intended for users, such as system administrators, who need to verify or integrate a client with CSP Vault for PKCS#11.

- Client libraries
- Operational restrictions
- Verify the client connection
- Troubleshoot connection problems

Client libraries

The CSP PKCS#11 Vault client package includes a dynamically loadable PKCS#11 library for each supported platform:

Platform	Library
Windows x86-64	`cspp11.dll`

Platform	Library
Linux x86-64	`libcspp11.so`

The package also contains the header files required to build your own C program using the library.

The application must be able to locate the library installed by the client package. Applications may load the library using its full path or the library name if the installation location is included in the system library search path.

- On Windows, ensure that the directory containing `cspp11.dll` is available to the application through its library search path.
- On Linux, provide the full path to `libcspp11.so` or add its directory to the system library search path as required by the application.

The client library reads the CSP Vault connection settings from its configuration file. For configuration instructions, see: Configuring the PKCS#11 Vault client.

Operational restrictions

Applications using the client must use serial sessions. Notification callbacks and asynchronous sessions are not supported. For the complete list of supported functions, see: Capabilities.

Verify the client connection

Use a PKCS#11 diagnostic tool that can dynamically load the PKCS#11 library by its path name to verify the connection. For example:

Linux

```
<diagnostic-tool> --library /path/to/libcspp11.so
```

Windows Powershell

```
<diagnostic-tool>.exe --library 'C:\Path\To\cspp11.dll'
```

Use the diagnostic tool's help option to confirm the exact command-line syntax. A successful diagnostic should initialize the library and display information about the available slots, tokens, or mechanisms.

Troubleshoot connection problems

If the diagnostic tool cannot initialize the library or does not display the expected slot or token:

- Confirm the application loads the correct library for the operating system and architecture.
- Confirm that the client configuration file exists at the expected path or that `CSPP11_CONFIG_PATH` it points to the correct file.

- Confirm the Vault address, port, CA certificate, client certificate, and private-key paths in the configuration file.
- Confirm that the application account can read the certificate and private-key files.
- Confirm network connectivity and firewall access to the Vault service.
- Confirm that the client certificate is valid and that its private key matches the certificate.
- Review the client log for additional information.

Errors that occur before the client reads its configuration are written to standard error. For log locations, logging levels, and server logs, see: Logging.

Capabilities

This page provides information on the PKCS#11 capabilities and restrictions that vault client users and developers need to consider when validating a CSP PKCS#11 Vault deployment.

- General restrictions
- Supported functions
- Mechanisms

General restrictions

By default, the server runs with Security Assurance Overrides set to None. With Release 10.6.1, you can only change the Security Assurance Overrides setting using the following REST API endpoint and not via the Cryptographic Security Platform Vault Management GUI.

```
/pkcs11/1.0/server/
```

Below is a list of general restrictions.

- The client supports PKCS#11 3.2 functions with the restrictions described on this page.
- Notification callbacks and asynchronous sessions are not supported.
- Multipart encryption, decryption, signing, and verification operations are not supported.
- All functions are forwarded to the nShield PKCS#11 Library, and all restrictions of that library apply.
- Vendor-defined mechanisms are not supported by the CSP PKCS#11 client.
- The client may filter mechanisms when it cannot serialize their parameters.
- The mechanisms available in a deployment can differ from the mechanisms available in another HSM or firmware environment.

For information on the PKCS#11 3.2 specification, see:

https://docs.oasis-open.org/pkcs11/pkcs11-spec/v3.2/pkcs11-spec-v3.2.html

Supported functions

The following PKCS#11 3.2 functions are supported with the restrictions listed below. Functions and options not supported by the nShield library will return its error code.

Function	Restriction
C_DecryptInit	
C_Decrypt	

Function	Restriction
C_EncryptInit	
C_Encrypt	
C_Initialize	Mutex function pointers are ignored
C_Finalize	
C_GetInfo	
C_GetFunctionList	
C_GetInterfaceList	
C_GetInterface	
C_GenerateKey	
C_GenerateKeyPair	
C_WrapKey	
C_UnwrapKey	
C_DeriveKey	
C_EncapsulateKey	
C_DecapsulateKey	
C_DigestInit	
C_Digest	
C_DigestUpdate	
C_DigestFinal	

Function	Restriction
C_CreateObject	
C_CopyObject	
C_DestroyObject	
C_GetObjectSize	
C_GetAttributeValue	
C_SetAttributeValue	
C_FindObjectsInit	
C_FindObjects	
C_FindObjectsFinal	
C_GenerateRandom	
C_OpenSession	Notification callbacks and CKF_ASYNC_SESSION are not supported; CKF_SERIAL_SESSION is required.
C_CloseSession	
C_CloseAllSessions	
C_GetSessionInfo	
C_Login	
C_Logout	
C_LoginUser	
C_SignInit	
C_Sign	

Function	Restriction
C_GetSlotList	
C_GetSlotInfo	
C_GetTokenInfo	
C_GetMechanismList	
C_GetMechanismInfo	
C_VerifyInit	
C_Verify	

Mechanisms

The available mechanisms depend on the connected nShield HSM and its firmware. The CSP PKCS#11 client also filters mechanisms that it cannot serialize safely. Do not use a mechanism solely because it is defined by the PKCS#11 standard or appears on another HSM.

- Use the PKCS#11 slot and mechanism information functions to confirm availability in the deployed environment. The nShield PKCS#11 mechanism restrictions documented by Entrust also apply.
- For an application-specific compatibility assessment, check the mechanisms returned by `C_GetMechanismList` and that the required functions are in the list above.

Logging

See below for details on logging.

- Client logs
- Server logs

Client logs

These are written to a log file specified in the client configuration or to the following default files.

Default Linux log file
`/var/log/entrust/cspp11/client.log`

Default Windows log file
`<PROGRAMDATA>\Entrust\cspp11\logs\client.log`

The client logging level is set with the log_level setting in the client configuration.

> The `DEBUG` log level includes sensitive information in log files. Use this level only for troubleshooting, then reduce the log level and purge the logs when troubleshooting is complete.

Server logs

Logging on the server is controlled by the following settings in the `pkcs11/1.0/server` API.

- The `log_level` setting controls logging from the server code and writes log messages to:

  ```
  /var/log/hcs/p11server.log
  ```

- The `debug_level` setting controls logging from the nCipher `libcknfast.so` library and writes log messages to:

  ```
  /var/log/hcs/p11server_debug.log
  ```

Changing either setting restarts the PKCS#11 server and drops any active client connections.

> `log_level DEBU G` or `debug_level 7` or higher also logs sensitive values.

Both log files are included in a support bundle.

Managing Authentication for Vault for PKCS#11

By default each vault is configured for local authentication. You can change the authentication method as required. In the current release, you can choose between local authentication, Active Directory, OpenID Connect (OIDC) with AD, or OIDC without AD.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users.

For details on configuring each authentication option, see:

- Configuring local authentication for Vault for PKCS#11
- Configuring Active Directory for the Vault for PKCS#11
- Configuring OIDC with Active Directory for Vault for PKCS#11
- Configuring OIDC for Vault for PKCS#11
- Managing two-factor authentication in Vault for PKCS#11

Configuring local authentication for Vault for PKCS#11

Local authentication is enabled by default when you create a vault. If using local authentication, no further authentication configuration is required. The next step is to configure your access policies and users.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users

Configuring Active Directory for the Vault for PKCS#11

See below for configuring Active Directory for the Vault for PKCS#11.

> By default, the vault uses local authentication. You can change the authentication method as required.

To configure Active Directory

1. Log in to the CSP Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. On the Authentication page, select **LDAP** as the Authentication Type.
5. On the **Domain** tab, enter:
   - Domain Name—Enter the domain name for the service account.
   - Directory Service Type—Select **Microsoft AD** if you plan to use Microsoft AD directory services, or **OpenLDAP** for all non-Microsoft AD directory services.
   - Service Account Name—Enter the name of the service account for the given domain (for example, Administrator).

     > The service account needs read-only access to users and groups on the domain and any subdomain used.

   - Service Account Password —Enter the password for the service account.
   - UID Attribute—Enter the Security Manager Account Name (sAMAccountName) for the user.

     > This is the attribute of the user or group object that would be queried during search.

6. Click **Apply** to save the changes.
7. Click the **Domain Controllers** tab.
8. Click **+**
9. Add the following details in the **Add Domain Controller** window.
   - Server URL
   - STARTTLS
   - CA Certificate
   - User Search Context (Base DN)
   - Group Search Context (Base DN)
   - Timeout
10. Click **Save and Close**.

Server URL

Select LDAP or LDAPS and enter the domain name or IP address. To include a port number, use the following syntax:

```
<ip>:<port>
```

STARTTLS

If you selected LDAP, check the checkbox if you want to use LDAP over TLS.

CA Certificate

The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller.

- The CA certificate must be in Base64-encoded PEM format.
- If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates.

Click Load File to select the CA certificate that you want to use.

User Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the user search should start. For performance reasons, make the base DN as specific as possible. For example:

```
dc=ldapserver,dc=com
```

This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP.

Group Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the search for Security groups should start.

This option applies to AD Security groups being associated with an admin group.

Timeout

Set the timeout in seconds before connecting to an alternate domain controller.

- If multiple domain controllers are specified, this is how long the Cryptographic Security Platform Vault waits for a response before re-sending the request to another domain controller.
- If the DNS server is down, Cryptographic Security Platform Vault may take longer than the time specified here before it fails over to the next domain controller in the list or considers the authentication request failed.

This option only applies to the TCP/LDAP request. It does not apply to the DNS request before the LDAP server has been successfully contacted.

Configuring OIDC with Active Directory for Vault for PKCS#11

By default, the vault uses local authentication. You can change the authentication method as required, and you can have multiple authentication modes active at the same time. However, OIDC without Active Directory cannot be used with Active Directory, and OIDC with Active Directory cannot be used without Active Directory.

> ⚠ You cannot disable OIDC authentication once it is configured. After you enable OIDC, you can no longer sign in with AD credentials. However, you can sign in using local authentication credentials without any issues.

To configure OIDC

1. Log in to the Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. In the **Choose Authentication Type** drop-down menu, select:
   - **OpenID Connect** to configure OIDC without Active Directory
   - **OpenID Connect (with AD)** to configure OIDC with Active Directory
5. Click the **Learn more about configuring the OIDC Provider** link to view the OIDC provider's login redirect URL and logout redirect URL.
6. Specify the OpenID Connect Configuration settings:
   - Name
   - Client ID
   - Client Secret
   - Base URL
7. Optionally, click **Load File** to upload the CA certificate in base64-encoded PEM format.
8. Click **Apply**.
9. Select **Verify and Enable**. After verification, a message appears confirming OpenID Connect has been successfully enabled. Vault is set for OIDC authentication.
10. Sign out from the vault and sign in to the vault as an OIDC user by selecting **Sign in with IDAAS** and entering your OIDC credentials.

Name

A user-defined name for the OpenID Connect provider.

> ℹ Cryptographic Security Platform Vault displays this name on the button in the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

> ⚠ This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Configuring OIDC for Vault for PKCS#11

By default, the KeyControl Vault Management application is configured for local authentication. You can change the authentication method as required, but you can use only one type of authentication per vault at a time.

- If you want to use OIDC without AD, you can only change to that mode from the local authentication mode.
- If you have configured AD or OIDC with AD, you cannot change to OIDC without AD.

Each vault can be configured with a separate OIDC server or a separate application from same server.

> ⚠ OIDC without AD is the recommended mode of OIDC authentication method where the OIDC provider independently manages identity and authentication. For new OIDC setups, this is the preferred option.

To configure OIDC

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Choose Authentication Type** drop-down list, select **OpenID Connect**.
6. Specify the OpenID Connect Configuration settings:
   - Name
   - Client ID
   - Client Secret
   - Base URL
7. Optional. Click **Browse** to upload the CA Certificate.

   > ℹ The certificate needs to be in base64 encoded pem format.

8. Enter the Admin Name and Admin Email for OIDC user. This user will be created and will act as the Vault Administrator. They will be assigned to the admin policy and receive the email with the registration URL.
9. Click **Apply**. The OpenID Connect Configuration window appears showing the current configuration.
10. Click **Verify and Enable**. The OpenID Connect Successfully Configured window displays the new login URL.
11. Copy the URL, and click **Log Out and Sign in with IDP**.
12. After you are logged out, paste the URL into the browser window.
13. Log in to the Identity Provider using the name and password that you created.

Name

A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

> ⚠ This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Managing two-factor authentication in Vault for PKCS#11

Two-factor authentication requires you to enter two forms of identification before you can access your CSP Vault.

- The first form is your standard username and password combination,
- The second is a one-time password (OTP) generated by an authorization app. The OTP is appended to your existing password.

See below for how to enable and manage it.

- Requirements for enabling two-factor authentication in Vault for PKCS#11
- Enforcing two-factor authentication in Vault for PKCS#11
- Disabling two-factor authentication in Vault for PKCS#11

> ℹ Two-factor authentication is supported with local authentication only. If you want to use two-factor authentication for non-local users, we recommend enabling it in your remote authentication provider.

Requirements for enabling two-factor authentication in Vault for PKCS#11

Make sure you have access to an authentication app that can generate HOTP or TOTP passwords. For example:

- For TOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. These applications continuously generate passwords valid for 30 seconds. If the current password expires before you can submit the login request, you must wait for it to generate a new password, then use that to log in.
- For HOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. A password generated through the application is valid from the time you create it until you use it to log in. To log in again, click **Next** in the app to generate a new password.

Enforcing two-factor authentication in Vault for PKCS#11

See below for enforcing two-factor authentication in Vault for PKCS#11.

- Enforcing two-factor authentication for the current user
- Enforcing two-factor authentication for all users

Enforcing two-factor authentication for the current user

See below for enforcing two-factor authentication for the current user.

To enforce two-factor authentication for the current user

1. Log in to the Cryptographic Security Platform Vault for PKCS#11 webGUI.
2. In the top menu bar, click **Settings**.
3. In the **Two-Factor Authentication** field, click **Set up Two-Factor Authentication**.
4. In the **Enable Two-Factor** dialog box, select the HOTP or TOTP radio button.
5. Scan the generated barcode with your authorization app.
6. Enter the six-digit verification code from your app in the dialog box.
7. Click **Continue**. Cryptographic Security Platform Vault verifies the code and displays a message indicating success or failure. If the code is not correct, re-enter it.
8. After the code has been accepted, click **Done**.
9. When you log into the Vault web GUI:
    - Enter a valid OTP along with your standard account password on the login page. Do not add any characters or spaces between your account password and the one-time password generated by your authorization app. For example, if your password is `XyZ123$`, and your OTP is `32325`, you enter `XyZ123$32325` in the password field.
    - If you use TOTP, make sure your password doesn't expire before you submit the login request.

Enforcing two-factor authentication for all users

See below for enforcing two-factor authentication for all Vault users

To enforce two-factor authentication for all users

1. Log into the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the **Two-Factor Authentication Settings** page, select **ENFORCED**.
5. Click **Apply**.

Disabling two-factor authentication in Vault for PKCS#11

See below for disabling two-factor authentication in Vault for PKCS#11.

- Disabling two-factor authentication for a user
- Disabling two-factor authentication for all users

Disabling two-factor authentication for a user

See below to disable two-factor authentication for a single Vault user.

To disable two-factor authentication

1. Log in to the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Security**.
3. Select the **Users** tab
4. Select the user for whom you want to disable two-factor authentication.
5. In the **Details** tab below the table, click the **Enabled** link for the **Two-Factor Authentication** row.
6. In the **Disable Two-Factor Authentication** window, click **Proceed**.

Disabling two-factor authentication for all users

See below to disable two-factor authentication for all Vault users.

To disable two-factor authentication for all users

1. Log into the Cryptographic Security Platform Vault for PKCS#11 webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.

3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the Two-Factor Authentication Settings page, select **NOT ENFORCED**.
5. Click **Apply**.

CSP Vault for Secrets

- CSP Vault for Secrets Overview
- CSP Vault for Secrets CLI
- Viewing CSP Vault for Secrets Audit Logs
- Configuring mTLS for the CSP Vault for Secrets
- Managing Secrets
- Managing Boxes
- Managing Authentication for Vault for Secrets

CSP Vault for Secrets Overview

The Entrust Cryptographic Security Platform Vault for Secrets provides centralized secure storage for managing and controlling access to secrets that are required to access systems and resources. Access to secrets are restricted to authorized applications and users. You can securely store, manage, and access-control secrets such as credentials, API keys, SSH keys, tokens, certificate private keys, and encryption keys. Secrets are managed, controlled and accessed through REST API interfaces or a CLI.

The Cryptographic Security Platform Vault for Secrets is composed of vaults, boxes, secrets, policies, and its own administrators and users. Each vault can hold multiple boxes. You can also enable secondary approval when you create a box, and all secrets in that box will require secondary approval before being checked out.

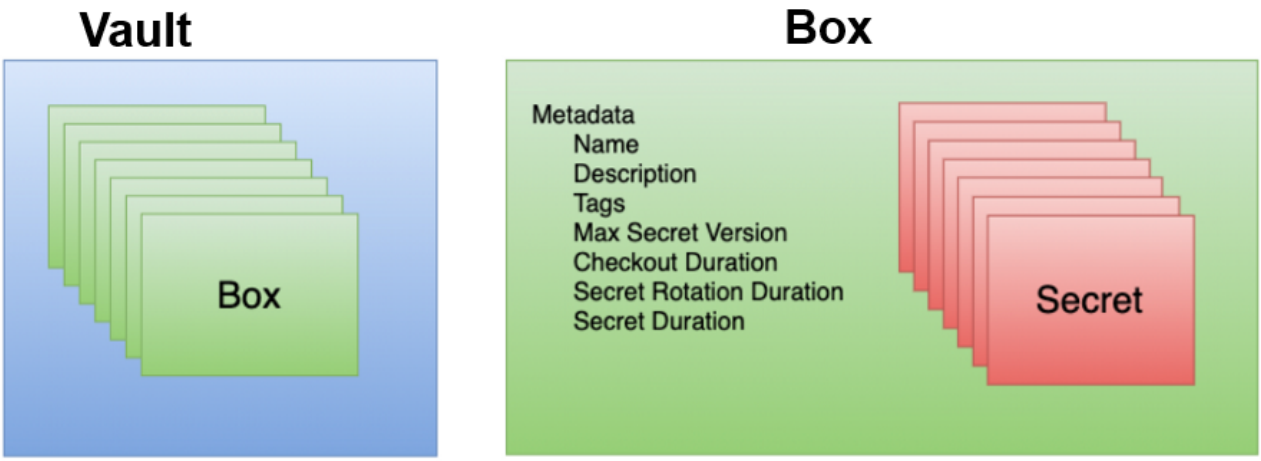
> Note: The Cryptographic Security Platform Vault for Secrets webGUI has an automatic timeout value of 15 minutes.

About Cryptographic Security Platform Vault for Secrets Boxes

Each box contains information (metadata) required to manage the secrets within the box, and a collection of secrets. The metadata can include:

- Name—The name of the box.
- Description—The description of the box.
- Tags—A list of name and value pairs.
- Max Secret Version—The maximum number of secret versions to keep. Changing a secret value creates a new version, and the previous secrets are kept according to the maximum number of versions that you configure.
  This field only takes into account non-staged Secret versions that would be persisted. For example, if Max Secret Versions is set to 5 and a Secret has 7 Secret versions but two are non-staged versions CURRENT and PENDING, 5+2=7 versions are kept.
  If the administrator changes the value of Max Secret Versions and some old versions that have been kept have to be deleted to keep the count consistent with the new Max Secret Versions value, deletion will only happen when a new Secret version is created. For example, the previous Max Secret Versions value was 10 and the administrator reduces it to 5. If a Secret had 10 non-staged versions and 2 staged versions, secret versions are not deleted right away and Cryptographic Security Platform Vault for Secrets webGUI continue to show the 10 non-staged + 2 staged, 12 versions, in total until a new Secret version is created. At that point, the older non-staged versions are deleted and 5 non-staged + 2 staged will be shown, 7 in total.
- Checkout Duration—The default leasing period for secrets. Secrets are leased when a user or an application wants to use the secret to access the resource. The secret must be checked-in before the lease expires.
- Secret Rotation Duration—How often the secrets must be rotated. Applies only to managed secrets.

- Secret Duration—The default expiration period for the secrets.



About Secondary Approval

Secondary approval is now supported in the in the Cryptographic Security Platform Vault for Secrets.

- Secondary approval is enabled at the box level. Once enabled, all secrets in that box must use secondary approval for check out. For more information, see Creating a Box.
- At least one user must have the Vault Secondary Approver Policy access policy before secondary approval can be enabled. Users with the Vault Secondary Approver Policy can review and approve secondary approval requests. For more information, see CSP Vault for Secrets Access Policies.
- You can enable secondary approval when the box is created or at any time when you edit the box settings.
- If any secrets in the box are checked out before secondary approval is enabled, secondary approval will apply after the secret has been checked in and on subsequent checkouts.

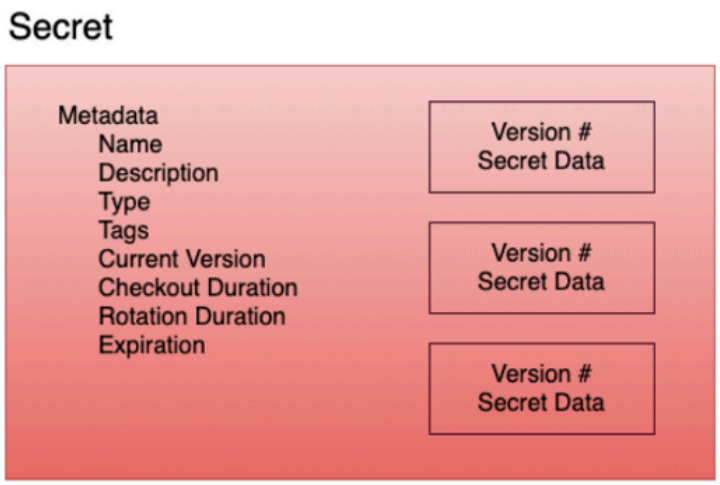
About Secrets

Secrets contain secret data or a secret value, and also metadata information that describes and manages the secret.

The metadata can include:

- Name—The name of the secret. The name can include a virtual folder, for example QueryAccess/CustomDB.
- Description—The description of the secret.
- Type—The following types of secrets are supported:
  - Managed—Managed secrets are automatically rotated by the Cryptographic Security Platform Vault for Secrets. These include:
    - ESXi host
    - SSH key
    - Postgres
    - Microsoft SQL Server
    - AWS Credentials
  - Static—Static secrets do not have automatic secret rotation. These include:
    - Password
    - File

    - Key-Value Pair
    - Text
    - P12
    - Terraform
- Tags—A list of name and value pairs.
- Versioning
    - Multiple versions of a secret are kept to support secret rotation and prevent accidental data loss.
    - The maximum number of versions to keep is configured at the Box level. Changing a secret value creates a new version, and the previous secrets are kept according to the maximum number of versions that you configure.
    - The version number is automatically incremented whenever a secret value is changed.
    - The current version points to the most recent version of the secret value that was created. Authorized users can change the current version to any of the previous available versions of the secret data.
- Checkout Duration—The leasing period for secrets. Secrets are leased when a user or an application wants to use the secret to access the resource. The secret must be checked-in before the lease expires.
- Rotation Duration—How often the secrets must be rotated or changed. Applies only to managed secrets.
- Expiration—The date and time that the secret expires. Secrets cannot be checked out after the expiration.
- Secret Data—The contents of the secret. This can be a text string, key-value pairs (JSON object), or base64-encoded binary data.



Creating CSP Vault for Secrets Local Users

If the vault tenant is configured to use local user authentication, create a user account for each user who needs to log in to the Cryptographic Security Platform Vault for Secrets webGUI.

Tenant user passwords are stored in the Cryptographic Security Platform Vault; user account details are managed in the Cryptographic Security Platform Vault for Secrets webGUI. Users who want to access multiple vault tenants must have a user account in each tenant. Add users to an access control policy before they can access the vault tenant portal.

To read more about access control policies, see CSP Vault for Secrets Access Policies.

1. Log in to the Cryptographic Security Platform Vault for Secrets webGUI.
2. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Security > Users**.
3. Click the blue **+** (Plus sign) to create a new user.

4. Specify the options you want to use:

Field	Description
Status	Check this box to enable the account after creation, allowing the user to log in to the Cryptographic Security Platform Vault for Secrets webGUI.
User Name	The login name for the Cryptographic Security Platform Vault for Secrets managed user account. The login name is case-sensitive. `tenantAdmin`, `Tenantadmin`, and `tenantadmin` are three different accounts. Important: The login name can contain standard alphanumeric characters, hyphens (-), underscores (_), and periods (.). It cannot contain spaces or other special characters.
Full Name	The full name of the user associated with the account.
Email	If your system is configured to send email alerts, they will be sent to this email address.
Password	Password for the user. Password requirements for local users are the same as for Cryptographic Security Platform Vault local users. For more information.
Confirm Password	Confirm the password of the user.
Password Expiration	The maximum number of days that a password can be used before it expires. When the password expires, the user is prompted to change it the next time they log in to the Cryptographic Security Platform Vault for Secrets webGUI.

5. Click **Add**

What to Do Next

Add the user to an existing access control policy or create a new one so the user can access the Cryptographic Security Platform Vault for Secrets webGUI. See CSP Vault for Secrets Access Policies.

CSP Vault for Secrets Access Policies

The Cryptographic Security Platform Vault for Secrets supports Role-based Access Control (RBAC) Policies. Access to secrets is denied by default, and must be explicitly granted through Access Control Policies.

Roles

Roles define actions or operations that can be performed on the Cryptographic Security Platform Vault for Secrets and secrets. The following pre-defined roles are supported:

Vault Admin Role

Vault administrators have full access to all aspects of the Cryptographic Security Platform Vault for Secrets. This access includes:

- Box management—Can create and manage boxes.
- Secret management—Can create and manage secrets within boxes, and checkout secrets.
- Policy management—Can create role-based access control policies to allow users or applications the ability to access secrets.
- View audit logs—Can view audit logs.

Vault User Role

The vault user role is assigned to users and applications who need access to the secrets. They have the following permissions:

- List box IDs—Can retrieve the list of boxes (the box name and ID only) that the user or application has been granted access to.
- List secrets—Can retrieve the list of secrets that the user or application has been granted access to.
- Checkout secrets—Can retrieve the secret value.
- Checkin secrets—Can checkin the secret after use.
- List my checkouts—Can retrieve the outstanding secret leases for the user or application.
- Get secret metadata—Can retrieve secret metadata such as description and tags, for secrets that the user is granted access.

Vault Box Admin Role

Vault box administrators can perform various tasks on boxes they are allowed to administer, including:

- Box management—Update box properties and tag boxes.
- Secret management—Can create and manage secrets, and checkout secrets within boxes they can administer.
  Note: The Vault Box Admin cannot checkout secrets by default. They must be part of the relevant Vault User Policy.
- Leases—View and delete checkout leases pertaining to secrets in the box administered by box administrator.
- View audit logs—Can view and download audit logs.

A summary of the roles and permissions:

Action	Vault Admin	Box Admin	Vault User
Create Box	Yes	No	No
Update Box properties	Yes	Yes - on boxes they are allowed to administer	No
Tag/Untag Box	Yes	Yes - on boxes they are allowed to administer	No
Delete Box	Yes	No	No

Action	Vault Admin	Box Admin	Vault User
Create Secret	Yes	Yes - on boxes they are allowed to administer	No
Update Secret properties	Yes	Yes - on boxes they are allowed to administer	No
Tag/Untag Secret	Yes	Yes - on boxes they are allowed to administer	No
Update Secret value	Yes	Yes - on boxes they are allowed to administer	No
Delete Secret	Yes	Yes - on boxes they are allowed to administer	No
Checkout Secret	Yes, provided that they are part of a Vault User Policy providing access to the secret	Yes, provided that they are part of a Vault User Policy providing access to the secret	Yes, provided that they are part of a Vault User Policy providing access to the secret
Create Policy	Yes	No	No
Update Policy	Yes	No	No
View Audit	Yes	Yes, but only those audits corresponding to Boxes & Secrets within the Boxes administered	No
Download Audit	Yes	Yes with restrictions same as above	No

Policies

Vault administrators can create and manage access control policies that manage access to the secrets. Policies consist of the following:

- Security principle—The list of users governed by this policy. This can be an individual local user, an AD user or an AD group.
- Role—The permissions or a list of actions/operations that are granted to the user. Only the vault user role is supported. For information on granting the vault admin role, see Default Admin Policy below.
- Resources—The list of boxes and secrets in the vault that the user or group can access.

The maximum number of policy change versions that can be kept is 25.

Note: If you modify a policy and a user is logged on to a session using the policy, the policy changes are not applied to the active session; the changes are applied the next time the user starts a session.

Default Admin Policy

When a new vault is created, the Cryptographic Security Platform Vault for Secrets creates a default admin policy that grants the vault administrator role to the local user, AD user, or AD group that is set as the first vault administrator. The default admin policy is the only policy you can use to grant the vault admin role to other users. To do so, the Vault Administrator can edit the 'security principle' part of the default admin policy to grant the vault administrator role to additional users.

Vault User Policy

The Vault User Policy provides checkout/access permissions to secrets. A Vault User Policy MUST be created and assigned to a box or secret before a non-admin user can access the value for a secret. Vault Admins and Box Admins are not able to directly view a secret or any previous versions of secrets without being part of the Vault User Policy.

Box Admin Policy

The Box Admin Policy allows management and administration of boxes. Note that the Box Admin must be part of a relevant Vault User Policy to be able to checkout and view secrets, even on boxes that they can administer.

Vault Secondary Approver Policy

The Vault Secondary Approver Policy allows users to enable or disable secondary approval, and to grant or deny approval for secondary approval requests.

Download the CSP Vault CA Certificate

The Cryptographic Security Platform Vault CA certificate is used with the PASM CLI.

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
2. Select **? > Download CA Certificate**.
   The Cryptographic Security Platform Vault downloads a `pem` file to your browser's default download location.

Hardware Security Modules with CSP Vault for Secrets

HSMs can be enabled or disabled for each Cryptographic Security Platform Vault for Secrets.

Important: HSMs must be enabled in the Cryptographic Security Platform Vault Management webGUI before they can be used in the Cryptographic Security Platform Vault for Secrets.

When enabled:

- A KEK (key encryption key) is created on the HSM for each box. KEKs are non-exportable and never leave the HSM.
- A corresponding DEK (data encryption key) is created by the HSM and wrapped by the KEK.
- Secret values are encrypted and decrypted with this DEK.
- A DEK cache timeout can be specified to cache it for a specific period of time.

Setting the Password-Policy for Users

The password policy allows you to set the expiration date for all Cryptographic Security Platform Vault for Secrets users.

1. Log into the Cryptographic Security Platform Vault for Secrets webGUI.
2. At the top right of the vault page, click the Settings icon.
3. On the Settings page, click the Password Policy tab.
4. Complete the following:

Option	Description
Password Expiration	The expiration value that you want to use for the password in months or days.
Minimum Length	The minimum length for the password.
Minimum Numbers	The minimum amount of numbers that must be included in the password.
Minimum Lowercase Characters	The minimum amount of lowercase characters that must be included in the password.
Minimum Uppercase Characters	The minimum amount of uppercase characters that must be included in the password.
Minimum Special Characters	The minimum amount of special characters that must be included in the password.

5. Click **Save**.

Using HSM with CSP Vault for Secrets

You can use an HSM to store your keys more securely.

Important: HSMs must be enabled in the Cryptographic Security Platform Vault Management webGUI before they can be used in the Cryptographic Security Platform Vault for Secrets.

To enable HSM:

1. Log into the Cryptographic Security Platform Vault for Secrets webGUI.
2. At the top right of the vault page, click the Settings icon.
3. On the Settings page, click the HSM tab.
4. Click the HSM toggle button to set it to **Enabled**. This allows you to use the HSM feature in the Cryptographic Security Platform Vault for Secrets.
5. Click **Test Connection** to verify the connection is working successfully. If not, please contact your HSM administrator.
6. Click **Enable HSM** to enable the HSM connection.
7. You will see an Encryption in progress... message while your keys are being encrypted. You do not need to remain on this page until it has finished.
8. Optionally update the data encryption key cache timeout values and click **Apply**.

To modify your HSM settings:

1. Log into the Cryptographic Security Platform Vault for Secrets webGUI.
2. At the top right of the vault page, click the Settings icon.
3. On the Settings page, click the HSM tab.
4. Click the **Rekey** button to rekey your encrypted data.
   You will see a Rekey in progress... message while the rekey occurs. You do not need to remain on this page until it has finished.
   Note: If the **Rekey** button is grayed out, click the **Test Connection** button to refresh.
5. Update the data encryption key cache timeout values as needed and click **Apply**.

To disable the HSM:

1. Log into the Cryptographic Security Platform Vault for Secrets webGUI.
2. At the top right of the vault page, click the Settings icon.
3. On the Settings page, click the HSM tab.
4. Click the HSM toggle button to set it to **Disabled**.
5. Click **Disable HSM** to disable the HSM connection.
   You will see a Decryption in progress... message while your keys are being decrypted. You do not need to remain on this page until it has finished.

Viewing CSP Vault for Secrets

On the Vault page, you can view all vaults that have been created.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Administrator privileges.
2. On the Vaults page, over the vault and click **View Details.**
   Note: Only the Vault Description can be edited.

Field	Description
Vault Name	The name of the vault.
Vault Description	The description of the vault.
Vault URL	The login URL to be used when connecting to the vault via the Cryptographic Security Platform Vault for Secrets webGUI.
API URL	The URL to be used when connecting to the vault via the API or CLI.
Admin Name	The name associated with the admin user or group.
Admin Email	The email address associated with the admin user or group.
Email Notifications	Whether the email notifications are enabled or disabled.

CSP Vault for Secrets CLI

- Accessing the PASM CLI
- PASM CLI Cancel-CSV-Import Command
- PASM CLI Checkin-Secret Command
- PASM CLI Checkout-Secret Command
- PASM CLI Create-Box Command
- PASM CLI Create-File-Secret Command
- PASM CLI Create-KV-Secret Command
- PASM CLI Create-Local-User Command
- PASM CLI Create-Policy Command
- PASM CLI Create-Pwd-Secret Command
- PASM CLI Create-Secret Command
- PASM CLI Create-SSH-Key-Secret Command
- PASM CLI Delete-Box Command
- PASM CLI Delete-Lease Command
- PASM CLI Delete-Policy Command
- PASM CLI Delete-Secret Command
- PASM CLI Download-Audit Command
- PASM CLI Download-Sample-CSV Command
- PASM CLI Download-SSH-Proxy-Audit Command
- PASM CLI Generate-Password Command
- PASM CLI Get-AD-Setting Command
- PASM CLI Get-Audit-Message-Template Command
- PASM CLI Get-Audit-Setting Command
- PASM CLI Get-Box Command
- PASM CLI Get-CSV-Import-Status Command
- PASM CLI Get-Lease Command
- PASM CLI Get-Policy Command
- PASM CLI Get-Secret Command
- PASM CLI Get-Secret-Value Command
- PASM CLI Import-CSV Command
- PASM CLI List-AD-Settings Command
- PASM CLI List-Audit-Messages Command
- PASM CLI List-Audit-Message-Templates Command
- PASM CLI List-Boxes Command
- PASM CLI List-Box-IDs Command
- PASM CLI List-Leases-by-Secret Command
- PASM CLI List-Leases Command
- PASM CLI List-My-Checkouts Command
- PASM CLI List-Policies Command
- PASM CLI List-Policy-Versions Command
- PASM CLI List-Secret-IDs Command
- PASM CLI List-Secrets Command
- PASM CLI List-Secret-Versions Command
- PASM CLI Login Command
- PASM CLI Put-File-Secret Command
- PASM CLI Put-Secret-Value Command
- PASM CLI Put-SSH-Key-Secret-Value Command
- PASM CLI Rotate-Secret Command
- PASM CLI Tag-Box Command
- PASM CLI Tag-Secret Command
- PASM CLI Untag-Box Command

- PASM CLI Untag-Secret Command
- PASM CLI Update AD Setting Command
- PASM CLI Update-Audit-Setting Command
- PASM CLI Update-Box Command
- PASM CLI Update-Policy Command
- PASM CLI Update-Secret Command
- PASM CLI Version Command

Accessing the PASM CLI

To access the PASM CLI, you will need the following:

- **The Cryptographic Security Platform Vault CA Certificate.**
- **The login URL of the vault. This is listed as the API URL on a vault's Details page.**

The PASM CLI is available for both Linux and Windows in the following public repository: https://github.com/EntrustCorporation/pasmcli.

You can use PASM CLI commands only after you create a vault. In all commands in this section, the PASM CLI application is located in the same directory as the downloaded Cryptographic Security Platform Vault CA certificate.

PASM CLI Cancel-CSV-Import Command

Use the PASM CLI cancel-csv-import command to cancel a CSV file import that is in progress.

If you run the command and no CSV file import is in progress, an error appears.

Syntax

pasmcli cancel-csv-import [*options*]

Option	Description
-h or --help	Displays usage text.

PASM CLI Checkin-Secret Command

Use the PASM CLI checkin-secret command to check a secret back into the box.

Syntax

pasmcli checkin-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The box ID or name where the secret is to be checked in. Strings must be enclosed in double quotes.

Option	Description
-f or --lease-file string	The lease ID file to use to check in the secret. Strings must be enclosed in double quotes.
-l or --leaseid string	The lease ID to use to check in the secret. Strings must be enclosed in double quotes.
-s or --secretid string	The ID or name of the secret to be checked in. Strings must be enclosed in double quotes.
-v or --version int	The version number of the secret to be checked in integer format.

PASM CLI Checkout-Secret Command

Use the PASM CLI checkout-secret command to check out a secret from a box in your Cryptographic Security Platform Vault for Secrets. If secret is of "file" type, on checkout, the corresponding secret file is downloaded to your current working directory.

Syntax

pasmcli checkout-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box where the secret is located. Strings must be enclosed in double quotes.
-d or --dont-save-lease string	When this option is added, the lease information will not be saved in a file.
-j or --json-output string	When this option is added, the JSON-formatted output is displayed.
-l or --lease-file string	The file location where the lease details will be saved upon successful checkout. If neither this option nor the `dont-save-lease` option is not provided, then the lease details will be stored by default at $HOMEDIR/vault.data/vault_lease_<id>.txt.

Option	Description
-s or --secretid string	The ID or name of the secret to fetch. Strings must be enclosed in double quotes.
-v, or --version int	The version of the secret to fetch in integer format. If not specified, fetch the latest version.

PASM CLI Create-Box Command

Use the PASM CLI create-box command to create a box in your Cryptographic Security Platform Vault for Secrets.

Syntax

pasmcli create-box [*options*]

Option	Description
-h or --help	Displays usage text.
-d or --description string	Short description for the box. Strings must be enclosed in double quotes.
-x or --exclusive-checkout string {enable|disable}	If this flag is set, all secret checkouts will be exclusive, and only one user can check out the secret at a time. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-l or --lease-duration string	The lease duration to enforce for all secrets that are checked out from a box. The duration must be in ISO 8601 format. For example, P1M15DT12H30M. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-L or --lease-renewable string {enable|disable}	Reserved for future use.
-m or --max-secret-versions int	The maximum number of secrets versions to persist in integer format.

Option	Description
-n or --name string	The name of the box. Strings must be enclosed in double quotes.
-r or --rotation-duration string	The duration for when secrets in the box will be rotated. The behavior depends on the `rotation-force` option. The duration must be in ISO 8601 format. For example, P1M15DT12H30M. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-f or --rotation-force string {enable|disable}	If this flag is set, it forces the rotation of all secrets in the box. The behavior varies depending on the `rotation-duration` and `rotation-on-checkin` options. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-o or --rotation-on-checkin string {enable|disable}	If this flag is set, the secret will be automatically rotated upon checkin. If the checkout lease expires, then the behavior depends on the `rotation-force` option.
-D or --secret-duration string	The expiration duration for secrets in the box, if the `expires-at` option is not provided with the `create-secret` command. The duration must be in ISO 8601 format. For example, P1M15DT12H30M. Strings must be enclosed in double quotes.
-t or --tagkey stringArray	The tag key to associate with the box. This option is repeatable.
-v or --tagvalue stringArray	The tag value to associate with the box. This option is repeatable.

PASM CLI Create-File-Secret Command

Use the PASM CLI create-kv-secret command to create a File Static Secret within the specified box in your Cryptographic Security Platform Vault for Secrets.

Syntax

pasmcli create-file-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b, --boxid string	ID or name of the Box.
-d, --description string	Short description for the Secret.
-e, --expires_at string	Expiration time in RFC 3339 format.
-f, --filename string	File to store as Secret data.
-n, --name string	Name of the Secret.
-t, --tagkey stringArray	Tag key to associate with the Secret. This option is repeatable.
-v, --tagvalue stringArray	Tag value to associate with the Secret. This option is repeatable.

PASM CLI Create-KV-Secret Command

Use the PASM CLI create-kv-secret command to create a Key-Value Static Secret within the specified box in your Cryptographic Security Platform Vault for Secrets.

Syntax

pasmcli create-kv-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b, --boxid string	ID or name of the Box.
-X, --datakey stringArray	The key to associate with the Secret data. This option is repeatable.
-Y, --datavalue stringArray	Value corresponding to specific Secret data. This option is repeatable.
-d, --description string	Short description for the Secret.

Option	Description
-e, --expires_at string	Expiration time in RFC 3339 format.
-n, --name string	Name of the Secret.
-t, --tagkey stringArray	Tag key to associate with the Secret. This option is repeatable.
-v, --tagvalue stringArray	Tag value to associate with the Secret. This option is repeatable.

PASM CLI Create-Local-User Command

Use the PASM CLI create-local-user command to create a local user in your Cryptographic Security Platform Vault for Secrets.

Syntax

pasmcli create-local-user [*options*]

Option	Description
-h or --help	Displays usage text.
-e, --email	Email address of the local user.
-n, --name	Full name of the local user.
-p, --password	Password for the local user.
-d, --password_expiration	Password expiry date in the format 'yyyy-mm-dd'.
-u, --username	Username for the local user logging in to the vault tenant.

PASM CLI Create-Policy Command

Use the PASM CLI create-policy command to create a role-based access control policy to allow users or applications to access secrets.

Syntax

pasmcli create-policy [*options*]

Option	Description
-h or --help	Displays usage text.
-g or --ad-group stringArray	||-separated string containing the DN & display name of AD groups to be added as principals.
-L or --ad-logon-name stringArray	Logon name of AD users to be added as principals. This option is repeatable.
-u or --ad-upn stringArray	The UPN of AD users to be added as principals. This option is repeatable.
-l or --local-user stringArray	Local user name of users to be added as principals. This option is repeatable.
-n or --name string	The name of the policy. Strings must be enclosed in double quotes.
-R or --Resource stringArray	A comma-separated string containing the box ID and secret IDs to be added as resources. Add * after the box ID to include all secrets in the box.
-r or --role string	The role of the user that is being assigned.
-t or --tagkey stringArray	The tag key to associate with the policy. This option is repeatable.
-v or --tagvalue stringArray	The tag value to associate with the policy. This option is repeatable.

PASM CLI Create-Pwd-Secret Command

Use the PASM CLI create-pwd-secret command to create a password static secret within the specified box in your Cryptographic Security Platform Vault for Secrets.

Syntax

pasmcli create-pwd-secret [*options*]

Option	Description
-h or --help	Displays usage text.

Option	Description
-b, --boxid string	ID or name of the Box.
-d, --description string	Short description for the Secret.
-e, --expires_at string	Expiration time in RFC 3339 format.
-n, --name string	Name of the Secret.
-p, --password string	Password for Secret.
-t, --tagkey stringArray	Tag key to associate with the Secret. This option is repeatable.
-v, --tagvalue stringArray	Tag value to associate with the Secret. This option is repeatable.

PASM CLI Create-Secret Command

Use the PASM CLI create-secret command to create a secret in a box.

Syntax

pasmcli create-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-T or --ESXi-tls-version string	Optional. If the `managed-type` option is set to ESXiHostAccount, you can use this option to set the TLS version to use while connecting to an ESXi host.
-c or --ESXicacert string	Optional. If the `managed-type` option is set to ESXiHostAccount, use this option to specify the CA certificate to use while connecting to an ESXi host.
-H or --ESXihost string	The ESXi host address. Required if the `managed-type` option is set to ESXiHostAccount.

Option	Description
-P or --ESXipasswd string	The password for the ESXi host. Required if the `managed-type` option is set to ESXiHostAccount.
-U or --ESXiuser string	The ESXi username. Required if the `managed-type` option is set to ESXiHostAccount.
-b or --boxid string	The name or ID of the box where the secret will be created.
-D or --data string	The secret data.
-X or --datakey stringArray	The key to associate with the secret data.
-Y or --datavalue stringArray	The value that corresponds to specific secret data.
-d or --description string	A short description of the secret.
-x or --exclusive-checkout string {enable|disable}	If this flag is set, all secret checkouts will be exclusive. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-e or --expires_at string	The expiration time in RFC 3339 format, prefixed with TS. For example, TS2020-12-12T22:04:16.162848Z.
-l or --lease-duration string	The lease duration to enforce for this secret. The duration must be in ISO 8601 format. For example, P1M15DT12H30M. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-L or --lease-renewable string	Reserved for future use.
-m or --managed-type string	The type of managed secret. For this release, only ESXiHostAccount is supported.

Option	Description
-B or --master-boxID string	Optional. The box ID or name of the master secret, if the `managed-type` option is set to ESXiHostAccount.
-I or --master-secretid string	Optional. The master secret ID or name, if the `managed-type` option is set to ESXiHostAccount.
-n or --name string	The name of the secret.
-r or --rotation-duration string	The duration for when the secret will be rotated. The behavior depends on the `rotation-force`option. The duration must be in ISO 8601 format. For example, P1M15DT12H30M. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-f or --rotation-force string {enable|disable}	If this flag is set, it forces the rotation of this secret. The behavior varies depending on the `rotation-duration` and `rotation-on-checkin` options. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-o or --rotation-on-checkin string {enable|disable}	If this flag is set, the secret rotation is attempted when the secret is checked in. The behavior depends on the `rotation-force` option. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-t or --tagkey stringArray	The tag key to associate with the secret. This option is repeatable.
-v or --tagvalue stringArray	The tag value to associate with the secret. This option is repeatable.

PASM CLI Create-SSH-Key-Secret Command

Use the PASM CLI create-ssh-key-secret command to create an SSH key-based secret within the specified box in your Cryptographic Security Platform Vault for Secrets.

Syntax

pasmcli create-ssh-key-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The name or ID of the box where the secret will be created.
-d or --description string	A short description of the secret.
-x or --exclusive-checkout string {enable|disable}	If this flag is set, all secret checkouts will be exclusive. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-e or --expires_at string	The expiration time in RFC 3339 format.
-H or --host string	The SSH endpoint IP address or host name.
-K, --key-file string	The private key file for SSH endpoint access.
-W, --key-pwd string	The passphrase of private key, if encrypted.
-l or --lease-duration string	The lease duration to enforce for this secret. The duration must be in ISO 8601 format. For example, P1M15DT12H30M. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-L, --lease-renewable string	Reserved for future use.
-B, --master-boxid string	Optional. The Box ID or name of the master secret.
-I or --master-secretid string	Optional. The master secret ID or name.
-n or --name string	Short description for the Secret.

Option	Description
-P, --port int	The SSH port.
-t, --tagkey stringArray	Tag key to associate with the Secret. This option is repeatable.
-v, --tagvalue stringArray	Tag value to associate with the Secret. This option is repeatable.
-U, --user string	The SSH user name.

PASM CLI Delete-Box Command

Use the PASM CLI delete-box command to delete the specified box.

Syntax

pasmcli delete-box [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box to delete. Strings must be enclosed in double quotes.

PASM CLI Delete-Lease Command

Use the PASM CLI delete-lease command to delete the specified lease.

Syntax

pasmcli delete-lease [*options*]

Option	Description
-h or --help	Displays usage text.
-l or --leaseid string	The ID or name of the lease to delete. Strings must be enclosed in double quotes.

PASM CLI Delete-Policy Command

Use the PASM CLI delete-policy command to delete the specified policy.

Syntax

pasmcli delete-policy [*options*]

Option	Description
-h or --help	Displays usage text.
-p or --policyid string	The ID of the policy to delete. Strings must be enclosed in double quotes.

PASM CLI Delete-Secret Command

Use the PASM CLI delete-secret command to delete the specified secret.

Syntax

pasmcli delete-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box that contains the specified secret.
-s or --secretid string	The ID or name of the secret to delete. Strings must be enclosed in double quotes.

PASM CLI Download-Audit Command

Use the PASM CLI download-audit command to download the vault audit logs as a bundle in `tar.gz` format.

Syntax

pasmcli download-audit [*options*]

Option	Description
-h or --help	Displays usage text.

PASM CLI Download-Sample-CSV Command

Use the PASM CLI download-sample-csv command to download a sample CSV file.

All secrets in the CSV file must be of the same type. The supported types are: esxi, static, or SSH key endpoint.

Syntax

pasmcli download-sample-csv [*options*]

Option	Description
-h or --help	Displays usage text.
t or --secret_type string	Secret type, corresponding to the secrets in the sample CSV file that you want to download. The secret type must be one of the following: esxi, static, or SSH key endpoint

PASM CLI Download-SSH-Proxy-Audit Command

Use the PASM CLI download-ssh-proxy-audit command to download the ssh proxy audit logs as a bundle in zip format.

Syntax

pasmcli download-ssh-proxy-audit [*options*]

Option	Description
-h or --help	Displays usage text.

PASM CLI Generate-Password Command

Use the PASM CLI gen-passwd command to impose requirements on passwords created for Cryptographic Security Platform Vault for Secrets.

Syntax

pasmcli gen-passwd [*options*]

Option	Description
-h or --help	Displays usage text.
-l, --length int	The length of the password. The minimum is 9.
-n, --nums int	Minimum number of digits in the password.
-s, --symbols int	Minimum number of special characters in the password.

Option	Description
-u, --upper int	Minimum number of upper case characters in the password.
-w, --lower int	Minimum number of lower case characters in the password.

PASM CLI Get-AD-Setting Command

Use the PASM CLI get-ad-setting command to fetch the specified AD settings.

> Note: If you have only one AD account, then using the `list-ad-settings` command displays the same information.

Syntax

pasmcli get-ad-setting [*options*]

Option	Description
-h or --help	Displays usage text.
-a or --ad-setting-id string	The ID or name of the AD setting to fetch. Strings must be enclosed in double quotes.

PASM CLI Get-Audit-Message-Template Command

Use the PASM CLI get-audit-messate-template command to fetch a specific audit message template.

Syntax

pasmcli get-audit-message-template [*options*]

Option	Description
-h or --help	Displays usage text.
-m or --msgid int	The message ID in integer format of the audit message template to fetch.

PASM CLI Get-Audit-Setting Command

Use the PASM CLI get-audit-setting command to fetch the current audit settings.

Syntax

pasmcli get-audit-setting [*options*]

Option	Description
-h or --help	Displays usage text.

PASM CLI Get-Box Command

Use the PASM CLI get-box command to fetch a specific AD setting.

Note: If you have only one box, then using the `list-boxes` command displays the same information.

Syntax

pasmcli get-box [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box to fetch. Strings must be enclosed in double quotes.

PASM CLI Get-CSV-Import-Status Command

Use the PASM CLI get-csv-import-status command to check the status of the current CSV file import. If no CSV file import is in progress, the status for the previous import is retrieved.

If you run the command and no CSV file import is in progress and there have been no previous CSV file imports, an error appears.

Syntax

pasmcli get-csv-import-status [*options*]

Option	Description
-h or --help	Displays usage text.

PASM CLI Get-Lease Command

Use the PASM CLI get-lease command to fetch a specific lease.

Note: If you have only one lease, then using the `list-lease` command displays the same information.

Syntax

pasmcli get-lease [*options*]

Option	Description
-h or --help	Displays usage text.
-l or --leaseid string	The ID or name of the lease to fetch. Strings must be enclosed in double quotes.

PASM CLI Get-Policy Command

Use the PASM CLI get-policy command to fetch a specific policy.

If you have only one policy, then using the `list-policy` command displays the same information.

Syntax

pasmcli get-policy [*options*]

Option	Description
-h or --help	Displays usage text.
-p or --policyid string	The ID of the policy to fetch. Strings must be enclosed in double quotes.

PASM CLI Get-Secret Command

Use the PASM CLI get-secret command to fetch a specific secret.

Syntax

pasmcli get-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box where the secret is located. Strings must be enclosed in double quotes.
-s or --secretid string	The ID or name of the secret to fetch. Strings must be enclosed in double quotes.
-v or --version int	The version of the secret to fetch. If not specified, the last version of the secret is fetched.

PASM CLI Get-Secret-Value Command

Use the PASM CLI get-secret-value command to fetch a specific secret value.

Syntax

pasmcli get-secret-value [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box where the secret is located. Strings must be enclosed in double quotes.
-s or --secretid string	The ID or name of the secret value to fetch. Strings must be enclosed in double quotes.
-v or --version int	The version of the secret to fetch. If not specified, the last version of the secret is fetched.

PASM CLI Import-CSV Command

Use the PASM CLI import-csv command to import secrets to your Vault from a CSV file.

All secrets in the CSV file must be of the same type. The supported types are: esxi, static, or SSH key endpoint.

Syntax

pasmcli import-csv [*options*]

Option	Description
-h or --help	Displays usage text.
-c or --csv_file string	CSV file to import.
-t or --secret_type string	Secret type, corresponding to the secrets in the CSV file. The secret type must be of the following: esxi, static, or SSH key endpoint.

PASM CLI List-AD-Settings Command

Use the PASM CLI list-ad-settings command to display all AD settings.

Syntax

pasmcli list-ad-settings [*options*]

Option	Description
-h or --help	Displays usage text.
-f or --field stringArray	The AD setting fields to include in the response.
-m or --max-items int	The maximum number of items to include in the response.
-n or --next-token string	The token from which the subsequent audit messages would be listed. Strings must be enclosed in double quotes.
-p or --prefix string	List only those AD settings secrets whose name begins with this prefix. Strings must be enclosed in double quotes.

PASM CLI List-Audit-Messages Command

Use the PASM CLI list-audit-messages command to display all audit messages.

Syntax

pasmcli list-audit-messages [*options*]

Option	Description
-h or --help	Displays usage text.
-f or --field stringArray	The audit message fields to include in the response.
-l or --filters string	The conditional filter expression to apply. Strings must be enclosed in double quotes.
-i or --include-info	Show additional information if available.
-j or --json-output	Show JSON-formatted audit messages.
-t or --local-time	Convert audit message timestamps to local time.

Option	Description
-m or --max-items int	The maximum number of items to include in the response.
-n or --next-token string	The token from which the subsequent audit messages would be listed. Strings must be enclosed in double quotes.

PASM CLI List-Audit-Message-Templates Command

Use the PASM CLI list-audit-message-templates command to display all audit message templates.

Syntax

pasmcli list-audit-message-templates [*options*]

Option	Description
-h or --help	Displays usage text.
-m or --max-items int	The maximum number of items to include in the response.
-n or --next-token string	The token from which the subsequent audit messages would be listed. Strings must be enclosed in double quotes.

PASM CLI List-Boxes Command

Use the PASM CLI list-boxes command to display all box details.

Syntax

pasmcli list-boxes [*options*]

Option	Description
-h or --help	Displays usage text.
-f or --field stringArray	The box fields to include in the response.
-l or --filters string	The conditional expression used to list filtered boxes. Strings must be enclosed in double quotes.

Option	Description
-m or --max-items int	The maximum number of items to include in the response.
-n or --next-token string	The token from which the subsequent boxes would be listed. Strings must be enclosed in double quotes.
-p or --prefix string	List only those boxes whose name begins with this prefix. Strings must be enclosed in double quotes.

PASM CLI List-Box-IDs Command

Use the PASM CLI" /> list-box-ids command to display all box names and IDs.

Syntax

pasmcli list-box-ids [*options*]

Option	Description
-h or --help	Displays usage text.
-l or --filters string	The conditional expression used to list filtered boxes. Strings must be enclosed in double quotes.
-m or --max-items int	The maximum number of items to include in the response.
-n or --next-token string	The token from which the subsequent boxes would be listed. Strings must be enclosed in double quotes.
-p or --prefix string	List only those boxes whose name begins with this prefix. Strings must be enclosed in double quotes.

PASM CLI List-Leases-by-Secret Command

Use the PASM CLI" /> list-leases-by-secret command to display all leases organized by secret.

Syntax

pasmcli list-leases-by-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box where the secret is located. Strings must be enclosed in double quotes.
-f or --field stringArray	The lease fields to include in the response.
-l or --filters string	The conditional expression used to list filtered leases. Strings must be enclosed in double quotes.
-m or --max-items int	The maximum number of items to include in the response.
-n or --next-token string	The token from which the subsequent leases would be listed. Strings must be enclosed in double quotes.
-p or --prefix string	List only those leases whose name begins with this prefix. Strings must be enclosed in double quotes.
-s or --secretid string	The ID or name of the secret whose lease we want to list. Strings must be enclosed in double quotes.

PASM CLI List-Leases Command

Use the PASM CLI list-leases command to display all leases.

Syntax

pasmcli list-leases [*options*]

Option	Description
-h or --help	Displays usage text.
-f or --field stringArray	The lease fields to include in the response.

Option	Description
-l or --filters string	The conditional expression used to list filtered leases. Strings must be enclosed in double quotes.
-m or --max-items int	The maximum number of items to include in the response.
-n or --next-token string	The token from which the subsequent leases would be listed. Strings must be enclosed in double quotes.
-p or --prefix string	List only those leases whose name begins with this prefix. Strings must be enclosed in double quotes.

PASM CLI List-My-Checkouts Command

Use the PASM CLI list-my-checkouts command to display all of the checkouts belonging to the current logged-in user.

Syntax

pasmcli list-my-checkouts [*options*]

Option	Description
-h or --help	Displays usage text.
-f or --field stringArray	The fields to include in the response.
-l or --filters string	The conditional expression used to list my filtered checkout leases. Strings must be enclosed in double quotes.
-m or --max-items int	The maximum number of items to include in the response.
-n or --next-token string	The token from which the subsequent items would be listed. Strings must be enclosed in double quotes.

Option	Description
-p or --prefix string	List only those checkouts whose name begins with this prefix. Strings must be enclosed in double quotes.

PASM CLI List-Policies Command

Use the PASM CLI list-policies command to display the specified policies.

Syntax

pasmcli list-policies [*options*]

Option	Description
-h or --help	Displays usage text.
-f or --field stringArray	The fields to include in the response.
-l or --filters string	The conditional expression used to list filtered leases. Strings must be enclosed in double quotes.
-m or --max-items int	The maximum number of items to include in the response.
-n or --next-token string	The token from which the subsequent items would be listed. Strings must be enclosed in double quotes.
-p or --prefix string	List only those policies whose name begins with this prefix. Strings must be enclosed in double quotes.

PASM CLI List-Policy-Versions Command

Use the PASM CLI list-policy-versions command to display the specified policy versions.

Syntax

pasmcli list-policy-versions [*options*]

Option	Description
-h or --help	Displays usage text.

Option	Description
-p or --policyid string	The ID of the policy. Strings must be enclosed in double quotes.

PASM CLI List-Secret-IDs Command

Use the PASM CLI list-secret-ids command to display all secret names and IDs within a box.

Syntax

pasmcli list-secret-ids [*option*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box where the secrets are located. Strings must be enclosed in double quotes.
-l or --filters string	The conditional expression used to list filtered secrets. Strings must be enclosed in double quotes.
-m or --max-items int	The maximum number of items to include in the response.
-n or --next-token string	The token from which the subsequent secrets would be listed. Strings must be enclosed in double quotes.
-p or --prefix string	List only those secrets whose name begins with this prefix. Strings must be enclosed in double quotes.

PASM CLI List-Secrets Command

Use the PASM CLI list-secrets command to display the specified secrets.

Syntax

pasmcli list-secrets [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box where the secrets are located. Strings must be enclosed in double quotes.
-f or --field stringArray	The fields to include in the response.
-l or --filters string	The conditional expression used to list filtered leases. Strings must be enclosed in double quotes.
-m or --max-items int	The maximum number of items to include in the response.
-n or --next-token string	The token from which the subsequent items would be listed. Strings must be enclosed in double quotes.
-p or --prefix string	List only those secrets whose name begins with this prefix. Strings must be enclosed in double quotes.

PASM CLI List-Secret-Versions Command

Use the PASM CLI list-secret-versions command to display all versions of a secret in the specified box.

Syntax

pasmcli list-secret-versions [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box where the secrets are located. Strings must be enclosed in double quotes.
-s or --secretid string	The ID or name of the secret. Strings must be enclosed in double quotes.

PASM CLI Login Command

Use the PASM CLI login command to log into your Cryptographic Security Platform Vault for Secrets. The login will expire in 30 minutes. You must have the Cryptographic Security Platform Vault for Secrets CA Certificate before you begin. For more information, see Download the Cryptographic Security Platform Vault CA Certificate.

Syntax

pasmcli login [*options*]

Option	Description
-h or --help	Displays usage text.
-C or --cacert string	The path to the KeyControl CA Certificate file that you downloaded, for example, cacert.pem. This is used to verify the Cryptographic Security Platform Vault for Secrets server. Strings must be enclosed in double quotes. If you have not yet downloaded the certificate, see Download the Cryptographic Security Platform Vault CA Certificate.
-l or --login-URL string	The API login URL for the Cryptographic Security Platform Vault for Secrets.
-p or --password string	Login password. You will be prompted to enter if not provided. Strings must be enclosed in double quotes.
-u or --username string	Login username. You will be prompted to enter if not provided. Strings must be enclosed in double quotes.

Example:

```
./pasmcli login -C "<CA-certificate-path>" -l <API-login-URL> -u "<user-login>"
```

```
./pasmcli login -C "/home/kc-cert/230907081009_cacert.pem" -l https://10.1.1.1/vault/1.0/Login/9283f901-fc73-4765-ac32-98d082d786dc/ -u "user@mycompany.com"
```

You will be prompted to enter the password. After entering the correct credentials, the command will completed with the following success message: Login is successful.

PASM CLI Put-File-Secret Command

Use the PASM CLI put-file-secret command to create a "file" secret type by providing a file as secret. The maximum file size limit is 5 MB.

Syntax

pasmcli put-file-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The name or ID of the box.
-f or --filename string	File to store as Secret data.
-s or --secretid string	The secret ID or name of the secret. Strings must be enclosed in double quotes.

PASM CLI Put-Secret-Value Command

Use the PASM CLI put-secret-value command to replace an existing secret with a new value.

Syntax

pasmcli put-secret-value [*options*]

Option	Description
-h or --help	Displays usage text.
-T or --ESXi-tls-version string	Optional. If the `managed-type` option is set to ESXiHostAccount, you can use this option to set the TLS version to use while connecting to an ESXi host.
-c or --ESXicacert string	Optional. If the `managed-type` option is set to ESXiHostAccount, use this option to specify the CA certificate to use while connecting to an ESXi host.
-H or --ESXihost string	The ESXi host address. Required if the `managed-type` option is set to ESXiHostAccount.
-P or --ESXipasswd string	The password for the ESXi host. Required if the `managed-type` option is set to ESXiHostAccount.
-U or --ESXiuser string	The ESXi username. Required if the `managed-type` option is set to ESXiHostAccount.

Option	Description
-b or --boxid string	The name or ID of the box where the secret will be replaced.
-D or --data string	The secret daa used to replace the existing secret.
-X or --datakey stringArray	The key to associate with the secret data.
-Y or --datavalue stringArray	The value that corresponds to specific secret data.
-m or --managed-type string	The type of managed secret. For this release, only ESXiHostAccount is supported.
-B or --master-boxID string	Optional. The box ID or name of the master secret, if the `managed-type` option is set to ESXiHostAccount.
-I or --master-secretid string	Optional. The master secret ID or name, if the `managed-type` option is set to ESXiHostAccount.
-s or --secretid string	The secret ID or name of the secret. Strings must be enclosed in double quotes.

PASM CLI Put-SSH-Key-Secret-Value Command

Use the PASM CLI put-ssh-key-secret-value command to replace an existing SSH key-based secret with a new secret value.

Syntax

pasmcli put-ssh-key-secret-value [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The name or ID of the box where the secret is stored.
-H or --host string	The SSH endpoint IP/hostname.

Option	Description
-K, --key-file string	The private key file for SSH endpoint access.
-W, --key-pwd string	The passphrase of private key, if encrypted.
-B, --master-boxid string	Optional. The Box ID or name of the master secret.
-I or --master-secretid string	Optional. The master secret ID or name.
-P, --port int	The SSH port.
-s, --secretid string	The ID or name of the Secret.
-U, --user string	The SSH user name.

PASM CLI Rotate-Secret Command

Use the PASM CLI rotate-secret command to manually rotate a managed secret.

Syntax

pasmcli rotate-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box where the secrets are located. Strings must be enclosed in double quotes.
-s or --secretid string	The secret ID or name of the secret to be checked in. Strings must be enclosed in double quotes.
-v or --version int	Optional. The current version number of the secret in integer format.

PASM CLI Tag-Box Command

Use the PASM CLI tag-box command to add or update tags for a box.

Syntax

pasmcli tag-box [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box. Strings must be enclosed in double quotes.
-R or --revision int	The revision number of the box in integer format.
-t or --tagkey stringArray	The tag key to associate with the box. This option is repeatable.
-v or --tagvalue stringArray	The tag value to associate with the box. This option is repeatable.

PASM CLI Tag-Secret Command

Use the PASM CLI tag-secret command to add or update tags for a secret.

Syntax

pasmcli tag-secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box where the secret is located. Strings must be enclosed in double quotes.
-R or --revision int	The revision number of the secret in integer format.
-s or --secretid string	The secret ID or name of the secret to be tagged. Strings must be enclosed in double quotes.
-t or --tagkey stringArray	The tag key to associate with the secret. This option is repeatable.
-v or --tagvalue stringArray	The tag value to associate with the secret. This option is repeatable.

PASM CLI Untag-Box Command

Use the PASM CLI untag-box command to remove tags from a box.

Syntax

pasmcli untag-box [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box. Strings must be enclosed in double quotes.
-R or --revision int	The revision number of the box in integer format.
-t or --tag stringArray	The tag to disassociate from the box. This option is repeatable.

PASM CLI Untag-Secret Command

Use the PASM CLI untag-secret command to remove tags from a secret.

Syntax

pasmcli untag secret [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box where the secret is located. Strings must be enclosed in double quotes.
-R or --revision int	The revision number of the secret in integer format.
-s or --secretid string	The ID or name of the secret to untag. Strings must be enclosed in double quotes.
-t or --tag stringArray	The tag to disassociate from the secret. This option is repeatable.

PASM CLI Update AD Setting Command

Use the PASM CLI update-ad-setting command to update your AD settings.

Syntax

pasmcli update-ad-setting [*options*]

Option	Description
-h or --help	Displays usage text.
-a or --ad-setting-id string	The Active Directory setting ID or name. Strings must be enclosed in double quotes.
-n or --netbios-name string	The Active Directory NetBIOS name. Strings must be enclosed in double quotes.
-r or --revision int	The Active Directory setting current revision.

Option	Description

-j, --servers-json-file string	The Active Directory Domain Controller List JSON File. This is an array of JSON objects, each object representing a Domain Controller. Strings must be enclosed in double quotes.
	The following keys are supported:
	• server_url - the (mandatory) full url of the Domain Controller
	• cacert (optional) - the path to the CA Certificate to verify with
	• user_base_dn (optional) - the user base DN
	• group_base_dn (optional) - the group base DN
	• timeout (optional) - the connection timeout in seconds. The default is 5 seconds.
	• tls (optional) - whether to enable StartTLS or not. The default is false.
	Example:
	[
	{
	"server_url": "ldaps://dc1.mycompany.eng.com",
	"cacert": "/root/cacert.pem",
	"user_base_dn": "DC=mycompany,DC=eng,DC=com",
	"group_base_dn": "DC=mycompany,DC=eng,DC=com",
	"timeout": 10,
	"tls": false,
	}
	]

-s, --service-account string	The Active Directory Service Account User Name. Strings must be enclosed in double quotes.
-p, --service-password string	The Active Directory Service Account User Password. Strings must be enclosed in double quotes.
-u, --uid-attribute string	The Active Directory UID Attribute. Strings must be enclosed in double quotes.

PASM CLI Update-Audit-Setting Command

Use the PASM CLI update-audit-setting command to update the audit settings.

Syntax

pasmcli update-audit-setting [*options*]

Option	Description
-h or --help	Displays usage text.
-m or --max-items int	The maximum size for the audit logs in bytes. Set 0 for no limit.
-r, --retention-days int32	The number of days to retain the audit logs. Retention days can be set between 30 - 365 days. Set 0 to retain all.

PASM CLI Update-Box Command

Use the PASM CLI update-box command to update the properties of a box.

Syntax

pasmcli update-box [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The ID or name of the box to update. Strings must be enclosed in double quotes.
-d or --description string	Short description for the box. Strings must be enclosed in double quotes.
-x or --exclusive-checkout string {enable|disable|unset}	If this flag is set, all secret checkouts will be exclusive, and only one user can check out the secret at a time. Use `unset` to clear the property. Important: If this property is set in a secret, it takes precedence over the property being set in a box.

Option	Description
-l or --lease-duration string {unset}	The lease duration to enforce for all secrets that are checked out from a box. The duration must be in ISO 8601 format. For example, P1M15DT12H30M. Use `unset` to clear the property. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-L or --lease-renewable string {enable|disable}	Reserved for future use.
-m or --max-secret-versions int	The maximum number of secrets versions to persist in integer format.
-n or --name string	The name of the box. Strings must be enclosed in double quotes.
-r or --rotation-duration string {unset}	The duration for when secrets in the box will be rotated. The behavior depends on the `rotation-force` option. The duration must be in ISO 8601 format. For example, P1M15DT12H30M. Use `unset`to clear the property. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-f or --rotation-force string {enable|disable|unset}	If this flag is set, it forces the rotation of all secrets in the box. The behavior varies depending on the `rotation-duration` and `rotation-on-checkin` options. Use `unset` to clear the property. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-o or --rotation-on-checkin string {enable|disable|unset}	If this flag is set, the secret will be automatically rotated upon checkin. If the checkout lease expires, then the behavior depends on the `rotation-force` option. Use `unset` to clear the property.

Option	Description
-D or --secret-duration string {unset}	The expiration duration for secrets in the box, if the `expires-at` option is not provided with the `create-secret` command. The duration must be in ISO 8601 format. For example, P1M15DT12H30M. Strings must be enclosed in double quotes. Use `unset` to clear the property.
-t or --tagkey stringArray	The tag key to associate with the box. This option is repeatable.
-v or --tagvalue stringArray	The tag value to associate with the box. This option is repeatable.

PASM CLI Update-Policy Command

Use the PASM CLI update-policy command to update the properties of a policy.

Syntax

pasmcli update-policy [*options*]

Option	Description
-h or --help	Displays usage text.
-g, --ad-group stringArray	A string separated by '||' containing the DN and display name of AD groups to be added as principals.
-L or --ad-logon-name stringArray	The logon name of AD users to be added as principals. This option is repeatable.
-u, --ad-upn stringArray	The UPN of AD users to be added as principals. This option is repeatable.
-d, --description string	Short description for the policy.
-l, --local-user stringArray	Local user name of users to be added as principals. This option is repeatable.
-p or --policyid string	The ID of the policy to update.

Option	Description
-e or --resource stringArray	A comma-separated string containing the box_id and secret_ids in subsequent order to be added as resources. Use "*: after the box_id to include all secrets in the box.
-R or --revision int	The revision number of the policy.
-r or --role string	The role of the user.
-t or --tagkey stringArray	The tag key to associate with the policy. This option is repeatable.
-v or --tagvalue stringArray	The tag value to associate with the policy. This option is repeatable.

PASM CLI Update-Secret Command

Use the PASM CLI update-secret command to update the properties of a secret.

Syntax

pasmcli update-secrets [*options*]

Option	Description
-h or --help	Displays usage text.
-b or --boxid string	The name or ID of the box where the secret will be created.
-d or --description string	A short description of the secret.
-x or --exclusive-checkout string {enable|disable|unset}	If this flag is set, all secret checkouts will be exclusive. Use `unset` to clear the property. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-e or --expires_at string {unset}	The expiration time in RFC 3339 format, prefixed with TS. For example, TS2020-12-12T22:04:16.162848Z. Use `unset` to clear the property.

Option	Description
-l or --lease-duration string {unset}	The lease duration to enforce for this secret. The duration must be in ISO 8601 format. For example, P1M15DT12H30M. Use `unset` to clear the property. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-L or --lease-renewable string	Reserved for future use.
-r or --revision int	The revision number of the secret.
-r or --rotation-duration string {unset}	The duration for when the secret will be rotated. The behavior depends on the `rotation-force`option. The duration must be in ISO 8601 format. For example, P1M15DT12H30M. Use `unset` to clear the property. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-f or --rotation-force string {enable|disable|unset}	If this flag is set, it forces the rotation of this secret. The behavior varies depending on the `rotation-duration` and `rotation-on-checkin` options. Use `unset` to clear the property. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-o or --rotation-on-checkin string {enable|disable|unset}	If this flag is set, the secret rotation is attempted when the secret is checked in. The behavior depends on the `rotation-force` option. Use `unset` to clear the property. Important: If this property is set in a secret, it takes precedence over the property being set in a box.
-s or --secretid string	The ID or name of the secret to update. Strings must be enclosed in double quotes.
-t or --tagkey stringArray	The tag key to associate with the secret. This option is repeatable.

Option	Description
-v or --tagvalue stringArray	The tag value to associate with the secret. This option is repeatable.

PASM CLI Version Command

Use the PASM CLI version command to view the current version of the Cryptographic Security Platform Vault for Secrets PASM CLI.

Syntax

pasmcli version [*options*]

Option	Description
-h or --help	Displays usage text.

Viewing CSP Vault for Secrets Audit Logs

The Cryptographic Security Platform Vault for Secrets audit logs page tracks all activity for the Cryptographic Security Platform Vault for Secrets. The audit logs are view only.

Audit logs generated by the Cryptographic Security Platform Vault for Secrets can be accessed both in the Cryptographic Security Platform Vault for Secrets webGUI, and in the Cryptographic Security Platform Vault Management webGUI audit logs.

Please note that unlike Cryptographic Security Platform Vault Management webGUI, the Cryptographic Security Platform Vault for Secrets does not support syslog and SNMP for audit logs.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Audit Logs**.
2. Click on a log entry to view the details or click **Download** to download all of the log entries.

Configuring mTLS for the CSP Vault for Secrets

Mutual Transport Layer Security (mTLS) adds two-way authentication and encryption using digital certificates.

When mTLS is enabled in the Cryptographic Security Platform Vault for Secrets, you can continue to use all of the original Cryptographic Security Platform Vault for Secrets APIs, the CLI, and the webGUI, but only the APIs located at https://<VAULT_IP_or_FQDN>/vault/mtls/1.0/ will use mTLS. The mTLS APIs function the same as the original APIs, but using mTLS is more secure.

- Using a mTLS API Commands
- Creating Client Certificate
- Enabling or Disabling-mTLS Authentication
- mTLS-Prerequisites

Using a mTLS API Commands

By default, all APIs in the Cryptographic Security Platform Vault for Secrets use https://<VAULT_IP_or_FQDN>/vault/1.0/API_COMMAND for the API endpoint. When you enable mTLS and want to use digital certificate authentication, you will need to change your API endpoint to https://<VAULT_IP_or_FQDN>/vault/mtls/1.0/API_COMMAND. If you do not, the API command will work, but will not use mTLS.

If you disable mTLS, you will need to switch the endpoint back to https://<VAULT_IP_or_FQDN>/vault/1.0/API_COMMAND.

Examples:

- Create a client certificate
  Post: https://<VAULT_IP_or_FQDN>/vault/1.0/CreateClientCertificate
  Request payload:
  Copy

```
{
 "csr": "csr content",
 "expiry_days": "20",
 "key_size": null,
 "name": "client1",
 "passphrase": "password@1234"
}
```

- Create a box
  Post: https://<VAULT_IP_or_FQDN>/vault/mtls/1.0/CreateBox
  Request payload:
  Copy

```
{
 "checkout_secapproval": {
  "access_window": 660,
  "approvers": [
   "approver1@domain.com",
   "approver2@domain.com"
  ],
  "min_approvals": 2,
  "request_expiry_window": 660,
  "whitelist_users": [
   "user@domain.com",
   "user2@domain.com"
  ]
 },
 "description": "ESXi Secrets Box",
 "exclusive_checkout": true,
 "lease": {
  "duration": "P3Y6M4DT12H30M5S",
```

```
  "renewable": true
 },
 "max_secret_versions": 5,
 "name": "box1",
 "rotation": {
  "duration": "P3Y6M4DT12H30M5S",
  "force": true,
  "on_checkin": true
 },
 "secret_duration": "P3Y6M4DT12H30M5S",
 "tags": {
  "hytrust": "security"
 }
}
```


- Create a secret
  Post: https://<VAULT_IP_or_FQDN>/vault/mtls/1.0/CreateSecret
  Request payload:
  Copy


```
{
 "box_id": "box1",
 "desc": "ESXi server 1 credentials",
 "exclusive_checkout": true,
 "expires_at": "2020-09-04T22:04:16.162848Z",
 "lease": {
  "duration": "P3Y6M4DT12H30M5S",
  "renewable": true
 },
 "name": "secret1",
 "rotation": {
  "duration": "P3Y6M4DT12H30M5S",
  "force": true,
  "on_checkin": true
 },
 "secret_config": {
  "ca_cert": "-----BEGIN CERTIFICATE-----
MIIEczCCA1ugAwIBAgIBADANBgkqhkiG9w0BAQQFADAkGA1UEBhMCR0IxEzARBgNVBAgTClNvbWUtU3RhdG
UxFDASBgNVBAoTC00EgTHRkMTcwNQYDVQQLEy5DbGFzcyAxIFB1YmxpYyBQcmltYXJ5IENlcnXRpb24gQXV0
aG9yaXR5MRQwEgYDVQQDEwtCZXN0IENBIEx0ZDAeFw0wMDTUwMTZaFw0wMTAyMDQxOTUwMTZaMIGH
MQswCQYDVQQGEwJHQjETMBEGA129tZS1TdGF0ZTEUMBIGA1UEChMLQmVzdCBDQSBMdGQxNzA1BgNVB
AsTLkDEgUHVibGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxFDAMTC0Jlc3QgQ0EgTHRkMIIBIjA
NBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgTz2mr7SZiAMfQyuvBjM9OiJjRazXBZ1BjP5CE/Wm/
```

Rr500PRK+Lh9x5eJ/ANBE0sTK0ZsDGMak2m1g7oruI3dY3VHqIxFTz0Ta1d+NAjwnLe4nOb7/
k05ShhBrJGBKKxb8n104o/
5p8HAsZPdzbFMIyNjJzBM2o5y5A13wiLitEfyYkQzaxCw0AwzIkVHilyCuaF4wj571pSzkv6sv+4IDMbT/
XpCo8L6wTash+etLD6FtTjYbbrvZ8RQM1tlKdoMHg2qxraAV+
+HNBYmNWs0duEdjUbJXl9TtnS4o1Ckj7POfljiQIDAQABo4HnMIHkMB0GA1UdDgQWBBQ8urMCRL5AkIp9NJHJ
w5TCBtAYDVR0jBIGsMIGpgBQ8urMCRLYYMHUKU5AkIp9NJHaSBijCBhzELMAkGA1UEBhMCR0IxEzARBgNVBA
gTCINvbWUtU3RhdGUxFDAoTC0Jlc3QgQ0EgTHRkMTcwNQYDVQQLEy5DbGFzcyAxIFB1YmxpYyBQcmENIcnR
pZmIjYXRpb24gQXV0aG9yaXR5MRQwEgYDVQQDEwtCZXN0IENBIEDAMBgNVHRMEBTADAQH/
MA0GCSqGSIb3DQEBBAUAA4IBAQC1uYBcsSncwADCsQer772C2ucpXxQUE/
C0pWWm6gDkwd5D0DSMDJRqV/
weoZ4wC6B73f5bLhGYHaXJeSD6KrXcoOwLdSaGmJYsILKZB3ZIDEp0wYTGhgteb6JFiTtnsf2xdrYfPCiIB7gBMAV
7Gzdc4VspS6ljrAhbiiawdBiQIQmsBeFz9JkF4b3I8BoGN+qMa56Ylt8una2gY4l2O//
on88r5IWJlm1L0oA8e4fR2yrBHXadsGeFKkyNrwGi/7vQMfXdGsRrXNGRGnX+vWDZ3/
zWI0joDtCkNnqEpVnHoX-----END CERTIFICATE-----",
"master_secret": {
"box_id": "b1",
"secret_id": "s1"
},
"tls_version": "1.2"
},
"secret_data": {
"host": "s1.esxi.hytrust.com",
"password": "Hytrust",
"uid": "root"
},
"secret_subtype_info": {
"info": {
"filename": "cacert.pem"
},
"type": "file"
},
"secret_type": "managed",
"tags": {
"hytrust": "security"
}
}

Creating Client Certificate

When you create a client certificate, it automatically creates a CA certificate.

1. Log into the Cryptographic Security Platform Vault for Secrets webGUI.

2. From the Home tab, select **Manage > Client Certificates**.
3. On the Manage Client Certificates page, click the **Create** button.
4. On the Create Client Certificate dialog box, complete the following:

Field	Description
Name	Enter the name for the client certificate.
Create for	Enter the name or group for whom the certificate is created.
Certificate Expiration	Enter the date the certificate will expire or accept the default of 1 year.
Certificate Signing Request (CSR)	Optionally click Browse and select the Certificate Signing Request.
Encrypt Certificate Bundle	Optionally choose to encrypt the certificate bundle. If selected, you will need to enter an encryption password and confirm it.
Access Policy	Select the access policy to associate with this client certificate.

5. Click **Create**.

Deleting the Client Certificate

1. Log into the Cryptographic Security Platform Vault for Secrets webGUI.
2. From the Home tab, select **Manage > Client Certificates**.
3. On the Manage Client Certificates page, select the client certificate that you want to delete.
4. Click the **Delete** button.
5. On the Delete Client Certificate screen, click **Delete**.

Downloading the Client Certificate

1. Log into the Cryptographic Security Platform Vault for Secrets webGUI.
2. From the Home tab, select **Manage > Client Certificates**.
3. On the Manage Client Certificates page, select the client certificate that you want to download.
4. Click **Download**.

The Cryptographic Security Platform Vault for Secrets webGUI downloads a zip bundle that contains the client certificate and the CA certificate.

Enabling or Disabling-mTLS Authentication

You can enable or disable mTLS from the Cryptographic Security Platform Vault for Secrets webGUI.

1. Log into the Cryptographic Security Platform Vault for Secrets webGUI.
2. At the top right of the vault page, click the Settings icon.
3. On the Settings page, click the mTLS tab.
4. Toggle the mTLS button to Enabled or Disabled.

5. Confirm your choice.

You can also use the UpdateVaultSettings API to enable mTLS. For example:

Copy

```
{
"degraded_mode_availability": true,
"mTLS_enabled": false,
"oidc_enabled": true,
"revision": 1
}
```

mTLS-Prerequisites

Before you can use mTLS APIs, you must complete the following:

- Enable mTLS on the Cryptographic Security Platform Vault for Secrets.
- Create and download the client certificate and the CA certificate. For more information, see Creating a client certificate.
  When you download the client certificate from the webGUI, the downloaded zip bundle contains both the client certificate and the CA certificate. For more information, see Downloading a client certificate.
  Note: If you want to use API commands, use the CreateClientCert API to create the certificate and the GetClientCertificateBundleInText API to download both the client certificate and the CA certificate.

Important: All APIs in the Cryptographic Security Platform Vault for Secrets can be used with mTLS except for login APIs. These include logging in or logging out with local authentication, AD, or OIDC, or renewing the authentication token.

Managing Secrets

On each individual box page, in the Secrets region, you can view all of your existing secrets, create, modify, or delete existing secrets, and perform various actions.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, click the box where you want to manage secrets.
3. On the Box page, in the Secrets region, click the **Create**, **Edit**, or **Delete** buttons to do one of the following:
   - Creating a Secret
   - Editing a Secret
   - Deleting a Secret
4. Select an existing secret and click the **Actions** button to do one of the following:
   - Checking Out a Managed Secret
   - Assigning Tags to a Secret
   - Removing Tags from a Secret
5. Select the Checked Out tag to delete the lease for any checked out secrets.

Viewing Static Secret

Note: Although static secrets do not have an explicit checkout option in the Cryptographic Security Platform Vault for Secrets webGUI, accessing a secret is referred to as a checkout in both the PASM CLI (`checkout-secret`) and the API (`CheckoutSecret`). So if you view the action in the audit log, the audit message will read that the secret was 'checked out' whether it is a managed or static secret.

To view a static secret as a vault user:

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Secrets**.
2. On the **Secrets** page, click the static secret that you want to view.
3. In the Secret window, click the eyeball icon to view the secret.
4. Click **Close** to close the window.

To view a static secret as an administrator:

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box that contains the secret that you want to view.
3. On the Box page, select the static secret that you want to view.
   The Secret Details page displays information about the secret.
4. Click the eyeball icon to view the secret.
5. Click **Close** to close the window.

Removing Tags from a Secret

You can remove any tags that were assigned to a secret.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, click the box that contains the secret from which you want to remove tags.
3. On the Box page, in the Secrets region, select the secret from which you want to remove tags.
4. Select **Actions > Remove Tags**.
5. In the Remove Tags window, select the tags that you want to remove and click **Remove**.

Importing a Secret

The Cryptographic Security Platform Vault for Secrets allows you to import secrets. We supply .csv files that will allow you to easily enter your information and import them.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to import a secret.
3. On the Box page, in the Secrets region, select **Actions > Import** Secrets.
4. In the About Importing Secrets section of the Import Secrets window, download the csv files for the types of secrets that you want to add. This can be one of the following:
   - ESXi Host template
   - SSH Key Template
   - Other Secrets Template

   You can use these template to create your import file, or create your own .csv file.
5. Create your import file.
6. In the Type of Secrets drop-down, select the secret type that you want to import. This can be one of the following:
   - ESXi Host
   - SSH Key
   - Other
     - Key-Value Pair
     - Password
     - Text

   Note: You cannot import a secret of type File.
7. Click **Browse** to locate the CSV file that you want to import and then click **Open**. You must pick a file that is the same type as the type of secret.
8. Click **Import**.
   The Import Summary window displays how many secrets were successfully read from the CSV.

Checking in a Secret

After a secret has been checked out, you must delete the lease to check it back in. For managed secrets, you can decide to simply delete the lease or force the secret to be rotated at the same time.

Note:

- You can only rotate managed secrets.
- Deleting the lease for a managed secret does not automatically rotate the secret. You need to click the Delete and Rotate button if you want the secret to be rotated.
- If you select Delete and Rotate for a secret without exclusive checkout, then all other current checkouts of the secret will be invalid. All users with that secret checked out will need to checkout the secret again.

Procedure

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Checkouts**.
2. Select the secret that you want to check back in.
3. Click **Delete Lease**.
4. On the Delete Secret Lease page, choose one of the following:
   - Click **Delete** to delete the lease and check in the secret without rotating. This is the only option for non-managed secrets.
   - Click **Delete and Rotate** to delete the lease and rotate the secret.

Note: You can also check in secrets from the Checked Out tab on the Box page that contains the secret.

Deleting a Secret

Note: When you delete a secret, ensure you remove the secret from any policy referencing the secret. If not, and a new secret is created using the same name, any policy still referencing the deleted secret will use the new secret automatically.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to delete a secret.
3. On the Box page, in the Secrets region, select the secret that you want to delete.
4. Click **Delete**.
5. In the confirmation screen, click **Delete**.

Editing a Secret

We recommend that you set secrets at the box level to ensure that they automatically apply to all of the secrets that you add to that box.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to modify a secret.
3. On the Box page, in the Secrets region, select the secret that you want to modify.
4. Click **Edit**.
5. In the About tab of the Edit Secret window, you can modify the following:

Option	Description
Description	The optional description of the secret.

Option	Description
Expires	Select one of the following: • Use Box Setting—Accepts the global box value. • No Expiration—The secret does not expire. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. Click the Checkout Details tab.
7. In the Checkout Details tab of the Edit Secret window, you can update the following:

Option	Description
Checkout Duration	How long the secret is checked out. By default, the Use Box Setting option is selected. • Use Box Setting—Use the duration set when creating the box. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.
Exclusive Checkout	If enabled, then the secret checkout will be exclusive and only one user can check out the secret at a time. However, if the checkout duration has expired, then a new checkout will be allowed. By default the Use Box Setting option is selected. • Use Box Setting—Use the value that was set when creating the box. • Yes—If set to Yes, the secrets checkout will be exclusive. • No—If set to No, multiple users can checkout the secret at the same time.

8. If you selected ESXi Hosts, click the Rotation Details tab.
9. In the Rotation Details tab of the Edit Secret window, you can update the following:

Option	Description
Rotation Duration	Sets the duration for this secret to be rotated. By default the Use Box Setting option is selected. • Use Box Setting—Use the duration set when creating the box. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.
Rotate on Check In	If enabled, the secret will automatically rotate when checked in. This requires that the checkout duration is set. By default the Use Box Setting option is selected. • Use Box Setting—Use the value that was set when creating the box. • Yes—If set to Yes, the secret will be rotated when it is checked in. • No—If set to No, the secret will not be rotated when it is checked in.
Force Rotation	If selected, this forces the rotation of all secrets in the box. • If Rotation Duration and Force Rotation are both checked, the secret will be rotated even if there are outstanding leases. • If Rotate on Check In and Force Rotation are both checked, the secret will rotate when the checkout expires. By default, the Use Box Setting option is selected. • Use Box Setting—Use the value that was set when creating the box. • Yes—If set to Yes, this forces the secret to rotate. • No—If set to No, the secret will not rotate.

10. Click **Save** to save your changes but remain in the wizard, **Save and Close** to save your changes and close the wizard, or **Cancel** to close the wizard without saving.

Creating a Secret

We recommend that you set secret parameters at the box level. Once set, you can ensure that those settings automatically apply to all of the secrets that you add to that box.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select the secret type and complete the information. The following secrets can be created:

Option	**Type**	Description
ESXi Host	Managed	Specify the secret for an ESXi host. This is a managed secret and you can set a rotation policy, instructing the Cryptographic Security Platform Vault for Secrets to rotate the secret periodically based on duration or on check in. For more information, see Creating an ESXi Host Secret.
File	Static	Upload a file containing a secret such as a key or certificate. For more information, see Creating a File Secret.
Key-Value Pair	Static	Create a secret containing one or more key-value pairs. For more information, see Creating a Key-Value Pair Secret.
Password	Static	Generate and store a password. You can specify your own password or use the provided password generator. Note: You can use the Cryptographic Security Platform Vault for Secrets password generator to generate a random password. The minimum length is 9 characters, and the maximum length is 64. Each password will contain at least 2 lowercase letters, 2 uppercase letters, 2 numbers, and 2 special characters. For more information, see Creating a Password Secret.
Text	Static	Plain text-based secret. For more information, see Creating a Text Secret.

Option	**Type**	Description
SSH Key	Managed	Upload and manage a SSH key. For more information, see About SSH Secrets . This is a managed secret and you can set a rotation policy, instructing the Cryptographic Security Platform Vault for Secrets to rotate the secret periodically based on duration or on check in. Note: The following algorithms are supported for SSH secrets: • ecdsa-sha2-nistp256 • ecdsa-sha2-nistp384 • ecdsa-sha2-nistp521 • rsa-sha2-256 • rsa-sha2-512 • rsa-2048 • rsa-4096 For more information, see Creating an SSH Secret.
P12	Static	Allows you to manage Public-Key Cryptography Standards (PKCS) files containing a collection of private key and certificate pairs. For more information, see Creating a P12 Secret.
Terraform	Managed	Allows you to manage User, Team, and Organization API tokens. This is a managed secret and you can set a rotation policy, instructing the Cryptographic Security Platform Vault for Secrets to rotate the secret periodically based on duration or on check in. For more information, see Creating a Terraform Secret.
Postgres	Managed	Allows you to manage Postgres and EnterpriseDB Postgres secrets with a password or certificate. This is a managed secret and you can set a rotation policy, instructing the Cryptographic Security Platform Vault for Secrets to rotate the secret periodically based on duration or on check in. For more information, see Creating a Postgres or EnterpriseDB Postgres Secret.

Option	**Type**	Description
Microsoft SQL Server	Managed	Allows you to manage Microsoft SQL Server credentials. This is a managed secret and you can set a rotation policy, instructing the Cryptographic Security Platform Vault for Secrets to rotate the secret periodically based on duration or on check in. For more information, see Creating a Microsoft SQL Server Secret.
AWS User	Managed	Allows you to manage AWS user credentials. This is a managed secret and you can set a rotation policy, instructing the Cryptographic Security Platform Vault for Secrets to rotate the secret periodically based on duration or on check in. For more information, see Creating an AWS User Credentials Secret.
Azure User	Managed	Allows you to manage Azure user credentials, such as access keys, secret access keys, and session tokens that are used to interact with Azure APIs and services. This is a managed secret and you can set a rotation policy, instructing the Cryptographic Security Platform Vault for Secrets to rotate the secret periodically based on duration or on check in. For more information, see Creating an Azure User Credentials Secret.

Creating an Azure User Credentials Secret

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **Azure User**.
5. On the About page of the Create Secret: Azure User wizard, complete the following:

Option	**Description**
Name	Enter the name to use for the secret.
Description	Enter the optional description for the secret.

Option	Description
Expires	Select one of the following: • Use Box Setting—Accepts the global box value. This is the default. • No Expiration—The secret does not expire. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. Click **Continue**.
7. On the Secret Details page of the Create Secret: Azure User wizard, complete the following:

Option	Description
Tenant ID	
Client ID	
Object ID	Optional.
Authentication Type	This can be Client Secret or Certificate.
Secret Key ID	Enter the key ID of the existing client secret or certificate currently active in your Azure App Registration.
Client Secret	If you selected Client Secret for the Authentication type, enter the client secret.
Client Certificate (PEM)	If you selected Certificate for the Authentication Type, click Browse to upload the certificate file in PEM format.
Private Key (PEM)	If you selected Certificate for the Authentication Type, click Browse to upload the private key file in PEM format.
Checkout Scope	This can be Azure Management API or Microsoft Graph API.

8. Click **Continue**.
9. On the Rotation Details page of the Create Secret: Azure User wizard, complete the following:

Option	Description
Rotation Duration	Sets the duration for this secret to be rotated. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.
Validity Days	

10. Click **Create**.

Creating an AWS User Credentials Secret

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **AWS User**.
5. On the About page of the Create Secret: AWS User wizard, complete the following:

Option	Description
Name	Enter the name to use for the secret.
Description	Enter the optional description for the secret.
Expires	Select one of the following: • Use Box Setting—Accepts the global box value. This is the default. • No Expiration—The secret does not expire. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. Click **Continue**.
7. On the Secret Details page of the Create Secret: AWS User wizard, complete the following:

Option	Description
Access Key ID	Enter the access key ID.

Option	Description
Access Key	Enter the access key.
Assumed Role	Enter the assumed role for this user.

8. Click **Continue**.
9. On the Checkout Details page of the Create Secret: AWS User wizard, complete the following:

Option	Description
Checkout Duration	How long the secret is checked out. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.
Exclusive Checkout	If enabled, then the secret checkout will be exclusive and only one user can check out the secret at a time. Users must wait for the checkout duration to expire or must manually delete the lease to make the secret available for new checkouts. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secrets checkout will be exclusive. • No—If set to No, multiple users can checkout the secret at the same time.

10. Click **Continue**.
11. On the Rotation Details page of the Create Secret: AWS User wizard, complete the following:

Option	Description
Rotation Duration	Sets the duration for this secret to be rotated. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.

Option	Description
Rotate on Check In	If enabled, the secret will automatically rotate when checked in. This requires that the checkout duration is set. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secret will be rotated when it is checked in. • No—If set to No, the secret will not be rotated when it is checked in.
Force Rotation	If selected, this forces the rotation of all secrets in the box. If Rotation Duration and Force Rotation are both checked, the secret will be rotated even if there are outstanding leases. If Rotate on Check In and Force Rotation are both checked, the secret will rotate when the checkout expires. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, this forces the secret to rotate. • No—If set to No, the secret will not rotate.

12. Click **Create**.

Creating a Microsoft SQL Server Secret

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **Microsoft SQL Server**.
5. On the About page of the Create Secret: Microsoft SQL Server wizard, complete the following:

Option	Description
Name	Enter the name to use for the secret.
Description	Enter the optional description for the secret.

Option	Description
Is a Master Secret?	Master secrets are secrets that can be referenced by other secrets. They are primarily used to manage credentials for other systems. Check the checkbox if this secret will be used as a master secret.
Expires	Select one of the following: • Use Box Setting—Accepts the global box value. This is the default. • No Expiration—The secret does not expire. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. Click **Continue**.
7. On the Secret Details page of the Create Secret: Microsoft SQL Server wizard, complete the following:

Option	Description
Server	Enter the hostname or IP address for the server.
User Name	Enter the user name used to log into the server.
Password	Enter the password for the server.
Authentication Type	Enter the authentication type that you want to use. This can be one of the following: • SQL Server—Uses the name and password stored in MS SQL Server. • Contained Database—Uses database-specific users with passwords, independent of server login.
Port	Enter the port used for the server.
Database	If you selected Contained Database for the authentication type, enter the database name.
Trust Server Certificate	Check the checkbox if you want to trust this server's certificate. We recommend that you do not use this for production environments.

Option	Description
Encrypt	Choose how you want to encrypt this server. This can be one of the following: • Yes • No • Optional • Strict
Server Certificate	Click Add Certificate to paste the server certificate to use while connecting.

8. Click **Continue**.
9. On the Checkout Details page of the Create Secret: Microsoft SQL Server wizard, complete the following:

Option	Description
Checkout Duration	How long the secret is checked out. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.
Exclusive Checkout	If enabled, then the secret checkout will be exclusive and only one user can check out the secret at a time. Users must wait for the checkout duration to expire or must manually delete the lease to make the secret available for new checkouts. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secrets checkout will be exclusive. • No—If set to No, multiple users can checkout the secret at the same time.

10. Click **Continue**.
11. On the Rotation Details page of the Create Secret: Microsoft SQL Server wizard, complete the following:

Option	Description
Rotation Duration	Sets the duration for this secret to be rotated. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.
Rotate on Check In	If enabled, the secret will automatically rotate when checked in. This requires that the checkout duration is set. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secret will be rotated when it is checked in. • No—If set to No, the secret will not be rotated when it is checked in.
Force Rotation	If selected, this forces the rotation of all secrets in the box. If Rotation Duration and Force Rotation are both checked, the secret will be rotated even if there are outstanding leases. If Rotate on Check In and Force Rotation are both checked, the secret will rotate when the checkout expires. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, this forces the secret to rotate. • No—If set to No, the secret will not rotate.

12. Click **Continue**.
13. On the Master Secret page of the Create Secret: Microsoft SQL Server wizard, if you are using a master secret to rotate this secret, complete the following:

Option	Description
Box	Select the box that contains the master secret that you want to use.

Option	Description
Secret	Select the name of the master secret that is used to rotate this secret.

14. Click **Create**.

Creating a Postgres or EnterpriseDB Postgres Secret

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **Postgres**.
5. On the About page of the Create Secret: Terraform wizard, complete the following:

Option	Description
Name	Enter the name to use for the secret.
Description	Enter the optional description for the secret.
Expires	Select one of the following: • Use Box Setting—Accepts the global box value. This is the default. • No Expiration—The secret does not expire. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. Click **Continue**.
7. On the Secret Details page of the Create Secret: Postgres wizard, complete the following:
   For Password-based:

Option	Description
Authentication Mode	Choose Password-based.
Host and Port	Enter the Postgres database hostname or IP address and the database port.
SSL Mode	Choose the type of SSL connection to use.
Database Name	Enter the name of your Postgres database.

Option	Description
Username	Enter the username.
Password	Enter the password for this user.
CA Certificate	Click Add Certificate to specify the CA certificate to use while connecting to the database. After you add the CA certificate, there is a link to modify it.

For Certificate-based:

Option	Description
Authentication Mode	Choose Certificate-based.
Host and Port	Enter the Postgres database hostname or IP address and the database port.
SSL Mode	Choose the type of SSL connection to use.
Database Name	Enter the name of your Postgres database.
Username	Enter the username.
Client Certificate	Click Add Certificate to specify the Client certificate.
Client Key	Click Add Client Key to specify the client key.
CA Certificate	Click Add Certificate to specify the CA certificate.
Postgres Host Information	
Postgres Config Path	Enter the path to the Postgres configuration file.
SSH	
Host Name	Enter the Postgres hostname or IP address.

Option	Description
Username	Enter the username.
Authentication Mode	Select whether to use password-based or private key. For password-based, enter the password, the Postgres database port, and choose whether or not to run as Sudo. For private key, upload the private key that you want to use, then enter the passphrase, the Postgres database port, and choose whether or not to run as Sudo.
CA Host Information	
OpenSSLConfig Path	Enter the path to the OpenSSL configuration file.
SSH	
Host Name	Enter the Postgres hostname or IP address.
Username	Enter the username.
Authentication Mode	Select whether to use password-based or private key. For password-based, enter the password, the Postgres database port, and choose whether or not to run as Sudo. For private key, upload the private key that you want to use, then enter the passphrase, the Postgres database port, and choose whether or not to run as Sudo.
Client Certificate DN Information	
Country	Optional. Enter the country.
State	Optional. Enter the state.
Locality	Optional. Enter the locality.

Option	Description
Organization	Enter the organization.
Organizational Unit	Enter the organizational unit.

8. Click **Continue**.
9. On the Checkout Details page of the Create Secret: Postgres wizard, complete the following:

Option	Description
Checkout Duration	How long the secret is checked out. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.
Exclusive Checkout	If enabled, then the secret checkout will be exclusive and only one user can check out the secret at a time. Users must wait for the checkout duration to expire or must manually delete the lease to make the secret available for new checkouts. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secrets checkout will be exclusive. • No—If set to No, multiple users can checkout the secret at the same time.

10. Click **Continue**.
11. On the Rotation Details page of the Create Secret: Postgres wizard, complete the following:

Option	Description
Rotation Duration	Sets the duration for this secret to be rotated. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.

Option	Description
Rotate on Check In	If enabled, the secret will automatically rotate when checked in. This requires that the checkout duration is set. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secret will be rotated when it is checked in. • No—If set to No, the secret will not be rotated when it is checked in.
Force Rotation	If selected, this forces the rotation of all secrets in the box. If Rotation Duration and Force Rotation are both checked, the secret will be rotated even if there are outstanding leases. If Rotate on Check In and Force Rotation are both checked, the secret will rotate when the checkout expires. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, this forces the secret to rotate. • No—If set to No, the secret will not rotate.

12. Click **Create**.

Creating a Terraform Secret

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **Terraform**.
5. On the About page of the Create Secret: Terraform wizard, complete the following:

Option	Description
Name	Enter the name to use for the secret.
Description	Enter the optional description for the secret.

Option	Description
Expires	Select one of the following: • Use Box Setting—Accepts the global box value. This is the default. • No Expiration—The secret does not expire. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. Click **Continue**.
7. On the Secret page of the Create Secret: Terraform wizard, complete the following:

Option	Description
Token	Enter the API token in plain text.
Type	The type of API token. Select one of the following: • Users • Teams • Organizations

8. Click **Continue**.
9. On the Checkout Details page of the Create Secret: Terraform wizard, complete the following:

Option	Description
Checkout Duration	How long the secret is checked out. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.

Option	Description
Exclusive Checkout	If enabled, then the secret checkout will be exclusive and only one user can check out the secret at a time. Users must wait for the checkout duration to expire or must manually delete the lease to make the secret available for new checkouts. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secrets checkout will be exclusive. • No—If set to No, multiple users can checkout the secret at the same time.

10. Click **Continue**.
11. On the Rotation Details page of the Create Secret: Terraform wizard, complete the following:

Option	Description
Rotation Duration	Sets the duration for this secret to be rotated. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.
Rotate on Check In	If enabled, the secret will automatically rotate when checked in. This requires that the checkout duration is set. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secret will be rotated when it is checked in. • No—If set to No, the secret will not be rotated when it is checked in.

Option	Description
Force Rotation	If selected, this forces the rotation of all secrets in the box. If Rotation Duration and Force Rotation are both checked, the secret will be rotated even if there are outstanding leases. If Rotate on Check In and Force Rotation are both checked, the secret will rotate when the checkout expires. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, this forces the secret to rotate. • No—If set to No, the secret will not rotate.

12. Click **Create**.

Creating a P12 Secret

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **P12**.
5. In the Create Secret: P12 dialog box, complete the following:

Option	Description
Name	Enter the name of secret.
Description	Enter a description for the secret.
Secret Expiration (under Advanced Settings)	Optional. Select one of the following: • No Expiration—The secret does not expire. This is the default. • Use Box Setting—Accepts the global box value. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. For each Private Key / Certificate Pair, enter the following:

Option	Description
Name	Enter the name of secret.

Option	Description
Profile ID	Enter the profile ID for the private key / certificate pair.
Description	Enter a description for the private key / certificate pair.
Private Key	Click Browse and select the private key that you want to upload.
Private Key Password	Enter the password for the private key / certificate pair.
Certificate	Click Browse and select the certificate that you want to upload. Click the plus sign (+) to upload an additional certificate.

7. Optionally click **Add another Private Key / Certificate Pair** to add additional private key / certificate pairs.
8. When you are finished, click **Create**.

Creating an SSH Secret

Before You Begin

Before you can create SSH secrets, you must have the following:

- A remote server with a user that is not the Vault user with permissions to log on to the remote server using their private SSH key.
- The user name and IP address of the remote server.
- An available public and private SSH key pair.
  - The public key of the SSH key pair must be copied to both the server in the user's **.ssh/ authorized_keys** file and the box where the SSH secret will be created.
    You can copy the public key using the command `ssh-copy-id`. This allows the user to log on to the server without a password.
  - A copy of the private key is required to configure the SSH secret in the Cryptographic Security Platform Vault for Secrets.

Procedure

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **SSH Key**.
5. On the About page of the Create Secret: SSH Key wizard, complete the following:

Option	Description
Name	Enter the name to use for the SSH secret.

Option	Description
Description	Enter the optional description for the SSH secret.
Expires	Select one of the following: • Use Box Setting—Accepts the global box value. This is the default. • No Expiration—The secret does not expire. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. Click **Continue**.
7. On the Secret page of the Create Secret: SSH Key wizard, complete the following:

Option	Description
Host	Enter the host name or IP address for the remote server.
User Name	Enter a user name. This name must match the user name used to log on to the remote server.
Port	Enter the port for the remote server.
Upload Private Key	Click Browse to upload the private key.
Passphrase	If the private key is encrypted, enter the password to decrypt the private key.

8. Click **Continue**.
9. On the Checkout Details page of the Create Secret: SSH Key wizard, complete the following:

Option	Description
Checkout Duration	How long the secret is checked out. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.

Option	Description
Exclusive Checkout	If enabled, then the secret checkout will be exclusive and only one user can check out the secret at a time. Users must wait for the checkout duration to expire or must manually delete the lease to make the secret available for new checkouts. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secrets checkout will be exclusive. • No—If set to No, multiple users can checkout the secret at the same time.

10. Click **Continue**.
11. On the Rotation Details page of the Create Secret: SSH Key wizard, complete the following:

Option	Description
Rotation Duration	Sets the duration for this secret to be rotated. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.
Rotate on Check In	If enabled, the secret will automatically rotate when checked in. This requires that the checkout duration is set. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secret will be rotated when it is checked in. • No—If set to No, the secret will not be rotated when it is checked in.

Option	Description
Force Rotation	If selected, this forces the rotation of all secrets in the box. If Rotation Duration and Force Rotation are both checked, the secret will be rotated even if there are outstanding leases. If Rotate on Check In and Force Rotation are both checked, the secret will rotate when the checkout expires. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, this forces the secret to rotate. • No—If set to No, the secret will not rotate.

12. Click **Create**.

What to Do Next

- If you are using local authentication, add the user. See Creating CSP Vault for Secrets Local Users. The user name must match the name used to log on to the remote server.
- Ensure that the user is added to the access policy so that they can access both the Cryptographic Security Platform Vault for Secrets and the box where the secret is stored. See CSP Vault for Secrets Access Policies.

Logging on to remote server using SSH Secret

This topic explains how users log on to their remote server using their SSH secret.

During configuration of an SSH key secret in the vault, a port value is automatically added and mapped to the secret. The port value specifies the remote server.

To log on to the remote server with their secret, users specify their vault credentials together with the port, as detailed below.

How to view the port mapped to the secret using the GUI

To see the port number mapped to the secret using the GUI.

1. Log on to your Cryptographic Security Platform Vault for Secrets webGUI
2. Depending on your role:
   a. If you are an admin, select **Manage > Manage Boxes**.
   b. If you are non-admin, select **Managed Secrets**.
3. Click on the name of the relevant secret.
   The secret details are displayed.
4. Note the port shown in the secret details.

How to view the port mapped to the secret using the CLI

To see the port number mapped to the secret using the CLI.

1. Log on to the PASM CLI
2. To see the secret details run `pasmcli get-secret`.
   The secret details are displayed.

3. Note the `proxy_port` value.

To log on to the remote server using the secret

To log on to the remote server, you specify your vault user name, the vault IP address and the port mapped to the secret (which defines the remote server).

1. Log on to the remote sever:
   `ssh -l <vault-user-name> <vault-ip-address> -p <port-number>`

Note:

- The SSH session remains live even if the lease of the secret expires in during the duration of the session.
- If an SSH secret expires during an active SSH session, the session continues as a standard SSH session despite the SSH secret expiry. After the active SSH session is terminated, any further attempts to use the SSH secret will fail.

When you log out of the SSH session, ensure the SSH secret is checked back in using either the CLI or GUI if a lease is created for the corresponding SSH secret checkout. If you do not check in the SSH secret and exclusive checkout is configured, other users are not able to use the secret until is checked back in or the lease expires.

About SSH Secrets

You can add Secure Shell (SSH) private keys as secrets to your Cryptographic Security Platform Vault for Secrets. This allows you to access a server via SSH using the secret.

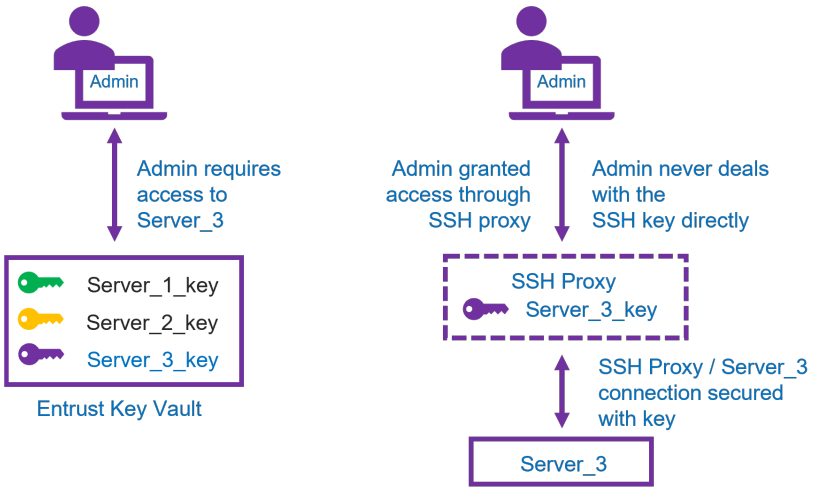
Each SSH secret is set up with a port through which the Cryptographic Security Platform Vault for Secrets proxy connection is established. Please note:

- The Cryptographic Security Platform Vault for Secrets ensures that two ports are never assigned to the same SSH secret.
- A Cryptographic Security Platform Vault for Secrets cluster can accommodate up to 6k SSH secrets.

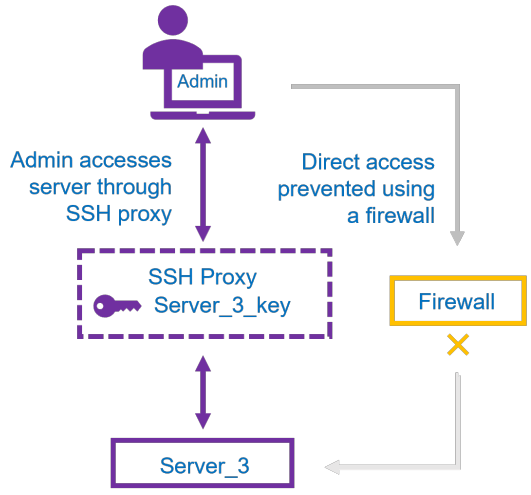
SSH secrets support the following algorithms:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- rsa-sha2-256
- rsa-sha2-512
- rsa-2048
- rsa-4096

Along with the SSH private key, you define the user and server details. You also define the access policy for the user for the relevant Cryptographic Security Platform Vault for Secrets. When you configure the SSH private key secret, you specify the host (IP), user (on the VM), and you upload the SSH private key (the same private key used to access the VM directly). You can then log on to your Cryptographic Security Platform Vault for Secrets to confirm the details and access the server using the SSH key secret.



For additional security and to protect important assets, you can restrict access, so it is only possible for the user to access the server using their SSH secret. For example:



Once configured, users/admins access their VMs using the Cryptographic Security Platform Vault for Secrets. Users log on to their remote VM through their vault, using the vault IP, the vault user name and the port specified in the SSH secret. The port is specific to the VM.

Users with access to many VMs over SSH can log on to all their VMs using their vault IP and vault user name, and simply change the port to specify the VM.

- For details on creating and configuring SSH secrets, see Creating an SSH Secret.
- For details on how users log on to remote servers using their SSH secret, see Logging on to remote server using SSH Secret.

Creating a Text Secret

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **Text**.
5. In the Create Secret: Text dialog box, complete the following:

Option	Description
Name	Enter the name of secret.
Description	Enter a description for the secret.
Secret Data	Enter the plain text secret.
Secret Expiration (under Advanced Settings)	Optional. Select one of the following: • No Expiration—The secret does not expire. This is the default. • Use Box Setting—Accepts the global box value. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. Click **Create**.

Creating a Password Secret

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **Password**.
5. In the Create Secret: Password dialog box, complete the following:

Option	Description
Name	Enter the name of secret.
Description	Enter a description for the secret.
Password	Enter your password or use the password generator to create one.

Option	Description
Secret Expiration (under Advanced Settings)	Optional. Select one of the following: • No Expiration—The secret does not expire. This is the default. • Use Box Setting—Accepts the global box value. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. Click **Create**.

Creating a Key-Value Pair Secret

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **Key-Value Pair**.
5. In the Create Secret: Key-Value Pair dialog box, complete the following:

Option	Description
Name	Enter the name of secret.
Description	Enter a description for the secret.
Key	Enter the key name.
Value	Enter the key value.
Secret Expiration (under Advanced Settings)	Optional. Select one of the following: • No Expiration—The secret does not expire. This is the default. • Use Box Setting—Accepts the global box value. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

Note: You can enter multiple key-value pairs.

6. Click **Create**.

Creating a File Secret

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **File**.
5. In the Create Secret: File dialog box, complete the following:

Option	Description
Name	Enter the name of the secret
Description	Enter a description for the secret
Upload File	Click Browse and select the file that you want to upload.
Secret Expiration (under Advanced Settings)	Optional. Select one of the following: • No Expiration—The secret does not expire. This is the default. • Use Box Setting—Accepts the global box value. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. Click **Create**.

Creating an ESXi Host Secret

Due to a limitation on the ESXi server, creating an ESXi host secret may fail with an "unable to connect" error. If this happens, check whether your ESXi server supports EMS. If it does, enable EMS in the Cryptographic Security Platform Vault appliance and retry. If your ESXi server does not support EMS, disable it.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box where you want to create a secret.
3. On the Box page, in the Secrets region, click **Add**.
4. In the Choose a type of secret to create dialog box, select **ESXi Host**.
5. On the About page of the Create Secret: ESXi Host wizard, complete the following:

Option	Description
Name	Enter the name to use for the secret.
Description	Enter the optional description for the secret.
Expires	Select one of the following: • Use Box Setting—Accepts the global box value. This is the default. • No Expiration—The secret never expires. • Specific Date and Time—Allows you to set the specific date and time for the secret to expire.

6. Click **Continue**.
7. On the Secret page of the Create Secret: ESXi Host wizard, complete the following:

Option	Description
Host	Enter the ESXi host address.
User Name	Enter the ESXI host user name.
Password	Enter the ESXi host password.
TLS Version	Select the TLS version used by the ESXi host.
CA Certificate	Click Add Certificate to specify the CA certificate to use while connecting to an ESXi host. After you add the CA certificate, you can modify it using the link.

8. Click **Continue**.
9. On the Checkout Details page of the Create Secret: ESXi Host wizard, complete the following:

Option	Description
Checkout Duration	How long the secret is checked out. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.
Exclusive Checkout	If enabled, the secret checkout will be exclusive, and only one user can check out the secret at a time. Users must wait for the checkout duration to expire or must manually delete the lease to make the secret available for new checkouts. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secret checkout will be exclusive. • No—If set to No, multiple users can check out the secret at the same time.

10. Click **Continue**.

11. On the Rotation Details page of the Create Secret: ESXi Host wizard, complete the following:

Option	Description
Rotation Duration	Sets how often this secret is rotated. • Use Box Setting—Use the duration set when creating the box. This is the default. • Duration—Enter a duration in days, minutes, or hours. This value will overwrite the box settings.
Rotate on Check In	If enabled, the secret will automatically rotate when checked in. This requires a checkout duration to be set. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, the secret will be rotated when it is checked in. • No—If set to No, the secret will not be rotated when it is checked in.
Force Rotation	If selected, this forces the rotation of all secrets in the box. If Rotation Duration and Force Rotation are both checked, the secret will be rotated even if there are outstanding leases. If Rotate on Check In and Force Rotation are both checked, the secret will rotate when the checkout expires. • Use Box Setting—Use the value that was set when creating the box. This is the default. • Yes—If set to Yes, this forces the secret to rotate. • No—If set to No, the secret will not rotate.

12. Click **Create**.

Checking-Out a Managed Secret

Managed secrets must be checked out in order to view.

To check out a managed secret as a vault user:

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Secrets**.
2. On the **Secrets** page, click the managed secret that you want to check out.

3. In the Secret window, click **Check Out**.
   The Successfully Checked Out Secret window displays the date and time the lease expires (if applicable), and the data contained in the secret.
4. Click **Close** to close the window.

Checked out managed secrets can be viewed by selecting Checkouts from the Cryptographic Security Platform Vault for Secrets webGUI.

To check out a managed secret that has secondary approval:

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Secrets**.
2. On the **Secrets** page, click the managed secret that you want to check out.
3. In the Secret window, click **Check Out**.
   The Secret Details page displays a warning that secondary approval is enabled. Click **submit request** in the warning text.
4. In the Request to Check Out Secret window, click **Submit Request**.

To check out a managed secret as an administrator:

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box that contains the secret that you want to check out.
3. On the Box page, select the secret that you want to check out.
4. Select **Actions > Check Out**.
   The Successfully Checked Out Secret window displays the date and time the lease expires (if applicable), and the data contained in the secret.

Checked out secrets can be viewed in the Checked Out tab on the Box page or by selecting Checkouts from the Cryptographic Security Platform Vault for Secrets webGUI.

Assigning Tags to a Secret

You can assign one or more tags to a selected secret.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, click the box that contains the secret where you want to add tags.
3. On the Box page, in the Secrets region, select the secret where you want to add tags.
4. Select **Actions > AddTags**.
5. In the Add Tag window, enter the name and value for the tag and click **Add**.

Accessing Secrets

You can view both managed secrets and static secrets in the Cryptographic Security Platform Vault for Secrets webGUI. Managed secrets include ESXi hosts and ssh keys. Static keys can be a file, key-value pair, password, or text.

For more information, see:

- Checking Out a Managed Secret
- Viewing a Static Secret

Checking Out a Managed Secret

Managed secrets must be checked out in order to view.

To check out a managed secret as a vault user:

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Secrets**.
2. On the **Secrets** page, click the managed secret that you want to check out.

3. In the Secret window, click **Check Out**.
   The Successfully Checked Out Secret window displays the date and time the lease expires (if applicable), and the data contained in the secret.
4. Click **Close** to close the window.

Checked out managed secrets can be viewed by selecting Checkouts from the Cryptographic Security Platform Vault for Secrets webGUI.

To check out a managed secret that has secondary approval:

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Secrets**.
2. On the **Secrets** page, click the managed secret that you want to check out.
3. In the Secret window, click **Check Out**.
   The Secret Details page displays a warning that secondary approval is enabled. Click **submit request** in the warning text.
4. In the Request to Check Out Secret window, click **Submit Request**.

To check out a managed secret as an administrator:

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box that contains the secret that you want to check out.
3. On the Box page, select the secret that you want to check out.
4. Select **Actions > Check Out**.
   The Successfully Checked Out Secret window displays the date and time the lease expires (if applicable), and the data contained in the secret.

Checked out secrets can be viewed in the Checked Out tab on the Box page or by selecting Checkouts from the Cryptographic Security Platform Vault for Secrets webGUI.

Viewing a Static Secret

> Note: Although static secrets do not have an explicit checkout option in the Cryptographic Security Platform Vault for Secrets webGUI, accessing a secret is referred to as a checkout in both the PASM CLI (`checkout-secret`) and the API (`CheckoutSecret`). So if you view the action in the audit log, the audit message will read that the secret was 'checked out' whether it is a managed or static secret.

To view a static secret as a vault user:

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Secrets**.
2. On the **Secrets** page, click the static secret that you want to view.
3. In the Secret window, click the eyeball icon to view the secret.
4. Click **Close** to close the window.

To view a static secret as an administrator:

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box that contains the secret that you want to view.
3. On the Box page, select the static secret that you want to view.
   The Secret Details page displays information about the secret.
4. Click the eyeball icon to view the secret.
5. Click **Close** to close the window.

Managing Boxes

On the Manage Boxes page, you can view all of your existing boxes, create, modify, or delete existing boxes, and perform various actions. If you click an individual box, you can view all details for that box.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.

2. On the **Manage Boxes** page, click the **Create**, **Edit**, or **Delete** buttons to do one of the following:
    - Creating a Box
    - Editing an Existing Box
    - Deleting a Box
3. Select an existing box and click the **Actions** button to do one of the following:
    - Rotate All Secrets in a Box
    - Remove Rotation
    - Adding Tags to a Box
    - Removing Tags from a Box
4. Click a box to view the Box page for that box. This page displays all of the details of the box, the secrets contained in the box, and any expired leases for secrets. From the box page, you can perform all of the tasks from the Manage Boxes page.

Removing Tags from a Box

You can remove any tags that were assigned to a box.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box or boxes from which you want to remove tags.
3. Select **Actions > Remove Tags**.
4. In the Remove Tags window, select the tags that you want to remove and click **Remove**.

Adding Tags to a Box

You can add one or more tags to a box.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box or boxes that you want to tag.
3. Select **Actions > Add Tags**.
4. In the Add Tag window, enter the name and value for the tag and click **Add**.

Remove Rotation

This removes all metadata info of the rotation job that was initiated on the selected box.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box or boxes where you want to remove the last rotation data.
3. Select **Actions > Remove Rotation**.
4. In the Rotate All Secrets window, click **Remove**.

Rotate All Secrets in a Box

This allows you to rotate all of the managed secrets within the selected boxes immediately.

Note: If a secret has any outstanding checkouts, the leases will be deleted.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box or boxes where you want to rotate the managed secrets.
3. Select **Actions > Rotate All Secrets**.
4. In the Rotate All Secrets window, click **Rotate Now**.

Editing an Existing Box

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box that you want to modify and click **Edit**.

3. In the About tab of the Edit Box window, you can update the following:

Option	Description
Description	The optional description of the box.
Secret Versions	The maximum number of a secret's versions to keep before they are deleted. The default is 10, and the maximum is 100.
Secret Expiration	If checked, then you can set the number of days, minutes, or hours before the secret expires. Otherwise there is no expiration date for the secrets.

4. Click the Checkout Details tab.
5. In the Checkout Details tab of the Edit Box window, you can update the following:

Option	Description
Secret Checkout Duration	If checked, then you can set a default duration for a secret lease. When set at the box level, it applies to all secrets that are checked out from a box. Otherwise, there is no expiration for checked out secrets and a lease is not created. Important: If this option is set in a secret, it will override any options that are set in the box.
Exclusive Checkout	If checked, then all secret checkouts will be exclusive and only one user can check out the secret at a time. However, if the checkout lease has expired, then a new checkout will be allowed. Important: If this option is set in a secret, it will override any options that are set in the box.

6. Click the Rotation Details tab.
7. In the Rotation Details tab of the Edit Box window, you can update the following:

Option	Description
Secret Rotation Duration	If checked, then you can set the default duration for when secrets in the box will be rotated. Important: If this option is set in a secret, it will override any options that are set in the box.
Rotate Secret on Check In	If checked, the secret will be automatically rotated when it is checked in. Requires that the Secret Checkout Duration is configured.
Force Secret Rotation	If checked, it forces the rotation of all secrets in the box. • If Secret Rotation Duration and Force Secret Rotate on Check In are both checked, the secret will be rotated even if there are outstanding leases. • If Rotate on Check In and Force Secret Rotation are both checked, the secret will rotate when the checkout expires. Important: If this option is set in a secret, it will override any options that are set in the box.

8. Click **Save** to save your changes but remain in the wizard, **Save and Close** to save your changes and close the wizard, or **Cancel** to close the wizard without saving.

Deleting a Box

Deleting a box will also delete all secrets that are in the box.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, select the box or boxes that you want to remove.
3. Click the **Delete** button.
4. In the confirmation screen, click **Delete**.

Creating a Box

Create a box in your Cryptographic Security Platform Vault for Secrets to store all of your secrets. Many of the options can be set in both the box and the secret, and the secret always takes precedence. We recommend that you set these options in the box so they will automatically apply to all of the secrets that you add.

Beginning with version 10.4.1, you can now enable Secondary Approval when you create a box. All secrets in that box will automatically require Secondary Approval before they can be checked out.

1. From the Cryptographic Security Platform Vault for Secrets webGUI, select **Manage > Manage Boxes**.
2. On the **Manage Boxes** page, click the **Create** button.
   Note: If there are no existing boxes, you can also click the **Add a Box Now** link on the **Manage Boxes** page.
3. In the About tab of the Create a Box window, complete the following:

Option	Description
Name	The name of the box.
Description	The optional description of the box.
Secret Versions	The maximum number of a secret's versions to keep before they are deleted. The default is 10, and the maximum is 100.
Secret Expiration	If checked, then you can set the number of days, hours, or minutes before the secret expires. Otherwise there is no expiration date for the secrets.

4. Click **Continue**.
5. In the Checkout Details tab of the Create a Box window, complete the following:

Option	Description
Secret Checkout Duration	If checked, then you can set a default duration for a secret lease. When set at the box level, it applies to all secrets that are checked out from a box. Otherwise, there is no expiration for checked out secrets and a lease is not created. Important: If this option is set in a secret, it will override any options that are set in the box.
Exclusive Checkout	If checked, then all secret checkouts will be exclusive and only one user can check out the secret at a time. However, if the checkout lease has expired, then a new checkout will be allowed. Important: If this option is set in a secret, it will override any options that are set in the box.

6. Click **Continue**.
7. In the Rotation Details tab of the Create a Box window, complete the following:

Option	Description
Secret Rotation Duration	If checked, then you can set the default duration for when secrets in the box will be rotated. Important: If this option is set in a secret, it will override any options that are set in the box.
Rotate Secret on Check In	If checked, the secret will be automatically rotated when it is checked in. This option requires that the Secret Checkout Duration is configured.
Force Secret Rotation	If checked, this option forces the rotation of all secrets in the box. • If Secret Rotation Duration and Force Secret Rotate on Check In are both checked, the secret will be rotated even if there are outstanding leases. • If Rotate Secret on Check In and Force Secret Rotation are both checked, the secret will rotate when the checkout expires. Important: If this option is set in a secret, it will override any options that are set in the box.

8. Click **Continue**.
9. In the Secondary Approval tab of the Create a Box window, complete the following:

Option	Description
Enable Secondary Approval	If checked, all secrets in the box require Secondary Approval before they can be checked out. Important: You must have at least one user with the Vault Checkout Secondary Approver Policy access policy before you can enable Secondary Approval.
Approvers	Enter the email addresses for one or more people to be secondary approvers. These users must have the Vault Checkout Secondary Approver Policy access policy.

Option	Description
Minimum Approvals	The minimum number of approvals needed before the checkout can be performed. This value must be equal or greater to the number of approvers that you entered.
Approval Expiration	The amount of time after a checkout is requested that the approvers must approve the request. For example, if the request is made at 12:00 pm, and this value is set to 20 minutes, then at 12:21 the request will no longer be valid.
Time to Use	The amount of time that a requester can check out secrets once the minimum number of approvals has been met. For example, if this is set to 20 minutes, and the minimum approvals is met at 12:20 PM, then the requester has until 12:40 to check out the secret.
Whitelist Users	Whitelist users do not require secondary approval, and can check out secrets without raising secondary approval requests.

10. Click **Create**.

Managing Authentication for Vault for Secrets

By default each vault is configured for local authentication. You can change the authentication method as required. In the current release, you can choose between local authentication, Active Directory, OpenID Connect (OIDC) with AD, or OIDC without AD.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users.

For details on configuring each authentication option, see:

- Configuring local authentication for Vault for Secrets
- Configuring Active Directory for the Vault for Secrets
- Configuring OIDC with Active Directory for Vault for Secrets
- Configuring OIDC for Vault for Secrets
- Managing two-factor authentication in Vault for Secrets

Configuring local authentication for Vault for Secrets

Local authentication is enabled by default when you create a vault. If using local authentication, no further authentication configuration is required. The next step is to configure your access policies and users.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users

Configuring Active Directory for the Vault for Secrets

See below for configuring Active Directory for the Vault for Secrets.

> By default, the vault uses local authentication. You can change the authentication method as required.

To configure Active Directory

1. Log in to the CSP Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. On the Authentication page, select **LDAP** as the Authentication Type.
5. On the **Domain** tab, enter:
   - Domain Name—Enter the domain name for the service account.
   - Directory Service Type—Select **Microsoft AD** if you plan to use Microsoft AD directory services, or **OpenLDAP** for all non-Microsoft AD directory services.
   - Service Account Name—Enter the name of the service account for the given domain (for example, Administrator).

     > The service account needs read-only access to users and groups on the domain and any subdomain used.

   - Service Account Password —Enter the password for the service account.
   - UID Attribute—Enter the Security Manager Account Name (sAMAccountName) for the user.

     > This is the attribute of the user or group object that would be queried during search.

6. Click **Apply** to save the changes.
7. Click the **Domain Controllers** tab.
8. Click **+**
9. Add the following details in the **Add Domain Controller** window.
   - Server URL
   - STARTTLS
   - CA Certificate
   - User Search Context (Base DN)
   - Group Search Context (Base DN)
   - Timeout
10. Click **Save and Close**.

Server URL

Select LDAP or LDAPS and enter the domain name or IP address. To include a port number, use the following syntax:

```
<ip>:<port>
```

STARTTLS

If you selected LDAP, check the checkbox if you want to use LDAP over TLS.

CA Certificate

The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller.

- The CA certificate must be in Base64-encoded PEM format.
- If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates.

Click Load File to select the CA certificate that you want to use.

User Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the user search should start. For performance reasons, make the base DN as specific as possible. For example:

```
dc=ldapserver,dc=com
```

This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP.

Group Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the search for Security groups should start.

This option applies to AD Security groups being associated with an admin group.

Timeout

Set the timeout in seconds before connecting to an alternate domain controller.

- If multiple domain controllers are specified, this is how long the Cryptographic Security Platform Vault waits for a response before re-sending the request to another domain controller.
- If the DNS server is down, Cryptographic Security Platform Vault may take longer than the time specified here before it fails over to the next domain controller in the list or considers the authentication request failed.

This option only applies to the TCP/LDAP request. It does not apply to the DNS request before the LDAP server has been successfully contacted.

Configuring OIDC with Active Directory for Vault for Secrets

By default, the vault uses local authentication. You can change the authentication method as required, and you can have multiple authentication modes active at the same time. However, OIDC without Active Directory cannot be used with Active Directory, and OIDC with Active Directory cannot be used without Active Directory.

> ⚠ You cannot disable OIDC authentication once it is configured. After you enable OIDC, you can no longer sign in with AD credentials. However, you can sign in using local authentication credentials without any issues.

To configure OIDC

1. Log in to the Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. In the **Choose Authentication Type** drop-down menu, select:
   - **OpenID Connect** to configure OIDC without Active Directory
   - **OpenID Connect (with AD)** to configure OIDC with Active Directory
5. Click the **Learn more about configuring the OIDC Provider** link to view the OIDC provider's login redirect URL and logout redirect URL.
6. Specify the OpenID Connect Configuration settings:
   - Name
   - Client ID
   - Client Secret
   - Base URL
7. Optionally, click **Load File** to upload the CA certificate in base64-encoded PEM format.
8. Click **Apply**.
9. Select **Verify and Enable**. After verification, a message appears confirming OpenID Connect has been successfully enabled. Vault is set for OIDC authentication.
10. Sign out from the vault and sign in to the vault as an OIDC user by selecting **Sign in with IDAAS** and entering your OIDC credentials.

Name

A user-defined name for the OpenID Connect provider.

> ℹ Cryptographic Security Platform Vault displays this name on the button in the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

> ⚠ This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Configuring OIDC for Vault for Secrets

By default, the KeyControl Vault Management application is configured for local authentication. You can change the authentication method as required, but you can use only one type of authentication per vault at a time.

- If you want to use OIDC without AD, you can only change to that mode from the local authentication mode.
- If you have configured AD or OIDC with AD, you cannot change to OIDC without AD.

Each vault can be configured with a separate OIDC server or a separate application from same server.

> ⚠ OIDC without AD is the recommended mode of OIDC authentication method where the OIDC provider independently manages identity and authentication. For new OIDC setups, this is the preferred option.

To configure OIDC

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Choose Authentication Type** drop-down list, select **OpenID Connect**.
6. Specify the OpenID Connect Configuration settings:
   - Name
   - Client ID
   - Client Secret
   - Base URL
7. Optional. Click **Browse** to upload the CA Certificate.

   > ℹ The certificate needs to be in base64 encoded pem format.

8. Enter the Admin Name and Admin Email for OIDC user. This user will be created and will act as the Vault Administrator. They will be assigned to the admin policy and receive the email with the registration URL.
9. Click **Apply**. The OpenID Connect Configuration window appears showing the current configuration.
10. Click **Verify and Enable**. The OpenID Connect Successfully Configured window displays the new login URL.
11. Copy the URL, and click **Log Out and Sign in with IDP**.
12. After you are logged out, paste the URL into the browser window.
13. Log in to the Identity Provider using the name and password that you created.

Name

A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

> This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Managing two-factor authentication in Vault for Secrets

Two-factor authentication requires you to enter two forms of identification before you can access your CSP Vault.

- The first form is your standard username and password combination,
- The second is a one-time password (OTP) generated by an authorization app. The OTP is appended to your existing password.

See below for how to enable and manage it.

- Requirements for enabling two-factor authentication in Vault for Secrets
- Enforcing two-factor authentication in Vault for Secrets
- Disabling two-factor authentication in Vault for Secrets

> Two-factor authentication is supported with local authentication only. If you want to use two-factor authentication for non-local users, we recommend enabling it in your remote authentication provider.

Requirements for enabling two-factor authentication in Vault for Secrets

Make sure you have access to an authentication app that can generate HOTP or TOTP passwords. For example:

- For TOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. These applications continuously generate passwords valid for 30 seconds. If the current password expires before you can submit the login request, you must wait for it to generate a new password, then use that to log in.
- For HOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. A password generated through the application is valid from the time you create it until you use it to log in. To log in again, click **Next** in the app to generate a new password.

Enforcing two-factor authentication in Vault for Secrets

See below for enforcing two-factor authentication in Vault for Secrets.

- Enforcing two-factor authentication for the current user
- Enforcing two-factor authentication for all users

Enforcing two-factor authentication for the current user

See below for enforcing two-factor authentication for the current user.

To enforce two-factor authentication for the current user

1. Log in to the Cryptographic Security Platform Vault for Secrets webGUI.
2. In the top menu bar, click **Settings**.
3. In the **Two-Factor Authentication** field, click **Set up Two-Factor Authentication**.
4. In the **Enable Two-Factor** dialog box, select the HOTP or TOTP radio button.
5. Scan the generated barcode with your authorization app.
6. Enter the six-digit verification code from your app in the dialog box.
7. Click **Continue**. Cryptographic Security Platform Vault verifies the code and displays a message indicating success or failure. If the code is not correct, re-enter it.
8. After the code has been accepted, click **Done**.
9. When you log into the Vault web GUI:
    - Enter a valid OTP along with your standard account password on the login page. Do not add any characters or spaces between your account password and the one-time password generated by your authorization app. For example, if your password is `XyZ123$`, and your OTP is `32325`, you enter `XyZ123$32325` in the password field.
    - If you use TOTP, make sure your password doesn't expire before you submit the login request.

Enforcing two-factor authentication for all users

See below for enforcing two-factor authentication for all Vault users

To enforce two-factor authentication for all users

1. Log into the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the **Two-Factor Authentication Settings** page, select **ENFORCED**.
5. Click **Apply**.

Disabling two-factor authentication in Vault for Secrets

See below for disabling two-factor authentication in Vault for Secrets.

- Disabling two-factor authentication for a user
- Disabling two-factor authentication for all users

Disabling two-factor authentication for a user

See below to disable two-factor authentication for a single Vault user.

To disable two-factor authentication

1. Log in to the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Security**.
3. Select the **Users** tab
4. Select the user for whom you want to disable two-factor authentication.
5. In the **Details** tab below the table, click the **Enabled** link for the **Two-Factor Authentication** row.
6. In the **Disable Two-Factor Authentication** window, click **Proceed**.

Disabling two-factor authentication for all users

See below to disable two-factor authentication for all Vault users.

To disable two-factor authentication for all users

1. Log into the Cryptographic Security Platform Vault for Secrets webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.

3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the Two-Factor Authentication Settings page, select **NOT ENFORCED**.
5. Click **Apply**.

CSP Vault for VM Encryption

- VM Encryption Vault Overview
- Microsoft Failover Clusters
- Windows Boot Drive Encryption
- Linux Root, Swap, and System Device Encryption
- Data Encryption
- VM and Disk Management
- Configuring Vault Authentication for CSP Vault for VM Encryption
- Managing Authentication for Vault for VM Encryption

VM Encryption Vault Overview

The VM Encryption vault lets you manage Virtual Machine and disk encryption.

> Note: The Cryptographic Security Platform Vault for VM Encryption webGUI has an automatic timeout value of 30 minutes.

Microsoft Failover Clusters

Decommissioning or Decrypting an Encrypted Drive Shared by Multiple Nodes

If you have encrypted disks managed by Microsoft's Windows Failover Clusters, you can decrypt or decommission one. By default, the encrypted disks are registered under more than one server, typically two servers. However, the encrypted disks are only attached to the active node. On the inactive node, the encrypted servers have the following status: `GONE`.

You can either decrypt the disks, or decommission them if the encrypted content is no longer needed.

The examples in the following procedure assume that you have two servers, Node 1 and Node 2, and the encrypted disks are currently attached to Node 1.

Important: The Policy Agent must be able to communicate with Cryptographic Security Platform Vault, and Cryptographic Security Platform Vault must be in a good state before attempting these this procedure.

1. Run `hcl status` on **Node 1** to list all encrypted disks.
2. If you plan to decrypt the disks, run the following command on **Node 1**:
   hcl decrypt <*drive_letter*>
   Wait until the decryption is completed. Multiple disks can be run in parallel.
   Important: Ensure that the disks are not failed over to the **Node 2** while the disks are being decrypted. After decryption, the disks will be removed.
3. If you plan to decommission the disks, run the following command on **Node 1**:
   hcl rm <*drive_letter*>
4. Run `hcl status` on **Node 1**.
   The decrypted or decommissioned drives should have the following status: `Available`.
5. Run `hcl status` on **Node 2**.
   The encrypted disks are not listed, and the status should be: `GONE` on the Cryptographic Security Platform Vault webGUI. The disks are not attached to this server.
6. To remove the encrypted devices with status `GONE`, run the following command on **Node 2**:

```
hcl destroy <drive_letter>
```

7. Verify that the disks are no longer displayed on the Cryptographic Security Platform Vault webGUI.

Testing Failover and Failback

1. Mount the exported CIFS share in the client nodes.
2. Bring the `fs` service online and offline a few times on one of the nodes.
3. Check the contents of `C:\fsonline.txt` to see if the online function executed correctly. It should read something like:
   `updateconfig succeeded Encrypted device \Device\Harddisk3\Partition1 attached; decrypted contents visible at G:`
4. Check the contents of `C:\fsoffline.txt` to see if the `offline` function executed correctly. It should read something like:
   `Encrypted device \Device\Harddisk3\Partition1 detached; decrypted contents no longer visible`
5. Using **Failover Manager**, try moving the `fs` service over to the other node. Again, check the contents of `C:\fsoffline` on the source node and `C:\fsonline` on the target node to ensure that everything worked.
6. Try rebooting a node and confirming that the `fs` service smoothly fails over to the new node.

Enabling Failover and Failback

In this procedure we will continue to use drive `G:` with two nodes, winhost1 and winhost2.

Before You Begin

- Make sure you have set up encryption as described in Encrypting a Drive Shared by Multiple Nodes.
- Review the dependencies discussed in Dependencies for Failover and Failback.

Procedure

1. Log into both **winhost1** and **winhost2** as an Administrator.
2. Copy the script `hcl-fs-service.vbs` to the same location on both nodes **winhost1** and **winhost2**.
   The script is located in the *PA-install-dir*\bin directory, where `PA-install-dir` is the Entrust Policy Agent installation directory.
3. Add the script as a resource to the FS service via the failover cluster manager.
4. In the dependency properties for the `hcl-fs-service.vbs` script, specify that the cluster disk `G:` must be brought online before this script is executed.

Dependencies for Failover and Failback

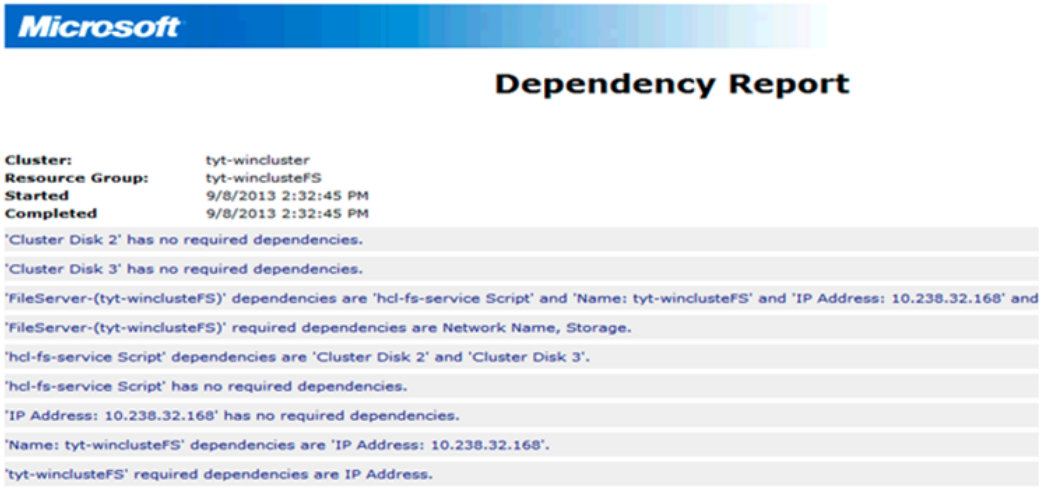
Entrust provides a vbscript called `hcl-fs-service.vbs` that is responsible for getting (via an online routine) and releasing (via an offline routine) keys from the Cryptographic Security Platform Vault node for devices that are protected.

The order of events when disks are brought up or taken down is extremely important.

1. The cluster disk must be brought online for the node before the online routine is called.
   Note: The online routine calls `hcl updateconfig`, which handles the cases where Windows changes the order of disks on the system. This typically happens across reboots when there are multiple iSCSI targets configured on the same host.

2. The online routine calls `hcl attach -a`, which fetches keys for all devices that have been encrypted on that node. Therefore, this routine must be called before the CIFS service is brought online.
3. The offline routine calls `hcl detach -a`, which releases keys for all devices that have been encrypted on that node. Therefore, this routine must be called after the CIFS service is taken down.

The following illustrations show these dependencies:



Microsoft

Dependency Report

Cluster:	tyt-wincluster
Resource Group:	tyt-winclusteFS
Started	9/8/2013 2:32:45 PM
Completed	9/8/2013 2:32:45 PM

'Cluster Disk 2' has no required dependencies.

'Cluster Disk 3' has no required dependencies.

'FileServer-(tyt-winclusteFS)' dependencies are 'hcl-fs-service Script' and 'Name: tyt-winclusteFS' and 'IP Address: 10.238.32.168' and

'FileServer-(tyt-winclusteFS)' required dependencies are Network Name, Storage.

'hcl-fs-service Script' dependencies are 'Cluster Disk 2' and 'Cluster Disk 3'.

'hcl-fs-service Script' has no required dependencies.

'IP Address: 10.238.32.168' has no required dependencies.

'Name: tyt-winclusteFS' dependencies are 'IP Address: 10.238.32.168'.

'tyt-winclusteFS' required dependencies are IP Address.

Encrypting a Drive Shared by Multiple Nodes

In addition to creating a Cryptographic Security Platform Vault cluster to support failover, you can use Microsoft's Windows Failover Clusters. What follows are specific instructions for the Entrust Cryptographic Security Platform Vault implementation of Failover Clusters.

Important: If you want to extend a disk that is part of a MS Failover Cluster, you must enable maintenance mode on the disk, extend the disk, and then disable maintenance mode on that disk.

The examples in the following procedure assume that you are using drive `G:` for your CIFS export from your Windows failover cluster nodes winhost1 and winhost2, and that `G:` on winhost1 appears as hard disk 3 and on winhost2 it appears as hard disk 4.

1. Log into both **winhost1** and **winhost2** as an Administrator.
2. Disconnect all existing clients that are currently using this share. To confirm that all clients have disconnected, run net session /list from the command prompt of both **winhost1** and **winhost2**. The command should not show any existing sessions.
3. On both **winhost1** and **winhost2**, run the command `hcl status` to get information about the state of your connection with the Cryptographic Security Platform Vault node, the number of devices available to encrypt, and so on.
4. Determine which node is the current owner of the shared disk and:
   - If you want to preserve the data that exists on the disk, run the command `hcl encrypt G:` on that node. Cryptographic Security Platform Vault encrypts the drive and the existing data.
   - If you want to reformat the disk, run the command `hcl add G:`. Cryptographic Security Platform Vault reformats the disk using NTFS and erases any existing data.

   In both cases, Cryptographic Security Platform Vault adds a unique GUID (Globally Unique Identifier) to `G:` and makes `G:` available as an encrypted drive.

5. Run `hcl status` on both nodes again. You should see the same **GUID** being reported for **hard disk 3** on **winhost1** and for **hard disk 4** on **winhost2**.
6. On **winhost1**, run `hcl encrypt G:` from the command prompt to begin encrypting existing data on the drive.
   - Depending on the size of the drive, this will take a few minutes to complete.
   - During the encryption, `G:` will no longer be visible and the CIFS export service will show as `offline` in the failover cluster manager.
   - Once `hcl encrypt G:` completes, its contents will be visible.
   - `G:` should now also show up under the disks owned by **winhost1** in the Cryptographic Security Platform Vault node.
7. Run `hcl detach -a` on **winhost1**. This will unmap drive `G:` from **winhost1** in preparation for the next step.
8. Use the failover cluster manager to move the CIFS service (and thus ownership of `G:`) from **winhost1** to **winhost2**. Note that `G:` will appear to be unformatted to **winhost2** and you will be prompted to format it. Ignore this prompt.
9. On **winhost2**, run `hcl import G:`. This should complete very quickly since `hcl` recognizes that this is an encrypted disk whose key is already registered with the Cryptographic Security Platform Vault node.
10. `G:` should now be readable on **winhost2**.

What to Do Next

Set up automatic failover and failback. For details, see Dependencies for Failover and Failback and Enabling Failover and Failback.

Windows Boot Drive Encryption

- Encrypting a Windows Boot Drive
- Bootloader Diagnostic Files
- Bootloader Time Sync Issues
- Troubleshooting Windows Boot Drive Issues
- Setting the Preferred Network Adapter
- Changing the Bootloader Network Settings
- Automated Bootloader Installation
- Installing the Bootloader After the Policy Agent Is Installed
- Access Management for Windows Boot Drives
- The Boot Process
- Requirements for Windows Boot Drive Encryption
- Windows Boot Drive Encryption Overview

Encrypting a Windows Boot Drive

After you have installed the Policy Agent and the Bootloader on the device and you have made sure that the device meets the prerequisites described in Requirements for Windows Boot Drive Encryption, you can encrypt the boot drive using any of the standard disk encryption methods.

- If you want to use the Cryptographic Security Platform Vault webGUI, see Encrypting a Disk Using the CSP Vault for VM Encryption webGUI.
- If you want to use the Entrust Policy Agent GUI, see Encrypting a Windows Disk Using the Entrust Policy Agent GUI.
- If you want to use the CLI, see Encrypting a Disk Using the CLI.

Bootloader Diagnostic Files

Bootloader Log File

The main Entrust Bootloader log file is called `htlog.log` and it is located at the root level in the Bootloader partition. For example, if the Bootloader is assigned to drive `P:`, the log file would be `P:\htlog.log`.

Entrust limits the size of the `htlog.log` file to 10 MB. When the log file reaches 10 MB, a new entry will automatically overwrite the oldest data in the log file.

Bootloader Silent Installation Status Files

In addition, if the Bootloader was installed silently using a command line script, the final state of installation can be inferred from four empty files created by the installer in the same directory as the installer executable:

- `HTDone` —This indicates the installation ended. You should poll for creation of this file to ensure that the installer process finished. If no other file is created, it means that the installation completed successfully. **Note:** Boot drive encryption is not available until AFTER a successful installation and reboot.
- `HTError` —The installation failed. This file contains the error string.
- `HTBLError` —Entrust Bootloader installation failed, but the rest of the installation succeeded. This file contains the error string.
- `HTRetryOnReboot` —If this file is present, the installation was not a failure, but it needs a reboot. To complete the installation, reboot and run the installer again.

For details about installing the Bootloader silently, see the installation and administration guide at https://api.managed.entrust.com/vault/latest

Bootloader Time Sync Issues

The Bootloader stores the time difference between local time and UTC along with a comma-separated list of NTP servers. If you need to change the list of NTP servers, you can update `htbl.conf` or you can use the following command:

`UpdateHTBootloaderNtpServers.ps1 [-ntpsrv <server list>] [-default] ntpsrv`, where `<server list>` is a list of comma-separated NTP servers in quotes. The default is to use NTP server settings from the host system, which overrides the `ntpsrv` parameter.

Troubleshooting Windows Boot Drive Issues

Because encryption keys are never stored locally, a VM with an encrypted boot partition requires access to Cryptographic Security Platform Vault when booting or the attempt will fail. If Cryptographic Security Platform Vault is not available when the system is booted, the VM repeatedly attempts to contact Cryptographic Security Platform Vault for 30 seconds. If contact cannot be established after that time, the VM presents a console menu with a number of options.

When using a shell on a Windows machine to access the bootloader, you may have to use one of the following options:

- Use git bash to connect.
- Use the following flags to access the bootloader:

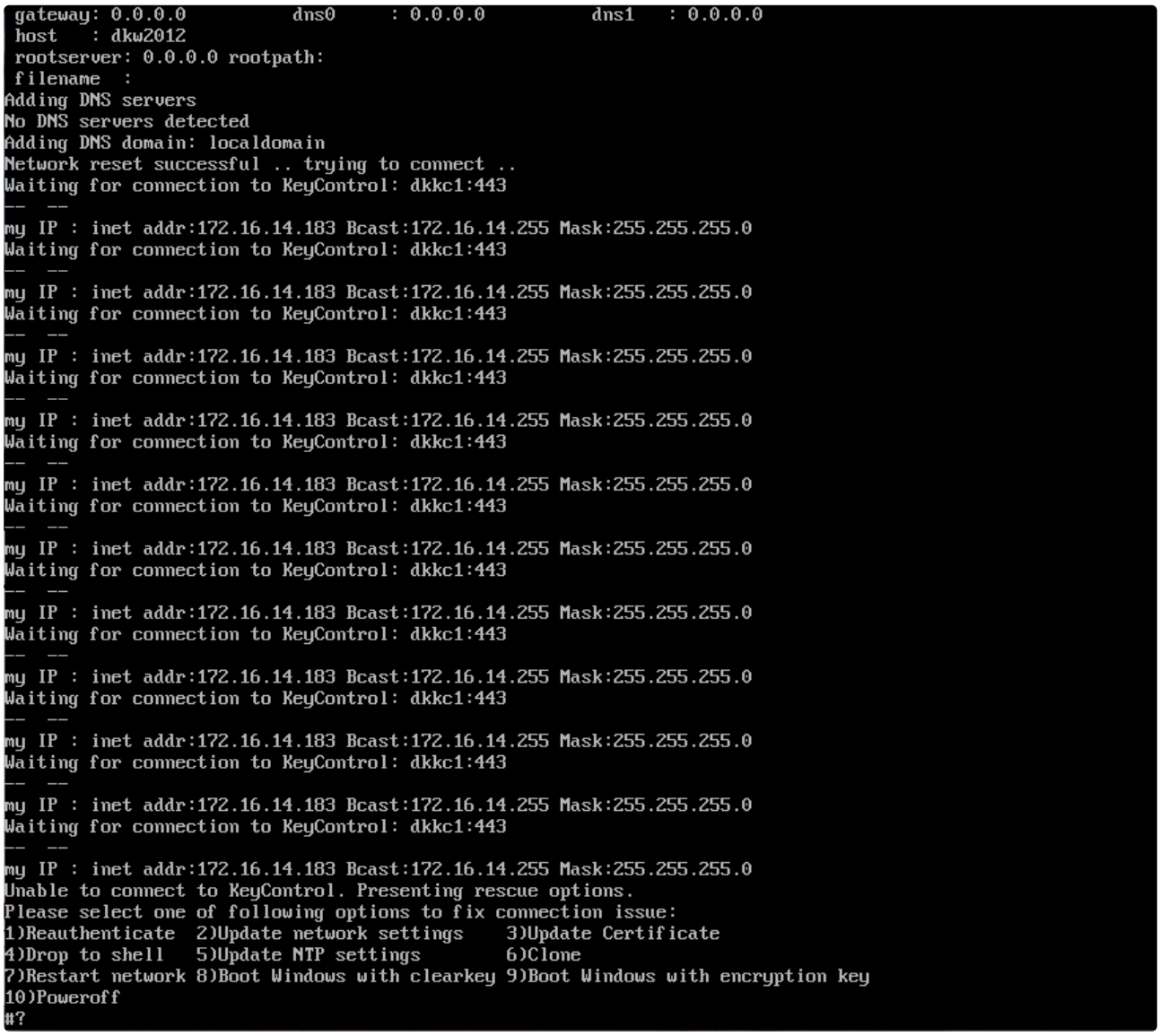
```
ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=ssh-rsa -i <machine-
name>.key root@<machine-IP>
```

If you are unable to view the console directly, for example in environments such as Amazon Web Services (AWS), you can access the console using an SSH client. This requires the `id_rsa` key file generated during the Policy Agent installation. Copy the `id_rsa` file to the server and then reboot.

> Tip: If you need another copy of the `id_rsa` key file, you can download it from the Cryptographic Security Platform Vault webGUI by selecting the VM on the Cloud > VMs tab and then selecting Actions > Download Bootloader SSH Key.

The console menu options are determined by the environment—some options are available on all platforms while others are not available on platforms like AWS. The full list of options is:

1. **Reauthenticate**—If the credentials of the VM become stale, then it must be re-authenticated with Cryptographic Security Platform Vault in much the same way as a running VM would have to. The most likely reason for this is that the grace period has expired. Another possibility is that the VM's IP address is configured via DHCP, which means it may have changed. We recommend static IP addresses for boot drives, or disabling the IP address check feature in Cryptographic Security Platform Vault. Key retrieval will proceed after re-authentication is successful.
2. **Update network settings**—This takes you back to the network settings screen so that you can update the settings.
3. **Update Certificate**—This allows you to update the VM certificate, if it has expired.
4. **Drop to shell**—Provides a simple recovery shell. Use the command `exit` to leave the recovery shell. We strongly recommend that you only use this option when instructed to do so by Entrust Support.
5. **Update NTP settings**—This allows you to update the NTP server address.
6. **Clone**—This allows you to clone a VM with an encrypted boot drive. This is similar to `hcl register -c` while cloning a non-boot-encrypted VM.
7. **Restart network**—This option instructs the VM to re-attempt to contact Cryptographic Security Platform Vault and try to retrieve the encryption key again. If no selection is made in this menu after 30 seconds, then this option will be taken automatically.
8. **Boot Windows with clearkey**—This option instructs the Bootloader to boot without an encryption key, and is done automatically if we detect that the boot partition is not encrypted.
9. **Boot Windows with encryption key**—This option instructs the Bootloader to boot Windows assuming that the encryption key has already been fetched.
10. **Poweroff**—Power down the computer.



Setting the Preferred Network Adapter

The "preferred network adapter" is the adapter used to communicate with Cryptographic Security Platform Vault. When encrypting the boot device, `hcl` checks to make sure that the preferred adapter is the adapter configured in the Bootloader. If not, the user is prompted to update the network configuration. This can be done either by using `SetupHTBootloaderNetwork.ps1` or `htblconf.exe`. Both utilities clearly identify the preferred adapter when presenting options.

When using the GUI, it automatically opens `htblconf.exe` if the user agrees to updating the Bootloader network settings. This is meant to be a safety net that ensures that the Bootloader will be

able to communicate with Cryptographic Security Platform Vault once the boot partition has been encrypted. However the user can choose to override this behavior.

When using the `hcl` command line, use the `-N` option on the `hcl encrypt` command to override the check for the preferred network adapter.

Changing the Bootloader Network Settings

1. Log into PowerShell on the Windows machine.
2. Navigate to the `bin` folder under the main Policy Agent installation directory. The default directory is `C:\Program Files\hcs`.
3. Do one of the following:
   - Run the PowerShell script `SetupHTBootloaderNetwork.ps1` by entering the command `powershell -File SetupHTBootloaderNetwork.ps1`.
   - Open the Bootloader GUI by running `htblconf.exe`. This GUI is similar to the Policy Agent installation GUI and it presents the same drive and network configuration options.
4. Reboot the VM.

Example 1, Network Configuration Using DHCP

```
PS C:\users\administrator> powershell -File "C:\Program Files\hcs\bin\SetupHTBootloaderNetwork.ps1"
Configuring HT Bootloader Network:
---------------------------------
Following network interfaces are available:
  1) Intel(R) PRO/1000 MT Network Connection 00:0C:29:45:59:93
  2) RAS Async Adapter 20:41:53:59:4E:FF
Select the primary interface by number or press Q to quit: 1
DHCP is currently enabled for the selected network interface.
Use DHCP during boot? [y/n] :y
Successfully updated HT Bootloader network configuration
```

Example 2, Network Configuration Using Current Static IP Settings

```
PS C:\users\administrator> powershell -File "C:\Program Files\hcs\bin\SetupHTBootloaderNetwork.ps1"
Configuring HT Bootloader Network:
---------------------------------
Following network interfaces are available:
  1) Intel(R) PRO/1000 MT Network Connection 00:0C:29:45:59:93
  2) RAS Async Adapter 20:41:53:59:4E:FF
Select the primary interface by number or press Q to quit: 1
DHCP is currently enabled for the selected network interface.
Use DHCP during boot? [y/n] : n
Setting up static IP for use during boot
Current configuration:
Network parameters provided:
IP address        : 172.16.14.222
Gateway address   : 172.16.14.2
Netmask           : 255.255.255.0
DNS server address    : 172.16.14.2
Host Name         : WINQ2FCCC3ALIH
DNS Domain        : localdomain
Is this correct? [y/n]    : y
Successfully updated HT Bootloader network configuration
```

Example 3, Network Configuration Using Custom Static IP Settings

```
PS C:\users\administrator> powershell -File "C:\Program Files\hcs\bin\SetupHTBootloaderNetwork.ps1"
Configuring HT Bootloader Network:
---------------------------------
Following network interfaces are available:
  1) Intel(R) PRO/1000 MT Network Connection 00:0C:29:45:59:93
  2) RAS Async Adapter 20:41:53:59:4E:FF
Select the primary interface by number or press Q to quit: 1
DHCP is currently enabled for the selected network interface.
Use DHCP during boot? [y/n] : n
Setting up static IP for use during boot
Current configuration:
Network parameters provided:
IP address        : 172.16.14.222
Gateway address     : 172.16.14.2
Netmask         : 255.255.255.0
DNS server address     : 172.16.14.2
Host Name         : WINQ2FCCC3ALIH
DNS Domain         : localdomain
Is this correct? [y/n]     : n
Please provide network parameters:
IP address        : 172.16.14.22
Netmask         : 172.16.14.2
Gateway address     : 255.255.255.0
DNS server address     : 172.16.14.3
Host Name         : MYPC
DNS Domain         : localdomain
Network parameters provided:
IP address        : 172.16.14.22
Netmask         : 172.16.14.2
Gateway address     : 255.255.255.0
DNS server address     : 172.16.14.3
Host Name         : MYPC
DNS Domain         : localdomain
Is this correct? [y/n]     :y
Successfully updated HT Bootloader network configuration
```

Automated Bootloader Installation

The `SetupHTBootloaderNetwork.ps1` script supports automation with a silent installation option. In keeping with the GUI installer, when used in interactive mode, this script displays the `ConnectionId` and `DeviceID` of the network adapter identification instead of just the hardware description.

The `DeviceID` displayed is the value of the `DeviceID` property of the `Win32_NetworkAdapter WMI` class. Note that value of `DeviceID` is the same as the `Index` property of the `Win32_NetworkAdapterConfiguration` class.

To use this script in interactive mode, do not use the `-silent` flag. In interactive mode, any parameters supplied to the script will be ignored.

When used in non interactive mode, using the `-silent` flag, the network adapter to be configured is specified through the `-deviceid` parameter (similar to `/NET` in the silent installer). The script will detect current

settings of the specified network adapter and use them if they are not overridden by any of the following optional parameters:

- `-dhcp` — Use `-dhcp` for configuring the adapter. This choice overrides all other settings
- `-ip` — IP address
- `-netmask` — Netmask
- `-gw` — Gateway IP address
- `-dns` — IP address of one or more DHCP servers, separated by commas
- `-hostname` — Hostname
- `-domain` — Domain

If the `-silent` flag is used without the `-deviceid` parameter, the script will try to detect the preferred network adapter, that is, the one used to connect to the KeyControl, and configure it.

For the purpose of automation, available network adapters can be listed by using the `-listadapters` parameter. The output is printed on the console. This flag overrides any other parameter.

Examples

Use `-listadapters` to get available devices and parse it to figure out the value of the `-deviceid` parameter you want to use. Note that the value of `DeviceID` can also be found by querying the `Win32_NetworkAdapter` or `Win32_NetworkAdapterConfiguration` WMI classes and using the `DeviceID` or `Index` property of the respective classes.

```
PS C:\users\administrator> SetupHTBootloaderNetwork.ps1 -listadapters
DeviceID|Description|IPAddress|MACAddress|DhcpEnabled|ConnectionID|Preferred
7|Intel(R) PRO/1000 MT Network Connection|172.16.14.222|00:0C:29:45:59:93|True|Local Area Connection|
False
10|Intel(R) PRO/1000 MT Network Connection #2|192.168.100.34|00:0C:29:45:59:9D|False|Connection 2|
False
```

Once the `DeviceID` has been determined, specify it as the value for the `-deviceid` parameter. This will configure the Bootloader to use the specified interface with its current configuration.

```
PS C:\users\administrator> SetupHTBootloaderNetwork.ps1 -deviceid 10
Successfully updated HT Bootloader network configuration
PS C:\users\administrator> cat T:\hcs\etc\ipconfig
DHCP=false
IP="192.168.100.34"
NETMASK="255.255.255.0"
GATEWAY=""
IPV4DNS0=""
DNSDOMAIN=""
```

If you want to override any of the default configuration, specify the required value with any of the parameters documented in previous section. The following example adds `Gateway` and `DNS server` information.

```
 PS C:\users\administrator> SetupHTBootloaderNetwork.ps1 -silent -deviceid 10 /
   -gw 192.168.100.1 -dns 192.168.100.1,192.168.1.1
Successfully updated HT Bootloader network configuration
PS C:\users\administrator> cat T:\hcs\etc\ipconfig
```

DHCP=false
IP="192.168.100.34"
NETMASK="255.255.255.0"
GATEWAY="192.168.100.1"
IPV4DNS0="192.168.100.1 192.168.1.1"
DNSDOMAIN=""

Installing the Bootloader After the Policy Agent Is Installed

If you originally installed the Policy Agent without the Bootloader component, you can install the Bootloader at any time as long as you have access to PowerShell.

To install the Bootloader with PowerShell:

1. Log into PowerShell on the Windows machine.
2. Locate the main Policy Agent installation directory. The PowerShell scripts are located in the `bin` folder under this main directory. The default directory is `C:\Program Files\hcs`.
3. Run the PowerShell script `InstallHTBootloader.ps1` by entering the command `powershell -File "C:\hytrust-install-dir\InstallHTBootloader.ps1" -drive n:`, where `-drive n` is an optional drive letter. If you do not assign a drive letter, the script selects the next available drive letter.
   The PowerShell script should return an exit code of zero. Any other exit code indicates an error, which will print in the log file `C:\hytrust-install-dir\InstallhtBootloader.log`.
   Example:
   PS C:\users\administrator> powershell -File "C:\Program Files\hcs\bin\InstallHTBootloader.ps1"
   This system already has a separate System volume and Boot volume.
   Creating new primary partition 1 of 1
   Failed, trying to free up space
   Shrinking C: by 360 MB, this may take some time
   DiskPart successfully shrunk the volume by: 360 MB
   Trying to create partition again
   Successfully created primary Partition 3 on Disk 0
   Formatting
   DiskPart successfully formatted the volume.
   DiskPart successfully assigned the drive letter or mount point.
   Creating SRP
   Boot files successfully created.
   Successfully created SRP on Partition 3 Disk 0
   Copying bootloader files
   Updating bootloader configuration
   Adding boot menu entries
   Marking new SRP active
   Winldr serial: 40604346 , Bootldr serial: 1155100468
   Please reboot for changes to take effect.
   If you have executed this script from Power Shell directly, please
   execute SetupHTBootloaderNetwork.ps1 before rebooting
4. Set up the network by entering the following PowerShell command:
   `powershell -File SetupHTBootloaderNetwork.ps1`

   Example:
   PS C:\users\administrator> powershell -File "C:\Program
   Files\hcs\bin\SetupHTBootloaderNetwork.ps1"
   Configuring HT Bootloader Network:

```
---------------------------------
Following network interfaces are available:
  1) Intel(R) PRO/1000 MT Network Connection 00:0C:29:45:59:93
  2) RAS Async Adapter 20:41:53:59:4E:FF
Select the primary interface by number or press Q to quit: 1
DHCP is currently enabled for the selected network interface.
Use DHCP during boot? [y/n] : n
Setting up static IP for use during boot
Current configuration:
Network parameters provided:
IP address        : 172.16.14.222
Gateway address     : 172.16.14.2
Netmask         : 255.255.255.0
DNS server address     : 172.16.14.2
Host Name         : WINQ2FCCC3ALIH
DNS Domain         : localdomain
Is this correct? [y/n]     : y
Successfully updated HT Bootloader network configuration
```

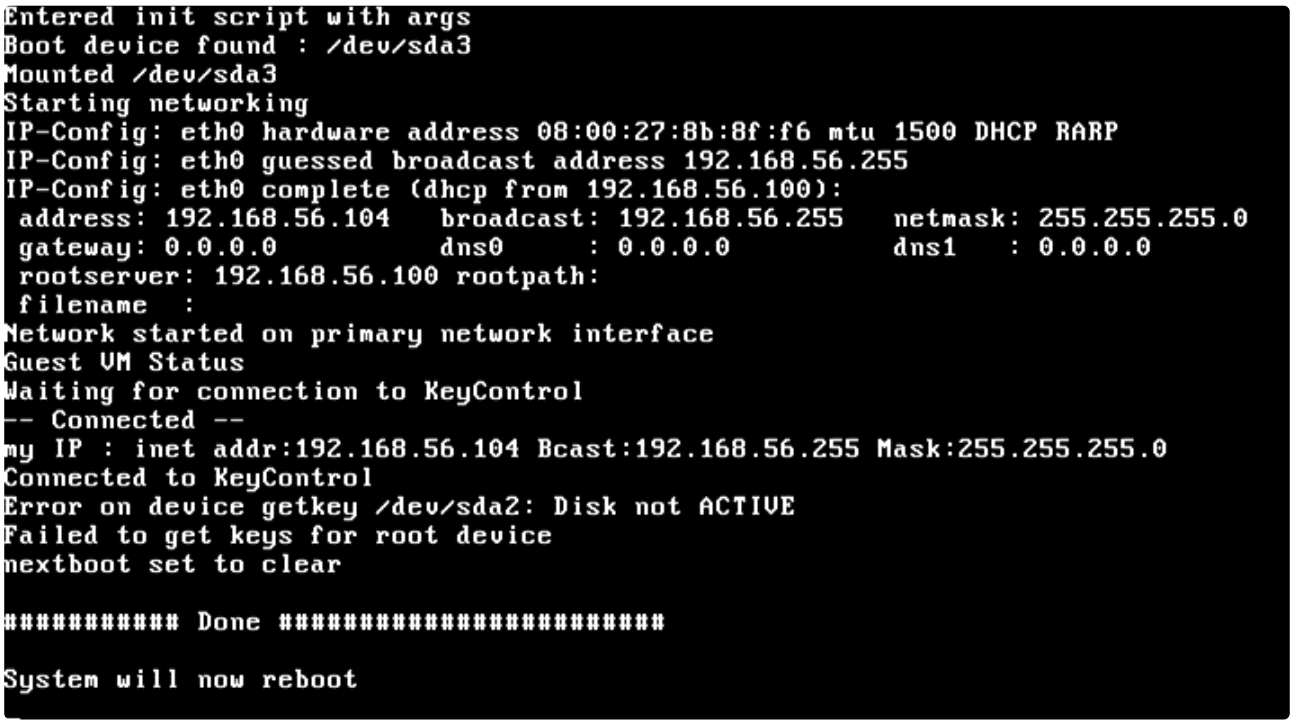
5. Reboot the VM.

Access Management for Windows Boot Drives

One of the important features offered by this system is the ability to control remote access to the encrypted data from the Cryptographic Security Platform Vault. Entrust boot encryption also offers this feature.
The `C:` drive is presented in the Cryptographic Security Platform Vault webGUI as simply another disk to be managed. Keys can be revoked and access granted in the same manner as non-root disks.

If access to the encrypted `C:` drive is revoked, the Policy Agent, upon the next heartbeat, will immediately present a stop error, better known as a "Blue Screen of Death" or BSOD. The BSOD status code is set to the value `"DEADDEAD"` so that it can be quickly determined that a key revocation is the reason for the BSOD.

The BSOD will eventually result in the VM attempting to reboot. Of course, at this time, the key is no longer available, since access has been revoked. Key retrieval will fail and the boot will fail with it.



The boot attempt will fail with the status code `0xC00000f`, indicating a failure to read the disk. This boot error persists until access to the key has been restored. After the key is restored, Windows will reboot normally.

For details about revoking the keys to a disk, see Revoking Access to a Disk.

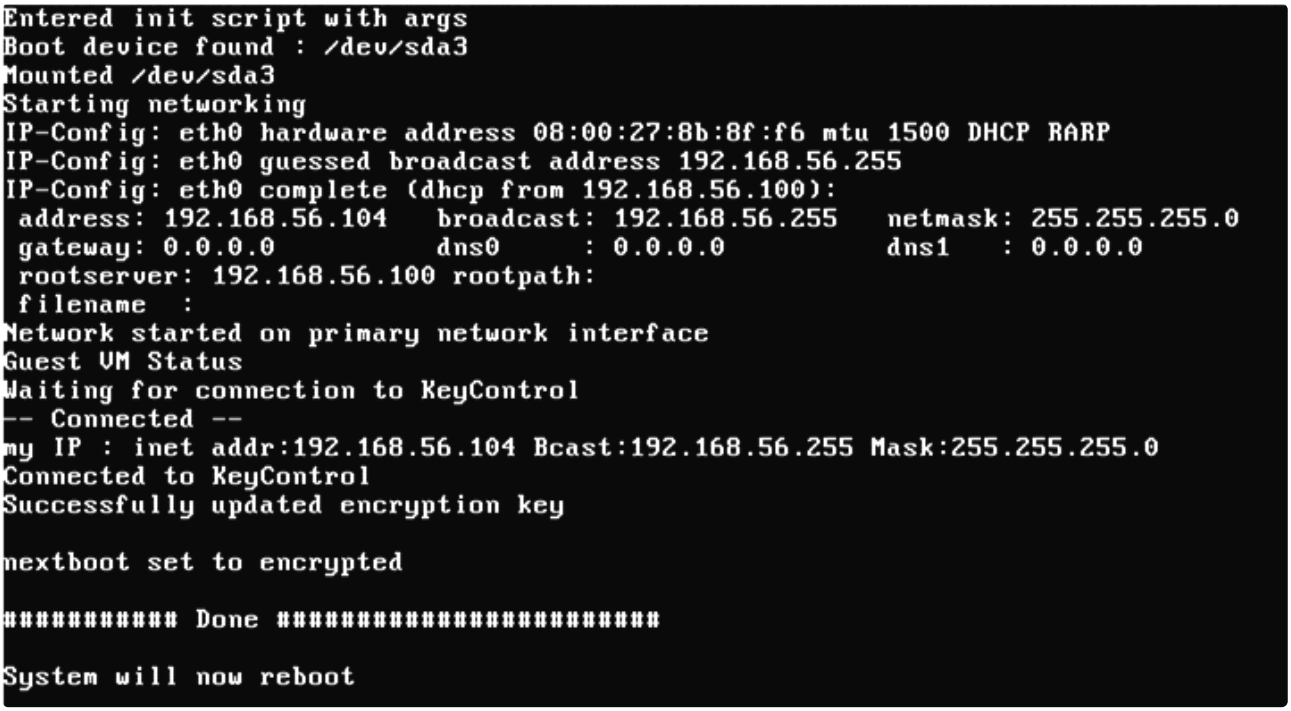
The Boot Process

The Bootloader uses a small pre-boot environment to retrieve encryption keys for the boot device each time the system starts up. The system is reconfigured to boot the Bootloader before booting Windows. Here are the steps:

1. A computer with has an encrypted boot drive reboots.
2. The Bootloader intercepts the boot request and sends a request to Cryptographic Security Platform Vault to retrieve the encryption key for the `C:` drive.
3. The Bootloader retrieves the key from Cryptographic Security Platform Vault and supplies it to the secondary boot stage, which will boot Windows.
4. Windows boots normally.

Note: Keys for the `C:` drive are never stored persistently on the VM—they are only stored in the remote, password protected, Cryptographic Security Platform Vault object store. The following topics describe some of the possible outcomes in the boot process.

While the Bootloader is running, you can watch its progress through messages displayed on the Windows boot screen.



Requirements for Windows Boot Drive Encryption

The Entrust Policy Agent supports encryption for Windows MBR and GPT boot disks, including any GPT boot disks that use UEFI Secure Boot, as long as those boot disks meet the following requirements.

- Make sure the version of Windows running on the target system is supported for boot drive encryption. For details, see Supported Platforms.
- The encrypted boot partition must be on the Windows `C:` drive. Although Windows itself can boot from alternate drive letters, the boot volume can only be encrypted if it is the `C:` drive or if it is mapped to `C:`. The Bootloader is automatically assigned a drive letter during installation. This default drive letter can be changed using the Windows Disk Manager after the Bootloader has been installed.
- The Bootloader requires a Windows System Reserved Partition (SRP). We will create an SRP if one does not already exist.
  The Bootloader SRP requires roughly 350 MB on Windows 2016 and above, and roughly 100 MB on Windows 10. As part of the installation process, the boot drive will shrink to free up space for the Bootloader (and Windows SRP if one does not already exist). If there is insufficient space on the boot drive, the Bootloader will fail to install.
  Note: If the Bootloader SRP has less than 50 MB free space, Cryptographic Security Platform Vault generates an alert every six hours until the issue is resolved.
- The SRP and the boot partition must both reside on `Harddisk0` (Disk 1). You cannot encrypt a boot partition that resides on any other disk, or split the SRP and the boot partition across disks.
- The boot disk must have at least 1 MB of free space at the beginning of the disk that Cryptographic Security Platform Vault can use to store encryption metadata. If this free space is not available, boot drive encryption will fail.

- If the VM is associated with a Cloud VM Set that is controlled by a Key Encryption Key (KEK), the HSM must be available before you can encrypt the root drive on the VM. For more information, see KEKs with Cloud VM Sets.
- The Disk Defragmenter service on the target server must be enabled before installing the Policy Agent software.
- The user account used for installing the software must have **SeRestorePrivilege** and **SeTakeOwnershipPrivilege**.
- For GPT boot disks:
    - The GPT disk must be running Windows Server 2016, Windows Server 2019, Windows Server 2022, or Windows 10.
    - The boot partition must be one of the first four partitions on the disk.
      Tip: If you try to encrypt the boot disk and the boot partition is not one of the first four partitions, the encryption will fail with the error "Maximum supported encrypted partition limit exceeded."
    - If you want to extend the boot partition, you must use the `hcl extend` command. For details, see Disk Size Management in Windows.

For details on installing the Policy Agent, see Windows Policy Agent Installation. If the Policy Agent is already installed but the Bootloader component is not, see Installing the Bootloader After the Policy Agent Is Installed.

Windows Boot Drive Encryption Overview

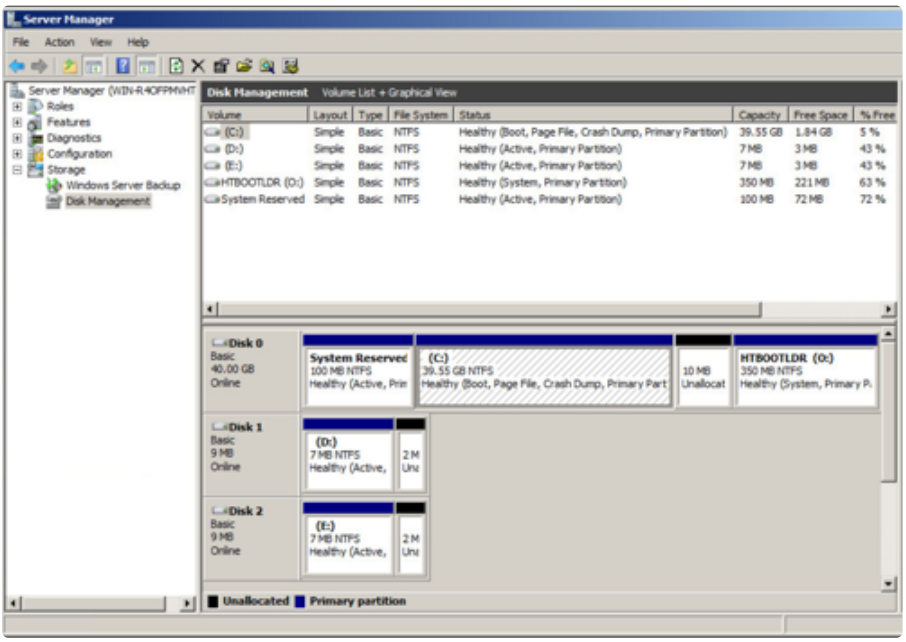
In addition to encrypting regular Windows data partitions, you can also encrypt your Windows boot disk (`C:`). Encrypting the `C:` drive ensures that clear-text data never leaves the VM on its way to storage. This prevents virtualization and storage admins from being able to view the data.

Note: Entrust does not support boot drive encryption on a dual-boot system.

Boot drive encryption is done using an optional component of the Entrust Policy Agent called the Entrust Bootloader for Windows (the Bootloader). If you install this component when you install the Policy Agent, Cryptographic Security Platform Vault can encrypt the boot drive partition using keys that are retrieved as needed from Cryptographic Security Platform Vault during the VM boot. The keys are not kept with the encrypted boot partition, thus providing an extra layer of security.

There are a number of steps required to set up your Windows system for boot drive encryption. If you are running within a virtual infrastructure, we recommend that you go through this process once and set up a template VM from which new VMs can be created.

After the Bootloader has been installed, you can see the distinction between the Windows boot partition and the root partition by running the Windows diskmgr utility. The small boot partition will be listed as System Reserved and the Bootloader appears as HTBOOTLDR. No part of the Windows root `C:` is ever decrypted on disk, and the Bootloader partition contains only a small part of the boot process. For example:



From a Cryptographic Security Platform Vault perspective, the boot drive is simply another Windows disk that can be managed just like any other Windows disk through the Cryptographic Security Platform Vault webGUI or `hicli`. You can also manage encryption on the VM itself using the Entrust Policy Agent GUI installed with the Policy Agent. For details, see Data Encryption.

Linux Root, Swap, and System Device Encryption

- Checking the Root Drive Encryption Status
- Encrypting Linux System Devices
- Verifying the Current VM Configuration
- Prerequisites and Restrictions

Checking the Root Drive Encryption Status

If Online Encryption*is* enabled for this VM, you can check the encryption status at any time by logging into the VM as `root` and using the `hcl status` command. If Online Encryption*is not* enabled, you can check the encryption status on the VM console through vSphere, Azure, or AWS.

When using a shell on a Windows machine to access the bootloader, you may have to use one of the following options:

- Use git bash to connect.
- Use the following flags to access the bootloader:
  `ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=ssh-rsa -i <machine-name>.key root@<machine-IP>`

If you need to troubleshoot the encryption process, you can check the encryption status using the Entrust Debug Console if you enabled that while running the `htroot setup` command, as described in Encrypting Linux System Devices.

1. If you need a copy of the `id_rsa` key file for the VM:
    a. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Cloud Admin privileges.
    b. In the top right, click the Switch to **Appliance Management** link.
    c. Navigate to the **Cloud > VMs** tab and select the VM whose key file you want to download.
    d. Select **Actions > Download Bootloader SSH Key**.
2. Open an `ssh` session by entering the command `ssh -i id_rsa root@vm_name`, where `id_rsa` is the name of the id_rsa file and `vm_name` is the IP address or hostname. For example:
   $ ssh -i Downloads/ht-centos75.key root@ht-centos75

   The authenticity of host 'ht-centos75 (192.168.15.239)' can't be established.
   RSA key fingerprint is SHA256:v1TDb5PTlGsncaPf6r9C0Z6ybtqVLxeGXf7XDnh3ltM.
   Are you sure you want to continue connecting (yes/no)? yes
   Warning: Permanently added 'ht-centos75,192.168.15.239' (RSA) to the list of known hosts.

   HyTrust Debug Console

   1. Show HT encryption log file
   2. Authenticate
   3. Show Network info
   4. Restart Network
   5. Advanced access
   6. logout (exit Debug Console)
3. Select option 1 and look for the status sections. For example, here are a few of the lines towards the end of the output:
   Starting HyTrust root encryption ----------

   Entered init script with args
   Starting debug shell
   Detected boot device uuid c01c3240-664b-412a-8440-dd0fa132eae5 device path /dev/sda1
   Check file system on device path /dev/sda1
   File system check on /dev/sda1 complete
   Mounted /dev/sda1
   Starting networking
   Network started on primary network interface
   Started debug console server
   Guest VM Status
   KeyControl: sdkc:443
   Waiting for connection to KeyControl

   Waiting for connection to KeyControl
   KeyControl: sdkc:443
   Connected
   network : ens160 00:50:56:a2:64:84 192.168.15.239
   Connected to KeyControl
   Starting root device encryption: sda2

   ---------- KeyControl and status ----------
   sdkc:443
   Connected
   ---------- Encryption / Decryption status ---------

```
root device encryption
Processing: 100% Time left: 00:00:00
swap device sda3 encryption
Processing: 100% Time left: 00:00:00
system device sdb1 encryption
Processing: 51% Time left: 00:13:39
```

We can see that we are connected to Cryptographic Security Platform Vault and that encryption is in progress. At this point, the `root` and `swap` devices have been fully encrypted and `sdb1` encryption (`/home` in this example) is 51% complete with just under 14 minutes left.

Encrypting Linux System Devices

The following procedure can be used for any Linux system device (such as `/root`, `swap`, or `/home`), including those that reside in Microsoft Azure or Amazon Web Services. The example used in this procedure shows how to encrypt the `/root`, `swap`, and `/home` devices at the same time, but you can also encrypt any system device separately at any time.

During this procedure, the VM will need to be rebooted to start the encryption process. If you have enabled Online Encryption for this VM, the VM will come back online immediately and the Policy Agent will encrypt the system devices as a background process. In this case, users can continue to access the data while it is being encrypted.

If Online Encryption is *not* enabled, the VM will remain inaccessible for normal operations until the encryption process completes.

For more information about Online Encryption, see Linux Online Encryption Prerequisites and Considerations.

Important: Do *not* encrypt a data drive with the `htroot` command. If you do so, Cryptographic Security Platform Vault will treat the data drive as a system device, which means that the data drive cannot be detached, it will appear in Cryptographic Security Platform Vault as a "root" device, and it must be rebooted when you want to encrypt, decrypt, or rekey it. To encrypt a data drive, see Encrypting a Disk Using the CLI or Encrypting a Disk Using the Cryptographic Security Platform Vault for VM Encryption webGUI.

Before You Begin

- Because issues during root device encryption can hang the VM, it is critical to make sure everything is properly configured before you start. For details, see Prerequisites and Restrictions and Verifying the Current VM Configuration.
- If there is a KEK associated with the Cloud VM Set to which this VM belongs, make sure that the hardware security module (HSM) in which the KEK is stored is accessible to Cryptographic Security Platform Vault. During the encryption process, the VM must be rebooted. If the KEK is unavailable when the VM attempts to reboot, the reboot will fail until Cryptographic Security Platform Vault can access the KEK in the HSM. For details, see KEKs with Cloud VM Sets and Hardware Security Modules with Cryptographic Security Platform Vault

Tip: Depending on the size of the disk, the encryption process can take a long time to run. If the encryption process is interrupted, you need to manually issue the `htroot cleanup` command and then reissue the `htroot setup` or `htroot encrypt` command to resume the process. We recommend you use the Linux `nohup` or `screen` command to avoid terminal-related interruptions during encryption.

Procedure

1. Log into the VM as `root`.

2. Enter the `htroot status` command to verify whether the Entrust Bootloader has already been installed on this VM.
   # htroot status

   HyTrust Bootloader setup is not done.
   You can complete Bootloader setup using "htroot setup"

   Root device "/dev/sda2" is not encrypted
   swap device "/dev/sda3" is not encrypted

3. If `htroot status` reports that the Bootloader setup is not done, enter the `htroot setup` command. If `htroot setup` reports that the Bootloader set up is complete, go to the next step.
   # htroot setup
   Debug console can be used to monitor the progress of root device encryption
   The following packages are required for debug console:
     dropbear
   Do you want to enable debug console? (y/N) y

   Note: The Entrust Debug Console allows `ssh` access to the server while the encryption process is running so you can check the status of the encryption process. After encryption is complete, the Debug Console provides limited access to the encrypted VM. If the encrypted VM fails to boot because it cannot retrieve the appropriate keys from Cryptographic Security Platform Vault, you can use the Debug Console to restore communication with Cryptographic Security Platform Vault. We highly recommend you enable this console. For more information, see Checking the Root Drive Encryption Status.
   Checking connection to software repositories (yum check-update)

   Connection to software repositories seems to be working fine

   The following packages are required for root encryption:

     cryptsetup
     dropbear

   Attempt to install required packages? (y/N) y

   Package dropbear can be found in the EPEL repository.
   More information on EPEL can be found at https://fedoraproject.org/wiki/EPEL

   NOTE: If you wish to configure EPEL using a private mirror
   (e.g. using Red Hat Satellite) then please exit htroot and
   configure the repository before re-running.

   Attempt to install EPEL release? (y/N) y

   Installing EPEL from CentOS Extras repo.....
   ok
   Installing cryptsetup.....
   ok
   Installing dropbear.....
   ok

   Uploaded keyfile /usr/lib/dracut/modules.d/91hcs/root/.ssh/id_rsa to KeyControl

```
You can download the key from KeyControl using WebGUI

Alternatively, copy the keyfile /usr/lib/dracut/modules.d/91hcs/root/.ssh/id_rsa to another
machine
This file will be used to access debug console using ssh
example: # ssh -i id_rsa root@server.ip.addr

Press Enter to continue...


Current Boot device setup
--------------------------------------------------------------------------------
Boot partition device path /dev/sda1
Boot partition device uuid c01c3240-664b-412a-8440-dd0fa132eae5
--------------------------------------------------------------------------------

Is this information correct? (y/N) y
Following network interfaces are available

--------------------------------------------------------------------------------
ens160 00:50:56:a2:64:84 192.168.15.239
--------------------------------------------------------------------------------
Preferred Network Interface is (ens160), which is used while authenticating with KeyControl

Select the primary network interface (ens160):
With encrypted root device, KeyControl needs to be contacted during
boot to get the encryption keys. IP address can be obtained using
DHCP or can be statically configured now
Use DHCP during boot? (y/N) y

Re-structuring HyTrust specific directories
Updating initrd

HyTrust Bootloader setup completed successfully
Run "htroot encrypt" to encrypt Linux root devices

# htroot status

HyTrust Bootloader setup is complete

Root device "/dev/sda2" is not encrypted
swap device "/dev/sda3" is not encrypted
```

4. Enter the `htroot encrypt` command and select which system devices you want to encrypt. You can encrypt the devices at any time and in any order. Similarly, once the devices have been encrypted, they can be rekeyed or decrypted at any time and in any order.
   Important: Do *not* encrypt a data drive with the `htroot` command. If you do so,Cryptographic Security Platform Vault will treat the data drive as a system device, which means that the data drive cannot be detached, it will appear in Cryptographic Security Platform Vault as a "root" device, and it must be rebooted when you want to encrypt, decrypt, or rekey it. To encrypt a data drive, see Encrypting a Disk Using the CLI or Encrypting a Disk Using the Cryptographic Security Platform Vault for VM Encryption webGUI.
   The following example shows how to encrypt the `root` , `swap` , and `/home` devices at the same time.

```
# htroot encrypt

Setting up system for root device encryption.
--------------------------------------------------------------------------------
Do you want to encrypt root device "sda2 (/dev/sda2)"? (y/N) y
Changing /etc/fstab to mount file system / from /dev/mapper/clear_htroot

Setting up system for swap device encryption.
--------------------------------------------------------------------------------
Do you want to encrypt swap device "sda3 (/dev/sda3)"? (y/N) y
Changing /etc/fstab to mount the swap from /dev/mapper/clear_B081FD59-
A74A-4F85-8D1BAA42212F3607

Do you want to encrypt any other file systems, like /var, /usr ?
--------------------------------------------------------------------------------
Please provide comma (,) separated list of mount points: /home
Do you want to encrypt block device "sdb1 (/dev/sdb1, /home)"? (y/N) y
Changing /etc/fstab to mount file system /home from /dev/mapper/
clear_EE57B642-2A00-49C8-9AC1-
31D300DB6D07

Updating initrd
The system has been updated to encrypt the Linux root device/s during next boot; please reboot
the system now
Do you want to reboot the system now? (y/N) y
```

Confirm the server reboot to continue. When the server has rebooted, it authenticates itself with Cryptographic Security Platform Vault to get the required encryption keys and then starts the encryption process. The time required to encrypt the devices depends on their size and the type of storage you have.

- If you have enabled Online Encryption for this VM, the VM reboots immediately and the Policy Agent encrypts the devices as a background process. In this case, you can check the encryption status at any time using the `hcl status` command.
- If Online Encryption is not enabled, the VM remains offline until the encryption process completes. In this case, you can see the encryption progress on the VM console through vSphere, Azure, or AWS. In addition, if you selected `y` when asked if you wanted to enable the Entrust Debug Console, you can view the progress through the Debug Console as described in Checking the Root Drive Encryption Status.

When it is finished, you can verify that the encryption succeeded using the `htroot status` command. For example:

```
# htroot status

HyTrust boot loader setup is complete

Root device "/dev/sda2" is encrypted
swap device "/dev/sda3" is encrypted
system device "/dev/sdb1 (/home)" is encrypted
```

5. After the encryption process completes, you can log in as normal. If you log in as `root` and enter the `hcl status` command, you will see that the system devices you encrypted are listed under **Registered Devices**. For example:

```
# hcl status

Summary
--------------------------------------------------------------------------------
KeyControl: sdkc:443
KeyControl list: sdkc:443
Status: Connected
Last heartbeat: Wed Jul 4 12:24:22 2018 (successful)
AES_NI: enabled
Certificate Expiration: Jul 4 06:22:12 2019 GMT
HTCRYPT: Not Installed

Registered Devices
--------------------------------------------------------------------------------
Disk Name        Cipher      Status              Clear
--------------------------------------------------------------------------------
sbd1             AES-XTS-512  Attached             /dev/mapper/
clear_EE57B642-2A00-49C8-9AC1-31D300DB6D07 (/home)
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
sda3             AES-XTS-512  Attached             /dev/mapper/clear_B081FD59-A74A-4F85-8D1B-
AA42212F3607 (/swap)
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
sda2             AES-XTS-512  Attached             /dev/mapper/clear_htroot
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
```

Warning: The `hcl status` command shows the clear text path to the encrypted system devices. (The clear text path is highlighted in the example above). You should only connect to the devices using these clear text paths. Accessing the encrypted devices through the direct paths such as `/dev/sda3` or `/dev/sda2` could cause data corruption.

Verifying the Current VM Configuration

Prerequisites and Restrictions

Creating a Boot Partition on RHEL 8, 9, and 10

Creating a Boot Partition on the AWS Root Volume

Creating a Boot Partition on Ubuntu

Data Encryption

- Migrating Files into AWS S3 Buckets
- Using Asymmetric KeyIDs
- File-Level Encryption Using KeyIDs
- Configuring Client-Side Key Caching
- Changing the Encryption/Decryption Speed on Windows
- Example: Encrypting a Windows VM with New Disks
- Example: Encrypting a Linux LVM Volume
- Example: Adding an Encrypting a Linux Disk with XFS
- Combining VMware vSphere VDI with the CSP Vault

- Decrypting a Linux System Device
- Decrypting a Disk Using the CLI
- Decrypting a Disk Using the Windows Policy Agent GUI
- Decrypting a Disk Using the webGUI
- Encryption Key Maintenance
- Windows Encryption Management with the Entrust Policy Agent GUI
- Troubleshooting Windows Online Encryption Issues
- Reversing an Encryption
- Encrypting a Disk Using the CLI
- Encrypting a Disk Using the CSP Vault for VM Encryption webGUI
- Automatic Data Encryption
- Using Data Encryption in Microsoft Azure
- Using Data Encryption in AWS
- Windows Encryption Prerequisites
- Linux Encryption Overview
- Data Encryption Overview

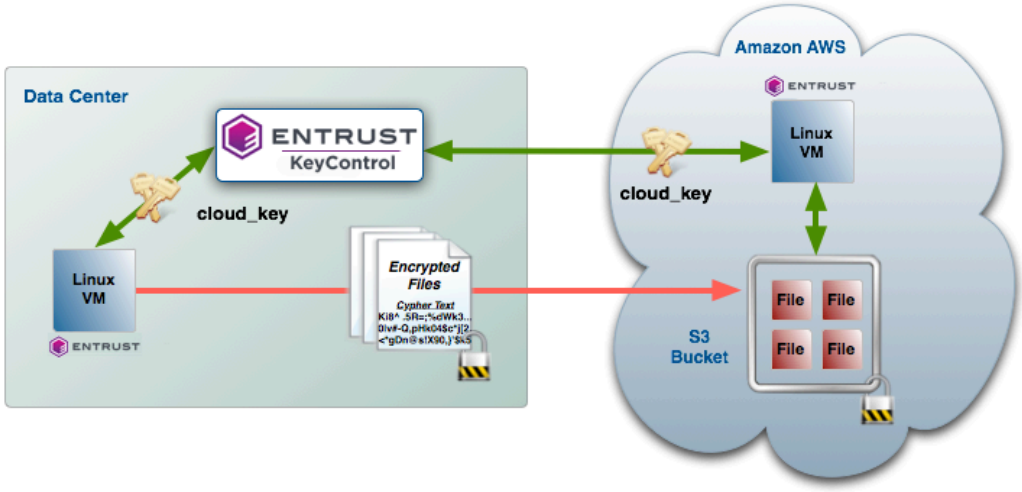
Migrating Files into AWS S3 Buckets

This section covers the tools that Entrust provides to encrypt files, place them within Amazon Web Services (AWS) S3 buckets and access the files securely from VMs that reside within the same Cloud VM Set, regardless of whether the other VMs in the set are running in AWS.

This is accomplished using KeyIDs, which are symbolic names that references the actual encryption keys.

Basically, you use the `hcs3` command to create an S3 bucket, then you securely add KeyID-encrypted files to the bucket. VMs within the same Cloud VM Set can access those files and decrypt them without having to manipulate or manage encryption keys.

For example, consider the following figure:



We want to create an S3 bucket, encrypt files and place them in the bucket and then access the files from the VM running in AWS. Here are the sequence of operations that are performed within the VM in the data center:

```
# hcs3 setstore TKIAN7ZDFBY2BU36DVPQ FZ9gsvIT1oDvuOiJrdSLRqBvmLZPcxzOWT4Qx7y5
# hcs3 create spate_aws
# hcs3 add spate_aws file1
# hcs3 add spate_aws file2
# hcs3 list spate_aws
file1 file2
```

First we call `hcs3 setstore` to provide our AWS access key id and secret. This is only called once. Next we create a bucket called `spate_aws`. Note that this will have the side effect of creating a KeyID which is also called `spate_aws`. Finally, we start adding files to the bucket. As the files are created, we first encrypt them before moving them to the bucket.

From within the VM in AWS, we can simply access the files as follows:

hcs3 get spate_aws file1 # ls file1

This section includes:

- Troubleshooting hcs3 Failures
- hcs3 Properties
- Enabling hcs3 Access to Non-Root Users
- Viewing a Bucket's Status and Contents
- Adding and Removing Files from Buckets
- Creating and Managing Buckets
- Using Environment Variables for AWS Credentials
- The hcs3 Interface

Troubleshooting hcs3 Failures

The only failure we are aware of manifests with an error message from Amazon, saying "Please reduce your request rate," sometimes referred to as the "SlowDown" error. We have modified our code to minimize the occurrence of this issue. For further information and additional workarounds, see this Amazon Forum thread: https://forums.aws.amazon.com/thread.jspa?threadID=218001.

hcs3 Properties

There is only one property supported at present: `tmp`. "tmp" can be set to the full path of any directory to which the user has access. This directory is used to hold the files temporarily as they are encrypted or decrypted, in transit.

The syntax of the command is:

hcs3 set tmp=<path to scratch space>

On Linux, the default value of the "tmp" property is set to "`/tmp`". However, on Windows temporary files are kept in the same directory as the source file. Therefore it is very important on Windows to set the "tmp" property to an appropriate value. This is especially important for users who do not have administrator privileges.

Enabling hcs3 Access to Non-Root Users

The command is:

```
# hcs3 useraccess <-d | -e no_of_days>
```

The command enables `hcs3` access for non-root (non-Administrator) users. Access can be enabled for a specific number of days (`-e`). If zero days are specified, then the access is enabled forever until specifically revoked using the `-d` option.

The root user can disable non-root access using the `-d` option.

If non-root user access is enabled, regular users can use `hcs3` to store encrypted files in S3. They can create / remove buckets just as the root user can.

It is recommended that the user provide his/her AWS credentials using environment variables, as discussed earlier. However, a non-root user can also store his/her credentials using `hcs3 setstore` . The credentials are stored in an encrypted file in the `$HOME/.hytrust` directory.

Non-root users can also set their temporary scratch space using the `hcs3 set` command.

Viewing a Bucket's Status and Contents

You can get status information about your Amazon ID and the list of buckets available to you as follows:

```
# hcs3 status
Summary
--------------------------------------------------
Registered Stores
--------------------------------------------------
Store Name        ID                  Owner
--------------------------------------------------
Amazon            AKIAJ7ZDFBY2BUT6DVPQ    spate

Buckets
--------------------------------------------------
hcs-aws-bucket
tmp_space

Properties
--------------------------------------------------
tmp directory = NOT SET
```

If you want to see which files are in a particular bucket:

```
# hcs3 list hcs-aws-bucket
file1
file2
files.tgz
```

Adding and Removing Files from Buckets

Once the bucket and its associated KeyID have been created, you can add, extract and delete files to and from the bucket from any VM within the Cloud VM Set that owns the bucket. Let's add some files:

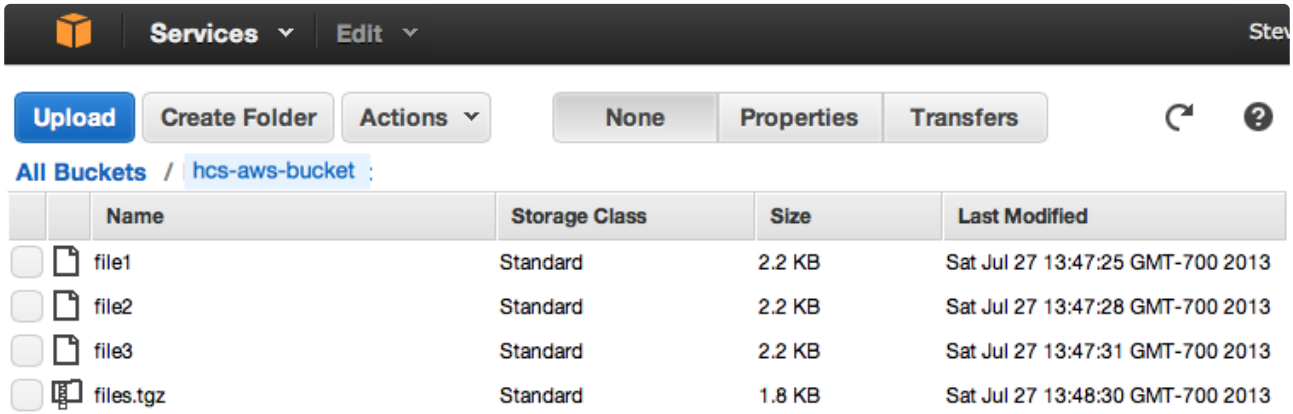
```
# ls
file1  file2  file3
# hcs3 add hcs-aws-bucket file1
# hcs3 add hcs-aws-bucket file2
# hcs3 add hcs-aws-bucket file3
# tar cvfz files.tgz *
```

file1
file2
file3
hcs3 add hcs-aws-bucket files.tgz

And from either the same VM or another VM we can view which files are in the bucket:

hcs3 list hcs-aws-bucket
file1
file2
file3
files.tgz

The files are also visible from within the AWS console:



To pull out a file and decrypt it:

hcs3 get hcs-aws-bucket file2

and to remove a file:

hcs3 rm hcs-aws-bucket file3
hcs3 list hcs-aws-bucket
file1
file2
files.tgz

The files added with `hcs3 add` are encrypted with the default KeyID for that bucket. However, the user can choose to encrypt the files with a custom KeyID. The custom KeyID can be created with a user-selected cipher using `hcl keyid -c`. See the man page for the `hcl` command for details.

The user can specify the custom KeyID with an entry like this:

hcs3 add -k my-own-key-for-s3 hcs-aws-bucket file4

Creating and Managing Buckets

Before uploading encrypted files, the first thing to do is to create a bucket. The following examples assume that you have a Cloud VM Set containing four VMs called client-1, finance, database-server, and acl-server.

Let's assume that we want to move encrypted files between these four VMs (in any direction) via S3 buckets. The first thing we must do is to create a bucket. Bucket names have rules as defined by Amazon, which you can find here: Amazon S3 Bucket Restrictions

Now let's create a bucket called `hcs-aws-bucket.`

```
# hcs3 create hcs-aws-bucket
```

The `hcs3` command creates a default KeyID that is used to encrypt files when they are uploaded to S3. The name of the default KeyID is derived by prepending the bucket name with the characters `hcs3`. This is done so that the admin can differentiate between general KeyIDs and KeyIDs that are created for S3 usage.

Tip: You can also create the bucket in the AWS console. For details, see your AWS documentation.

The list of S3 buckets created can be obtained by running the following command:

```
# hcs3 list
Buckets
--------------------------------------------------
hcs-aws-bucket
```

The S3 bucket created by hcs3 can be deleted by using the following command:

```
# hcs3 delete <bucketname>
```

To remove a bucket, the bucket must first be empty. If not, you will see the following warning:

```
# hcs3 delete hcs-aws-bucket
Error deleting bucket: The bucket you tried to delete is not empty
```

If the bucket is empty and you request that the bucket be deleted, we delete both the bucket and the KeyID, so be warned: if you do use that KeyID to encrypt other files, you will no longer be able to decrypt those files. We highly recommend that you do not use S3 KeyIDs for any other purpose than with the S3 bucket for which they were created.

Using Environment Variables for AWS Credentials

Alternatively, the user can also use environment variables to pass AWS credentials to `hcs3` commands. The following variables are required:

- `AWS_ACCESS_KEY_ID` —AWS access key.
- `AWS_SECRET_ACCESS_KEY` —AWS secret key.

Access and secret key variables override credentials stored in credential and config files.

The hcs3 Interface

The `hcs3` command has a number of options, as follows:

```
Usage: hcs3 [params]
 cmd:
    status
    useraccess <-d | -e no_of_days>
    setstore aws_access_key_id aws_secret_access_key
    create bucketname
    delete bucketname
    list [bucketname]
    add [-k keyid] [-s] bucketname filename
```

```
    rm bucketname filename
    get [-s] bucketname filename [ofilename]
    set property=value
    version
    -h | -?
 property:    tmp    : [pathname, default: /tmp]
```

To use `hcs3`, the first thing you need to do is to create an Amazon AWS account and provide your AWS access key id and secret to the `hcs3` command. This should be called once using `hcs3 setstore` command. For example:

hcs3 setstore TKIAN7ZDFBY2BU36DVPQ FZ9gsvIT1oDvuOiJrdSLRqBvmLZPcxzOWT4Qx7y5

Where:

- `TKIAN7ZDFBY2BU36DVPQ` is the AWS Access KeyId
- `FZ9gsvIT1oDvuOiJrdSLRqBvmLZPcxzOWT4Qx7y5` is the AWS Secret Key

This call should be made on all VMs that are going to require access to the bucket. Once again note that these VMs must reside within the same Cloud VM Set and this call only needs to be made once.

The rest of the options are fairly self explanatory and involve creating or deleting buckets, listing the contents of buckets, adding or extracting encrypted files from the bucket and removing files.

Using Asymmetric KeyIDs

Asymmetric KeyIDs can be used to manage asymmetric keys in Cryptographic Security Platform Vault. Cloud Administrators can either create the asymmetric keys in Cryptographic Security Platform Vault when they create the asymmetric KeyID or can import private and/or public keys. All keys imported should be in Base64 encoded pem format.

This section includes:

- Deleting an Asymmetric KeyID
- Managing Asymmetric KeyID Access
- Managing Asymmetric KeyIDs
- Creating an Asymmetric KeyID

Deleting an Asymmetric KeyID

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. On the **VM Sets** tab, select the Cloud VM Set where you want to revoke the asymmetric KeyID.
4. In the Details area below the list of Cloud VM Sets, click the **Asymmetric KeyIDs** tab.
5. Select the asymmetric KeyID that you want to delete.
6. Select **Actions > Delete Asymmetric KeyID**.
7. In the confirmation window, click **Proceed**.

Managing Asymmetric KeyID Access

You can revoke or restore access to asymmetric KeyIDs using the webGUI. If you revoke access to an asymmetric KeyID, the KeyID is retained in Cryptographic Security Platform Vault but it cannot be used to encrypt or decrypt data until it has been restored.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.

2. In the top menu bar, click **Workloads**.
3. On the **VM Sets** tab, select the Cloud VM Set where you want to revoke asymmetric KeyID access.
4. In the Details area below the list of Cloud VM Sets, click the **Asymmetric KeyIDs** tab.
5. Select the asymmetric KeyID whose access you want to manage and do one of the following:
    - To revoke access to the KeyID, select **Actions > Revoke Asymmetric KeyID Access**, then click **Proceed** at the prompt.
    - To restore access to a revoked KeyID, select **Actions > Unrevoke Asymmetric KeyID Access**, then click **Proceed** at the prompt.

Managing Asymmetric KeyIDs

After you create an asymmetric KeyID, you can change the description in the Cryptographic Security Platform Vault for VM Encryption webGUI . You can also change the expiration date and what happens when the asymmetric KeyID expires.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. On the **VM Sets** tab, select the Cloud VM Set to which the asymmetric KeyID belongs.
4. In the **Details** area below the list of Cloud VM Sets, click the **Asymmetric KeyIDs** tab.
   The Asymmetric KeyIDs tab displays the name, description, expiration date, action open expiration, and the status of the asymmetric KeyID.
5. Select the asymmetric KeyID you want to change from the list.
6. In the Details area below the asymmetric KeyID list, you can change the following information:

Field	Description
Description	A description for the asymmetric KeyID.
Expiration Date	The date on which this asymmetric KeyID expires.
On Expiration	What happens when the asymmetric KeyID expires. You can select: • **No Use**—The key is deactivated but retained. It can then be reactivated by setting a future date in the **Expiration Date** field. This is the default. • **Shred**—The key is destroyed and cannot be retrieved. You should only use this option if you are absolutely certain that you will never need to decrypt files with the selected KeyID again.

Creating an Asymmetric KeyID

When you create an asymmetric KeyID, you can either load a public and private key or allow Cryptographic Security Platform Vault to create the KeyID.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. On the **VM Sets** tab, select the Cloud VM Set where you want to create an asymmetric KeyID.
4. Select **Actions > Create Asymmetric KeyID**.
5. In the Create New Asymmetric KeyID window, complete the following:

Option	Description
KeyID Name	Enter the name to use for the asymmetric KeyID .
CVM Set Name	This field is automatically populated with the selected Cloud VM Set. If you want to add the KeyID to a different Cloud VM Set, enter its name in this field. If you change this name, make sure you use the exact name of the Cloud VM Set shown in the webGUI. The field is case-sensitive, so "SF-Datacenter" is different from "SF-datacenter". If you specify an invalid Cloud VM Set name, the key will not be created.
Description	Enter the optional description for the asymmetric KeyID.
Key Size	Enter the key size. This can be 4096 or 2048.
Public Key	Optionally click Load File to upload the public key in base64 encoded pem format. If you upload a public key you must also upload a matching private key.
Private Key	Optionally click Load File to upload the private key in base64 encoded pem format. If you upload a private key you must also upload a matching public key.

6. Click **Create**.

File-Level Encryption Using KeyIDs

This section describes how to use KeyIDs with the Entrust Cryptographic Security Platform Vault to encrypt objects that can be moved between VMs within a single Cloud VM Set.

An encryption object is simply a file that is encrypted using an encryption key stored within the Cryptographic Security Platform Vault cluster. We refer to these keys by their KeyID names, a symbolic name that references the actual encryption key. The KeyID is available to all VMs within a single Cloud VM Set. You cannot share encrypted data across Cloud VM Sets because the members of one set cannot see the members of any other set.

This section includes:

- Deleting KeyIDs
- Managing KeyID Access
- Changing KeyID Properties
- Envelope Encryption Using KeyIDs
- Using KeyIDs for Encryption and Decryption
- Creating KeyIDs in the webGUI
- Creating KeyIDs with the CLI

Deleting KeyIDs

You can delete KeyIDs with the CLI or the webGUI.

Warning: If you confirm and remove the key, you can no longer decrypt any files that were encrypted using the key. You should not remove a KeyID unless you are absolutely sure that it will not be needed to decrypt a file in the future. If you want to temporarily revoke access to the KeyID, see Managing KeyID Access.

Deleting KeyIDs with the CLI

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. If you want to see the available list of KeyIDs available in this Cloud VM Set, enter the command `hcl keyid -l`. For example:
   ```
   # hcl keyid -l
   Keyid       Algorithm    Description
   -----       ---------    -----------
   hq_key      AES-XTS-512  Secure exchange of HQ data
   ```
3. Enter the command `hcl keyid -r keyid-name`, where *keyid-name* is the name of the KeyID you want to delete.
4. Confirm the removal at the prompt. For example:
   ```
   # hcl keyid -r hq_key
   WARNING: Removal of keyid will result in permanent failure to decrypt anything using that keyid.
   Do you want to proceed? (y/n) y
   ```

Deleting KeyIDs with the webGUI

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. In the **VM Sets** tab, select the Cloud VM Set to which the KeyID belongs.
4. In the **Details** area below the list of Cloud VM Sets, click the **KeyIDs** tab.
5. Select the KeyID you want to delete from the list.
6. Select **Actions > Delete KeyID**.
7. Click **Proceed** at the prompt.

Managing KeyID Access

You can revoke or restore access to KeyIDs using the webGUI. If you revoke access to a KeyID, the KeyID is retained in Cryptographic Security Platform Vault but it cannot be used to encrypt or decrypt data until it has been restored.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. In the **VM Sets** tab, select the Cloud VM Set to which the KeyID belongs.
4. In the **Details** area below the list of Cloud VM Sets, click the **KeyIDs** tab.
5. Select the KeyID whose access you want to manage and do one of the following:
   - To revoke access to the KeyID, select **Actions > Revoke KeyID Access**, then click **Proceed** at the prompt.
   - To restore access to a revoked KeyID, select **Actions > Activate KeyID Access**.

Changing KeyID Properties

After you create a KeyID, you can change the description in either the CLI or the webGUI. In addition, the webGUI allows you to change the expiration date and what happens when the KeyID expires.

Changing the KeyID Description with the CLI

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. If you want to see the available list of KeyIDs available in this Cloud VM Set, enter the command `hcl keyid -l`. For example:
```
# hcl keyid -l
Keyid       Algorithm    Description
-----       ---------    -----------
hq_key      AES-XTS-512  Secure exchange of HQ data
```
3. Enter the command `hcl keyid –u [-d "description"]`, where *description* is the new description for the KeyID. For example:
```
# hcl keyid -u hq_key -d "Key for secure transfer of HQ data"
# hcl keyid -l
Keyid       Algorithm    Description
-----       ---------    -----------
hq_key      AES-XTS-512  Key for secure transfer of HQ data
```

Changing KeyID Properties in the webGUI

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. In the **VM Sets** tab, select the Cloud VM Set to which the KeyID belongs.
4. In the **Details** area below the list of Cloud VM Sets, click the **KeyIDs** tab.
5. Select the KeyID you want to change from the list.
6. In the Details area below the KeyID list, you can change the following information:

Field	Description
Description	A description for the KeyID. This description is shown in the webGUI and the CLI.
Expiration Date	The date on which this KeyID expires.
On Expiration	What happens when the KeyID expires. You can select: • **No Use**—The key is deactivated but retained. It can then be reactivated by setting a future date in the **Expiration Date** field. This is the default. • **Shred**—The key is destroyed and cannot be retrieved. You should only use this option if you are absolutely certain that you will never need to decrypt files with the selected KeyID again.

Envelope Encryption Using KeyIDs

Envelope encryption allows you to encrypt data with a data encryption key (DEK) and then encrypt the DEK for further security. You can use a KeyID to encrypt a DEK that is used for envelope encryption. Cryptographic Security Platform Vault uses the AES-GCM algorithm for encryption. Only 256-bit KeyIDs can be used to encrypt DEKs.

Using KeyIDs for Encryption and Decryption

Once you have created KeyIDs in the Cloud VM Set as described in Creating KeyIDs with the CLI, you can use those KeyIDs to encrypt and decrypt files on any of the VMs in the set.

1. Log into the VM that contains the files you want to copy.
2. If desired, add the files into a single archive file.
   Example:
   ```
   # ls
   file1  file2  file3  file4  file5
   #> zip files.zip *
     adding: file1 (deflated 55%)
     adding: file2 (deflated 55%)
     adding: file3 (deflated 55%)
     adding: file4 (deflated 55%)
     adding: file5 (deflated 55%)
   ```
3. If you want to see the available list of KeyIDs available in this Cloud VM Set, enter the command `hcl keyid -l`.
   For example:
   ```
   # hcl keyid -l
   Keyid         Algorithm    Description
   -----         ---------    -----------
   hq_key        AES-256      Secure exchange of HQ data
   sf_datacenter AES-128      Key for the San Francisco datacenter
   ```
4. Encrypt the files using the command `hcl encryptfile -k keyid filename [encryptedfile]`, where:
   - `keyid` is the name of the KeyID that you want to use for encryption.
   - `filename` is the name of the file that you want to encrypt.
   - `encryptedfile` is the name of the output file that you want `hcl` to create. If you omit this option the command writes the output to `stdout`.

   For example:
   ```
   # hcl encryptfile -k hq_key files.zip files.zip.enc
   ```
5. Copy the encrypted files to any target VM that resides in the same Cloud VM Set.
6. Log into the target VM as an Administrator.
7. Decrypt the file on the target VM using the command `hcl decryptfile encryptedfile [filename]`, where:
   - `encryptedfile` is the name of the encrypted file that you want `hcl` to decrypt. The encrypted file contains information about the KeyID that was used during encryption and uses that KeyID to decrypt the file as long as the KeyID is part of the VM's Cloud VM Set.
   - `filename` is the name of the file to which `hcl` should write the decrypted output. If you omit this option the command writes the output to `stdout`.

   For example:
   ```
   # hcl decryptfile files.zip.enc files.zip
   # unzip files.zip
   Archive:  files.zip
     inflating: file1
     inflating: file2
     inflating: file3
     inflating: file4
     inflating: file5
   ```

Creating KeyIDs in the webGUI

You can also create KeyIDs with the CLI as described in Creating KeyIDs with the CLI.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. On the **VM Sets** tab, select the Cloud VM Set for which you want to add a KeyID. All VMs in the selected set will have access to the KeyID.
4. Select **Actions > Create KeyID**.
5. In the Create New KeyID dialog box, specify the options you want to use.

Field	Description
KeyID Name	The name of the KeyID. You can use special characters and spaces in the KeyID name.
Cloud VM Set	This field is automatically populated with the selected Cloud VM Set. If you want to add the KeyID to a different Cloud VM Set, enter its name in this field. If you change this name, make sure you use the exact name of the Cloud VM Set shown in the webGUI. The field is case-sensitive, so "SF-Datacenter" is different from "SF-datacenter". If you specify an invalid Cloud VM Set name, the key will not be created.
Description	A description for the KeyID. This description is shown in the webGUI and the CLI.
Algorithm	The encryption cipher to use for the KeyID. Note: More ciphers are available if you use the CLI to create the KeyID. For details, see Creating KeyIDs with the CLI.

6. When you are finished, click **Create**.

For details about using the KeyIDs to encrypt and decrypt data, see Using KeyIDs for Encryption and Decryption.

Creating KeyIDs with the CLI

You can also create KeyIDs in the Cryptographic Security Platform Vault webGUI as described in Creating KeyIDs in the webGUI.

1. Log into any one of the VMs in the Cloud VM Set as an Administrator. The KeyID will be shared by all VMs in the set, regardless of which VM it was created on.
2. Create the key by entering the command `hcl keyid -c keyid_to_create [-s] [-a cipher] [-d description] [-e days_to_expire] [-o "NO USE"|"SHRED"]` , where:
   - `-c` specifies the name of the KeyID you want to create. You can use special characters and spaces in the KeyID name.
   - `-s` tells Cryptographic Security Platform Vault to make sure the cipher specified with the `–a` option is compatible with the version of OpenSSL currently installed on the VM.
   - `-a` is the encryption cipher that Cryptographic Security Platform Vault should use for the KeyID.

- On Windows, we support AES-256 and AES-128 only.
- On Linux, to view a list of available ciphers use the `hcl ciphers` command and look at the "List of openssl supported ciphers for (KeyIDs)" section. For example:

```
# hcl ciphers
List of available ciphers:
  AES-XTS-512 (default)
  AES-XTS-256
  AES-256

List of openssl supported ciphers(for KeyIDs):
  AES-XTS-256
  AES-256
  AES-128
```

- `-d` is a description for the KeyID. This description is displayed in the Cryptographic Security Platform Vault webGUI and in the `hcl keyid -l` command, as shown below.
- `-e` allows you to specify the number of days the key should be active before it expires. If you omit this option, the key never expires. What happens when a key expires is controlled by the `-o` option.
- `-o` controls what happens when the key expiry date is reached. You can specify:
  - `"NO USE"` — The key is deactivated but retained. It can then be reactivated by setting a future date in the **Expiry Date** field in the Cryptographic Security Platform Vault webGUI. This is the default.
  - `"SHRED"` — The key is destroyed and cannot be retrieved. You should only use this option if you are absolutely certain that you will never need to access the selected disk again.

  For example:

```
# hcl keyid -c hq_key -a AES-256 -d "Secure exchange of HQ data"
# hcl keyid -c sf-datacenter -a AES-128 -d "Key for the San Francisco datacenter"
```

3. To verify the KeyIDs you have created, enter the command `hcl keyid -l`. For example:

```
# hcl keyid -l
Keyid        Algorithm   Description
-----        ---------   -----------
hq_key       AES-256     Secure exchange of HQ data
sf_datacenter AES-128    Key for the San Francisco datacenter
```

For details about using the KeyIDs to encrypt and decrypt data, see Using KeyIDs for Encryption and Decryption.

Configuring Client-Side Key Caching

When a VM is first registered with Cryptographic Security Platform Vault, Cryptographic Security Platform Vault creates a new key and delivers it to that VM. After the initial registration, Cryptographic Security Platform Vault delivers a new key whenever the VM re-boots and authenticates itself with Cryptographic Security Platform Vault.

If the VM cannot access the Cryptographic Security Platform Vault cluster for a time exceeding the Grace Period, access to clear-text devices is revoked. Also, if the VM is not able to contact the Cryptographic Security Platform Vault cluster on boot, the keys will not be accessible and access will be revoked.

If you want to maintain data access even when Cryptographic Security Platform Vault is not reachable, you can use the CLI to enable the client-side cached key mode for a specific drive in a VM. In this mode, keys can be wrapped in a passphrase and cached on the VM for a specified period of time. If the VM boots and is not

able to access the Cryptographic Security Platform Vault cluster, the keys for this drive can still be accessed by typing the passphrase.

> Note: Client-side key caching is not available for root-encrypted drives, and is not supported on the Windows boot partition.

After a disk has been attached using cached keys, access remains available until either the keys expire or an explicit `hcl detach` command is issued. If the keys have expired, the next time a user attempts to access the disk they will see an error message stating that access is denied. We recommend that you reattach all disks using the normal Cryptographic Security Platform Vault keys as soon as access to Cryptographic Security Platform Vault is restored.

Procedure

1. Log into the VM as `root`.
2. Enter the command `hcl cache [-n number-of-days] [-p passphrase] <diskname | -a>` where:
   - `-n number-of-days` is the number of days for which the keys should be cached. If the `-n` option is not specified, keys will be cached for a default of one day. The max number of days the keys should be cached is 9999 days.
   - `-p passphrase` is the passphrase that should be used to access the cached keys.
   - `diskname | -a` is either a specific disk name or -a for all disks in the VM.

   For example, if you have two disks called sdb1 and sdb2 and you want to cache the keys for sdb1 for 3 days using the passphrase "MyPass", you would enter:
   `# hcl cache -n 3 -p MyPass sdb1`
   If you want to cache the keys for both disks for one day and be prompted for the passphrase, you would enter:
   ```
   # hcl cache -n 1 -a
   Enter passphrase (min 4 characters): ********
   Re-enter passphrase: ********
   Cached keys for device sdb1 sdb2
   ```
3. To verify that the keys are properly cached, enter the command: **hcl cache -l**.
   For example:
   ```
   # hcl cache -l

   Cached keys for Devices
   -------------------------------------------------
   Disk Name       Valid till
   -------------------------------------------------
   sdb1            06/30/17
   sdb2            06/30/17
   ```
4. To access the disks using the cached keys if the Cryptographic Security Platform Vault cluster is unavailable, enter the command: `hcl attach [-l [-p passphrase] ] <diskname | -a>`, where:
   - `-l` instructs Cryptographic Security Platform Vault to look for cached keys.
   - `-p passphrase` is the passphrase for the cached keys.
   - `diskname | -a` is either a specific disk name or -a for all disks in the VM.

   For example, let's say that you cached the keys for disk sdb1 for 3 days but you did *not* cache the keys for device sdb2. Now you want to access both disks when the Cryptographic Security Platform Vault cluster is down. You would enter the following command:
   ```
   # hcl attach -l -a
   passphrase: ********
   ```

Encrypted device sdb1 (/dev/sdb1) attached; decrypted contents visible at /dev/mapper/clear_sdb1
Could not get encryption key for device sdb2
Failed to attach sdb2

Cryptographic Security Platform Vault can access the keys cached for sdb1, but as there is no cached key for sdb2, the attach command fails for sdb2. There is no way to access the content of disk sdb2 until the connection to Cryptographic Security Platform Vault is restored.
A similar issue occurs if you cached the keys for both disks but you used a different passphrase for each one. For example, if you cached the keys for sdb1 using the passphrase "MyPass" and you cached the keys for sdb2 using the passphrase "MyKeys" and you try to attach all disks, you will get the following messages:
hcl attach -l -p MyPass -a
Encrypted device sdb1 (/dev/sdb1) attached; decrypted contents visible at /dev/mapper/clear_sdb1
Could not get encryption key for device sdb2
Failed to attach sdb2

In this case, you would need to issue two separate attach commands to access both disks:
hcl attach -l -p MyPass sdb1
Encrypted device sdb1 (/dev/sdb1) attached; decrypted contents visible at /dev/mapper/clear_sdb1
hcl attach -l -p MyKeys sdb2
Encrypted device sdb2 (/dev/sdb2) attached; decrypted contents visible at /dev/mapper/clear_sdb2

5. To remove the keys cached on a VM, enter the command `cache -r <diskname | -a>`, where:
   diskname | -a is either a specific disk name or -a for all disks in the VM.
   For example, to remove the keys cached for disk sdb1, you would enter:
   `# hcl cache -r sdb1`
   To remove the keys for all disks in the VM, you would enter:
   `# hcl cache -r -a`

Changing the Encryption/Decryption Speed on Windows

When you encrypt, decrypt, or rekey a disk, Cryptographic Security Platform Vault throttles the processing speed so that applications running on the server take priority. If your Windows system is operating under a light load or if you have multiple CPUs, you can increase the processing speed on the disk in real time by changing the rekey throttle speed. You can also save your rekey throttle configuration so that it becomes the default configuration for any disk in the selected VM.

Note: In this procedure, we are using "rekey" to mean initial encryption or decryption as well as actually changing the current encryption key on an already encrypted disk. The rekey throttle speed applies to all three of these operations.

This section includes:

- Changing Encryption/Decryption Speed on a Disk
- Changing the Encryption/Decryption Speed on a VM
- Viewing Encryption/Decryption Settings

Changing Encryption/Decryption Speed on a Disk

Running this command against a particular disk takes effect immediately. However, the rekey throttle setting is effective for that disk only until the system is rebooted.

Before You Begin

To locate the disk number, run the hcl status command.

Summary

KeyControl: 10.238.67.241:443
KeyControl list: 10.238.67.241:443 10.238.67.242:443
Status: Connected
Last heartbeat: Thu May 7 16:36:29 2020 (successful)
AES_NI: enabled

Device details

```
------------------------------------------------------------------------------
Drive     Disk Part Cipher     Status    GUID
------------------------------------------------------------------------------
C:        0    2    none       Avail-Sys N/A
E:        1    1    AES-XTS-512 Attached  758704BF-8E41-4BED-AD8E-2753EED5F469
```

Procedure

1. Log into the Windows VM as an administrator.
2. Enter the following command:
   `hcl set_rekey_throttle [DiskNumber] PendingIoCount PollInterval MaxWaitTime`
   Where:
   - `DiskNumber` is the number of the disk whose configuration you want to set. The changes take effect immediately if a rekey operation is in progress, and are saved until the server is rebooted. If you want to set these values permanently for the VM, use the `config` option.
   - `PendingIoCount` —The background rekey task only runs if the number of pending I/O requests is less than this value. The default is 1, which means that Cryptographic Security Platform Vault will wait for the length of time specified in `MaxWaitTime` before it continues processing if there are any I/O requests on the server. If you want to remove all throttling, set this value to 0 (zero).
     We recommend that you only remove throttling if the server is not running any mission-critical applications or if you have four or more CPUs on your system. Even in these cases, we recommend that you monitor the disk performance during a rekey operation before you set this value to 0 in the default configuration.
   - `PollInterval` is the number of seconds to wait before Cryptographic Security Platform Vault polls the queue to see if there are any pending I/O requests. The default is 1 second.
   - `MaxWaitTime` is the maximum number of seconds to wait before Cryptographic Security Platform Vault rekeys one block of data even if the pending I/O count exceeds the value set in `PendingIoCount`. This ensures that the rekey task will complete eventually with minimal impact to the applications running on the server. The default is 60 seconds.

Changing the Encryption/Decryption Speed on a VM

Running this command will update the rekey speed for all devices on the VM. However, it requires a reboot to take effect.

1. Log into the Windows VM as an administrator.
2. Enter the following command:
   `hcl set_rekey_throttle [config] PendingIoCount PollInterval MaxWaitTime`
   Where:
   - `config` sets the default value for rekey throttle.
   - `PendingIoCount` —The background rekey task only runs if the number of pending I/O requests is less than this value. The default is 1, which means that Cryptographic Security Platform Vault will wait for the length of time specified in `MaxWaitTime` before it continues processing if there are any I/O requests on the server. If you want to remove all throttling, set this value to 0 (zero).

We recommend that you only remove throttling if the server is not running any mission-critical applications or if you have four or more CPUs on your system. Even in these cases, we recommend that you monitor the disk performance during a rekey operation before you set this value to 0 in the default configuration.

- `PollInterval` is the number of seconds to wait before Cryptographic Security Platform Vault polls the queue to see if there are any pending I/O requests. The default is 1 second.
- `MaxWaitTime` is the maximum number of seconds to wait before Cryptographic Security Platform Vault rekeys one block of data even if the pending I/O count exceeds the value set in `PendingIoCount`. This ensures that the rekey task will complete eventually with minimal impact to the applications running on the server. The default is 60 seconds.

These changes will take effect after the next server boot.

Viewing Encryption/Decryption Settings

1. Log into the Windows VM as an administrator.
2. To view the current rekey throttle configuration, enter the command `hcl get_rekey_throttle [DiskNumber|config]`, where:
   - `DiskNumber` is the number of the disk whose configuration you want to check.
   - `config` displays the default values for rekey throttle.

   Examples:

```
C:\Users\Administrator > hcl get_rekey_throttle config
Rekey Throttle Configuration is not set. Default values are
PendingIoCount  : 1
PollInterval    : 1 seconds
Max Wait Time   : 60 seconds
```

   or

```
C:\Users\Administrator > hcl get_rekey_throttle 1
PendingIoCount  : 10
PollInterval    : 5 seconds
Max Wait Time   : 60 seconds
```

Example: Encrypting a Windows VM with New Disks

Empty drives must be given drive letters or folder mounts prior to being managed by Entrust through the Windows Disk Manager. If no drive letters or folder mounts are associated with the drives, Entrust cannot encrypt them.

For example, if you have a new system with two disks (`E:` and `F:`) and a folder mount (`C:\data`) that has been registered with Cryptographic Security Platform Vault, the `hcl status` command would return something similar to the following:

```
C:\> hcl status
Summary
--------------------------------------------------------------------------------
KeyControl: 172.16.163.129:443
KeyControl list: 172.16.163.129:443
Status: Connected
Last heartbeat: Fri May 26 15:31:05 2017 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT
```

```
Device details
--------------------------------------------------------------------------------
Drive      Disk Part Cipher      Status    GUID
--------------------------------------------------------------------------------
C:         0    2    none        Available N/A
E:         1    1    none        Available N/A
C:\data    2    1    none        Available N/A
F:         3    1    none        Available N/A
```

We can now add/attach the drives as follows. Please note that this operation is destructive. It will add the drive and format it.

In this example, the `E:` disk will use the default cipher of AES-XTS-512 and the folder mount `C:\data` disk will use AES-256. For details on the encryption ciphers, see Encryption Key Sizes and Algorithms.

```
C:\>hcl add e:
Encrypted device E: has been added.
dismounting the volume...
formatting...
The type of the file system is RAW.
The new file system is NTFS.
QuickFormatting 535.0 MB
Creating file system structures.
Format complete.
535.0 MB total disk space.
530.6 MB are available.
verify succeeded


C:\>hcl add -c AES-256 C:\data
Encrypted device C:\data has been added.
dismounting the volume...
formatting...
The type of the file system is RAW.
The new file system is NTFS.
QuickFormatting 500.0 MB
Creating file system structures.
Format complete.
500.0 MB total disk space.
495.7 MB are available.
verify succeeded
```

You can now view the attached disks as follows:

```
C:\>hcl status

Summary
--------------------------------------------------------------------------------
KeyControl: 172.16.163.129:443
KeyControl list: 172.16.163.129:443
Status: Connected
Last heartbeat: Fri May 26 15:44:42 2017 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT
```

```
Device details
--------------------------------------------------------------------------------
Drive     Disk Part Cipher     Status    GUID
--------------------------------------------------------------------------------
C:        0    2    none       Available N/A
E:        1    1    AES-XTS-512 Attached  9999CF72-8C81-4B86-BB9B-9F3D9928D635
C:\data   2    1    AES-256    Attached  7B894336-5BC8-41A7-81F8-00BBCF74CA64
F:        3    1    none       Available N/A
```

At this point the encrypted folder mount and disk are formatted and ready to use.

Example: Encrypting a Linux LVM Volume

In Linux, Logical Volume Manager (LVM) is a device mapper target that provides logical volume management for the Linux kernel. You can use the same `hcl add` and `hcl encrypt` commands to register an LVM volume withCryptographic Security Platform Vault, but the Policy Agent cannot stamp a GUID on LVM volumes the way it can with MBR partitions such as `sdb1`. Therefore an LVM cannot be migrated across VMs because that process requires a GUID.

The following examples show the process of encrypting a volume with existing data and registering a new LVM volume.

> Tip: Depending on the size of the disk, the encryption process can take a long time to run. If the process is interrupted, you need to manually restart the process. We recommend you use the Linux `nohup` or `screen` command to avoid terminal-related interruptions during encryption.

Encrypting an LVM Volume with an Existing File System

`hcl encrypt` allows you to encrypt an LVM volume while preserving any data that already exists on the volume. For example:

```
# umount /dev/hytrust-vg/datalv

# hcl encrypt hytrust--vg-datalv -o
All the data on hytrust--vg-datalv will be encrypted
The cleartext data will be available on /dev/mapper/clear_hytrust--vg-datalv
This operation may take long time.
Do you want to proceed? (y/n) y
hytrust--vg-datalv (/dev/dm-2) appears to contain an existing filesystem (ext2)
Do you want to proceed? (y/n) y
WARNING: device hytrust--vg-datalv will be added but will not have unique ID that ensures detection if disks are reordered or moved.
Encrypted device hytrust--vg-datalv (/dev/dm-2) attached; decrypted contents visible at /dev/mapper/clear_hytrust--vg-datalv
total device size 102400 K
Processing: 100%    Time left: 00:00:00
Completed encryption of hytrust--vg-datalv successfully
```

Registering a New LVM Volume

`hcl add` allows you to add a new volume to Cryptographic Security Platform Vault, or to erase any data from an existing volume before the volume is encrypted. For example:

```
# lvs
  LV   VG     Attr     LSize    Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  datalv hytrust-vg -wi-a-----  100.00m
  root   sub1504-vg -wi-ao----    6.73g
  swap_1 sub1504-vg -wi-ao---- 1020.00m

# hcl status
Summary
--------------------------------------------------------------------------------
KeyControl: skc1:443
KeyControl list: skc1:443
Status: Connected

Registered Devices
--------------------------------------------------------------------------------
Disk Name         Cipher      Status               Clear
--------------------------------------------------------------------------------

Available Devices
--------------------------------------------------------------------------------
Disk Name         Device Node                Size (in MB)
--------------------------------------------------------------------------------
hytrust--vg-datalv  /dev/dm-2                  100

Other Devices
--------------------------------------------------------------------------------
Disk Name         Device Node                Status
--------------------------------------------------------------------------------
sda1              /dev/sda1                  Mounted (/boot)
sdb               /dev/sdb                   LVM (hytrust-vg)
sda5              /dev/sda5                   LVM (sub1504-vg)
sub1504--vg-root    /dev/dm-0                    Mounted (/)
sub1504--vg-swap_1  /dev/dm-1                     Mounted (swap)

# hcl add hytrust--vg-datalv
WARNING: device hytrust--vg-datalv will be added but will not have unique ID that ensures detection if
disks are reordered or moved.
WARNING: This operation will destroy the contents of the disk.
If you wish to preserve them, run "hcl encrypt" instead.
Do you want to proceed? (y/n) y
Encrypted device hytrust--vg-datalv (/dev/dm-2) attached; decrypted contents visible at /dev/mapper/
clear_hytrust--vg-datalv

Creating file system ext3 on /dev/mapper/clear_hytrust--vg-datalv
--------------------------------------------------------------------------------
mke2fs 1.42.12 (29-Aug-2014)
Creating filesystem with 102400 1k blocks and 25688 inodes
Filesystem UUID: d3d987b4-4773-4e15-995d-a1669603db0a
Superblock backups stored on blocks:
    8193, 24577, 40961, 57345, 73729

Allocating group tables: done
Writing inode tables: done
```

```
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done
-------------------------------------------------------------------------------

# hcl status
Summary
-------------------------------------------------------------------------------
KeyControl: skc1:443
KeyControl list: skc1:443
Status: Connected

Registered Devices
-------------------------------------------------------------------------------
Disk Name         Cipher      Status               Clear
-------------------------------------------------------------------------------
                  AES-XTS-512 Attached             hytrust--vg-datalv/dev/mapper/clear_hytrust--vg-datalv
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT

Available Devices
-------------------------------------------------------------------------------
Disk Name         Device Node                Size (in MB)
-------------------------------------------------------------------------------

Other Devices
-------------------------------------------------------------------------------
Disk Name      Device Node                Status
-------------------------------------------------------------------------------
sda1           /dev/sda1                  Mounted (/boot)
sdb            /dev/sdb                   LVM (hytrust-vg)
sda5           /dev/sda5                  LVM (sub1504-vg)
sub1504--vg-root    /dev/dm-0             Mounted (/)
sub1504--vg-swap_1  /dev/dm-1             Mounted (swap)

# lvs
  LV   VG     Attr     LSize    Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  datalv hytrust-vg -wi-a-----  100.00m
  root   sub1504-vg -wi-ao----    6.73g
  swap_1 sub1504-vg -wi-ao---- 1020.00m

# hcl status
Summary
-------------------------------------------------------------------------------
KeyControl: skc1:443
KeyControl list: skc1:443
Status: Connected

Registered Devices
-------------------------------------------------------------------------------
Disk Name         Cipher      Status               Clear
-------------------------------------------------------------------------------

Available Devices
-------------------------------------------------------------------------------
```

```
Disk Name         Device Node                Size (in MB)
-------------------------------------------------------------------------------
hytrust--vg-datalv  /dev/dm-2                  100

Other Devices
-------------------------------------------------------------------------------
Disk Name         Device Node                Status
-------------------------------------------------------------------------------
sda1              /dev/sda1                  Mounted (/boot)
sdb               /dev/sdb                   LVM (hytrust-vg)
sda5              /dev/sda5                   LVM (sub1504-vg)
sub1504--vg-root    /dev/dm-0                    Mounted (/)
sub1504--vg-swap_1  /dev/dm-1                     Mounted (swap)

# hcl add hytrust--vg-datalv
WARNING: device hytrust--vg-datalv will be added but will not have unique ID that ensures detection if
disks are reordered or moved.
WARNING: This operation will destroy the contents of the disk.
If you wish to preserve them, run "hcl encrypt" instead.
Do you want to proceed? (y/n) y
Encrypted device hytrust--vg-datalv (/dev/dm-2) attached; decrypted contents visible at /dev/mapper/
clear_hytrust--vg-datalv

Creating file system ext3 on /dev/mapper/clear_hytrust--vg-datalv
-------------------------------------------------------------------------------
mke2fs 1.42.12 (29-Aug-2014)
Creating filesystem with 102400 1k blocks and 25688 inodes
Filesystem UUID: d3d987b4-4773-4e15-995d-a1669603db0a
Superblock backups stored on blocks:
    8193, 24577, 40961, 57345, 73729

Allocating group tables: done
Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done
-------------------------------------------------------------------------------

# hcl status
Summary
-------------------------------------------------------------------------------
KeyControl: skc1:443
KeyControl list: skc1:443
Status: Connected

Registered Devices
-------------------------------------------------------------------------------
Disk Name         Cipher       Status               Clear
-------------------------------------------------------------------------------
                  AES-XTS-512  Attached             hytrust--vg-datalv/dev/mapper/clear_hytrust--vg-datalv
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT

Available Devices
-------------------------------------------------------------------------------
```

```
Disk Name          Device Node                 Size (in MB)
-------------------------------------------------------------------------------

Other Devices
-------------------------------------------------------------------------------
Disk Name       Device Node                 Status
-------------------------------------------------------------------------------
sda1            /dev/sda1                   Mounted (/boot)
sdb             /dev/sdb                    LVM (hytrust-vg)
sda5            /dev/sda5                   LVM (sub1504-vg)
sub1504--vg-root    /dev/dm-0                   Mounted (/)
sub1504--vg-swap_1  /dev/dm-1                   Mounted (swap)
```

The file system can now be created on the clear-text device.

```
# mkfs /dev/mapper/clear_hytrust--vg-datalv
mke2fs 1.42.12 (29-Aug-2014)
/dev/mapper/clear_hytrust--vg-datalv contains a ext3 file system
   created on Tue May  3 17:54:22 2016
Proceed anyway? (y,n) y
Creating filesystem with 102400 1k blocks and 25688 inodes
Filesystem UUID: f4a9c9ca-d451-4d20-9a32-6cdf5de844d8
Superblock backups stored on blocks:
   8193, 24577, 40961, 57345, 73729

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done

# mkdir /tmp/mnt
# mount /dev/mapper/clear_hytrust--vg-datalv /tmp/mnt

# hcl rm hytrust--vg-datalv
WARNING: Removal of devices will cause any data stored on them to be permanently lost.
Do you want to proceed? (y/n) y
Removed device hytrust--vg-datalv
```

Example: Adding an Encrypting a Linux Disk with XFS

> Tip: Depending on the size of the disk, the encryption process can take a long time to run. If the process is interrupted, you need to manually restart the process. We recommend you use the Linux `nohup` or `screen` command to avoid terminal-related interruptions during encryption.

Encrypting an Existing XFS Disk

In following example we create an XFS filesystem and then use `hcl encrypt` to register that filesystem with Cryptographic Security Platform Vault. The example that follows shows how to do this in a single step using `hcl add`.

```
# mkfs -t xfs /dev/sdc1
meta-data=/dev/sdc1              isize=256    agcount=4, agsize=62436 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0
data     =                       bsize=4096   blocks=249744, imaxpct=25
```

```
=                   sunit=0      swidth=0 blks
naming   =version 2             bsize=4096   ascii-ci=0 ftype=0
log      =internal log          bsize=4096   blocks=853, version=2
=                   sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                  extsz=4096   blocks=0, rtextents=0

# mount | grep sdc1
/dev/sdc1 on /mnt type xfs (rw,relatime,seclabel,attr2,inode64,noquota)

# cp /etc/* /mnt
# find  /mnt -type f -exec md5sum {} \; | md5sum
     5cf56f73de26edf599cb3a8c5887ebe0  -

# umount /mnt

# hcl encrypt /dev/sdc1
All the data on /dev/sdc1 will be encrypted
The cleartext data will be available on /dev/mapper/clear_sdc1
This operation may take long time
Do you want to proceed? (y/n) y

total device size 998976 KB

Processing: 100%  Time left: 00:00:00
rekey finished

Completed encryption of /dev/sdc1 successfully
# mount /dev/mapper/clear_sdc1 /mnt

# mount | grep sdc1
/dev/mapper/clear_sdc1 on /mnt type xfs (rw,relatime,seclabel,attr2,inode64,noquota)

#  find  /mnt -type f -exec md5sum {} \; | md5sum
     5cf56f73de26edf599cb3a8c5887ebe0  -
```

Adding a New Disk with XFS

In following example we use `hcl add` to create an XFS filesystem on the disk and then register the disk with Cryptographic Security Platform Vault.

```
# hcl add -F xfs /dev/sdc1
/dev/sdc1 (/dev/sdc1) appears to contain an existing filesystem (ext3)
Do you want to proceed? (y/n) y

WARNING: This operation will destroy the contents of the disk.
If you wish to preserve them, run "hcl encrypt" instead.
Do you want to proceed? (y/n) y

In case of error remove the disk using "hcl rm" and run "hcl add" again

Encrypted device sdc1 (/dev/sdc1) attached; decrypted contents visible at /dev/mapper/clear_sdc1

Creating file system xfs on /dev/mapper/clear_sdc1
--------------------------------------------------------------------------------
```

```
meta-data=/dev/mapper/clear_sdc1 isize=256    agcount=4, agsize=62436 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0
data     =                       bsize=4096   blocks=249744, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal log           bsize=4096   blocks=853, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
-------------------------------------------------------------------------
```

mount /dev/mapper/clear_sdc1 /mnt

> Note: If the `mkfs` command is done as part of the `hcl add` command and it fails, then you will need to run it separately after resolving the issue. This must be done before you run the `mount | grep sdc1` command.

```
# mount | grep sdc1
/dev/mapper/clear_sdc1 on /mnt type xfs
(rw,relatime,seclabel,attr2,inode64,noquota)
```

Combining VMware vSphere VDI with the CSP Vault

You can use VMware vSphere and Entrust Cryptographic Security Platform Vault in combination to create an encrypted virtual desktop infrastructure (VDI) that you can then clone as many times as needed. The clones can be managed individually through Cryptographic Security Platform Vault, and each clone can have its own set of encryption keys.

Before You Begin

Make sure you know the IP addresses or MAC addresses that you want to use for the clones. You need to register the addresses with Cryptographic Security Platform Vault before you create a clone from the master VM.

Every clone must have a unique IP or MAC address registered with Cryptographic Security Platform Vault. Therefore, if you want to deploy 10 clones, you would need to register 10 unique IP addresses or MAC addresses with Cryptographic Security Platform Vault before you deployed the 10 clones.

Procedure

1. Create the master VM that you want to use to create the clones. If you already have a VM that is fully set up and encrypted by Entrust Cryptographic Security Platform Vault, proceed to the next step.
    a. Set up a VM with all the required software and configuration settings according to your company's VDI requirements. Once the VM is fully set up it becomes the "Master VM".
    b. Install the latest Entrust Policy Agent on the Master VM and register it with Cryptographic Security Platform Vault as described in Linux Policy Agent Installation.
    c. Encrypt the required data disks as described in Encrypting a Windows Disk Using the Entrust Policy Agent GUI or Encrypting a Disk Using the CLI.
    d. If required, encrypt the root or system drives as described in Linux Root, Swap, and System Device Encryption or Windows Boot Drive Encryption.
2. As a precaution, take a snapshot of the Master VM at this point.
3. Register the IP addresses or MAC addresses you want to use for the clones by running the `hcl template` command on the Master VM once for each clone you want to register. To do so:

a. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
b. Enter the command `hcl template <-i ipaddr | -m macaddr> [-u username [-p password]] days_to_expire`, where:
   - `<-i ipaddr | -m macaddr>` is either `-i` and an IP address or `-m` and a MAC address.
   - `-u` is a Cryptographic Security Platform Vault user account with Cloud Admin privileges. If you do not specify the account name, hcl prompts you for the information.
   - `-p` is the password for the Cryptographic Security Platform Vault account. If you do not specify this password you will be prompted for the information.
   - `days_to_expire` is the number of days for which the access will remain valid for the clone. After access expires the clone will not be able to register itself with Cryptographic Security Platform Vault and access to the clone will be denied. If you do not want the access to ever expire, specify 0 (zero) for this option.

   For example, if you want to register a template with the MAC address `00-80-c0-8f-45-c8` that is valid for 30 days, you would enter:

   ```
   # hcl template -m 0080c08f45c8 -u CloudAdmin -p DogDays123! 30
   ```

   If you want to register a template with the IP address 192.168.140.150 that never expires, you would enter:

   ```
   # hcl template -i 192.168.140.150 -u CloudAdmin -p DogDays123! 0
   ```

   If you want to prepare a group of clones with consecutive IP addresses, you can create a script that calls the `hcl template` command once for each clone. For example, if you want to prepare 30 clones that will be available for 365 days starting with the IP address 192.168.140.150 and ending with the IP address 192.168.140.180, you could include the following in your script:

   ```
   i=150
   while [[ $i -lt 181 ]]; do
     hcl template -i 192.168.140.$i -u CloudAdmin -p DogDays123! 365
     i='expr+1'
   done
   ```

c. For each clone you want register for this VM, repeat the `hcl template` command specifying a unique IP or MAC address each time.
d. To view a list of reserved IP and MAC addresses in the system, enter the command `hcl template list`.
e. If you want to unregister a clone IP or MAC address, enter the command `hcl template remove <-i ipaddr | -m macaddr> [-u username [-p password]]`.

4. When you are done registering the IP or MAC addresses you want to use, you can either create a vSphere Template from the Master VM, or you can simply clone the existing Master VM without making it a Template. Both methods work equally well with Cryptographic Security Platform Vault. For more information about vSphere Templates, see your vSphere documentation.
5. Create the clones you want to use by selecting either **Clone > Clone to Virtual Machine** or **New VM from This Template**, depending on whether you set the master VM up as a vSphere Template in the proceeding step.
   Important: Do NOT power on the clones at this point.
6. After the clones have been deployed, manually set the IP or MAC addresses to match the ones you already registered with Cryptographic Security Platform Vault. How you do this depends on what version of the vSphere Client that you are using.
7. After you have verified that the IP or MAC for the clones match the addresses that were registered with Cryptographic Security Platform Vault, you can power on the clones.

If the root drive of the master VM was encrypted, when each clone VM boots, it contacts Cryptographic Security Platform Vault during boot. Cryptographic Security Platform Vault provides the keys for root drive and lets the clone VM boot. If the root drive was not encrypted, the clone VM will simply boot normally.
If you log into the Cryptographic Security Platform Vault webGUI, the clone VM appears on the **Cloud > VMs** tab with the following name:

<original hostname>-<mac address of clone>

For example, you could see the following VM names in the webGUI:
win2016master
win2016master-0080c01f45c5
win2016master-0080c02f46c6
win2016master-0080c03f47c7

Once a clone has successfully powered on and contacted Cryptographic Security Platform Vault, you can then manage it like any other VM that is registered with Cryptographic Security Platform Vault. By default, Cryptographic Security Platform Vault uses the same encryption key for the Master VM and all of the clone VMs. If you want each clone to have its own encryption key, you can rekey each clone VM as described in Rekeying a Disk Using the webGUI or Rekeying a Disk using the CLI.

Removing Expired Clones

At the end of the VDI life cycle, the clone VM is deleted from the hypervisor. This can happen as a result of administrator action through the vSphere Client or the Horizon GUI.

Before a clone VM is deleted, you need to unregister it from Cryptographic Security Platform Vault. This removes the address of the clone from Cryptographic Security Platform Vault so that the same address can be used again later. Otherwise, you will have "orphan" names in Cryptographic Security Platform Vault which will prevent you from reusing those addresses.

Important: Removing a clone from Cryptographic Security Platform Vault without decrypting the data first means that the data on all encrypted disks will be lost. If you want to decrypt the data first, see Decrypting a Disk Using the CLI.

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. Remove the VM using the CLI or the Entrust Python-based REST API. After the clone VM has been removed, none of its encrypted drives can be accessed. If the clone boot partition was encrypted, the clone is powered off after it is removed from Cryptographic Security Platform Vault.
    - If you want to use the CLI, enter the command `hcl unregister [-a] [-u username [-p password]] [-y]`, where:
        - `-a` tells `hcl` that the VM is registered with Cryptographic Security Platform Vault but it is currently unauthenticated. This option requires Cryptographic Security Platform Vault Cloud Admin user account credentials. Omit this option if the VM is currently registered and authenticated with Cryptographic Security Platform Vault.
        - `-u` is a Cryptographic Security Platform Vault user account with Cloud Admin privileges. If you do not specify the account name, `hcl` prompts you for the information.
        - `-p` is the password for the Cryptographic Security Platform Vault account. If you do not specify this password you will be prompted for the information.
        - `-y` tells the command to run non-interactively.
    - If you want to use the API:
        i. Make sure Python is available on the VM.
        ii. If needed, install the Entrust APIs on the machine from which you want to do the clean up. You can download the API package from the Cryptographic Security Platform Vault webGUI by clicking **Cloud** in the top menu bar, selecting **Actions > Download Policy Agent**, then

downloading the file called `hcs-api-RelaseNumber-BuildNumber.tgz`. For example, `hcs-api-10.4.6-12346M.tgz`.

iii. Copy the `hcs-api-RelaseNumber-BuildNumber.tgz` file to the VM and unpack the archive so that you have an `hcs-api` directory with 5 python files and one executable called `hicli`.

iv. Create a Python script with the following lines:

```
keycontrol=$1
cvmset=$2
clonevm=$3
username=$4
password=$5
hicli kc select $keycontrol
hicli user login $username --password=$password
hicli cvmset select $cvmset
yes | hicli cvm rm $clonevm
```

Where `$username` is a Cryptographic Security Platform Vault user account with Cloud Admin privileges and `$password` is the password for that Cryptographic Security Platform Vault account.

Decrypting a Linux System Device

If you encrypted a Linux system device (such as `/root`, `swap`, or `/home`) with the `htroot encrypt` command, you need to decrypt that system device with the `htroot decrypt` command.

Important: This procedure applies to Linux system devices *only*. If you want to decrypt a Linux data drive, see Decrypting a Disk Using the webGUI or Decrypting a Disk Using the CLI.

During this procedure, the VM will need to be rebooted to start the decryption process. If you have enabled Online Encryption for this VM, the VM will come back online immediately and the Policy Agent will decrypt the system devices as a background process. In this case, users can continue to access the data while it is being decrypted as long as the VM remains online. If the VM reboots during this process, the VM will remain inaccessible for normal operations until the Policy Agent has finished decrypting all of the specified system devices.

If Online Encryption is *not* enabled, the VM will remain inaccessible for normal operations until the decryption process completes.

For more information about Online Encryption, see Linux Online Encryption Prerequisites and Considerations.

Before You Begin

You cannot decrypt a disk if it has an Access Control Policy associated with it. Make sure that no such policy association exists before you decrypt the disk. For details, see Viewing the Access Control Status for a Disk.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**, and then click the VMs tab.
3. On the **Details** tab for the VM, make sure that:
   - The **Auto Encryption** property is either **Disabled** or the Automatic Data Encryption Policy does *not* include the disk you want to decrypt. If the Auto Encryption Policy Type is set to exclude, then the disks included as per policy can *not* be decrypted.

- The **Decryption Allowed** property is set to **Yes**. If this field is set to **No**, click **No**, select **Yes** from the drop-down list, then click **Save**.

Tip: If you want to decrypt the disks on multiple VMs in this Cloud VM Set, you can change these properties at the Cloud VM Set level and propagate the changes to all VMs in the Cloud VM Set. For more information, see Changing Cloud VM Set Properties.

4. Log into the VM as `root`.
5. If you want to check the available disks on this VM, enter the `hcl status` command. The Registered Devices section shows all devices that have been encrypted on the VM, with the short form of the disk name in the first column. You will need this short name in order to decrypt the device.
   Example:

```
# hcl status

Summary
--------------------------------------------------------------------------------
KeyControl: sdkc:443
KeyControl list: sdkc:443
Status: Connected
Last heartbeat: Tue Jul 31 12:06:22 2018 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT
HTCRYPT: Not Installed

Registered Devices
--------------------------------------------------------------------------------
Disk Name       Cipher      Status              Clear
--------------------------------------------------------------------------------
sda3            AES-XTS-512  Attached           /dev/mapper/
clear_D4044351-4C2C-4582-8935-479B5238B23A (swap)
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
sda2            AES-XTS-512  Attached           /dev/mapper/clear_htroot (/)
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT

Available Devices
--------------------------------------------------------------------------------
Disk Name       Device Node              Size (in MB)
--------------------------------------------------------------------------------
sdc2            /dev/sdc2                119
sdc1            /dev/sdc1                118

Other Devices
--------------------------------------------------------------------------------
Disk Name       Device Node              Status
--------------------------------------------------------------------------------
sda1            /dev/sda1                Mounted (/boot)
sdd             /dev/sdd                 LVM (vg-sdd)
```

6. If you want to check the encryption status of the system devices, enter the `htroot status` command. You cannot decrypt a device that is in the process of being encrypted or rekeyed.

```
# htroot status

HyTrust boot loader setup is complete
```

Root device "/dev/sda2" is encrypted
swap device "/dev/sda3" is encrypted

7. Enter the `htroot decrypt <diskname1,diskname2,... | -a>` command, where each `diskname` is the short form of the disk name. (For example, `sda2` instead of `/dev/sda2`.) To specify multiple disks, use a comma-seperated list. To decrypt all available system devices, specify `-a` instead of a list of disk names. (If you specify `-a`, Cryptographic Security Platform Vault only decrypts the system devices. It does *not* decrypt any encrypted data devices.)
For example:
htroot decrypt -a

Setting up system for root device decryption.
This operation may take a long time

Do you want to proceed? (y/N) y
Changing /etc/fstab to mount file system / from UUID=03d7a977-72b1-48bc-b1f0-3bc78f61a815
Changing /etc/fstab to mount the swap from UUID=9217649b-e08c-4703-9d51-c7000b3321a8
The system has been updated to decrypt the Linux root device/s during next boot; please reboot the system now
Do you want to reboot the system now? (y/N) y

8. Confirm the server reboot to continue. When the server has rebooted, it authenticates itself with Cryptographic Security Platform Vault to get the required keys and then starts the decryption process. The time required to decrypt the devices depends on their size and the type of storage you have.
   - If you have enabled Online Encryption for this VM, the VM reboots immediately and the Policy Agent decrypts the devices as a background process. In this case, you can check the decryption status at any time using the `hcl status` command.
   - If Online Encryption is not enabled, the VM remains offline until the decryption process completes. In this case, you can see the decryption progress on the VM console through vSphere, Azure, or AWS.

Decrypting a Disk Using the CLI

The following procedure explains how to decrypt a disk and remove it from Cryptographic Security Platform Vault. If you want to remove the disk but you don't care about the contents of the disk, see Removing a Disk from the CSP Vault for VM Encryption.

The following procedure applies to all types of Windows disks and to Linux data disks. You cannot, however, decrypt a Linux system device (such as `/root`, `swap`, or `/home`) using this procedure. Instead, use the `htroot decrypt` command as described in Decrypting a Linux System Device.

Before You Begin

You cannot decrypt a disk if it has an Access Control Policy associated with it. Make sure that no such policy association exists before you decrypt the disk. For details, see Viewing the Access Control Status for a Disk.

> Tip: Depending on the size of the encrypted disk, the decryption process can take a long time to run. If the decryption process is interrupted on Windows, it will be resumed automatically when the disk comes back online. If the process is interrupted on Linux, you need to manually reissue the `hcl decrypt` command to resume the process. We recommend you use the Linux `nohup` or `screen` command to avoid terminal-related interruptions during decryption.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**, and then click the VMs tab.
3. On the **Details** tab for the VM, make sure that:
   - The **Auto Encryption** property is either **Disabled** or the Automatic Data Encryption Policy does *not* include the disk you want to decrypt. If the Auto Encryption Policy Type is set to exclude, then the disks included as per policy can *not* be decrypted.
   - The **Decryption Allowed** property is set to **Yes**. If this field is set to **No**, click **No**, select **Yes** from the drop-down list, then click **Save**.

   Tip: If you want to decrypt the disks on multiple VMs in this Cloud VM Set, you can change these properties at the Cloud VM Set level and propagate the changes to all VMs in the Cloud VM Set. For more information, see Changing Cloud VM Set Properties.
4. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
5. If this is a Linux system and you have *not* enabled Online Encryption for this VM, unmount the disk you want to decrypt. For more information about enabling Online Encryption, see Linux Online Encryption Prerequisites and Considerations.
6. Enter the `hcl decrypt [-s] [-y] diskname` command, where:
   - `-s` (Linux only) tells Cryptographic Security Platform Vault to only process allocated blocks which can improve performance dramatically. Cryptographic Security Platform Vault uses system-provided utilities to determine the allocated blocks on the disk. This option is supported for ext2, ext3, and ext4 file systems. It is *not* supported on XFS. (To change the speed for Windows, see Changing the Encryption/Decryption Speed on Windows.)
     Important: This option does not work if online encryption has been enabled for the VM, even if you unmount the drive during the process. If online encryption has been enabled or if the disk is mounted, using the `-s` option will cause the command to fail.
   - `-y` makes the command non-interactive.
   - `diskname` is the name of the disk that you want to encrypt. For Linux, use the short form of the disk name. (For example, `sdb1` instead of `/dev/sdb1`.) For Windows, specify the drive letter or folder mount associated with the disk. (For example, `f:` or `g:\data`).

   Cryptographic Security Platform Vault decrypts the disk and unregisters it with Cryptographic Security Platform Vault. Any keys associated with the disk are deleted.
   For Linux, you can now mount the disk in the standard manner and access its contents in plain text. For Windows, all drives and folder mounts are immediately accessible in plain text.
   For example:

```
# hcl decrypt -s sdb1

All the data on /dev/mapper/clear_sdb1 will be decrypted
The clear text data will be available on /dev/sdb1
This operation may take long time
Do you want to proceed? (y/n) y
total device size 1044193 KB
Processing: 100%    Time left: 00:00:00
Completed decryption of sdb1 successfully
Removed device sdb1
```

Decrypting a Disk Using the Windows Policy Agent GUI

The following procedure explains how to decrypt a disk and remove it from Cryptographic Security Platform Vault. If you want to remove the disk but you don't care about the contents of the disk, see Removing a Disk from the Cryptographic Security Platform Vault for VM Encryption.

The following procedure applies to Windows disks only.

Before You Begin

You cannot decrypt a disk if it has an Access Control Policy associated with it. Make sure that no such policy association exists before you decrypt the disk. For details, see Viewing the Access Control Status for a Disk.

> Tip: Depending on the size of the encrypted disk, the decryption process can take a long time to run. If the decryption process is interrupted on Windows, it will be resumed automatically when the disk comes back online.

Procedure

1. Log into the Windows system using an account with Administrator privileges.
2. Select **Start > All Programs > Entrust > Entrust DataControl** or start Windows PowerShell and enter the `hclGUI` command.
3. Right-click on the disk that you want to decrypt and select **Decrypt**.
4. Click **Yes** on the confirmation screen.

You can track the decryption status on the Policy Agent GUI. When the decryption has finished, click the Refresh button at the top to refresh the window.

Decrypting a Disk Using the webGUI

The following procedure applies to all types of Windows disks and to Linux data disks. You cannot, however, decrypt a Linux system device (such as `/root`, `swap`, or `/home`) using this procedure. Instead, use the `htroot decrypt` command as described in Decrypting a Linux System Device.

Before You Begin

You cannot decrypt a disk if it has an Access Control Policy associated with it. Make sure that no such policy association exists before you decrypt the disk. For details, see Viewing the Access Control Status for a Disk.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab and select the VM you want to work with from the list.
4. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
5. On the **Details** tab for the VM, make sure that:
   - The **Auto Encryption** property is either **Disabled** or the Automatic Data Encryption Policy does *not* include the disk you want to decrypt. If the Auto Encryption Policy Type is set to exclude, then the disks included as per policy can *not* be decrypted.
   - The **Decryption Allowed** property is set to **Yes**. If this field is set to **No**, click **No**, select **Yes** from the drop-down list, then click **Save**.

   Tip: If you want to decrypt the disks on multiple VMs in this Cloud VM Set, you can change these properties at the Cloud VM Set level and propagate the changes to all VMs in the Cloud VM Set. For more information, see Changing Cloud VM Set Properties.
6. Click on the **Encrypted Disks** tab.
7. Select the disk you want to decrypt and select **Actions > Decrypt Disk** from the VM-specific **Actions** menu.

Cryptographic Security Platform Vault displays a message that the decrypt request was successfully created and adds a **Decrypt Disk** task for the VM that will begin on the VM's next heartbeat. The length of time the operation will take depends on the amount of data already present on the disk and the encryption settings configured for this system.
You can track the progress of the decrypt task on the Dashboard in the **Tasks** tile.
When the decrypt request begins processing, Cryptographic Security Platform Vault sets the state to **Active/Decrypt**. When the encryption process has finished, Cryptographic Security Platform Vault moves the disk back to the **Unencrypted Disks** tab and changes the state to **Available**.

Encryption Key Maintenance

Disks are encrypted with a key created and safeguarded by Cryptographic Security Platform Vault. If the key is lost, the encrypted data on the disk cannot be accessed because it cannot be decrypted. When a disk is rekeyed, each block of data is decrypted using the old key and then re-encrypted using the new key.

You should immediately rekey a disk if you believe there has been a security breach. As a precaution, you can also have Cryptographic Security Platform Vault rekey all or selected disks in the system on a periodic basis. The trade off is in performance—rekeying a disk increases the security but takes system resources and may adversely affect the applications running on the server that is being rekeyed.

Important: After you rekey one or more disks, you should create a new Cryptographic Security Platform Vault backup file that contains the new keys. If you restore Cryptographic Security Platform Vault from a backup file made before the disks were rekeyed, the new keys will be lost and you will not be able to access the encrypted data.

This section includes:

- Setting the Key Expiration Date for a Disk
- Pausing a Rekey Operation on Windows
- Configuring Auto Rekey for a VM
- Configuring Auto Rekey for a Cloud VM Set
- Rekeying a Linux System Device
- Rekeying a Disk using the CLI
- Rekeying a Disk using the Policy Agent GUI
- Rekeying a Disk Using the webGUI

Setting the Key Expiration Date for a Disk

By default, the key assigned to a disk never expires. If you want the disk to only be available for a specified amount of time, you can set a key expiration date. What happens when the key expires depends on how you have configured the system.

Before you change the date, keep in mind that:

- If the VM belongs to a Cloud VM Set that has an associated KEK (Key Encryption Key), you cannot set the disk key expiration date beyond the expiration date set for the KEK. For details about viewing the KEK properties, see Changing KEK Properties.
- If the VM belongs to a Cloud VM Set that uses the SEK (Single Encryption Key) option, changing the key expiry date or expiration option for the disk changes the expiry date or expiration option for all disks in the Cloud VM Set that use the same version of the SEK key as the selected disk. For more information about the SEK option, see Data Deduplication with Cloud VM Sets.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.

3. Click the **VMs** tab and select the VM you want to work with from the list.
4. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
5. Click the **Encrypted Disks** tab and select the disk whose expiration date you want to set. Cryptographic Security Platform Vault displays the **Expiry Date** and **On Expiration** properties for the selected disk below the table.
6. If the **Expiry Date** field displays:
   - **Never**, click **Never** and enter a date in the format mm/dd/yyyy or click the calendar icon and select the day from the pop up calendar.
   - A date, change the date using the field or the calendar icon. To set the key expiration back to **Never**, click **Clear**.

   If the date is valid and the Cloud VM Set to which this VM belongs uses a SEK key, confirm that you want to make the same expiry date change to all disks on all VMs in the Cloud VM Set that use the same version of the SEK key as the selelcted disk.
   Cryptographic Security Platform Vault displays a message that the request was successful and updates the information for the disk in the Disk table. If there is a problem, check whether the Cloud VM Set to which this VM belongs has an associated KEK. If it does, you cannot change the key expiration date for the disk beyond the date specified for the KEK.
7. If desired, change what happens when the expiration date arrives. You can select:
   - **No Use**—The key is deactivated but retained. It can be reactivated by setting a future expiration date, or by setting the expiration date to "Never". At that point, all access to the encrypted data will be restored. This is the default.
   - **Shred**—The key is destroyed and cannot be retrieved. You should only use this option if you are absolutely certain that you will never again need to access the data encrypted by this key. If a key is shredded, any data encrypted by this key *cannot* be decrypted.

   When you are finished, click **Save**. If the Cloud VM Set to which this VM belongs uses a SEK key, confirm that you want to make the same expriration option change to all disks on all VMs in the Cloud VM Set that use the same version of the SEK key as the selelcted disk.

Pausing a Rekey Operation on Windows

If you run into bottleneck issues during a rekey operation on a Windows VM, you can pause the rekey operation and resume it at a later time.

Pausing and Resuming the Rekey Operation using the Policy Agent GUI

1. Log into the Windows system using an account with Administrator privileges.
2. Select **Start > All Programs > Entrust > Entrust DataControl** or start Windows PowerShell and enter the `hclGUI` command.
3. Right-click on the disk that you want to pause and select **Pause**.
4. When the status update window appears, click **OK**.
5. Refresh the window to confirm that the operation was paused.
6. Right-click on the disk that you paused and select **Resume**.
7. When the status update window appears, click **OK**.
8. Refresh the window to confirm that the operation was resumed.

Pausing the Rekey Operation using the CLI

1. Log into the VM as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. Enter the command `hcl rekey pause diskname`, where `diskname` is the drive letter or folder mount of the Windows disk whose rekey operation you want to pause.
   Note: This command pauses the rekey operation but the CLI does *not* display a confirmation message.
3. To verify that the rekey operation has been paused, enter the `hcl status` command.
   Example:

```
C:\Users\Administrator> hcl rekey pause g:
C:\Users\Administrator> hcl status
Summary
--------------------------------------------------------------------------------
KeyControl: 10.238.66.232:443
KeyControl list: 10.238.66.232:443
Status: Connected
Last heartbeat: Fri May 19 14:08:40 2017 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT


Device details
--------------------------------------------------------------------------------
Drive   Disk Part Cipher     Status    GUID
--------------------------------------------------------------------------------
C:     0    2    AES-XTS-512 Attached  3CBE4043-390C-49D6-BA81-CA225ED991C8
E:     1    1    AES-XTS-512 Detached  8652CAC7-F991-43B0-A092-693628AC1633
G:     2    1    AES-XTS-512 PS 28.28% FD19E39B-01F7-4E60-9354-76F6BABA0F31
C:\Users\Administrator>
```

In the above example, you can see that the status for G: is **PS**, which means Paused, and that the operation was 28.8% complete.

4. To resume the rekey operation, enter the command d `hcl rekey resume` *diskname* , where `diskname` is the drive letter or folder mount of the Windows disk whose rekey operation you want to resume.
5. To verify that the rekey operation has resumed, enter the `hcl status` command.

Example:

```
C:\Users\Administrator> hcl rekey resume g:
C:\Users\Administrator> hcl status
Summary
--------------------------------------------------------------------------------
KeyControl: 10.238.66.232:443
KeyControl list: 10.238.66.232:443
Status: Connected
Last heartbeat: Fri May 19 14:21:45 2017 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT


Device details
--------------------------------------------------------------------------------
Drive   Disk Part Cipher     Status    GUID
--------------------------------------------------------------------------------
C:     0    2    AES-XTS-512 Attached  3CBE4043-390C-49D6-BA81-CA225ED991C8
E:     1    1    AES-XTS-512 Detached  8652CAC7-F991-43B0-A092-693628AC1633
G:     2    1    AES-XTS-512 RK 35.10% FD19E39B-01F7-4E60-9354-76F6BABA0F31
C:\Users\Administrator>
```

In the above example, you can see that the status for G: is **RK**, which means Rekey, and that the operation is 35.10% complete.

Configuring Auto Rekey for a VM

The default Auto Rekey settings for a VM come from the settings in the parent Cloud VM Set as described in Configuring Auto Rekey for a Cloud VM Set.

This procedure describes how to override the default Auto Rekey setting for a specific VM.

> Note: If you configure Auto Rekey for a VM in a Cloud VM Set that has the Single Encryption Key (SEK) option enabled, Cryptographic Security Platform Vault uses the current version of the SEK key when it performs the auto rekey. It does *not* automatically create a new SEK key version. If you want to automatically rekey all of the encrypted disks in the VM, make sure you generate a new SEK key before the auto rekey process begins. For details, see Generating a New SEK Key.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab and select the VM you want to work with from the list.
4. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
5. Set the following property on the **Details** tab:

Option	Description
Rekey Interval	If you specify any value other than 0 (zero) for this option, Cryptographic Security Platform Vault periodically creates a rekey task for every encrypted disk in the VM. You can select any number of days, weeks, months, or years and the Cryptographic Security Platform Vault for VM Encryptionwill automatically rekey the encrypted disks on that schedule. To disable Auto Rekey, enter 0 in this field. By default, Auto Rekey is disabled.

6. When you are finished entering a value in each field, click **Save**. Cryptographic Security Platform Vault sends the changes to the VM on the next heartbeat.
7. You can track the progress of the rekey operation on the **Dashboard** in the **Tasks** tile.

> Note: For Linux VMs, Auto Rekey only works if the online encryption driver has been configured and is active on the Linux VM. On Linux VMs, Auto Rekey does not work for system devices such as root or swap.

Configuring Auto Rekey for a Cloud VM Set

You can configure Cryptographic Security Platform Vault to automatically rekey all disks on all VMs in a Cloud VM Set on a specific schedule. This provides additional security but may impact system performance depending on the size of the encrypted disks and the server load.

For maximum flexibility, you can override the default Auto Rekey settings on a VM by VM basis as well. For details, see Configuring Auto Rekey for a VM.

> Note: If you configure Auto Rekey for a Cloud VM Set that has the Single Encryption Key (SEK) option enabled, Cryptographic Security Platform Vault uses the current version of the SEK key when it performs the auto rekey. It does *not* automatically create a new SEK key version. If you want to automatically rekey all of the encrypted disksin the VMs in theCloud VM Set, make sure you generate a new SEK key before the auto rekey process begins. For details, see Generating a New SEK Key.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workload**.
3. Select the Cloud VM Set for which you want to configure Auto Rekey.
4. Set the following properties on the **Details** tab:

Option	Description
Max Parallel Rekey Operations	The number of concurrent Auto Rekey operations that can be performed for VMs in the Cloud VM Set. The default is 1.
Rekey Interval	If you specify any value other than 0 (zero) for this option, Cryptographic Security Platform Vault periodically creates a rekey task for every encrypted disk in every VM that is registered with this Cloud VM Set. You can select any number of days, weeks, months, or years and the Cryptographic Security Platform Vault for VM Encryptionwill automatically rekey the encrypted disks on that schedule. To disable Auto Rekey, enter 0 in this field. By default, Auto Rekey is disabled.

5. When you are finished entering a value in each field, click **Save**. Cryptographic Security Platform Vault sends the changes to the VMs in the Cloud VM Set on the next heartbeat.
6. You can track the progress of all rekey operations on the **Dashboard** in the **Tasks** tile.

Note: For Linux VMs, Auto Rekey only works if the online encryption driver has been configured and is active on the Linux VM. On Linux VMs, Auto Rekey does not work for system devices such as root or swap.

Rekeying a Linux System Device

If you encrypted a Linux system device (such as `/root`, `swap`, or `/home`) with the `htroot encrypt` command, you need to rekey that system device with the `htroot rekey` command.

Important: This procedure applies to Linux system devices *only*. If you want to rekey a Linux data drive, see Rekeying a Disk Using the webGUI or Rekeying a Disk using the CLI. If you use this procedure to rekey a data drive, Cryptographic Security Platform Vault will treat the data drive as a system device and all future rekey tasks will require you to reboot the device.

During this procedure, the VM will need to be rebooted to start the rekey process. If you have enabled Online Encryption for this VM, the VM will come back online immediately and the Policy Agent will rekey the system devices as a background process. In this case, users can continue to access the data while it is being rekeyed.

If Online Encryption is *not* enabled, the VM will remain inaccessible for normal operations until the rekey process completes.

For more information about Online Encryption, see Linux Online Encryption Prerequisites and Considerations.

Procedure

1. Log into the VM as `root`.
2. If you want to check the available disks on this VM, enter the `hcl status` command. The Registered Devices section shows all devices that have been encrypted on the VM, with the short form of the disk name in the first column. You will need this short name in order to rekey the device.

Example:
hcl status

Summary

KeyControl: sdkc:443
KeyControl list: sdkc:443
Status: Connected
Last heartbeat: Tue Jul 31 12:06:22 2018 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT
HTCRYPT: Not Installed

Registered Devices

Disk Name Cipher Status Clear
---
sda3 AES-XTS-512 Attached /dev/mapper/
clear_D4044351-4C2C-4582-8935-479B5238B23A (swap)
'--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
sda2 AES-XTS-512 Attached /dev/mapper/clear_htroot (/)
'--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT

Available Devices

Disk Name Device Node Size (in MB)
---
sdc2 /dev/sdc2 119
sdc1 /dev/sdc1 118

Other Devices

Disk Name Device Node Status
---
sda1 /dev/sda1 Mounted (/boot)
sdd /dev/sdd LVM (vg-sdd)

3. Enter the `htroot rekey <diskname1,diskname2,... | -a>` command, where each `diskname` is the short form of the disk name. (For example, `sda2` instead of `/dev/sda2`.) To specify multiple disks, use a comma-seperated list. To rekey all availabl e system devices, specify `-a` instead of a list of disk names. (If you specify `-a`, Cryptographic Security Platform Vault only rekeys the system devices. It does *not* rekey the data devices.)
For example:
htroot rekey sda2,sda3

Setting up system for root device rekey.
This operation may take a long time

Do you want to proceed? (y/N) y
The system has been updated to rekey the Linux root device/s during next boot; please reboot the system now
Do you want to reboot the system now? (y/N) y

4. Confirm the server reboot to continue. When the server has rebooted, it authenticates itself with Cryptographic Security Platform Vault to get the required encryption keys and then starts the rekey process. The time required to rekey the devices depends on their size and the type of storage you have.
    - If you have enabled Online Encryption for this VM, the VM reboots immediately and the Policy Agent rekeys the devices as a background process. In this case, you can check the rekey status at any time using the `hcl status` command.
    - If Online Encryption is not enabled, the VM remains offline until the rekey process completes. In this case, you can see the rekey progress on the VM console through vSphere, Azure, or AWS.

Rekeying a Disk using the CLI

When Cryptographic Security Platform Vault rekeys a disk, it creates a new key and then begins decrypting the disk using the old key. As each block is decrypted, the Policy Agent re-encrypts it using the new key.

The following procedure applies to all types of Windows disks and to Linux data disks. You cannot, however, rekey a Linux system device (such as `/root`, `swap`, or `/home`) using this procedure. Instead, use the `htroot rekey` command as described in Rekeying a Linux System Device.

> Tip: Depending on the size of the encrypted disk, the rekey process can take a long time to run. If the rekey process is interrupted on Windows, it will be resumed automatically when the disk comes back online. If the process is interrupted on Linux, you need to manually reissue the `hcl rekey` command to resume the process. We recommend you use the Linux `nohup` or `screen` command to avoid terminal-related interruptions during the rekey.

Procedure

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. If you want to check the available disks on this VM, enter the `hcl status` command.
3. If this VM belongs to a Cloud VM Set that uses the Single Encryption Key (SEK) option and you want to verify that there is a new version of the SEK key available, enter the `hcl keyversion` *`diskname`* command, where `diskname` is the name of the disk that you want to rekey. For Linux, use the short form of the disk name. (For example, `sdb1` instead of `/dev/sdb1`.) For Windows, specify the drive letter or folder mount associated with the disk. (For example, `f:` or `g:\data`).
   The command returns the key version being used by the disk as well as the current SEK key version. The following example shows a disk that is currently encrypted with an older version of the SEK key:
   # hcl keyversion sdb1
   keyversion: 2 SEKversion: 4

   In this case, you should rekey the disk to bring it up to date. If the key version matches the SEK version however, there is no need to rekey the disk. For more information on the SEK option, see Data Deduplication with Cloud VM Sets.
4. If this is a Linux system and you have *not* enabled Online Encryption for this VM, unmount the disk you want to rekey. For more information, see Linux Online Encryption Prerequisites and Considerations.
5. Enter the command `hcl rekey [-s]` *`diskname`*, where:
    - `-s` (Linux only) tells Cryptographic Security Platform Vault to only process allocated blocks which can improve performance dramatically. Cryptographic Security Platform Vault uses system-provided utilities to determine the allocated blocks on the disk. This option is supported for ext2, ext3, and ext4 file systems. It is *not* supported on XFS. (To change the speed for Windows, see Changing the Encryption/Decryption Speed on Windows.)

Important: This option does not work if online encryption has been enabled for the VM, even if you unmount the drive during the process. If online encryption has been enabled or if the disk is mounted, using the `-s` option will cause the command to fail.

- `diskname` is the name of the disk that you want to encrypt. For Linux, use the short form of the disk name. (For example, `sdb1` instead of `/dev/sdb1`.) For Windows, specify the drive letter or folder mount associated with the disk. (For example, `f:` or `g:\data`).

6. For Linux, the progress of the command is displayed automatically. For Windows, use the `hcl status` command to check the progress.
7. If the rekey operation is interrupted on Windows, the Policy Agent automatically restarts it when the system comes back online. For Linux, you can:
   - Resume the rekey operation by reissuing the `hcl rekey` command.
   - Revert the rekey operation using the `hcl rekey -u diskname` command.

Windows Example:

The following example shows the rekey operation for the Windows folder mount E:\data:

```
C:\Users\Administrator> hcl rekey e:\data

C:\Users\Administrator> hcl status
Summary
--------------------------------------------------------------------------------
KeyControl: 10.238.66.232:443
KeyControl list: 10.238.66.232:443
Status: Connected
Last Heartbeat: Fri May 12 16:16:34 2017 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT

Device Details
--------------------------------------------------------------------------------
Drive     Disk Part Cipher      Status    GUID
--------------------------------------------------------------------------------
C:        0    2    none        Avail-Sys D74E94B8-0067-4652-935D-E1BA96B6E8F5
E:\data   1    1    AES-XTS-512  RK 43.89% 20500265-AC34-4966-8A40-40A98F08BEE7
C:\Users\Administrator> hcl rekey e:\data

C:\Users\Administrator> hcl status
Summary
--------------------------------------------------------------------------------
KeyControl: 10.238.66.232:443
KeyControl list: 10.238.66.232:443
Status: Connected
Last Heartbeat: Fri May 12 16:16:34 2017 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT

Device Details
--------------------------------------------------------------------------------
Drive     Disk Part Cipher      Status    GUID
--------------------------------------------------------------------------------
```

```
C:      0   2   none       Avail-Sys D74E94B8-0067-4652-935D-E1BA96B6E8F5
E:\data   1   1   AES-XTS-512  RK 43.89% 20500265-AC34-4966-8A40-40A98F08BEE7
```

The RK in the status column for disk `E:\data` indicates that it is being rekeyed. The operation is currently 43.89% done.

Linux Example:

The following example shows a Linux filesystem that is mounted with several files at the top directory. We unmount the filesystem, issue the `rekey` command, then remount it and show that the files are still accessible.

```
# mount /dev/mapper/clear_sdc1 /mnt
# ls /mnt
file1  file2  file3  files.tgz    lost+found/
# umount /mnt
# hcl rekey sdc1
All the data on /dev/sdc1 will be rekeyed
The clear text data will be available on /dev/mapper/clear_sdc1
This operation may take long time

Do you want to proceed? (y/n) y
Starting rekey of sdc1
In case of failure run 'hcl rekey [-u] sdc1'
total device size 10206 KB

Processing: 100%     Time left: 00:00:00
Completed rekey of sdc1 successfully
# mount /dev/mapper/clear_sdc1 /mnt
# ls /mnt file1  file2  file3  files.tgz lost+found/
```

If you have rekeyed previously, you will see the following additional prompt:

```
# hcl rekey sdc1
WARNING: rekey operation was successfully performed for device sdc1
Run rekey again
Do you want to proceed? (y/n) y
All the data on /dev/sdc1 will be rekeyed
The clear text data will be available on /dev/mapper/clear_sdc1
This operation may take long time

Do you want to proceed? (y/n) y
Starting rekey of sdc1
In case of failure run 'hcl rekey [-u] sdc1'
total device size 10206 KB

Processing: 100%     Time left: 00:00:00
Completed rekey of sdc1 successfully
```

You will also see a similar prompt if you have already encrypted or decrypted a disk.

If the operation fails for any reason, for example a system crash, run the `hcl rekey` command again. You will see the following:

```
# hcl rekey sdb1
WARNING: Incomplete rekey operation detected for device sdb1
Continue rekey
Do you want to proceed? (y/n)
```

If you want to reverse a rekey that only partially completed:

```
# hcl rekey -u sdb1
Starting undo of rekey operation on sdb1;
In case of failure run 'hcl rekey -u sdb1' again
Processing: 100%     Time left: 00:00:00
Completed undo for sdb1 successfully
```

Rekeying a Disk using the Policy Agent GUI

When Cryptographic Security Platform Vault rekeys a disk, it creates a new key and then begins decrypting the disk using the old key. As each block is decrypted, the Policy Agent re-encrypts it using the new key.

The following procedure applies to Windows disks only.

> Tip: Depending on the size of the encrypted disk, the rekey process can take a long time to run. If the rekey process is interrupted on Windows, it will be resumed automatically when the disk comes back online.

Procedure

1. Log into the Windows system using an account with Administrator privileges.
2. Select **Start > All Programs > Entrust > Entrust DataControl** or start Windows PowerShell and enter the `hclGUI` command.
3. Right-click on the disk that you want to rekey and select **Rekey**.
4. Click **Yes** on the confirmation screen.

Rekeying a Disk Using the webGUI

When Cryptographic Security Platform Vault rekeys a disk, it creates a new key and then begins decrypting the disk using the old key. As each block is decrypted, the Policy Agent re-encrypts it using the new key.

> Note: If you are using the Single Encryption Key (SEK) option to support data deduplication (dedupe), make sure there is a new version of the SEK key available before you rekey the disk. If the disk already uses the current version of the key, the rekey request may fail. For more information, see Viewing the SEK Key Version for a Disk.

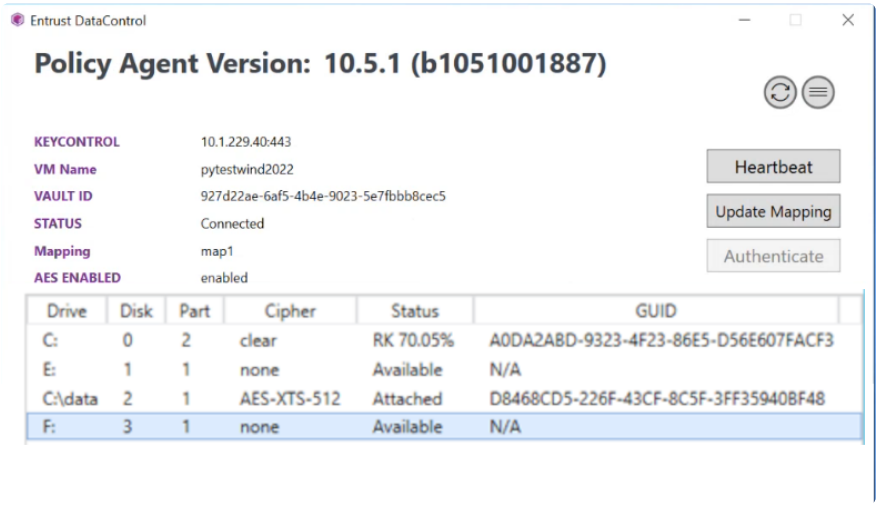
The following procedure applies to all types of Windows disks and to Linux data disks. You cannot, however, rekey a Linux system device (such as `/root`, `swap`, or `/home`) using this procedure. Instead, use the `htroot rekey` command as described in Rekeying a Linux System Device.

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab and select the VM you want to work with from the list.
4. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
5. In the Details area, click on the **Encrypted Disks** tab.
6. Select the disk you want to rekey and select **Actions > Rekey Disk** from the VM-specific **Actions** menu. Cryptographic Security Platform Vault displays a message that the rekey request was successfully created and adds a **Rekey Disk** task for the VM that will begin on then VM's next heartbeat. The

length of time the operation will take depends on the amount of data already present on the disk and the encryption settings configured for this system.
You can track the progress of the rekey task on the Dashboard in the **Tasks** tile.
When the rekey request begins processing, Cryptographic Security Platform Vault sets the state to **Active/Rekey**. When the encryption process has finished, Cryptographic Security Platform Vault changes the state to **Active/Attached**.

Windows Encryption Management with the Entrust Policy Agent GUI

Windows disks can be encrypted or decrypted using the Cryptographic Security Platform Vault for VM Encryption webGUI, `hicli`, or the Entrust Policy Agent GUI that is installed locally on the Windows server with the Entrust Policy Agent. The Entrust Policy Agent GUI provides basic encryption and decryption functionality without requiring the use of the Cryptographic Security Platform Vault webGUI. The GUI looks similar to the following:



The GUI shows the Cryptographic Security Platform Vault connection information and the status of the VM with Cryptographic Security Platform Vault. The VM status can be one of the following:

- **Not registered** — The Policy Agent software is installed but the VM has not yet been registered with Cryptographic Security Platform Vault.
- **Connected** — The VM can communicate with the Cryptographic Security Platform Vault for VM Encryption and everything is running normally.
- **Could not connect** — The Cryptographic Security Platform Vault for VM Encryption is not reachable. If this condition continues, the VM will need to be re-authenticated with the Cryptographic Security Platform Vault for VM Encryption when communication is re-established.
- **Need to update certificate** — The certificate for the is VM is no longer valid and should be updated.
- **Reauth needed** — The VM needs to be re-authenticated.
- **Virtual Machine not authenticated** — VM permissions have been revoked from the Cryptographic Security Platform Vault for VM Encryption. To fix this issue, see Reactivating a Revoked Disk.
- **Identity verification failed** — Permissions are not available because the VM heartbeat has timed out or its IP address or hardware signature has changed. This can occur if you have changed the IP address on a VM or copied the VM to a new server.
- **Unknown error from KeyControl cluster** — An unknown error has occurred. Please contact support if you see this message.

The table beneath the status area shows the disks on the VM and their encryption status. In the screenshot above, `C:` is in the process of encrypting and the folder mount `C:\data` has been encrypted, but disks `E:` and `F:` are not encrypted.

- Encrypting a Windows Disk Using the Entrust Policy Agent GUI

Encrypting a Windows Disk Using the Entrust Policy Agent GUI

The following procedure describes how to encrypt a Windows data drive, boot drive, or folder mount using the Entrust Policy Agent GUI.

Before You Begin

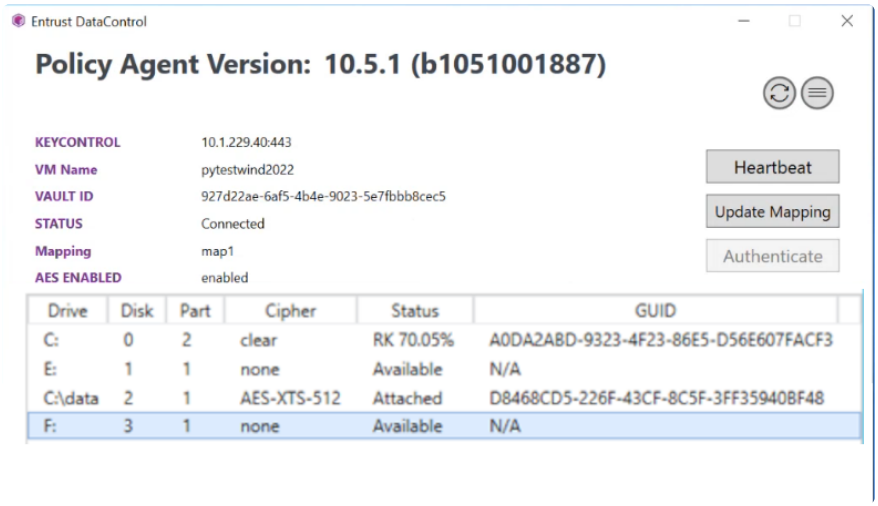
- If this is a data partition, make sure the disk you want to encrypt meets the prerequisites described in Windows Encryption Prerequisites.
- If this is a Windows boot partition, make sure the partition has been set up as described in Windows Boot Drive Encryption.
  Note: The boot partition may not appear as an available disk until after the Entrust Bootloader is installed.

Procedure

1. Log into the VM as a System Administrator.
2. Select **Start > All Programs > Entrust > Entrust DataControl** or start Windows PowerShell and enter the `hclGUI` command.
3. Right-click on the disk and select one of the following:
   - **Add**—Registers the disk with the Cryptographic Security Platform Vault for VM Encryption and reformats it using NTFS. Any existing data on the disk is lost. This is equivalent to the `hcl add` command with all defaults selected.
   - **Encrypt**—Registers the disk with the Cryptographic Security Platform Vault for VM Encryption and encrypts the data that already exists on the disk. This is equivalent to the `hcl encrypt` command with all defaults selected.
     If the disk is sparse, the Cryptographic Security Platform Vault for VM Encryption only encrypts the allocated blocks to ensure that the sparseness remains. Sparse is not available for `C:` drives.

   After you select the option you want to use, confirm the selection at the prompt. The Cryptographic Security Platform Vault for VM Encryption displays a status message while the encryption is in process and updates the disk list in the Entrust Policy Agent GUI while it is running.

   For example, the following screenshot shows that the folder mount `C:\data` is encrypted and attached to Cryptographic Security Platform Vault, while the `C:` disk is 70.05% encrypted.



The encryption proceeds in the background and you can continue to use the disk while it is being performed. If you want to change the encryption speed, see Changing the Encryption/Decryption Speed on Windows.

Troubleshooting Windows Online Encryption Issues

If you are encrypting, rekeying, or decrypting a Windows drive using Online Encryption and the process appears to hang, there may be I/O errors on the device. To check for this problem, you can use the `hcl rekey status` command.

1. Log into the VM as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. Enter the `hcl rekey status drive` command, where `drive` is the drive that you are encrypting, decrypting or rekeying and look at the value in the **current** field.
   ```
   C:\>hcl rekey status J:
   device: \Device\Harddisk1\Partition2
   drive: J
   state: in progress
   begin: 33619968
   end: 1108279296
   current: 160432128
   sector offset (from 0): 313344
   total sectors: 2098944
   total size: 1074659328
   pct done: 14.93%
   elapsed time (seconds): 11
   ```
3. Wait for a least two minutes and run the `hcl rekey status drive` command again. Compare the value in the **current** field to the value from the first iteration of the command. If the value is unchanged, then the rekey process is no longer responding. If the values are the same, you can:
   - Reboot the VM. The encryption, decryption, or rekeying process should resume once the VM reboots.
   - Contact Entrust Support.

Reversing an Encryption

An encryption can be interrupted, but cannot be canceled or reversed. To reverse an encryption is to allow the encryption to complete, then to start a decryption.

Encrypting a Disk Using the CLI

The following procedure describes how to use the CLI to encrypt a Linux data partition or a Windows boot drive, folder mount, or data drive. During this procedure you can elect to reformat the drive and remove any existing data or keep and encrypt the existing data.

You cannot encrypt a Linux system device (such as `/root`, `swap`, or `/home`) using this procedure. Instead, follow the procedure described in Encrypting Linux System Devices in AWS.

Before You Begin

For Linux disks:

- If this is a Linux data disk, make sure you have partitioned the disk and that the disk meets the qualifications described in Windows Encryption Prerequisites.
- If an entry for the Linux device you intend to encrypt already exists in the Filesystem Table (`/etc/fstab`), you need to remove that entry until the encryption process is complete and the Entrust-created clear text path to the device is available. If you reboot the device after encryption with the `/etc/fstab` entry still pointing to the original device path, the system may hang because the encrypted version of the device will fail the filesystem check. For details, see Automatically Mounting Linux Filesystems.
- If you want to encrypt the existing data while the disk remains online and accessible, make sure you enable Online Encryption on the VM as described in Enabling Linux Online Encryption with the CLI and Enabling Linux Online Encryption with the CSP Vault for VM Encryption webGUI. For details about Online Encryption, see Linux Online Encryption Prerequisites and Considerations.

For Windows disks:

- If this is a Windows data drive, make sure the disk you want to encrypt meets the prerequisites described in Windows Encryption Prerequisites.
- If this is a Windows boot partition, make sure the partition has been set up as described in Windows Boot Drive Encryption.
  Note: The boot partition may not appear as an available disk until after the Entrust Bootloader is installed.

  Tip: Depending on the size of the disk, the encryption process can take a long time to run. If the process is interrupted on Windows, it will be resumed automatically when the disk comes back online. If the process is interrupted on Linux, you need to manually restart the process. We recommend you use the Linux `nohup` or `screen` command to avoid terminal-related interruptions during encryption.

Procedure

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. If you want to reformat the disk and, optionally, create a new filesystem, enter the command `hcl add [-F fstype | "none"] [-n] [-c cipher] [-m mapped_device] [-p parent-disk] [-e days_to_expire] [-z "NO USE"|"SHRED"] [-o] [-y] [-x] diskname`
   Details:
   - `-F` (Linux only) allows you to specify the filesystem you want to use. If you do not specify a filesystem, the `hcl add` command uses the same filesystem as `root`. If that information is not available, the `hcl add` command uses `ext4`. If you do not want Cryptographic Security Platform Vault to format the disk, specify `"none"` for this option.
     Tip: To use XFS (Extents File System), specify "**xfs**". For more information, see Example: Adding an Encrypting a Linux Disk with XFS.

- `-n` indicates that the disk should not be attached immediately. Use this option if you want to prepare the disk but not bring it online until later.
- `-c` is the encryption cipher that Cryptographic Security Platform Vault should use for the disk. The default cipher is AES-XTS-512. To view a list of available ciphers, use the `hcl ciphers` command. For details, see Encryption Key Sizes and Algorithms.
- `-m` (Linux only) sets the default clear text path, which is constructed based on the current path to the disk. For example, if the disk is `/dev/sdb1`, the default clear text path would be `/dev/mapper/clear_sdb1`. To set the clear text path to `/dev/entrust/clear_sdb1`, you would use `–m /dev/entrust/clear_sdb1`.
- `-p` indicates that this is a snapshot of the encrypted LVM (Logical Volume Management) volume, or MBR partition copy/snapshot, whose parent is named in *parent-disk*. Use the `hcl status` command to determine the exact format for the parent disk name. For more information, see Example: Encrypting a Linux LVM Volume.
  Warning: If the snapshot was taken before the parent volume was registered with CSP Vault, the snapshot will not have encrypted data.
- `-e` allows you to specify the number of days the key should be active before it expires. If you omit this option, the key never expires. What happens when a key expires is controlled by the `-z` option.
- `-z` controls what happens when the key expiry date is reached. You can specify:
  - `"NO USE"` — The key is deactivated but retained. It can then be reactivated by setting a future date in the **Expiry Date** field in the Cryptographic Security Platform Vault for VM Encryption webGUI. This is the default.
  - `"SHRED"` — The key is destroyed and cannot be retrieved. You should only use this option if you are absolutely certain that you will never need to access the selected disk again.
- `-o` overrides the default setting that prevents you from encrypting a non-partitioned disk. You should always use partitioned disks because we can easily identify them and find the associated keys.
  Warning: We recommend you do NOT use this option, or access to your encrypted data will be lost if the disk name changes.
- `-y` makes the command non-interactive.
- `-x` (Windows data drive only) tells Cryptographic Security Platform Vault to check for the existence of a pagefile on the designated Windows data drive. If one is found, the command is aborted.
- `diskname` is the name of the disk that you want to encrypt. For Linux, use the short form of the disk name. (For example, `sdb1` instead of `/dev/sdb1`.) For Windows, specify the drive letter or folder mount associated with the disk. (For example, `f:` or `g:\data`).

Example:

```
# hcl add sdb1
WARNING: This operation will destroy the contents of the disk.
If you wish to preserve them, run "hcl encrypt" instead.
Do you want to proceed? (y/n) y

In case of error remove the disk using "hcl rm" and run "hcl add" again

Encrypted device sdb1 (/dev/sdb1) attached; decrypted contents visible at /dev/mapper/clear_sdb1

Creating file system ext3 on /dev/mapper/clear_sdb1
-------------------------------------------------
```

```
mke2fs 1.41.11 (14-Mar-2017)
...
This filesystem will be automatically checked every 22 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
-------------------------------------------------
```

3. If you want to retain and encrypt the data that currently exists on the disk, enter the command `hcl encrypt [-s] [-c cipher] [-e days_to_expire] [-z "NO USE"|"SHRED"] [-o] [-y] [-x] diskname`

   Details:

   - `-s` (Linux only) tells Cryptographic Security Platform Vault to only process allocated blocks which can improve performance dramatically. Cryptographic Security Platform Vault uses system-provided utilities to determine the allocated blocks on the disk. This option is supported for ext2, ext3, and ext4 file systems. It is *not* supported on XFS. (To change the speed for Windows, see Changing the Encryption/Decryption Speed on Windows.)
     Important: This option does not work if online encryption has been enabled for the VM, even if you unmount the drive during the process. If online encryption has been enabled or if the disk is mounted, using the `-s` option will cause the command to fail.
   - `-c` is the encryption cipher that Cryptographic Security Platform Vault should use for the disk. The default cipher is AES-XTS-512. To view a list of available ciphers, use the `hcl ciphers` command. For details, see Encryption Key Sizes and Algorithms.
   - `-e` allows you to specify the number of days the key should be active before it expires. If you omit this option, the key never expires. What happens when a key expires is controlled by the `-z` option.
   - `-z` controls what happens when the key expiry date is reached. You can specify:
     - `"NO USE"` — The key is deactivated but retained. It can then be reactivated by setting a future date in the **Expiry Date** field in the Cryptographic Security Platform Vault for VM Encryption webGUI. This is the default.
     - `"SHRED"` — The key is destroyed and cannot be retrieved. You should only use this option if you are absolutely certain that you will never need to access the selected disk again.
   - `-o` overrides the default setting that prevents you from encrypting a non-partitioned disk. You should always use partitioned disks because we can easily identify them and find the associated keys.
     Warning: We recommend you do NOT use this option, or access to your encrypted data will be lost if the disk name changes.
   - `-y` makes the command non-interactive.
   - `-x` (Windows data drive only) tells Cryptographic Security Platform Vault to check for the existence of a pagefile on the designated Windows data drive. If one is found, the command is aborted.
   - `diskname` is the name of the disk that you want to encrypt. For Linux, use the short form of the disk name. (For example, `sdb1` instead of `/dev/sdb1`.) For Windows, specify the drive letter or folder mount associated with the disk. (For example, `f:` or `g:\data`).

   Example:

```
# hcl encrypt sdb1
All the data on sdb1 will be encrypted
The cleartext data will be available on /dev/mapper/clear_sdb1
This operation may take long time
Do you want to proceed? (y/n) y

Encrypted device sdb1 (/dev/sdb1) attached; decrypted contents visible at /dev/mapper/clear_sdb1
```

```
total device size 1044193 KB

Processing: 100%     Time left: 00:00:00
Completed encryption of sdb1 successfully
```

Note: During encryption, you may see the message "WARNING: unable to add private region to *<disk-name>*. Disk will still have a unique ID." This message means that the Policy Agent cannot create a private region on the disk and therefore cannot assign a GUID to the disk. All data encryption will proceed normally, but you will not be able to move this disk to a new VM. For details, see Moving Disks Between VMs.

4. For Linux, the progress of the command is displayed automatically. For Windows, use the `hcl status` command to check the progress.
   Notes:
   - If the `hcl encrypt` command is interrupted for any reason, you can re-issue the same `hcl encrypt` command. The encryption process will start at the point where it was interrupted.
   - If the encryption fails for a Windows disk with the message that there are too many partitions on the disk, see Detecting and Removing a Windows Snapshot Partition.

What to Do Next

If you removed the `/etc/fstab` entry for the device, you can recreate that entry using the clear text path created during encryption. For details, see Automatically Mounting Linux Filesystems.

Encrypting a Disk Using the CSP Vault for VM Encryption webGUI

The following procedure describes how to use the Cryptographic Security Platform Vault for VM Encryption webGUI to encrypt a Linux data partition or a Windows boot drive, folder mount, or data drive.

> Note: You cannot encrypt a Linux system device (such as `/root`, `swap`, or `/home`) using this procedure. Instead, follow the procedure described in Encrypting Linux System Devices in AWS.

Before You Begin

For Linux disks:

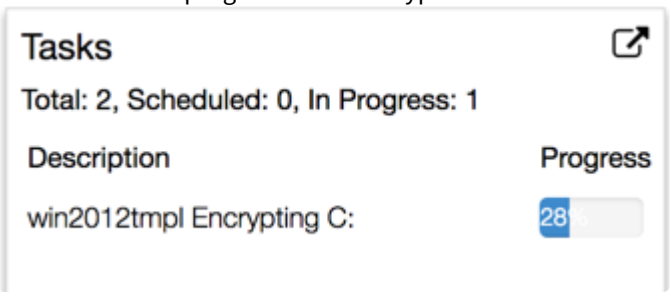
- Make sure you have partitioned the Linux data disk and that the disk meets the qualifications described in Linux Encryption Prerequisites.
- If an entry for the Linux device you intend to encrypt already exists in the Filesystem Table (`/etc/fstab`), you need to remove that entry until the encryption process is complete and the Entrust-created clear text path to the device is available. If you reboot the device after encryption with the `/etc/fstab` entry still pointing to the original device path, the system may hang because the encrypted version of the device will fail the filesystem check. For details, see Automatically Mounting Linux Filesystems.
- If you want to encrypt the existing data while the disk remains online and accessible, make sure you enable Online Encryption on the VM as described in Enabling Linux Online Encryption with the CLI and Enabling Linux Online Encryption with the CSP Vault for VM Encryption webGUI. For details about Online Encryption, see Linux Online Encryption Prerequisites and Considerations.

For Windows disks:

- If this is a Windows data drive, make sure the disk you want to encrypt meets the prerequisites described in Windows Encryption Prerequisites.
- If this is a Windows boot partition, make sure the partition has been set up as described in Windows Boot Drive Encryption.
  Note: The boot partition may not appear as an available disk until after the Entrust Bootloader is installed.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab and select the VM you want to work with from the list.
4. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
5. In the Details area, click on the **Unencrypted Disks** tab.
6. Select the disk you want to encrypt and select **Actions > Encrypt Disk** from the VM-specific **Actions** menu. Cryptographic Security Platform Vault displays a message that the encryption request was successfully created and adds an **Encrypt Disk** task for the VM that will begin on then VM's next heartbeat. The length of time the operation will take depends on the amount of data already present on the disk and the encryption settings configured for this system.
   You can track the progress of the encryption task on the Dashboard in the **Tasks** tile.



   When the encryption request begins processing, Cryptographic Security Platform Vault moves the disk from the **Unencrypted Disks** tab to the **Encrypted Disks** tab and sets the state to **Active/Encrypt**. When the encryption process has finished, Cryptographic Security Platform Vault changes the state to **Active/Attached**.
   Tip: If the encryption fails for a Windows disk with the message that there are too many partitions on the disk, see Detecting and Removing a Windows Snapshot Partition.
   What to Do Next
   If you removed the `/etc/fstab` entry for a Linux disk, you can recreate that entry using the clear text path created during encryption. For details, see Automatically Mounting Linux Filesystems.

Automatic Data Encryption

When you create a Cloud VM Set, you can specify that, when a VM is registered with the Cloud VM Set, Cryptographic Security Platform Vault will automatically tell the Policy Agent on that VM to encrypt the available drives on the VM. If you enable this feature, you can also specify an Automatic Data Encryption Policy that tells Cryptographic Security Platform Vault which drives to include or exclude by default.

For example, If you enable Automatic Data Encryption and you want to:

- Automatically encrypt all available drives on the VM *except* the `C:` drive, you would set the Automatic Data Encryption Policy to **Exclude** the `C:` drive.
- Automatically encrypt *only* the `C:` drive, you would set the Automatic Data Encryption Policy to **Include** the `C:` drive.
- Automatically encrypt all available drives on the VM *including* the `C:` drive, you would set the Automatic Data Encryption Policy to **Encrypt All Devices**.

You can specify as many paths in the Automatic Data Encryption Policy as you want, and you can specify a mixture of Windows drives and Linux device names. You cannot, however, set some paths as included and some as excluded. The Automatic Data Encryption Policy must be configured to either exclude all of the specified paths or include all of the specified paths.

When you register a VM with the Cloud VM Set, the VM inherits the Automatic Data Encryption settings from the Cloud VM Set. You can override the default settings for an individual VM at any time, allowing you to customize the Automatic Data Encryption feature on a VM-by-VM basis.

This section includes:

- Configuring Automatic Data Encryption for a VM
- Configuring Automatic Data Encryption for a Cloud VM Set
- Prerequisites and Considerations for Automatic Data Encryption

Configuring Automatic Data Encryption for a VM

The following procedure describes how to change the Automatic Data Encryption settings for the VM. For details about changing other VM properties, see Changing the Properties for a Specific VM. For details about configuring Automatic Data Encryption for a Cloud VM Set, see Configuring Automatic Data Encryption for a Cloud VM Set.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select the VM whose properties you want to set and click the **Expand** button (**>**) at the end of the row.
4. On the **Details** tab, look at the **Auto Encryption** field. If it says **Disabled**, then no automatic encryption will be performed for the VM.
   If it says **Enabled**, then whenever Cryptographic Security Platform Vault detects a new disk on the VM, Cryptographic Security Platform Vault will automatically instruct the Policy Agent on that VM to encrypt the new disk if it matches the settings in the Automatic Data Encryption Policy.
5. To change the Auto Encryption Settings, click the current setting and, in the Auto Encryption Settings for VM Set dialog box, do the following:
   a. To change whether the feature is enabled or disabled, in the **Auto Encrypt** field, click the current setting and select **Enabled** or **Disabled** from the drop-down list, then click **Save**.
   b. If the feature is enabled, make sure the Auto Encryption Policy Type is set correctly. You can select:
      - **Exclude**—The Windows drives and Linux devices listed in the **Auto Encryption Policy Path(s)** field will *not* be automatically encrypted, although they can be encrypted manually at any time. This is the default.
      - **Include**—The Windows drives and Linux devices listed in the **Auto Encryption Policy Path(s)** field *will be* automatically encrypted. All other drives or devices on the VM must be encrypted manually.
      - **Encrypt All Devices**—All Windows drives and Linux devices will be automatically encrypted.
   c. If the policy type is Exclude or Include, make sure the Auto Encryption Policy Paths are set correctly. To add additional paths, click the blue **+** (Plus sign) in this field. You can enter either a Windows drive a Linux device name. For example, any of the following would be valid path names: `C:` , `C:\data` , or `sdb1` .
      Important: Each path *must* be on its own line.
6. When you are done, click **Save**.

Configuring Automatic Data Encryption for a Cloud VM Set

The following procedure describes how to configure Automatic Data Encryption for an existing Cloud VM Set. If you want to create a new Cloud VM Set with Automatic Data Encryption, see Creating a Cloud VM Set for the CSP Vault for VM Encryption.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.

3. On the **VM Sets** tab, select the Cloud VM Set you want to change. The Cryptographic Security Platform Vault webGUI displays the Cloud VM Set properties below the list of Cloud VM Sets.
4. On the **Details** tab, look at the **Auto Encryption** field. If it says **Disabled**, then no automatic encryption will be performed for the VMs in this Cloud VM Set.
   If it says **Enabled**, then whenever a new VM is registered with this Cloud VM Set, Cryptographic Security Platform Vault will automatically instruct the Policy Agent on that VM to encrypt one or more of the drives on that VM based on the Automatic Data Encryption Policy.
5. To change the Auto Encryption Settings, click the current setting and, in the Auto Encryption Settings for VM Set dialog box, do the following:
   a. To change whether the feature is enabled or disabled, in the **Auto Encrypt** field, click the current setting and select **Enabled** or **Disabled** from the drop-down list, then click **Save**.
   b. If the feature is enabled, make sure the Auto Encryption Policy Type is set correctly. You can select:
      - **Exclude**—The Windows drives and Linux devices listed in the **Auto Encryption Policy Path(s)** field will *not* be automatically encrypted, although they can be encrypted manually at any time. This is the default.
      - **Include**—The Windows drives and Linux devices listed in the **Auto Encryption Policy Path(s)** field *will be* automatically encrypted. All other drives or devices on the VMs must be encrypted manually.
      - **Encrypt All Devices**—All Windows drives and Linux devices will be automatically encrypted.
   c. If the policy type is Exclude or Include, make sure the Auto Encryption Policy Paths are set correctly. To add additional paths, click the blue **+** (Plus sign) in this field. You can enter either a Windows drive a Linux device name. For example, any of the following would be valid path names: `C:` , `C:\data` , or `sdb1` .
      Important: Each path *must* be on its own line.
6. When you are done, click **Save**.
7. When prompted, choose whether you want the changes you just made propagated to all VMs currently registered with the Cloud VM Set. If you select **No**, the new settings will only be inherited by any new VMs that are registered with the Cloud VM Set after the changes have been saved. No changes will be made on the currently-registered VMs.
   If you select **Yes**:
   - All local changes made to the Auto Encryption settings on the individual VMs will be lost.
   - If you enabled the feature or if you changed the Auto Encryption Policy paths, Cryptographic Security Platform Vault will analyze all disks on all VMs currently registered with the Cloud VM Set and it will automatically tell the appropriate Policy Agents to encrypt any unencrypted disks that meet the new criteria. Cryptographic Security Platform Vault will *not*, however, tell the Policy Agents to decrypt any disk that no longer meets the auto encryption criteria. Once a disk has been encrypted, it must be decrypted manually.

Prerequisites and Considerations for Automatic Data Encryption

- Automatic Data Encryption only works for Linux and Windows devices that meet the qualifications described in Linux Encryption Prerequisites and Windows Encryption Prerequisites.
- Automatic Data Encryption only works for Linux devices that are not mounted. Therefore, you cannot use Automatic Data Encryption to encrypt Linux system devices such as `/root` , `swap` , or `/home` .
- Automatic Data Encryption for Linux works with partitioned disks only.
- If you want to encrypt a Windows boot drive, you must install the Entrust Bootloader option with the Policy Agent on that VM. Auto encryption on the boot drive will fail if the Bootloader is not installed. For details, see Windows Boot Drive Encryption.
- If you change the Automatic Data Encryption Policy for a Cloud VM Set, you can choose whether to propagate the changes to the VMs already registered with the set. If you do so, any changes you made on the individual VMs will be overwritten by the settings in the Cloud VM Set. All customizations on the individual VMs will be lost.

- If you change the Automatic Data Encryption Policy to include a device that was not included before, Cryptographic Security Platform Vault automatically schedules a task to encrypt the newly- added device.
- After a device has been encrypted (either manually or through an Automatic Data Encryption Policy), Cryptographic Security Platform Vault will *not* automatically decrypt it, even if you change the Automatic Data Encryption Policy to *exclude* that device. Once encrypted, all devices must be decrypted manually.
- If you try to decrypt a device that is specified as **Included** in the Automatic Data Encryption Policy, the decryption task will fail. You must first remove the device from the Automatic Data Encryption Policy before you can decrypt it. If you remove the device from the policy at the VM-level, that device can only be decrypted on that VM. If you remove the device from the policy on the Cloud VM Set level and you propagate the changes from the Cloud VM Set to the registered VMs, then you can decrypt that device on any registered VM.

Using Data Encryption in Microsoft Azure

The following topics explain how to encrypt VMs in Microsoft Azure.

- Checking the Root Drive Encryption Status in Azure
- Encrypting Linux System Devices in Azure
- Verifying the Current VM Configuration in Azure
- Preparing a Linux System Device for Encryption in Azure
- Data Encryption in Azure

Checking the Root Drive Encryption Status in Azure

If Online Encryption*is* enabled for this VM, you can check the encryption status at any time by logging into the VM as `root` and using the `hcl status` command. If Online Encryption*is not* enabled, you can check the encryption status on the VM console through vSphere, Azure, or AWS.

When using a shell on a Windows machine to access the bootloader, you may have to use one of the following options:

- Use git bash to connect.
- Use the following flags to access the bootloader:
  `ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=ssh-rsa -i <machine-name>.key root@<machine-IP>`

If you need to troubleshoot the encryption process, you can check the encryption status using the Entrust Debug Console if you enabled that while running the `htroot setup` command, as described in Encrypting Linux System Devices in Azure.

1. If you need a copy of the `id_rsa` key file for the VM:
   a. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Cloud Admin privileges.
   b. In the top right, click the Switch to **Appliance Management** link.
   c. Navigate to the **Cloud > VMs** tab and select the VM whose key file you want to download.
   d. Select **Actions > Download Bootloader SSH Key**.
2. Open an `ssh` session by entering the command `ssh -i id_rsa root@vm_name`, where `id_rsa` is the name of the id_rsa file and `vm_name` is the IP address or hostname. For example:
   $ ssh -i Downloads/ht-centos75.key root@ht-centos75

   The authenticity of host 'ht-centos75 (192.168.15.239)' can't be established.
   RSA key fingerprint is SHA256:v1TDb5PTlGsncaPf6r9C0Z6ybtqVLxeGXf7XDnh3ltM.

```
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ht-centos75,192.168.15.239' (RSA) to the list of known hosts.

HyTrust Debug Console

1. Show HT encryption log file
2. Authenticate
3. Show Network info
4. Restart Network
5. Advanced access
6. logout (exit Debug Console)
```

3. Select option 1 and look for the status sections. For example, here are a few of the lines towards the end of the output:

```
Starting HyTrust root encryption ------------

Entered init script with args
Starting debug shell
Detected boot device uuid c01c3240-664b-412a-8440-dd0fa132eae5 device path /dev/sda1
Check file system on device path /dev/sda1
File system check on /dev/sda1 complete
Mounted /dev/sda1
Starting networking
Network started on primary network interface
Started debug console server
Guest VM Status
KeyControl: sdkc:443
Waiting for connection to KeyControl

Waiting for connection to KeyControl
KeyControl: sdkc:443
Connected
network : ens160 00:50:56:a2:64:84 192.168.15.239
Connected to KeyControl
Starting root device encryption: sda2

---------- KeyControl and status ----------
sdkc:443
Connected
---------- Encryption / Decryption status ---------
root device encryption
Processing: 100% Time left: 00:00:00
swap device sda3 encryption
Processing: 100% Time left: 00:00:00
system device sdb1 encryption
Processing: 51% Time left: 00:13:39
```

We can see that we are connected to Cryptographic Security Platform Vault and that encryption is in progress. At this point, the `root` and `swap` devices have been fully encrypted and `sdb1` encryption (`/home` in this example) is 51% complete with just under 14 minutes left.

Encrypting Linux System Devices in Azure

The following procedure can be used for any Linux system device (such as `/root`, `swap`, or `/home`). The example used in this procedure shows how to encrypt the `/root`, `swap`, and `/home` devices at the same time, but you can also encrypt any system device separately at any time.

During this procedure, the VM will need to be rebooted to start the encryption process. If you have enabled Online Encryption for this VM, the VM will come back online immediately and the Policy Agent will encrypt the system devices as a background process. In this case, users can continue to access the data while it is being encrypted.

If Online Encryption is *not* enabled, the VM will remain inaccessible for normal operations until the encryption process completes.

For more information about Online Encryption, see Prerequisites and Restrictions for Azure.

Important: Do *not* encrypt a data drive with the `htroot` command. If you do so, Cryptographic Security Platform Vault will treat the data drive as a system device, which means that the data drive cannot be detached, it will appear in Cryptographic Security Platform Vault as a "root" device, and it must be rebooted when you want to encrypt, decrypt, or rekey it. To encrypt a data drive, see

Before You Begin

- Because issues during root device encryption can hang the VM, it is critical to make sure everything is properly configured before you start. For details, see Prerequisites and Restrictions for Azure and Verifying the Current VM Configuration in Azure.
- If there is a KEK associated with the Cloud VM Set to which this VM belongs, make sure that the hardware security module (HSM) in which the KEK is stored is accessible to Cryptographic Security Platform Vault. During the encryption process, the VM must be rebooted. If the KEK is unavailable when the VM attempts to reboot, the reboot will fail until Cryptographic Security Platform Vault can access the KEK in the HSM. For details,

Tip: Depending on the size of the disk, the encryption process can take a long time to run. If the encryption process is interrupted, you need to manually issue the `htroot cleanup` command and then reissue the `htroot setup` or `htroot encrypt` command to resume the process. We recommend you use the Linux `nohup` or `screen` command to avoid terminal-related interruptions during encryption.

Procedure

1. Log into the VM as `root`.
2. Enter the `htroot status` command to verify whether the Entrust Bootloader has already been installed on this VM.
   ```
   # htroot status

   HyTrust Bootloader setup is not done.
   You can complete Bootloader setup using "htroot setup"

   Root device "/dev/sda2" is not encrypted
   swap device "/dev/sda3" is not encrypted
   ```
3. If `htroot status` reports that the Bootloader setup is not done, enter the `htroot setup` command. If `htroot setup` reports that the Bootloader set up is complete, go to the next step.
   ```
   # htroot setup
   Debug console can be used to monitor the progress of root device encryption
   The following packages are required for debug console:
   ```

dropbear
Do you want to enable debug console? (y/N) y

Note: The Entrust Debug Console allows `ssh` access to the server while the encryption process is running so you can check the status of the encryption process. After encryption is complete, the Debug Console provides limited access to the encrypted VM. If the encrypted VM fails to boot because it cannot retrieve the appropriate keys from Cryptographic Security Platform Vault, you can use the Debug Console to restore communication with Cryptographic Security Platform Vault. We highly recommend you enable this console. For more information, see Checking the Root Drive Encryption Status.

Checking connection to software repositories (yum check-update)

Connection to software repositories seems to be working fine

The following packages are required for root encryption:

cryptsetup
dropbear

Attempt to install required packages? (y/N) y

Package dropbear can be found in the EPEL repository.
More information on EPEL can be found at https://fedoraproject.org/wiki/EPEL

NOTE: If you wish to configure EPEL using a private mirror
(e.g. using Red Hat Satellite) then please exit htroot and
configure the repository before re-running.

Attempt to install EPEL release? (y/N) y

Installing EPEL from CentOS Extras repo.....
ok
Installing cryptsetup.....
ok
Installing dropbear.....
ok

Uploaded keyfile /usr/lib/dracut/modules.d/91hcs/root/.ssh/id_rsa to KeyControl
You can download the key from KeyControl using WebGUI

Alternatively, copy the keyfile /usr/lib/dracut/modules.d/91hcs/root/.ssh/id_rsa to another machine
This file will be used to access debug console using ssh
example: # ssh -i id_rsa root@server.ip.addr

Press Enter to continue...

Current Boot device setup

Boot partition device path /dev/sda1
Boot partition device uuid c01c3240-664b-412a-8440-dd0fa132eae5

```
Is this information correct? (y/N) y
Following network interfaces are available

--------------------------------------------------------------------------------
ens160 00:50:56:a2:64:84 192.168.15.239
--------------------------------------------------------------------------------
Preferred Network Interface is (ens160), which is used while authenticating with KeyControl

Select the primary network interface (ens160):
With encrypted root device, KeyControl needs to be contacted during
boot to get the encryption keys. IP address can be obtained using
DHCP or can be statically configured now
Use DHCP during boot? (y/N) y

Re-structuring HyTrust specific directories
Updating initrd

HyTrust Bootloader setup completed successfully
Run "htroot encrypt" to encrypt Linux root devices

# htroot status

HyTrust Bootloader setup is complete

Root device "/dev/sda2" is not encrypted
swap device "/dev/sda3" is not encrypted
```

4. Enter the `htroot encrypt` command and select which system devices you want to encrypt. You can encrypt the devices at any time and in any order. Similarly, once the devices have been encrypted, they can be rekeyed or decrypted at any time and in any order.
   Important: Do *not* encrypt a data drive with the `htroot` command. If you do so,Cryptographic Security Platform Vault will treat the data drive as a system device, which means that the data drive cannot be detached, it will appear in Cryptographic Security Platform Vault as a "root" device, and it must be rebooted when you want to encrypt, decrypt, or rekey it.
   The following example shows how to encrypt the `root`, `swap`, and `/home` devices at the same time.

```
# htroot encrypt

Setting up system for root device encryption.
--------------------------------------------------------------------------------
Do you want to encrypt root device "sda2 (/dev/sda2)"? (y/N) y
Changing /etc/fstab to mount file system / from /dev/mapper/clear_htroot

Setting up system for swap device encryption.
--------------------------------------------------------------------------------
Do you want to encrypt swap device "sda3 (/dev/sda3)"? (y/N) y
Changing /etc/fstab to mount the swap from /dev/mapper/clear_B081FD59-
A74A-4F85-8D1BAA42212F3607

Do you want to encrypt any other file systems, like /var, /usr ?
--------------------------------------------------------------------------------
Please provide comma (,) separated list of mount points: /home
Do you want to encrypt block device "sdb1 (/dev/sdb1, /home)"? (y/N) y
```

```
Changing /etc/fstab to mount file system /home from /dev/mapper/
clear_EE57B642-2A00-49C8-9AC1-
31D300DB6D07

Updating initrd
The system has been updated to encrypt the Linux root device/s during next boot; please reboot
the system now
Do you want to reboot the system now? (y/N) y
```

Confirm the server reboot to continue. When the server has rebooted, it authenticates itself with Cryptographic Security Platform Vault to get the required encryption keys and then starts the encryption process. The time required to encrypt the devices depends on their size and the type of storage you have.

- If you have enabled Online Encryption for this VM, the VM reboots immediately and the Policy Agent encrypts the devices as a background process. In this case, you can check the encryption status at any time using the `hcl status` command.
- If Online Encryption is not enabled, the VM remains offline until the encryption process completes. In this case, you can see the encryption progress on the VM console through vSphere, Azure, or AWS. In addition, if you selected `y` when asked if you wanted to enable the Entrust Debug Console, you can view the progress through the Debug Console as described in Checking the Root Drive Encryption Status.

When it is finished, you can verify that the encryption succeeded using the `htroot status` command. For example:

```
# htroot status

HyTrust boot loader setup is complete

Root device "/dev/sda2" is encrypted
swap device "/dev/sda3" is encrypted
system device "/dev/sdb1 (/home)" is encrypted
```

5. After the encryption process completes, you can log in as normal. If you log in as `root` and enter the `hcl status` command, you will see that the system devices you encrypted are listed under **Registered Devices**. For example:

```
# hcl status

Summary
--------------------------------------------------------------------------------
KeyControl: sdkc:443
KeyControl list: sdkc:443
Status: Connected
Last heartbeat: Wed Jul 4 12:24:22 2018 (successful)
AES_NI: enabled
Certificate Expiration: Jul 4 06:22:12 2019 GMT
HTCRYPT: Not Installed

Registered Devices
--------------------------------------------------------------------------------
Disk Name       Cipher      Status              Clear
--------------------------------------------------------------------------------
sbd1            AES-XTS-512 Attached            /dev/mapper/
clear_EE57B642-2A00-49C8-9AC1-31D300DB6D07 (/home)
```

```
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
sda3            AES-XTS-512  Attached              /dev/mapper/clear_B081FD59-A74A-4F85-8D1B-
AA42212F3607 (/swap)
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
sda2            AES-XTS-512  Attached              /dev/mapper/clear_htroot
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
```

Warning: The `hcl status` command shows the clear text path to the encrypted system devices. (The clear text path is highlighted in the example above). You should only connect to the devices using these clear text paths. Accessing the encrypted devices through the direct paths such as `/dev/sda3` or `/dev/sda2` could cause data corruption.

Verifying the Current VM Configuration in Azure

This procedure describes how to verify that the VM is ready for root and swap drive encryption. Because issues during root drive encryption can hang the VM, it is critical to make sure everything is properly configured before you start.

1. If the VM uses a dynamic IP address and you cannot change it to use a static IP address, make sure the **Reauthentication on IP Change** property is set to **No**. To do so:
   a. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Cloud Admin privileges.
   b. In the top menu bar, click **Workloads**.
   c. Click the **VMs** tab and select the VM you want to work with from the list.
   d. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
   e. Look at the value for **Reauthentication on IP Change**. If it is set to **Yes**, click the word **Yes**, select **No** in the field, then click **Save**.
2. Make sure you have a separate `boot` partition. To do so:
   a. Log into the VM as `root`.
   b. Enter the command `hcl status`. For example:

```
# hcl status
Summary
--------------------------------------------------------------------------------
KeyControl: 192.168.200.175:443
KeyControl list: 192.168.200.175:443
Status: Connected
Last heartbeat: Fri Jul 27 11:31:57 2018 (pass)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT
HTCRYPT: Not Installed

Registered Devices
--------------------------------------------------------------------------------
Disk Name       Cipher      Status              Clear
--------------------------------------------------------------------------------


Available Devices
--------------------------------------------------------------------------------
Disk Name       Device Node              Size (in MB)
--------------------------------------------------------------------------------
```

```
Other Devices
------------------------------------------------------------------------------
Disk Name        Device Node              Status
------------------------------------------------------------------------------
sda3             /dev/sda3                Mounted (swap)
sda1             /dev/sda1                Mounted (/boot)
sda2             /dev/sda2                Mounted (/)
```

You can see that the VM is registered with the KeyControl server (the **Status** shows **Connected**), there are the root (/) and swap devices that we want to encrypt and you can see that there is a separate boot disk. The root and swap disks are listed under **Other Devices** since they are in use.

What to Do Next

Encrypt the boot disk as described in Encrypting Linux System Devices in Azure.

Preparing a Linux System Device for Encryption in Azure

In order to encrypt a Linux system device (such as `/root`, `swap`, or `/home`) in Azure, you need to partition the Linux OS disk so that it has a separate boot partition. Then you need to format the new boot partition and tell Linux to boot from that partition. To do so, perform the following tasks:

Step	Description	Details
1	Make sure the Linux VM meets the Cryptographic Security Platform Vault encryption requirements.	Prerequisites and Restrictions for Azure
2	Partition the Linux OS disk then format and mount the new boot partition.	Partitioning a Linux OS Disk in Azure
3	Verify the VM's configuration.	Verifying the Current VM Configuration in Azure
4	Encrypt one or more Linux system devices.	Encrypting Linux System Devices in Azure

Partitioning a Linux OS Disk in Azure

In order to prepare a Linux VM for system device encryption, you must first create a separate partition for the boot drive. Because many Azure VMs are configured with the `growroot` option, you first need to turn off this option on the VM. Then you can increase the boot disk size and partition it.

During this procedure the VM must be powered off briefly while it is resized.

> Note: If your version of ARM is different from what is described below, please see your Azure documentation.

Before You Begin

This procedure requires `ssh` access to the VM. To set up `ssh` access, see your Azure documentation.

Procedure

1. Log into the VM via `ssh` and do the following:
   a. Make sure that the boot disk is not already on a separate partition using the `df -h` command and looking at the **Mounted on** column. If `/boot` is listed in this column, then the boot device is already running in a separate partition and you can skip to Verifying the Current VM Configuration. For example:
   ```
   # df -h
   Filesystem     Size  Used Avail Use% Mounted on
   devtmpfs       1.8G     0  1.8G   0% /dev
   tmpfs          1.9G     0  1.9G   0% /dev/shm
   tmpfs          1.9G   26M  1.8G   2% /run
   tmpfs          1.9G     0  1.9G   0% /sys/fs/cgroup
   /dev/sda1       30G  1.4G   28G   5% /
   /dev/sbd1       18G   53M   18G   1% /home
   tmpfs          370M   20K  370M   1% /run/user/467
   tmpfs          370M     0  370M   0% /run/user/0
   ```
   b. Determine the size of the current boot partition by entering the `du -sh /boot` command.
   ```
   # du -sh /boot
   52M   /boot
   ```
   The new partition you create should be about twice the size currently being used by `/boot`.
   c. Turn off the `growroot` option on the VM by entering the following command:
   ```
   # touch /etc/growroot-disabled
   ```
2. Log out of the `ssh` session.
3. Log into the Azure Resource Manager and navigate to the VM.
4. Click **Stop** and confirm the action at the prompt to power off the VM.
5. After the VM has been fully powered off, select **Settings > Disks** in the left-hand tree menu.
6. Click the name of the OS disk in the list.
7. Click **Settings > Configuration**.
8. In the **Size** field, enter the new size for the disk and click **Save**. You should increase the disk by at least twice the size of the current boot partition.
9. Navigate back to the main server page and click **Start** to power the server on.
10. After the server has powered on, log back into the server via `ssh`.
11. To verify that the OS disk did not automatically expand to the new disk size, enter the `df -h` command. The size of the OS disk should be the same as it was in the first step.
    For example:
    ```
    # df -h
    Filesystem     Size  Used Avail Use% Mounted on
    devtmpfs       1.8G     0  1.8G   0% /dev
    tmpfs          1.9G     0  1.9G   0% /dev/shm
    tmpfs          1.9G   26M  1.8G   2% /run
    tmpfs          1.9G     0  1.9G   0% /sys/fs/cgroup
    /dev/sda1       30G  1.4G   28G   5% /
    /dev/sbd1       18G   53M   18G   1% /home
    tmpfs          370M   20K  370M   1% /run/user/467
    tmpfs          370M     0  370M   0% /run/user/0
    ```
12. Format the new boot partition in `ext3` or `ext4` and copy the files from the existing boot partition to the new boot partition. Then you can mount the new boot partition and use that to boot the VM.
    How you do this depends on the version of Linux that you are using. For your convenience, we have included the instructions for formatting the new boot partition in Ubuntu, and RHEL 8. For more information, see:

- Formatting the Boot Partition on Ubuntu Without GPT
- Formatting the Boot Partition in Ubuntu with GPT.
- Formatting the Boot Partition in RHEL 8.

Prerequisites and Restrictions for Azure

In addition to encrypting regular data partitions, you can also encrypt your Linux system devices, such as `/root`, `swap`, `/home`, `/var`, and `/opt`. This ensures that clear-text data never leaves the VM on its way to storage and prevents virtualization and storage admins from being able to view the data. You can encrypt these devices at any time and in any order.

At power on, the system will first go to POST, and then hand off the boot process to a destination on the OS volume. Because of this, `/boot` must remain un-encrypted to facilitate early startup activities, including obtaining the key to decrypt the rest of the system. We recommend that you do not store any highly secure data on the boot partition.

> Tip: We recommend you use a server with AES-NI support, which will improve encryption time dramatically. For more information, see Encryption Key Sizes and Algorithms.

Prerequisites

- The VM *must* have a static IP address or you must have the **Reauthentication on IP Change** property set to **No** for the VM. During the encryption process, the VM needs to be rebooted. If you are using a dynamic IP address and the **Reauthentication on IP Change** property is set to **Yes**, the system could hang during the encryption cycle because the VM cannot authenticate itself with Cryptographic Security Platform Vault and the encryption process cannot complete.
  Tip: If you encrypt the root drive and then authentication fails for any reason, you can re-authenticate the VM as described in Re-Authenticating a VM with an Encrypted Root Device or Boot Disk in the *Administration Guide*.
- Entrust requires a separate boot partition in which the Policy Agent can be installed. How you create this partition depends on the version of Linux running on the server.
- If you want to use Online Encryption so that users can continue to access the root and swap drives while they are being encrypted, you must enable Online Encryption on the VM before you encrypt it. For details, see Linux Online Encryption Prerequisites and Considerations in the *Administration Guide*.
- If the VM is associated with a Cloud VM Set that is controlled by a Key Encryption Key (KEK), the HSM must be available before you can encrypt the root drive on the VM. For more information, see KEKs with Cloud VM Sets in the *Administration Guide*.

> Note: Linux initializes `mdadm` devices late in the VM boot cycle. If you encrypt the root drive and there are any `mdadm` devices registered with the Policy Agent, you may receive alerts during the boot process warning you that the `mdadm` device is missing and its name has been changed to GONE In Cryptographic Security Platform Vault. After the `mdadm` device is initialized, another alert is generated telling you that the `mdadm` device has been renamed from GONE back to its original name. You can safely ignore both of these alerts.

Data Encryption in Azure

You can use Entrust Cryptographic Security Platform Vault to encrypt any Linux or Windows data drive or Windows boot drive in Azure the same way you would any other drive in any other system.

If you want to encrypt a Linux root, swap, or system drive, you must first prepare the Linux VM.

Device to be Encrypted	Details
Linux or Windows Data Drive	All data drives in Azure can be encrypted using the standard procedures described in the Data Encryption section.
Windows Boot Drive	Windows boot drives in Azure can be encrypted using the standard procedures described in the Windows Boot Drive Encryption section.
Linux Root, Swap, or System Drive	For details, see Preparing a Linux System Device for Encryption in Azure and Encrypting Linux System Devices in Azure.

Using Data Encryption in AWS

- Checking the Root Drive Encryption Status in AWS
- Encrypting Linux System Devices in AWS
- Verifying the Current VM Configuration in AWS
- Creating a Boot Partition on a New AWS Volume
- Creating a Boot Partition on the Existing AWS Root Volume
- Prerequisites and Restrictions for AWS
- Data Encryption in AWS

Checking the Root Drive Encryption Status in AWS

If Online Encryption *is* enabled for this VM, you can check the encryption status at any time by logging into the VM as `root` and using the `hcl status` command. If Online Encryption *is not* enabled, you can check the encryption status on the VM console through vSphere, Azure, or AWS.

When using a shell on a Windows machine to access the bootloader, you may have to use one of the following options:

- Use git bash to connect.
- Use the following flags to access the bootloader:
  `ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedKeyTypes=ssh-rsa -i <machine-name>.key root@<machine-IP>`

If you need to troubleshoot the encryption process, you can check the encryption status using the Entrust Debug Console if you enabled that while running the `htroot setup` command, as described in Encrypting Linux System Devices in AWS.

1. If you need a copy of the `id_rsa` key file for the VM:
   a. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Cloud Admin privileges.
   b. In the top right, click the Switch to **Appliance Management** link.
   c. Navigate to the **Cloud > VMs** tab and select the VM whose key file you want to download.
   d. Select **Actions > Download Bootloader SSH Key**.
2. Open an `ssh` session by entering the command `ssh -i id_rsa root@vm_name`, where `id_rsa` is the name of the id_rsa file and `vm_name` is the IP address or hostname. For example:
   $ ssh -i Downloads/ht-centos75.key root@ht-centos75

   The authenticity of host 'ht-centos75 (192.168.15.239)' can't be established.

RSA key fingerprint is SHA256:v1TDb5PTlGsncaPf6r9C0Z6ybtqVLxeGXf7XDnh3ltM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ht-centos75,192.168.15.239' (RSA) to the list of known hosts.

HyTrust Debug Console

1. Show HT encryption log file
2. Authenticate
3. Show Network info
4. Restart Network
5. Advanced access
6. logout (exit Debug Console)

3. Select option 1 and look for the status sections. For example, here are a few of the lines towards the end of the output:
Starting HyTrust root encryption ----------

Entered init script with args
Starting debug shell
Detected boot device uuid c01c3240-664b-412a-8440-dd0fa132eae5 device path /dev/sda1
Check file system on device path /dev/sda1
File system check on /dev/sda1 complete
Mounted /dev/sda1
Starting networking
Network started on primary network interface
Started debug console server
Guest VM Status
KeyControl: sdkc:443
Waiting for connection to KeyControl

Waiting for connection to KeyControl
KeyControl: sdkc:443
Connected
network : ens160 00:50:56:a2:64:84 192.168.15.239
Connected to KeyControl
Starting root device encryption: sda2

---------- KeyControl and status ----------
sdkc:443
Connected
---------- Encryption / Decryption status ---------
root device encryption
Processing: 100% Time left: 00:00:00
swap device sda3 encryption
Processing: 100% Time left: 00:00:00
system device sdb1 encryption
Processing: 51% Time left: 00:13:39

We can see that we are connected to Cryptographic Security Platform Vault and that encryption is in progress. At this point, the `root` and `swap` devices have been fully encrypted and `sdb1` encryption (`/home` in this example) is 51% complete with just under 14 minutes left.

Encrypting Linux System Devices in AWS

The following procedure can be used for any Linux system device (such as `/root`, `swap`, or `/home`). The example used in this procedure shows how to encrypt the `/root`, `swap`, and `/home` devices at the same time, but you can also encrypt any system device separately at any time.

During this procedure, the VM will need to be rebooted to start the encryption process. If you have enabled Online Encryption for this VM, the VM will come back online immediately and the Policy Agent will encrypt the system devices as a background process. In this case, users can continue to access the data while it is being encrypted.

If Online Encryption is *not* enabled, the VM will remain inaccessible for normal operations until the encryption process completes.

For more information about Online Encryption, see Prerequisites and Restrictions for AWS.

Important: Do *not* encrypt a data drive with the `htroot` command. If you do so, Cryptographic Security Platform Vault will treat the data drive as a system device, which means that the data drive cannot be detached, it will appear in Cryptographic Security Platform Vault as a "root" device, and it must be rebooted when you want to encrypt, decrypt, or rekey it. To encrypt a data drive, see

Before You Begin

- Because issues during root device encryption can hang the VM, it is critical to make sure everything is properly configured before you start. For details, see Prerequisites and Restrictions for AWS and Verifying the Current VM Configuration in AWS.
- If there is a KEK associated with the Cloud VM Set to which this VM belongs, make sure that the hardware security module (HSM) in which the KEK is stored is accessible to Cryptographic Security Platform Vault. During the encryption process, the VM must be rebooted. If the KEK is unavailable when the VM attempts to reboot, the reboot will fail until Cryptographic Security Platform Vault can access the KEK in the HSM. For details,

Tip: Depending on the size of the disk, the encryption process can take a long time to run. If the encryption process is interrupted, you need to manually issue the `htroot cleanup` command and then reissue the `htroot setup` or `htroot encrypt` command to resume the process. We recommend you use the Linux `nohup` or `screen` command to avoid terminal-related interruptions during encryption.

Procedure

1. Log into the VM as `root`.
2. Enter the `htroot status` command to verify whether the Entrust Bootloader has already been installed on this VM.
   ```
   # htroot status

   HyTrust Bootloader setup is not done.
   You can complete Bootloader setup using "htroot setup"

   Root device "/dev/sda2" is not encrypted
   swap device "/dev/sda3" is not encrypted
   ```
3. If `htroot status` reports that the Bootloader setup is not done, enter the `htroot setup` command. If `htroot setup` reports that the Bootloader set up is complete, go to the next step.
   ```
   # htroot setup
   Debug console can be used to monitor the progress of root device encryption
   The following packages are required for debug console:
   ```

dropbear
Do you want to enable debug console? (y/N) y

Note: The Entrust Debug Console allows `ssh` access to the server while the encryption process is running so you can check the status of the encryption process. After encryption is complete, the Debug Console provides limited access to the encrypted VM. If the encrypted VM fails to boot because it cannot retrieve the appropriate keys from Cryptographic Security Platform Vault, you can use the Debug Console to restore communication with Cryptographic Security Platform Vault. We highly recommend you enable this console. For more information, see Checking the Root Drive Encryption Status.

Checking connection to software repositories (yum check-update)

Connection to software repositories seems to be working fine

The following packages are required for root encryption:

cryptsetup
dropbear

Attempt to install required packages? (y/N) y

Package dropbear can be found in the EPEL repository.
More information on EPEL can be found at https://fedoraproject.org/wiki/EPEL

NOTE: If you wish to configure EPEL using a private mirror
(e.g. using Red Hat Satellite) then please exit htroot and
configure the repository before re-running.

Attempt to install EPEL release? (y/N) y

Installing EPEL from CentOS Extras repo.....
ok
Installing cryptsetup.....
ok
Installing dropbear.....
ok

Uploaded keyfile /usr/lib/dracut/modules.d/91hcs/root/.ssh/id_rsa to KeyControl
You can download the key from KeyControl using WebGUI

Alternatively, copy the keyfile /usr/lib/dracut/modules.d/91hcs/root/.ssh/id_rsa to another machine
This file will be used to access debug console using ssh
example: # ssh -i id_rsa root@server.ip.addr

Press Enter to continue...

Current Boot device setup

Boot partition device path /dev/sda1
Boot partition device uuid c01c3240-664b-412a-8440-dd0fa132eae5

```
Is this information correct? (y/N) y
Following network interfaces are available

--------------------------------------------------------------------------------
ens160 00:50:56:a2:64:84 192.168.15.239
--------------------------------------------------------------------------------
Preferred Network Interface is (ens160), which is used while authenticating with KeyControl

Select the primary network interface (ens160):
With encrypted root device, KeyControl needs to be contacted during
boot to get the encryption keys. IP address can be obtained using
DHCP or can be statically configured now
Use DHCP during boot? (y/N) y

Re-structuring HyTrust specific directories
Updating initrd

HyTrust Bootloader setup completed successfully
Run "htroot encrypt" to encrypt Linux root devices

# htroot status

HyTrust Bootloader setup is complete

Root device "/dev/sda2" is not encrypted
swap device "/dev/sda3" is not encrypted
```

4. Enter the `htroot encrypt` command and select which system devices you want to encrypt. You can encrypt the devices at any time and in any order. Similarly, once the devices have been encrypted, they can be rekeyed or decrypted at any time and in any order.
   Important: Do *not* encrypt a data drive with the `htroot` command. If you do so,Cryptographic Security Platform Vault will treat the data drive as a system device, which means that the data drive cannot be detached, it will appear in Cryptographic Security Platform Vault as a "root" device, and it must be rebooted when you want to encrypt, decrypt, or rekey it.
   The following example shows how to encrypt the `root`, `swap`, and `/home` devices at the same time.

```
# htroot encrypt

Setting up system for root device encryption.
--------------------------------------------------------------------------------
Do you want to encrypt root device "sda2 (/dev/sda2)"? (y/N) y
Changing /etc/fstab to mount file system / from /dev/mapper/clear_htroot

Setting up system for swap device encryption.
--------------------------------------------------------------------------------
Do you want to encrypt swap device "sda3 (/dev/sda3)"? (y/N) y
Changing /etc/fstab to mount the swap from /dev/mapper/clear_B081FD59-
A74A-4F85-8D1BAA42212F3607

Do you want to encrypt any other file systems, like /var, /usr ?
--------------------------------------------------------------------------------
Please provide comma (,) separated list of mount points: /home
Do you want to encrypt block device "sdb1 (/dev/sdb1, /home)"? (y/N) y
```

```
Changing /etc/fstab to mount file system /home from /dev/mapper/
clear_EE57B642-2A00-49C8-9AC1-
31D300DB6D07

Updating initrd
The system has been updated to encrypt the Linux root device/s during next boot; please reboot
the system now
Do you want to reboot the system now? (y/N) y
```

Confirm the server reboot to continue. When the server has rebooted, it authenticates itself with Cryptographic Security Platform Vault to get the required encryption keys and then starts the encryption process. The time required to encrypt the devices depends on their size and the type of storage you have.

- If you have enabled Online Encryption for this VM, the VM reboots immediately and the Policy Agent encrypts the devices as a background process. In this case, you can check the encryption status at any time using the `hcl status` command.
- If Online Encryption is not enabled, the VM remains offline until the encryption process completes. In this case, you can see the encryption progress on the VM console through vSphere, Azure, or AWS. In addition, if you selected `y` when asked if you wanted to enable the Entrust Debug Console, you can view the progress through the Debug Console as described in Checking the Root Drive Encryption Status.

When it is finished, you can verify that the encryption succeeded using the `htroot status` command. For example:

```
# htroot status

HyTrust boot loader setup is complete

Root device "/dev/sda2" is encrypted
swap device "/dev/sda3" is encrypted
system device "/dev/sdb1 (/home)" is encrypted
```

5. After the encryption process completes, you can log in as normal. If you log in as `root` and enter the `hcl status` command, you will see that the system devices you encrypted are listed under **Registered Devices**. For example:

```
# hcl status

Summary
--------------------------------------------------------------------------------
KeyControl: sdkc:443
KeyControl list: sdkc:443
Status: Connected
Last heartbeat: Wed Jul 4 12:24:22 2018 (successful)
AES_NI: enabled
Certificate Expiration: Jul 4 06:22:12 2019 GMT
HTCRYPT: Not Installed

Registered Devices
--------------------------------------------------------------------------------
Disk Name       Cipher      Status              Clear
--------------------------------------------------------------------------------
sbd1            AES-XTS-512 Attached            /dev/mapper/
clear_EE57B642-2A00-49C8-9AC1-31D300DB6D07 (/home)
```

```
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
sda3            AES-XTS-512  Attached              /dev/mapper/clear_B081FD59-A74A-4F85-8D1B-
AA42212F3607 (/swap)
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
sda2            AES-XTS-512  Attached              /dev/mapper/clear_htroot
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
```

Warning: The `hcl status` command shows the clear text path to the encrypted system devices. (The clear text path is highlighted in the example above). You should only connect to the devices using these clear text paths. Accessing the encrypted devices through the direct paths such as `/dev/sda3` or `/dev/sda2` could cause data corruption.

Verifying the Current VM Configuration in AWS

This procedure describes how to verify that the VM is ready for root and swap drive encryption. Because issues during root drive encryption can hang the VM, it is critical to make sure everything is properly configured before you start.

1. If the VM uses a dynamic IP address and you cannot change it to use a static IP address, make sure the **Reauthentication on IP Change** property is set to **No**. To do so:
   a. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Cloud Admin privileges.
   b. In the top menu bar, click **Workloads**.
   c. Click the **VMs** tab and select the VM you want to work with from the list.
   d. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
   e. Look at the value for **Reauthentication on IP Change**. If it is set to **Yes**, click the word **Yes**, select **No** in the field, then click **Save**.
2. Make sure you have a separate `boot` partition. To do so:
   a. Log into the VM as `root`.
   b. Enter the command `hcl status`. For example:

```
# hcl status
Summary
--------------------------------------------------------------------------------
KeyControl: 192.168.200.175:443
KeyControl list: 192.168.200.175:443
Status: Connected
Last heartbeat: Fri Jul 27 11:31:57 2018 (pass)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT
HTCRYPT: Not Installed

Registered Devices
--------------------------------------------------------------------------------
Disk Name       Cipher      Status              Clear
--------------------------------------------------------------------------------


Available Devices
--------------------------------------------------------------------------------
Disk Name       Device Node              Size (in MB)
--------------------------------------------------------------------------------
```

```
Other Devices
-------------------------------------------------------------------------------
Disk Name        Device Node              Status
-------------------------------------------------------------------------------
sda3             /dev/sda3                Mounted (swap)
sda1             /dev/sda1                Mounted (/boot)
sda2             /dev/sda2                Mounted (/)
```

You can see that the VM is registered with the KeyControl server (the **Status** shows **Connected**), there are the root (/) and swap devices that we want to encrypt and you can see that there is a separate boot disk. The root and swap disks are listed under **Other Devices** since they are in use.

What to Do Next

Encrypt the boot disk as described in Encrypting Linux System Devices in AWS.

Creating a Boot Partition on a New AWS Volume

If a Linux VM in AWS is *not* running Amazon Linux, we recommend that you create a boot partition on the existing root volume and then boot from the root volume. Because the root volume will be larger than a new volume created exclusively as a boot volume, AWS will assign more IOPS (Input/Output Operations per Second) to the root volume than to a new volume. This usually results in faster encryption speeds due to the higher number of IOPS available. This method is described in Creating a Boot Partition on the Existing AWS Root Volume.

If the VM is running Amazon Linux, or if you do not want to add a boot partition to your root volume, you can create a new volume that will become the boot partition. To do so:

1. Create and add another volume from EBS to the existing instance. For example, say the current Linux is installed on device `/dev/sda1` and the GRUB stage1 is also installed on `/dev/sda1`. This is a typical Linux installation. Find out the space required by the `/boot` subtree:
   # du -sh /boot

   In general, the space provided should be twice the space used by `/boot` plus 100MB. So if `/boot` uses 200MB, the space should be (200MB * 2) + 100 MB = 500MB.
2. Run the script `aws-prepare-boot.sh` that is installed as part of the Entrust Policy Agent package. For example, if you add a new device named `/dev/xvdf`, you would enter:

   ```
   # /opt/hcs/bin/aws-prepare-boot.sh /dev/xvdf
   ```
3. Power OFF the AWS instance.
4. From the EC2 console, detach the original volume and the new volume from the VM instance.
5. Reattach both volumes but with names exchanged. So the new volume should be added as `/dev/sda1` and the original volume should be added as `/dev/sdf`. This changes the boot device for the VM instance.

   Tip: Note the use of `/dev/sda1` and not `/dev/sda`, as the EC2 console typically uses this name for the OS boot disk.

What to Do Next

Verify the configuration as described in Verifying the Current VM Configuration in AWS and then encrypt the boot device as described in Encrypting Linux System Devices in AWS.

Creating a Boot Partition on the Existing AWS Root Volume

We recommend that you create a boot partition on the existing AWS root volume and then boot from the root volume. Because the root volume will be larger than a new volume created exclusively as a boot volume,

AWS will assign more IOPS (Input/Output Operations per Second) to the root volume than to a new volume. This usually results in faster encryption speeds due to the higher number of IOPS available.

Alternatively, if you do not want to create a boot partition on your existing root volume, you can create a new volume that will become the boot partition. For details, see Creating a Boot Partition on a New AWS Volume.

Important: The following method *cannot* be used for VMs running Amazon Linux. For these VMs you *must* create a boot partition on a new AWS volume.

Before You Begin

Make sure the VM is powered on and is accessible. You cannot perform this procedure if the VM is powered off.

Procedure

1. Log into the EC2 console, make sure the VM is powered on, then increase the size of the root volume by 1 GB. **Important:** Do *not* reboot the VM at this point. If you do, RedHat will auto-extend the root file system to fill the new disk space. You must create the boot partition before you reboot the VM.
2. If you do not know whether the VM uses MBR or GPT partitions, log into the VM as `root` and enter one of the following commands.
   - `fdisk -l /dev/xvda`. For MBR partitions, the operating system will be shown in the **Disklabel type** field.
     ```
     # fdisk -l /dev/xvda

     Welcome to fdisk (util-linux 2.27.1).
     Changes will remain in memory only, until you decide to write them.
     Be careful before using the write command.

     Command (m for help): p
     Disk /dev/xvda: 9 GiB, 9663676416 bytes, 18874368 sectors
     Units: sectors of 1 * 512 = 512 bytes
     Sector size (logical/physical): 512 bytes / 512 bytes
     I/O size (minimum/optimal): 512 bytes / 512 bytes
     Disklabel type: dos
     Disk identifier: 0xe5c7298c
     ```
   - `gdisk -l /dev/xvda`. For GPT partitions, the **GPT** field in the **Partition Label Scan** section will display "present".
     ```
     # gdisk -l /dev/xvda

     GPT fdisk (gdisk) version 0.8.6
     Partition table scan:
       MBR: protective
       BSD: not present
       APM: not present
       GPT: present

     Found valid GPT with protective MBR; using GPT.
     ```
3. If the disk contains MBR partitions, use `fdisk` to create the boot partition and reboot the VM.
   Example:
   ```
   # fdisk /dev/xvda

   Welcome to fdisk (util-linux 2.27.1).
   Changes will remain in memory only, until you decide to write them.
   ```

Be careful before using the write command.

```
Command (m for help): p
Disk /dev/xvda: 9 GiB, 9663676416 bytes, 18874368 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xe5c7298c

Device     Boot Start      End  Sectors Size Id Type
/dev/xvda1 *     2048 16777182 16775135   8G 83 Linux

Command (m for help): n
Partition type
   p   primary (1 primary, 0 extended, 3 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (2-4, default 2):
First sector (16777183-18874367, default 16777216):
Last sector, +sectors or +size{K,M,G,T,P} (16777216-18874367, default 18874367):

Created a new partition 2 of type 'Linux' and of size 1 GiB.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Re-reading the partition table failed.: Device or resource busy

The kernel still uses the old table. The new table will be used at the next reboot or after you run
partprobe(8) or kpartx(8).

# reboot
```

When the VM has finished rebooting, proceed to Step 5.

4. If the disk contains GPT partitions, use `gdisk` to create the boot partition and reboot the VM. During this process you must relocate the backup data structures to the end of the disk in order to create the required free space, as highlighted in the following example.
   Important: If the disk contains MBR partitions, you must use `fdisk` to create the boot partition. If you use `gdisk`, the VM will become unusable and all data will be lost. If you have MBR partitions, return to Step 3.
   Example:

```
# gdisk /dev/xvda

GPT fdisk (gdisk) version 0.8.6
Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: present

Found valid GPT with protective MBR; using GPT.
```

```
Command (? for help): x

Expert command (? for help): e
Relocating backup data structures to the end of the disk

Expert command (? for help): m

Command (? for help): p
Disk /dev/xvda: 211812352 sectors, 101.0 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): F27664E9-0E9F-434A-9AB6-62C730E0F0DF
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 211812318
Partitions will be aligned on 2048-sector boundaries
Total free space is 2099166 sectors (1.0 GiB)

Number  Start (sector)    End (sector)  Size       Code  Name
  1            2048            4095   1024.0 KiB  EF02
  2            4096       209715166   100.0 GiB   0700

Command (? for help): n
Partition number (3-128, default 3):
First sector (34-211812318, default = 209715200) or {+-}size{KMGTP}:
Last sector (209715200-211812318, default = 211812318) or {+-}size{KMGTP}: +800M
Current type is 'Linux filesystem'
Hex code or GUID (L to show codes, Enter = 8300): 0700
Changed type of partition to 'Microsoft basic data'

Command (? for help): c
Partition number (1-3): 3
Enter name:

Command (? for help): p
Disk /dev/xvda: 211812352 sectors, 101.0 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): F27664E9-0E9F-434A-9AB6-62C730E0F0DF
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 211812318
Partitions will be aligned on 2048-sector boundaries
Total free space is 460765 sectors (225.0 MiB)

Number  Start (sector)    End (sector)  Size       Code  Name
  1            2048            4095   1024.0 KiB  EF02
  2            4096       209715167   100.0 GiB   0700
  3       209715200       211353599   800.0 MiB   0700

Command (? for help): w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!!

Do you want to proceed? (Y/N): Y
```

```
OK; writing new GUID partition table (GPT) to /dev/xvda.
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot.
The operation has completed successfully.

# reboot
```

5. Log back into the VM as `root` and run the script `aws-prepare-boot.sh` that is installed as part of the Entrust Policy Agent package. For example, if you add a new device named `/dev/xvda3`, you would enter:

```
# /opt/hcs/bin/aws-prepare-boot.sh /dev/xvda3
```

6. Reboot the VM.

What to Do Next

Verify the configuration as described in Verifying the Current VM Configuration and then encrypt the boot device as described in Encrypting Linux System Devices.

Prerequisites and Restrictions for AWS

In addition to encrypting regular data partitions, you can also encrypt your Linux system devices, such as `/root`, `swap`, `/home`, `/var`, and `/opt`. This ensures that clear-text data never leaves the VM on its way to storage and prevents virtualization and storage admins from being able to view the data. You can encrypt these devices at any time and in any order.

At power on, the system will first go to POST, and then hand off the boot process to a destination on the OS volume. Because of this, `/boot` must remain un-encrypted to facilitate early startup activities, including obtaining the key to decrypt the rest of the system. We recommend that you do not store any highly secure data on the boot partition.

Tip: We recommend you use a server with AES-NI support, which will improve encryption time dramatically. For more information, see Encryption Key Sizes and Algorithms.

Prerequisites

- The VM *must* have a static IP address or you must have the **Reauthentication on IP Change** property set to **No** for the VM. During the encryption process, the VM needs to be rebooted. If you are using a dynamic IP address and the **Reauthentication on IP Change** property is set to **Yes**, the system could hang during the encryption cycle because the VM cannot authenticate itself with Cryptographic Security Platform Vault and the encryption process cannot complete.
  Tip: If you encrypt the root drive and then authentication fails for any reason, you can re-authenticate the VM as described in Re-Authenticating a VM with an Encrypted Root Device or Boot Disk in the *Administration Guide*.
- Entrust requires a separate boot partition in which the Policy Agent can be installed. How you create this partition depends on whether you want to create the boot partition on the existing AWS root volume or on a new AWS volume.
- If you want to use Online Encryption so that users can continue to access the root and swap drives while they are being encrypted, you must enable Online Encryption on the VM before you encrypt it. For details, see Linux Online Encryption Prerequisites and Considerations in the *Administration Guide*.
- If the VM is associated with a Cloud VM Set that is controlled by a Key Encryption Key (KEK), the HSM must be available before you can encrypt the root drive on the VM. For more information, see KEKs with Cloud VM Sets in the *Administration Guide*.

Note: Linux initializes `mdadm` devices late in the VM boot cycle. If you encrypt the root drive and there are any `mdadm` devices registered with the Policy Agent, you may receive alerts during the boot

process warning you that the `mdadm` device is missing and its name has been changed to GONE In Cryptographic Security Platform Vault. After the `mdadm` device is initialized, another alert is generated telling you that the `mdadm` device has been renamed from GONE back to its original name. You can safely ignore both of these alerts.

Data Encryption in AWS

You can use Entrust Cryptographic Security Platform Vault to encrypt any Linux or Windows data drive or Windows boot drive in AWS the same way you would any other drive in any other system.

If you want to encrypt a Linux root, swap, or system drive, you must first create a boot partition either on the existing AWS root volume or on a new AWS volume.

Device to be Encrypted	Details
Linux or Windows Data Drive	All data drives in AWS can be encrypted using the standard procedures described in Data Encryption.
Windows Boot Drive	Windows boot drives in AWS can be encrypted using the standard procedures described in Windows Boot Drive Encryption.
Linux Root, Swap, or System Drive	For details, see: • Prerequisites and Restrictions. • Creating a Boot Partition on the Existing AWS Root Volume. • Creating a Boot Partition on a New AWS Volume.

Windows Encryption Prerequisites

- Make sure the Windows version you are using is supported.
- If you intend to use this VM with a BoundaryControl-enabled Cloud VM Set, you must install the latest version of VMware Tools on the VM. For all other VMs, installing VMware Tools is recommended but not required.
- Cryptographic Security Platform Vault creates a 10 MB private RAW partition for storing metadata the first time you encrypt a partition on a disk. This metadata is required for all subsequent client operations on the encrypted drives. Back it up with the drives whenever you take backups. If the metadata partition is inadvertently removed, the encrypted drives will become inaccessible because the data encryption keys will not be found.
  Cryptographic Security Platform Vault first attempts to create the private partition from unallocated space. If the disk does not have at least 10 MB of unallocated space, it automatically shrinks the data partition to create space for the private RAW partition. On large partitions, this can be very time-consuming. If the Virtual Disk does not have 10 MB of unallocated space, we recommend using your Hypervisor tools to extend the virtual disk to ensure Cryptographic Security Platform Vault can create the private partition from unallocated space.
- Make sure that the disk contains no more than two partitions, excluding the Microsoft Reserved Partition and the Cryptographic Security Platform Vault private partition.
  Cryptographic Security Platform Vault only supports encrypting either two data partitions *or* encrypting the root drive partition and one data partition. You cannot encrypt the boot drive and multiple data partitions.
  Note: Only primary partitions can be encrypted. Logical or extended partitions are not supported.

If the disk contains a hidden Snapshot partition, remove that snapshot partition as described in Detecting and Removing a Windows Snapshot Partition.

- The virtual disks you want to encrypt must support NTFS or ReFS.
- The disks you want to encrypt must be basic Windows disks. Cryptographic Security Platform Vault does *not* support Windows dynamic disks.
- The virtual disks you want to encrypt must have a drive letter or folder mount assigned. You can change the assigned drive letter or folder mount at any time using Windows Disk Manager. Cryptographic Security Platform Vault automatically detects the change and updates the configuration. The new drive assignment will be displayed in the Cryptographic Security Platform Vault webGUI after the next heartbeat.

Detecting and Removing a Windows Snapshot Partition

If a request to add, encrypt, or extend a Windows disk (`hcl add`, `hcl encrypt`, or `hcl extend`) fails with an error stating there are too many partitions on the disk, the problem may be that Windows added a Snapshot partition at the beginning of the disk. If the Windows Disk Manager shows only two partitions, excluding the Microsoft Reserved Partition and the Cryptographic Security Platform Vault private partition, use this procedure to see if there is a hidden Snapshot partition on the disk.

1. Log into the VM as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. Determine the disk # of the drive letter using one of the following methods:
   - Using the Policy Agent: run `hcl status`
   - Using the Windows Disk Manager: run `diskmgmt.msc`

   Running one of these commands will display the disk number of the drive letter that you want to use.
3. Enter the command `diskpart`.
4. At the `DISKPART` prompt, enter the command `select Disk disk-number`, where `disk-number` is the number of the Windows disk that you want to check.
5. Enter the command `list partition`.
   If there is a Snapshot partition, it typically starts at offset 273 KB. For example:
   DISKPART> list partition

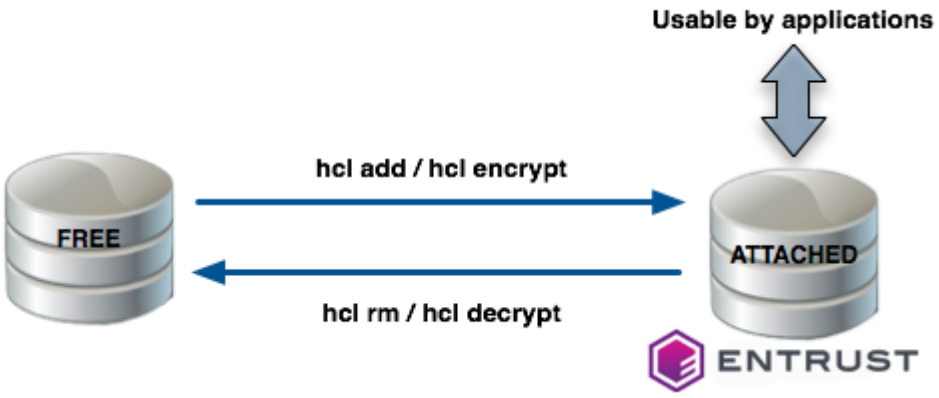
   ```
   Partition ### Type          Size    Offset
   ------------- --------------- ------- -------
   Partition  4  Unknown        256 KB  273 KB
   Partition  2  Reserved        31 MB   529 KB
   Partition  3  Primary        300 MB  32 MB
   Partition  1  Unknown         10 MB   332 MB
   ```

6. To verify that the partition is a Snapshot partition, enter the command `select partition partition-number`, where `partition-number` is the number of the partition you want to check. For example:
   DISKPART> select partition 4
7. Enter the command detail partition. If this is a Snapshot partition, the type will be listed as `caddebf1-4400-4de8-b103-12117dcf3ccf`. For example:
   DISKPART> detail partition
   Partition 4
   Type : `caddebf1-4400-4de8-b103-12117dcf3ccf`
   Hidden : Yes
   Required: No
   Attrib : 0000000000000000
   Offset in Bytes: 279552
8. To delete the Snapshot partition, enter the command `delete partition`.

9. Repeat the `select partition` and `detail partition` commands for each partition on this disk, but ensure that you only delete partitions where the Type matches the value `caddebf1-4400-4de8-b103-12117dcf3ccf`.
   The type `caddebf1-4400-4de8-b103-12117dcf3ccf` indicates that this is a Microsoft snapshot, which was only used when Microsoft VSS created it, and is no longer used. Microsoft VSS will create a new snapshot when necessary.
10. Resubmit the `hcl add`, `hcl encrypt`, or `hcl extend` request.

Linux Encryption Overview

In Linux, a disk can be either free or under Entrust control. If Entrust controls it, then it must be attached before applications can access it.



Entrust allows you to register:

- New disks with no existing data (using the `hcl add` command).
- Existing disks that already contain data you want to retain (using the `hcl encrypt` command).

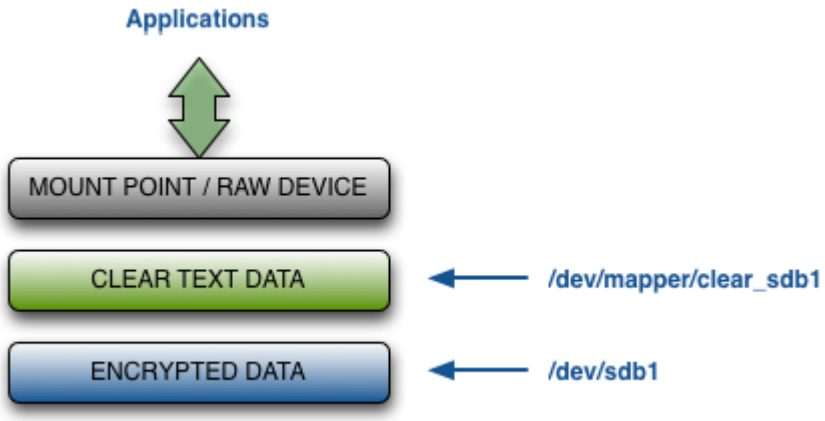
After you register a disk with Cryptographic Security Platform Vault for VM Encryption and perform the initial encryption, you can rekey the disk, move the disk, or reimport the disk using the Cryptographic Security Platform Vault for VM Encryption webGUI or `hicli`.

The Cryptographic Security Platform Vault for VM Encryption creates an unencrypted path to the data that is accessible when the disk is attached. The default pathname is `/dev/mapper/clear_diskname` (for example: `/dev/mapper/clear_sdb1`), but you can change that path when you register the disk.

Warning: Once you set up the encrypted disk, you should NOT access the unencrypted device through anything other than the clear text path. In other words, you always need to use `/dev/mapper/clear_sdb1` instead of `/dev/sdb1`. The Linux kernel caches data, which it may flush periodically. If you write to the raw device without going through the `/dev/mapper` interface, you could end up with corrupted data.

This means that any existing entries for the unencrypted device in the Filesystem Table (`/etc/fstab`) need to be updated to point to the clear text version of the device. An incorrect `fstab` entry can result in the system hanging when it reboots. For details, see Automatically Mounting Linux Filesystems,Changing the Mount Order on Linux.

The following figure summarizes the layers at which encrypted and unencrypted data is available:



This section includes:

- Changing the Mount Order on Linux
- Automatically Mounting Linux Filesystems
- Troubleshooting the HTCrypt Driver
- Uninstalling the HTCrypt Driver
- Updating the HTCrypt Kernel Dependencies
- Configuring UEFI Secure Boot
- Viewing HTCrypt Driver Status
- Enabling Linux Online Encryption with the CSP Vault for VM Encryption webGUI
- Enabling Linux Online Encryption with the CLI
- Linux Online Encryption Prerequisites and Considerations
- Linux Encryption Prerequisites

Changing the Mount Order on Linux

1. To view the current mount order, use the `hcl devorder print` command. For example:
   ```
   # hcl devorder print
   Disk | Path | Clear | Cipher | auto_attach | mntpt | mntopts
   ------------------------------------------------------------------------------
   sdb1 | /dev/sdb1 | /dev/mapper/clear_sdb1 | AES-XTS-512 | ENABLED | my_mountpoint | -t ext4 -o
   ro,noatime
   sdb4 | /dev/sdb4 | /dev/mapper/clear_sdb4 | AES-XTS-512 | ENABLED | mount4 | -o rw
   sdc3 | /dev/sdc3 | /dev/mapper/clear_sdc3 | AES-XTS-512 | ENABLED | |
   ```
2. To change the mount order, use the `hcl devorder up|down diskname` command, where `diskname` is the short form of the device name and `up` or `down` moves the device one position in the specified direction. For example, to move `sdc3` to the top of the list, you need to use the `devorder up sdc3` command twice:
   ```
   # hcl devorder up sdc3
   Device re-order: move device sdc3 UP

   Successfully changed order of device sdc3
   ```

```
# hcl devorder up sdc3
Device re-order: move device sdc3 UP

Successfully changed order of device sdc3

# hcl devorder print
Disk | Path | Clear | Cipher | auto_attach | mntpt | mntopts
------------------------------------------------------------------------------
sdc3 | /dev/sdc3 | /dev/mapper/clear_sdc3 | AES-XTS-512 | ENABLED | |
sdb1 | /dev/sdb1 | /dev/mapper/clear_sdb1 | AES-XTS-512 | ENABLED | my_mountpoint | -t ext4 -o
ro,noatime
sdb4 | /dev/sdb4 | /dev/mapper/clear_sdb4 | AES-XTS-512 | ENABLED | mount4 | -o rw
```

Automatically Mounting Linux Filesystems

On Linux, it is normal to add entries to the Filesystem Table (`/etc/fstab`) to have the filesystems automatically mount on boot. While you *could* add the clear text path to the device in the `/etc/fstab` file manually, doing so could cause the system to hang during reboot.

The issues arise because the Linux boot process is asynchronous. As the Entrust Policy Agent is querying Cryptographic Security Platform Vault to get the keys for the registered devices and then attaching them, Linux is processing the `/etc/fstab` file in the background. If the system processes an `fstab` entry for a device that the Policy Agent has not yet attached, the clear text path will not be available yet and the device will fail to mount. If the device is marked as "required at boot", the system will hang during the boot process.

In addition, if the device name changes during the boot process due to a hardware device swap or similar process, then the clear text path to the device will change and any manually-created `fstab` entry will be incorrect. Again, the system will hang during boot if this renamed device is marked "required at boot".

To resolve all of these issues, Entrust provides a way to automatically mount the drives using `hcl` . By letting Entrust control the auto-mount process, you can be certain that the devices are mounted after the clear text paths are available, and that device name changes will be handled automatically.

> Note: If you specified the `-m` option and provided a user-defined clear text path name when you added the VM to Cryptographic Security Platform Vault, `hcl` always uses that clear text path regardless of the device name.

Procedure

1. Log into the VM as `root` .
2. To check the existing mount points and options, use `hcl status` command:

```
# hcl status
Summary
------------------------------------------------------------------------------
KeyControl: 192.168.140.151:443
KeyControl list: 192.168.140.151:443
Status: Connected
Last heartbeat: Thu Apr 19 09:42:58 2016 (successful)


Registered Devices
------------------------------------------------------------------------------
Disk Name       Cipher     Status          Clear
```

```
--------------------------------------------------------------------------------
sdb1            AES-XTS-512  Attached          /dev/mapper/clear_sdb1
```

3. Enable auto-mount for the device using the `hcl set mntpt=/path diskname` command, where `path` is the mount point for the device and `diskname` is the short form of the device name. For example, you would use `sdb1` instead of `/dev/sdb1`. For example:
   # hcl set mntpt=/my_mountpoint sdb1
4. If you want to set any mount options, use the `hcl set mntopts="option1 option2 ..." diskname` command. For example:
   # hcl set mntopts="-t ext4 -o ro,noatime" sdb1

   `hcl` stores these options and then, whenever the VM reboots, `hcl` checks to make sure that the mount point exists and then mounts the filesystem using the specified options. Using the example above, `hcl` would make the following call during boot:
   # mount -t ext4 -o ro,noatime /dev/mapper/clear_sdb1 /my_mountpoint

   Note: To see the default attach handler script Entrust uses.
5. To verify your changes, use the `hcl status` command.

```
# hcl status
Summary
--------------------------------------------------------------------------------
KeyControl: 192.168.140.151:443
KeyControl list: 192.168.140.151:443
Status: Connected
Last heartbeat: Thu Apr 19 09:42:58 2018 (successful)


Registered Devices
--------------------------------------------------------------------------------
Disk Name       Cipher      Status            Clear
--------------------------------------------------------------------------------
sdb1            AES-XTS-512  Attached          /dev/mapper/clear_sdb1
'--> auto_attach=ENABLED, mntpt=/my_mountpoint, mntopts="-t ext4 -o ro,noatime",
attach_handler=DEFAULT, detach_handler=DEFAULT
```

What to Do Next

If you want to change the order in which the devices are mounted, see Changing the Mount Order on Linux.

Troubleshooting the HTCrypt Driver

When you upgrade the Policy Agent or the kernel files on a Linux VM, the Policy Agent automatically rebuilds the HTCrypt Driver using DKMS. If the required packages are not available at this time, the Policy Agent reverts to using offline encryption and will no longer encrypt, decrypt, or rekey devices using Online Encryption.

The following `hcl status` output indicates that there are issues with the HTCrypt Driver.

```
# hcl status

Summary
--------------------------------------------------------------------------------
KeyControl: None
Status: Not registered
```

AES_NI: enabled
HTCRYPT: unavailableERROR !!!!! htcrypt is installed but not accessible, run "htdrv status" for details

If this happens, you can manually update and rebuild the HTCrypt Driver. If rebuilding it does not work, you can also reinstall the driver.

Rebuilding the HTCrypt Driver

1. Log into the VM on which you want to re-enable the HTCrypt Driver as `root`.
2. Display the status of the HTCrypt Driver by entering the `htdrv status` command. If some packages are out of date, this command will show which packages need to be updated.
   The following example shows the results of the `htdrv status` command before the HTCrypt Driver has been installed:
   ```
   # htdrv status
   HyTrust online encryption driver status
   ---------------------------------------------------------------------
   package htcrypt is not installed

   >>> htcrypt driver is not installed on this VM

   ERROR !!!!! Missing kernel headers for the current kernel version: 3.10.0-514.el7.x86_64 or higher
   ERROR !!!!! Missing kernel development package for the current kernel version: 3.10.0-514.el7.x86_64
   ERROR !!!!! gcc missing -- required for htcrypt driver
   ERROR !!!!! dkms missing -- required for htcrypt driver

   Here are the Linux kernel and related packages installed on this system
   ---------------------------------------------------------------------
   Installed Packages
   kernel.x86_64              3.10.0-514.el7              @anaconda
   kernel-tools.x86_64        3.10.0-514.el7              @anaconda
   kernel-tools-libs.x86_64   3.10.0-514.el7              @anaconda
   ```
3. Install the required supporting packages by entering the `htdrv prepare` command.
4. Recompile the HTCrypt Driver by entering the `htdrv rebuild` command.
5. To verify that the rebuild worked, use the `hcl status` command and make sure the HTCrypt Driver status is **enabled**.
   ```
   # hcl status

   Summary
   ---------------------------------------------------------------------------
   KeyControl: None
   Status: Not registered
   AES_NI: enabled
   HTCRYPT: enabled
   ```
   If the rebuild worked and the HTCrypt Driver is now available, proceed to the next step and finish the process by rebooting the VM. If the rebuild did *not* work, you should reinstall the HTCrypt Driver as described below.
6. If the VM has its root devices encrypted before the installation of the online encryption driver, then in order to extend the online encryption driver support to the root devices, the admin should run the following commands:
   ```
   # htroot update
   # reboot
   ```

7. If the root or swap disk is encrypted on this VM, you need to reboot the VM to complete the installation process.
   If only data disks are encrypted on the VM, you can either reboot the VM or detach and then reattach all attached data disks to start the HTCrypt Driver on those disks. To detach and reattach the disks, use the `hcl detach -a` and `hcl attach -a` commands. For example:
   ```
   # hcl detach -a
   Encrypted device sdi7 detached; encrypted contents no longer visible
   Encrypted device sdi1 detached; encrypted contents no longer visible
   # hcl attach -a
   Encrypted device sdi7 (/dev/sdi7) attached; encrypted contents visible at /dev/mapper/clear_sdi7
   Encrypted device sdi1 (/dev/sdi1) attached; encrypted contents visible at /dev/mapper/clear_sdi1
   ```

Reinstalling the HTCrypt Driver

If rebuilding the HTCrypt Driver does not work, you can uninstall the driver, clean up any old installation files, and then reinstall the driver from scratch.

1. Uninstall the HTCrypt Driver. For RHEL run the command `rpm -e htcrypt`, and for Ubuntu run the command `dpkg -r htcrypt-dkms`.
2. Clean up all HTCrypt Driver files by entering the `rm -rf /var/lib/dkms/htcrypt` command.
3. Reinstall the HTCrypt Driver.
   - For RHEL, reinstall the HTCrypt Driver RPM by entering the command `rpm -ivh /opt/hcs/drivers/htcrypt-10.5.3-buildnum.noarch.rpm`, where `buildnum` is the build number that you are installing. For example:
     ```
     # rpm -ivh htcrypt-10.5.3-12345M.noarch.rpm
     Preparing...                ########################################### [100%]
     Updating / installing...
       1:htcrypt-10.5.3-12345M   ########################################### [100%]
     Loading new htcrypt-10.5.3 DKMS files...
     Building for 3.10.0-693.17.1.el7.x86_64
     Building initial module for 3.10.0-693.17.1.el7.x86_64
     Done.

     htcrypt:
     Running module version sanity check.
      - Original module
        - No original module exists within this kernel
      - Installation
        - Installing to /lib/modules/3.10.0-693.17.1.el7.x86_64/extra/

     depmod....

     Backing up initramfs-3.10.0-693.17.1.el7.x86_64.img to /boot/
     initramfs-3.10.0-693.17.1.el7.x86_64.img.old-dkms
     Making new initramfs-3.10.0-693.17.1.el7.x86_64.img
     (If next boot fails, revert to initramfs-3.10.0-693.17.1.el7.x86_64.img.old-dkms image)
     dracut.....

     DKMS: install completed.
     ```

- For Ubuntu, reinstall the HTCrypt Driver DEB by entering the command `dpkg -i /opt/hcs/drivers/htcrypt-dkms_<buildver>_all.deb`, where buildver is the build version that you are installing. For example:

```
# dpkg -i /opt/hcs/drivers/htcrypt-dkms_5.40012345_all.deb
Selecting previously unselected package htcrypt-dkms.
(Reading database ... 169211 files and directories currently installed.)
Preparing to unpack .../htcrypt-dkms_5.40000655_all.deb ...
Unpacking htcrypt-dkms (5.40012345) ...
Setting up htcrypt-dkms (5.40012345) ...
Loading new htcrypt-5.40012345 DKMS files...
Building for 5.4.0-64-generic
Building for architecture x86_64
Building initial module for 5.4.0-42-generic
Done.

htcrypt.ko:
Running module version sanity check.
 - Original module
   - No original module exists within this kernel
 - Installation
   - Installing to /lib/modules/5.4.0-42-generic/updates/dkms/

depmod.....

Backing up initrd.img-5.4.0-42-generic to /boot/initrd.img-5.4.0-42-generic.old-dkms
Making new initrd.img-5.4.0-42-generic
(If next boot fails, revert to initrd.img-5.4.0-42-generic.old-dkms image)
update-initramfs.................

DKMS: install completed.
Building initial module for 5.8.0-38-generic
Done.

htcrypt.ko:
Running module version sanity check.
 - Original module
   - No original module exists within this kernel
 - Installation
   - Installing to /lib/modules/5.8.0-38-generic/updates/dkms/

depmod.....

Backing up initrd.img-5.8.0-38-generic to /boot/initrd.img-5.8.0-38-generic.old-dkms
Making new initrd.img-5.8.0-38-generic
(If next boot fails, revert to initrd.img-5.8.0-38-generic.old-dkms image)
update-initramfs.................

DKMS: install completed.
```

4. To verify that the installation succeeded, enter the `hcl status` command. For example:

```
# hcl status
```

```
Summary
--------------------------------------------------------------------------------
KeyControl: 10.238.66.235:443
KeyControl list: 10.238.66.235:443
Status: Connected
Last heartbeat: Wed Mar 21 12:48:19 2019 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT
HTCRYPT: enabled
```

At this point, the HTCrypt Driver is installed but is not yet running on any disks that are currently attached.

5. If the VM has its root devices encrypted before the installation of the online encryption driver, then in order to extend the online encryption driver support to the root devices, the admin should run the following commands:

```
# htroot update
# reboot
```

6. If the root or swap disk is encrypted on this VM, you need to reboot the VM to complete the installation process.
   If only data disks are encrypted on the VM, you can either reboot the VM or detach and then reattach all attached data disks to start the HTCrypt Driver on those disks. To detach and reattach the disks, use the `hcl detach -a` and `hcl attach -a` commands. For example:

```
# hcl detach -a
Encrypted device sdi7 detached; encrypted contents no longer visible
Encrypted device sdi1 detached; encrypted contents no longer visible
# hcl attach -a
Encrypted device sdi7 (/dev/sdi7) attached; encrypted contents visible at /dev/mapper/clear_sdi7
Encrypted device sdi1 (/dev/sdi1) attached; encrypted contents visible at /dev/mapper/clear_sdi1
```

Uninstalling the HTCrypt Driver

Note: If you uninstall the HTCrypt Driver, the Policy Agent will need to detach a Linux disk before it can encrypt, decrypt, or rekey that disk.

1. Log into the VM as `root`.
2. Run the appropriate command.
   - For RHEL, run the command `rpm -e htcrypt`. For example:

```
# rpm -e htcrypt

Uninstall of htcrypt module (version 4.2) beginning:

-------- Uninstall Beginning --------
Module:  htcrypt
Version: 4.2
Kernel:  3.10.0-693.17.1.el7.x86_64 (x86_64)
-------------------------------------

Status: Before uninstall, this module version was ACTIVE on this kernel.

htcrypt.ko:
 - Uninstallation
   - Deleting from: /lib/modules/3.10.0-693.17.1.el7.x86_64/extra/
 - Original module
```

```
  - No original module was found for this module on this kernel.
  - Use the dkms install command to reinstall any previous module version.


Running the post_remove script:
depmod....

Backing up initramfs-3.10.0-693.17.1.el7.x86_64.img to /boot/
initramfs-3.10.0-693.17.1.el7.x86_64.img.old-dkms
Making new initramfs-3.10.0-693.17.1.el7.x86_64.img
(If next boot fails, revert to initramfs-3.10.0-693.17.1.el7.x86_64.img.old-dkms image)
dracut.....

DKMS: uninstall completed.

------------------------------
Deleting module version: 4.2
completely from the DKMS tree.
------------------------------
Done.
```

- For Ubuntu, run the command `dpkg -r htcrypt-dkms`. For example:

```
# dpkg -r htcrypt-dkms
(Reading database ... 169211 files and directories currently installed.)
Removing htcrypt-dkms (5.40012345) ...

-------- Uninstall Beginning --------
Module:  htcrypt
Version: 5.40012345
Kernel:  5.8.0-38-generic (x86_64)
-------------------------------------

Status: Before uninstall, this module version was ACTIVE on this kernel.

htcrypt.ko:
 - Uninstallation
   - Deleting from: /lib/modules/5.8.0-38-generic/updates/dkms/
 - Original module
   - No original module was found for this module on this kernel.
   - Use the dkms install command to reinstall any previous module version.


Running the post_remove script:
depmod.....

update-initramfs.....

DKMS: uninstall completed.

------------------------------
Deleting module version: 5.40012345
completely from the DKMS tree.
```

```
------------------------------
Done.
```

At this point, the HTCrypt Driver status shows as "Not Installed" but it is still running on any disks that are currently attached.

3. If the root or swap disk is encrypted on this VM, you need to reboot the VM to completely remove the HTCrypt Driver from the VM.
   If only data disks are encrypted on the VM, you can either reboot the VM or detach and then reattach all attached data disks to remove the HTCrypt Driver from those disks. To detach and reattach the disks, use the `hcl detach -a` and `hcl attach -a` commands. For example:

```
# hcl detach -a
Encrypted device sdi7 detached; encrypted contents no longer visible
Encrypted device sdi1 detached; encrypted contents no longer visible
# hcl attach -a
Encrypted device sdi7 (/dev/sdi7) attached; encrypted contents visible at /dev/mapper/clear_sdi7
Encrypted device sdi1 (/dev/sdi1) attached; encrypted contents visible at /dev/mapper/clear_sdi1
```

4. Verify the uninstallation by entering the `hcl status` command. For example:

```
# hcl status

Summary
--------------------------------------------------------------------------------
KeyControl: 10.238.66.235:443
KeyControl list: 10.238.66.235:443
Status: Connected
Last heartbeat: Wed Mar 21 13:50:45 2018 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT
HTCRYPT: Not Installed
```

Updating the HTCrypt Kernel Dependencies

If you update the Linux kernel on the VM, you need to update the `kernel-devel` and `kernel-headers` packages as well. To do so:

1. Log into the VM as `root`.
2. If you want to:
   - Update the kernel and all dependencies at the same time, enter the `htdrv update` command.
   - Update just the `kernel-headers` and `kernel-devel` packages, enter the `yum update kernel kernel-devel kernel-headers` command.
3. Reboot the VM.

What to Do Next

If the HTCrypt Driver still reports kernel errors or that there is a mismatch between the kernel and its dependencies, you can rebuild the driver using the `htdrv rebuild` command. If this does not fix the issue, use the `htdrv update` command.

Configuring UEFI Secure Boot

You can use the Policy Agent online encryption driver with UEFI secure boot. This is supported on the following platforms:

- Red Hat 8.x

- Red Hat 9.x
- Ubuntu 22.04
- Oracle 8.7, 8.8, 9.1, 9.2, and 9.3

Important: UEFI and Secure Boot is only supported with VMware ESXi. It is not supported on AWS, Azure, and GCP.

Configuring UEFI Secure Boot in Ubuntu

To configure UEFI Secure Boot in Ubuntu, you need to install the driver package using `dpkg -i /opt/hcs/drivers/htcrypt-dkms_<buildver>_all.deb`.

If the dkms has not created any Machine-Owner key(MOK) in the system, the installation process should prompt you to create a new MOK, and will guide you through the steps to enroll that key in your system's firmware. This process requires a reboot.

> Note: Since the MOK enrolling process requires user interaction and a reboot, the Cryptographic Security Platform Vault htcrypt installation process will fail if the secure boot is enabled on the ubuntu VM and no MOK is created by the dkms. You will receive an alert to try it manually.

Configuring UEFI Secure Boot in RHEL or Oracle Linux

Policy Agent provides helper scripts to facilitate driver signing based on the Machine Owner Key (MOK) facility provided by Red Hat. For more information on MOK, see Signing Kernel Modules for Secure Boot. The helper script is located at `/opt/hcs/bin/htdrv` and helps the administrator sign the online encryption driver, htcrypt. The htcrypt driver needs to be signed when it is built for the first time or when it is rebuilt after installing a new Linux kernel.

To sign a driver as part of the MOK facility, you must create a Entrust driver signing key and register it with the MOK database, then perform a virtual machine reboot. We recommend that you use a password for the Entrust signing key.

Before You Begin

- Make sure the VM meets the requirements described in Linux Encryption Prerequisites and Linux Online Encryption Prerequisites and Considerations. UEFI secure boot must also be enabled on your Linux platform.
- For Linux, you must update the grub and shim packages before you run htdrv secure-boot. For more information see the following articles:
  - https://bugzilla.redhat.com/show_bug.cgi?id=1878773
  - https://access.redhat.com/solutions/5395851
  - https://access.redhat.com/security/vulnerabilities/grub2bootloader
- You will need to access the VM console immediately after running the script, as the MOK database enrollment screen is only available for approximately 10 seconds after the reboot. Make sure your VM console is easily accessible before you reboot.

Procedure

1. Log into the VM as `root`.
2. Run the htdrv secure-boot command as follows:
   [root@uefi-rhel8 ~]# htdrv secure-boot
   Preparing system for signing HyTrust online encryption driver with Machine owner key (MOK)

   Creating HyTrust signing key for UEFI secure boot

   The signing key can, optionally, be protected with a PEM pass phrase
   If the signing key is protected with PEM pass phrase then the driver can not be automatically signed

The new driver is created when the online driver RPM is installed, or a new kernel is installed on the system
If signing key is PEM pass phrase protected then administrator has to manually sign the htcrypt driver every time that the new driver module is built. This can be done using command "htdrv sign"

Please refer the Admin Guide for details

Do you want to proceed without PEM pass phrase? (yes/no) no

Generating a RSA private key
.....++++
.....++++
writing new private key to '/opt/hcs/etc/htsecboot.priv'
Enter PEM pass phrase: ##############
Verifying - Enter PEM pass phrase: ##############

Successfully created HyTrust signing key

We need to enroll HyTrust signing key to Machine owner key (MOK) list
The system will have to be rebooted for this operation

Plese enter a "One Time use Password (OTP)" for MOK enrollment request
input password: ##############
input password again: ##############

The system will be rebooted to complete MOK enrollment request

Please make sure that you are in hold of active system console, before proceeding to reboot
Enter the password at the system console when asked

Press Enter to reboot
Rebooting...

3. Quickly access the VM system console to use the MOK database enrollment screen. The MOK database enrollment screen is only available for approximately 10 seconds after the reboot. If you miss the screen, you can run the `htdrv secure-boot` command again.
4. On the main screen, press any key to enter the MOK database enrollment screen.
5. Select `Enroll MOK`.
6. Select `Yes`.
7. Run the following command again to ensure that the Entrust signing key has been successfully created and enrolled in the MOK database:
   [root@uefi-rhel8 ~]# htdrv secure-boot
   Preparing system for signing HyTrust online encryption driver with Machine owner key (MOK)

   HyTrust signing key already present on the system

   HyTrust signing key already enrolled in Machine owner key (MOK) list
8. Run the `htdrv sign` command to sign the driver. If you entered a password for the Entrust signing key, you have to enter that same password twice. The Signing key is located at /opt/hcs/etc/htsecboot.priv.
   # htdrv sign
   Signing HyTrust online encryption driver with Machine owner key (MOK)

Please give Machine Owner Key's passphrase for HyTrust signing key: ##############
Enter pass phrase for /opt/hcs/etc/htsecboot.priv: ##############
Successfully signed /lib/modules/3.10.0-1062.12.1.el7.x86_64/extra/htcrypt.ko with HyTrust signing key
Rebuilding initrd

If you did not enter a password for the Entrust signing key when you ran the htdrv secure-boot command, this is provided internally, you will not be prompted for any passwords, and you will not need to run this command after initial configuration.
Otherwise, you will need to run `htdrv sign` command to resign the driver at the following times:

- When the Policy Agent is upgraded.
- When the Red Hat kernel is upgraded.

9. Run the following command to check the status of the htcrypt driver:
   [root@uefi-rhel8 ~]# htdrv status

   HyTrust online encryption driver status

   Name : htcrypt
   Version : 5.1
   Release : 510001412
   Architecture: noarch
   Install Date: Thu 26 Dec 2019 03:23:42 AM EST
   Group : System/Kernel
   Size : 99657
   License : GPLv2
   Signature : DSA/SHA1, Tue 24 Dec 2019 09:49:45 PM EST, Key ID 4a1ed78762b480bf
   Source RPM : htcrypt-5.1-510001412.src.rpm
   Build Date : Tue 24 Dec 2019 09:43:57 PM EST
   Build Host : htcrypt-rhel7.dc.hytrust.com
   Relocations : (not relocatable)
   Packager : HYTRUST <htdc-devel@hytrust.com>
   Summary : htcrypt 5.1 dkms package
   Description :
   Kernel modules for htcrypt 5.1 in a DKMS wrapper.

   >>> htcrypt driver is installed on this VM

   UEFI Secure boot status

   This system is setup with UEFI boot
   Secure boot option is only supported with UEFI boot
   SecureBoot enabled
   HyTrust signing key is present on the system

   HyTrust signing key is enrolled in Machine owner key (MOK) list
10. Run the hcl status command to ensure that htcrypt is enabled. If htcrypt is not enabled, then run htdrv update, then htdrv rebuild, and then reboot the VM. For more information, see Troubleshooting the HTCrypt Driver.

Note: If you want to delete the Entrust signing key, log into the VM as `root` and run `htdrv secure-boot cleanup`. This will remove the signing key from MOK as well as delete the signing key file.

Viewing HTCrypt Driver Status

To view the status of the HTCrypt Driver module, use the `modinfo htcrypt` command.

```
# modinfo htcrypt
filename:       /lib/modules/5.14.0-362.24.1.el9_3.x86_64/extra/htcrypt.ko.xz
license:        GPL
version:        10.20001189
description:    Entrust Online Encryption Driver
author:         Entrust
rhelversion:    9.3
srcversion:     64DA9E0427C6CED03256E07
depends:        dm-mod
retpoline:      Y
name:           htcrypt
vermagic:       5.14.0-362.24.1.el9_3.x86_64 SMP preempt mod_unload modversions
sig_id:         PKCS#7
signer:         HyTrust signing key
sig_key:        54:77:F7:9C:51:31:8B:16:81:44:43:CF:2B:6A:07:71:46:0B:90:F5
sig_hashalgo:   sha256
signature:      A0:16:BA:9C:7D:A0:67:E0:B6:21:35:27:E4:FF:66:2F:AF:A1:7B:79:
        F4:B4:79:D5:15:84:18:6E:08:E5:51:CA:D9:AE:B7:0E:95:EE:B1:BE:
        B2:63:B9:FD:36:BE:F5:BA:AD:19:7D:2B:7A:17:98:C2:86:81:D8:1C:
        4A:21:32:B1:EB:64:8E:F7:46:7D:D3:CE:59:4D:F8:8B:CD:43:14:ED:
        01:09:13:00:15:50:B7:D5:4E:B5:E3:D0:A6:35:7F:A0:1A:B9:3B:6C:
        67:CB:97:4E:79:7E:17:CA:59:FE:C3:96:A9:AA:BE:17:E0:05:55:CC:
        DB:D7:07:71:82:C0:92:63:69:58:94:0D:FB:2F:57:71:9D:AF:BD:A4:
        78:2E:AE:D0:79:DD:94:5D:0F:9B:1E:92:DA:25:04:FD:46:14:8F:A0:
        4E:BD:4E:46:58:40:0F:B2:FA:5C:7A:17:60:02:88:5C:2D:80:DE:BA:
        A9:22:B3:E6:50:32:EF:29:AF:C1:E7:86:1D:04:A4:A4:A0:92:1A:72:
        A6:84:A7:58:FE:52:7D:89:2D:DD:9B:DD:DF:BF:83:CE:EE:29:42:AC:
        80:C0:AE:A4:4E:CD:22:3B:80:DA:2A:47:1C:CD:FC:5E:52:0B:C2:85:
        46:96:5D:FA:50:BC:DC:B3:9C:26:F2:E4:D2:26:EF:1D:EE:D4:18:75:
        D5:78:16:30:FF:A2:FE:0D:4D:41:DA:8D:C4:03:DD:17:7C:78:1C:73:
        50:25:4D:78:26:41:FA:0C:83:E9:B0:57:F0:9E:D4:6C:D6:AB:C6:CE:
        4A:44:B1:97:58:3C:AB:24:13:76:7F:3D:D1:35:63:1F:C7:0C:AA:1D:
        74:EC:BD:06:C9:97:56:A6:A7:A1:F5:84:CB:92:D6:E9:F4:DB:47:0C:
        BB:57:B6:A6:83:8C:EA:56:FF:F8:52:1A:71:A2:E1:37:68:84:C1:A2:
        93:D0:92:4F:DD:C2:2B:11:9C:64:4C:B8:AA:A4:06:C9:48:D4:C9:6A:
        2A:B5:31:D4:06:23:0E:08:00:B9:F6:B7:CC:56:6E:5F:CB:61:66:74:
        D0:D8:90:18:28:EE:C4:D1:9C:57:FF:0E:3A:F1:6F:17:85:A8:BB:44:
        F8:3E:93:88:EC:7C:B7:54:34:57:F7:17:57:C8:21:24:60:1E:31:EC:
        DC:FB:23:40:E8:4F:C5:1D:A4:4A:F8:59:EC:3F:47:35:AE:0D:07:93:
        25:A4:59:41:94:EB:B7:13:BD:EE:A6:E7:85:9A:3C:4B:2C:A9:FC:02:
        5A:D9:A5:F6:88:93:07:7C:87:00:94:9D:9C:6D:72:82:F1:DF:D5:3F:
        8E:72:D4:58:51:2D:60:2B:ED:A6:C0:87
parm:           max_targets:int
```

To view detailed status information for the driver rpm, use the `htdrv status` command.

```
# htdrv status
-----------------------------------------------------------------
HyTrust online encryption driver status
-----------------------------------------------------------------
```

```
Name        : htcrypt
Version     : 10.20001189
Release     : 1020001189
Architecture: noarch
Install Date: Tue 09 Apr 2024 02:00:33 PM CDT
Group       : System/Kernel
Size        : 105123
License     : GPLv2
Signature   : DSA/SHA1, Tue 19 Dec 2023 10:08:42 AM CST, Key ID 4a1ed78762b480bf
Source RPM  : htcrypt-10.20001189-1020001189.src.rpm
Build Date  : Tue 19 Dec 2023 10:06:36 AM CST
Build Host  : htcrypt-rhel8.dc.hytrust.com
Packager    : ENTRUST <htdc-devel@hytrust.com>
Summary     : htcrypt 10.20001189 dkms package
Description :
Kernel modules for htcrypt 10.20001189 in a DKMS wrapper.

>>> htcrypt driver is installed on this VM

------------------------------------------------------------------
UEFI Secure boot status
------------------------------------------------------------------
This system is setup with UEFI boot
Secure boot option is only supported with UEFI boot
SecureBoot enabled

HyTrust signing key is enrolled in Machine owner key (MOK) list

------------------------------------------------------------------
Linux kernel and related packages installed on this system
------------------------------------------------------------------
Installed Packages
kernel.x86_64             5.14.0-362.8.1.el9_3  @anaconda
kernel.x86_64             5.14.0-362.24.1.el9_3 @rhel-9-for-x86_64-baseos-rpms
kernel-core.x86_64        5.14.0-362.8.1.el9_3  @anaconda
kernel-core.x86_64        5.14.0-362.24.1.el9_3 @rhel-9-for-x86_64-baseos-rpms
kernel-devel.x86_64       5.14.0-362.8.1.el9_3  @rhel-9-for-x86_64-appstream-rpms
kernel-devel.x86_64       5.14.0-362.24.1.el9_3 @rhel-9-for-x86_64-appstream-rpms
kernel-headers.x86_64     5.14.0-362.24.1.el9_3 @rhel-9-for-x86_64-appstream-rpms
kernel-modules.x86_64     5.14.0-362.8.1.el9_3  @anaconda
kernel-modules.x86_64     5.14.0-362.24.1.el9_3 @rhel-9-for-x86_64-baseos-rpms
kernel-modules-core.x86_64 5.14.0-362.8.1.el9_3  @anaconda
kernel-modules-core.x86_64 5.14.0-362.24.1.el9_3 @rhel-9-for-x86_64-baseos-rpms
kernel-tools.x86_64       5.14.0-362.8.1.el9_3  @anaconda
kernel-tools-libs.x86_64  5.14.0-362.8.1.el9_3  @anaconda
```

Enabling Linux Online Encryption with the CSP Vault for VM Encryption webGUI

To enable Online Encryption for Linux disks, you need to install the HTCrypt Driver on the VM hosting those disks. During this process, the VM may need to be rebooted if the Linux kernel on the VM needs to be updated in order to install the required packages. The webGUI allows you to specify whether you want this reboot to happen automatically if it is required.

You only need to perform this procedure once for each Linux VM. After the HTCrypt Driver has been installed, the Policy Agent will automatically use it every time it encrypts, decrypts, or rekeys a disk on that VM.

> Note: You cannot use Online Encryption if there is an Access Control Policy associated with the VM. If you enable the HTCrypt Driver and apply an Access Control Policy to the disk, online encryption will fail.

The following procedure describes how to install the HTCrypt Driver for the first time using the webGUI. You can also install the driver using the CLI as described in Enabling Linux Online Encryption with the CLI. If your Linux kernel version has changed, see Updating the HTCrypt Kernel Dependencies.

Before You Begin

Make sure the VM meets the requirements described in Linux Encryption Prerequisites and Linux Online Encryption Prerequisites and Considerations.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Navigate to the **VMs** tab, select the VM on which you want to install the HTCrypt Driver, then click the **Expand** button (**>**) at the end of the row to view the VM details.
4. In the Details tab, click **Install Now** in the **HTCrypt State** field.
5. If you want Cryptographic Security Platform Vault for VM Encryption to reboot the VM automatically to complete the driver installation, check the **Reboot VM** check box in the confirmation dialog box.
   If you do not check the **Reboot VM** check box, the driver will be installed on the VM but it will not be active on any disk that is currently attached. After the installation finishes, you need to either reboot the VM manually or detach and then reattach any currently attached disks so that the Policy Agent can use the HTCrypt Driver for online encryption on those disks.
6. Click **Install Driver**.
   The HTCrypt State field shows that the HTCrypt Driver is scheduled for installation. When the installation is finished, Cryptographic Security Platform Vault raises an alert and changes the HTCrypt State to "Installed".
   Note: The installation could take a few minutes to complete depending on how long it takes to install the dependencies. When the installation is finished, the HTCrypt State field will display "Installed" and the HTCrypt Version field will display the correct driver version number. You can monitor the progress of the installation task on the Dashboard in the Tasks tile.
7. If the **HTCrypt Version** field indicates that the VM needs to be rebooted, either reboot the VM or detach and reattach all currently attached disks to finish the installation process.

What to Do Next

If your system is setup with UEFI boot, see Configuring UEFI Secure Boot in RHEL or Oracle Linux.

Enabling Linux Online Encryption with the CLI

To enable Online Encryption for Linux disks, you need to install the HTCrypt Driver on the VM hosting those disks. During this process, the VM may need to be rebooted if the Linux kernel on the VM needs to be updated in order to install the required packages.

You only need to perform this procedure once for each Linux VM. After the HTCrypt Driver has been installed, the Policy Agent will automatically use it every time it encrypts, decrypts, or rekeys a disk on that VM.

> Note: You cannot use Online Encryption if there is an Access Control Policy associated with the VM. If you enable the HTCrypt Driver and apply an Access Control Policy to the disk, online encryption will fail.

The following procedure describes how to install the HTCrypt Driver for the first time using the CLI. You can also install the driver using the Cryptographic Security Platform Vault for VM Encryption webGUI as

described in Enabling Linux Online Encryption with the Cryptographic Security Platform Vault for VM Encryption webGUI. If your Linux kernel version has changed, see Updating the HTCrypt Kernel Dependencies.

Before You Begin

Make sure the VM meets the requirements described in Linux Encryption Prerequisites and Linux Online Encryption Prerequisites and Considerations.

Procedure

1. Log into the VM as `root`.
2. If you want to verify that the HTCrypt Driver is not already installed, use the `hcl status` command. For example:
   ```
   # hcl status

   Summary
   --------------------------------------------------------------------------------
   KeyControl: 10.238.66.235:443
   KeyControl list: 10.238.66.235:443
   Status: Connected
   Last heartbeat: Wed Mar 21 12:48:19 2018 (successful)
   AES_NI: enabled
   Certificate Expiration: Sep 11 22:16:13 2020 GMT
   HTCRYPT: Not Installed
   ```
   If the HTCRYPT status is **enabled**, the HTCrypt Driver has already been installed on this VM.
3. To make sure the proper dependencies are installed, enter the `htdrv prepare` command. For example:
   ```
   # htdrv prepare
   Preparing system for HyTrust encryption driver installation
   Loaded plugins: fastestmirror, langpacks
   Loading mirror speeds from cached hostfile
    * base: mirrors.sonic.net
    * epel: mirror.beyondhosting.net
   ...
   DKMS: install completed.
   ```
   The script goes through the dependency list, installing or updating the required packages as needed. If it cannot install the required packages for the current kernel, it updates the kernel and prompts you to reboot the VM. Rebooting is not necessary unless you are prompted to do so by the script.
4. If prompted, reboot the VM and then enter the `htdrv prepare` command again to install the required packages on the updated kernel.
   Note: If the Linux kernel version changes on this VM after you install the HTCrypt Driver, you need to update the kernel-devel and kernel-headers dependencies to match the new version. For details, see Updating the HTCrypt Kernel Dependencies.
5. Install the HTCrypt Driver for your OS.
   - For RHEL, install the HTCrypt Driver RPM by entering the command `rpm -ivh /opt/hcs/drivers/htcrypt-10.5.3-*buildnum*.noarch.rpm`, where `buildnum` is the build number that you are installing. For example:
     ```
     # rpm -ivh htcrypt-10.5.3-12345M.noarch.rpm
     Preparing...                ########################################### [100%]
     Updating / installing...
       1:htcrypt-10.5.3-12345M   ########################################### [100%]
     Loading new htcrypt-10.5.3 DKMS files...
     ```

```
Building for 3.10.0-693.17.1.el7.x86_64
Building initial module for 3.10.0-693.17.1.el7.x86_64
Done.

htcrypt:
Running module version sanity check.
 - Original module
   - No original module exists within this kernel
 - Installation
   - Installing to /lib/modules/3.10.0-693.17.1.el7.x86_64/extra/

depmod....

Backing up initramfs-3.10.0-693.17.1.el7.x86_64.img to /boot/
initramfs-3.10.0-693.17.1.el7.x86_64.img.old-dkms
Making new initramfs-3.10.0-693.17.1.el7.x86_64.img
(If next boot fails, revert to initramfs-3.10.0-693.17.1.el7.x86_64.img.old-dkms image)
dracut.....

DKMS: install completed.
```

Important: Installation might fail on FIPS-enabled Red Hat Linux 8 and above with the following message:

```
in rpm installation package htcrypt-10.5.3-12345M.noarch does not verify: no digest
```

Use the following command as a workaround:

```
rpm -ivh --nodigest --nofiledigest htcrypt-10.5.3-12345M.noarch.rpm
```

- For Ubuntu, install the HTCrypt Driver DEB by entering the command dpkg -i /opt/hcs/drivers/htcrypt-dkms_<buildver>_all.deb, where buildver is the build version that you are installing. For example:

```
#dpkg -i /opt/hcs/drivers/htcrypt-dkms_5.40012345_all.deb
Selecting previously unselected package htcrypt-dkms.
(Reading database ... 169211 files and directories currently installed.)
Preparing to unpack .../htcrypt-dkms_5.40000655_all.deb ...
Unpacking htcrypt-dkms (5.40012345) ...
Setting up htcrypt-dkms (5.40012345) ...
Loading new htcrypt-5.40012345 DKMS files...
Building for 5.4.0-64-generic
Building for architecture x86_64
Building initial module for 5.4.0-42-generic
Done.

htcrypt.ko:
Running module version sanity check.
 - Original module
   - No original module exists within this kernel
 - Installation
   - Installing to /lib/modules/5.4.0-42-generic/updates/dkms/

depmod.....

Backing up initrd.img-5.4.0-42-generic to /boot/initrd.img-5.4.0-42-generic.old-dkms
Making new initrd.img-5.4.0-42-generic
```

```
(If next boot fails, revert to initrd.img-5.4.0-42-generic.old-dkms image)
update-initramfs.....

DKMS: install completed.
Building initial module for 5.8.0-38-generic
Done.

htcrypt.ko:
Running module version sanity check.
 - Original module
   - No original module exists within this kernel
 - Installation
   - Installing to /lib/modules/5.8.0-38-generic/updates/dkms/

depmod.....

Backing up initrd.img-5.8.0-38-generic to /boot/initrd.img-5.8.0-38-generic.old-dkms
Making new initrd.img-5.8.0-38-generic
(If next boot fails, revert to initrd.img-5.8.0-38-generic.old-dkms image)
update-initramfs.....

DKMS: install completed.
```

6. To verify that the installation succeeded, enter the `hcl status` command. For example:

```
# hcl status

Summary
--------------------------------------------------------------------------------
KeyControl: 10.238.66.235:443
KeyControl list: 10.238.66.235:443
Status: Connected
Last heartbeat: Wed Mar 21 12:48:19 2019 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT
HTCRYPT: enabled
```

   At this point, the HTCrypt Driver is installed but is not yet running on any disks that are currently attached.
7. If the root or swap disk is encrypted on this VM, you need to reboot the VM to complete the installation process.
   If only data disks are encrypted on the VM, you can either reboot the VM or detach and then reattach all attached data disks to start the HTCrypt Driver on those disks. To detach and reattach the disks, use the `hcl detach -a` and `hcl attach -a` commands. For example:

```
# hcl detach -a
Encrypted device sdi7 detached; encrypted contents no longer visible
Encrypted device sdi1 detached; encrypted contents no longer visible
# hcl attach -a
Encrypted device sdi7 (/dev/sdi7) attached; encrypted contents visible at /dev/mapper/clear_sdi7
Encrypted device sdi1 (/dev/sdi1) attached; encrypted contents visible at /dev/mapper/clear_sdi1
```

8. If the VM has its root devices encrypted before the installation of the online encryption driver, then in order to extend the online encryption driver support to the root devices, the admin should run the following commands:

```
                # htroot update
# reboot
```

What to Do Next

If your system is setup with UEFI boot, see Configuring UEFI Secure Boot in RHEL or Oracle Linux.

Linux Online Encryption Prerequisites and Considerations

By default, when you encrypt, rekey, or decrypt a Linux block device, the filesystem on that block device must be unmounted during the entire procedure and the data is inaccessible until the procedure is finished. With Online Encryption:

- During the initial encryption phase, the filesystem only needs to be unmounted briefly when the Entrust Policy Agent changes the device to attach the clear text version it creates during the encryption process. After the device has been reattached on the clear text version, the encryption process continues while the disk remains online and the data remains accessible.
- During any subsequent rekeys, the device remains online and the data remains accessible during the entire rekey process.
- During the decryption process, the data is decrypted dynamically and the device remains online and the data remains accessible during the decryption process. If you are decrypting a Linux system device (such as `/root`, `swap`, or `/home`), the device remains accessible after the decryption procedure is complete. If you are decrypting a Linux data drive, however, the data drive is automatically *unmounted* after the decryption is complete.
  Note: The only exception to this is if a VM reboots while a Linux system device is being decrypted. In this case, when the VM finishes rebooting, the decryption process resumes in offline mode and the system device and its data will be inaccessible until decryption is complete. If the VM remains online during the entire decryption process, the data will be available the entire time.

Prerequisites

In order to enable Online Encryption, you need to install the HTCrypt Driver on each Linux VM whose disks you want to encrypt.

The HTCrypt Driver is a Dynamic Kernel Module Support (DKMS)-based package that requires the following:

- The VM must be running RHEL 8 or later, or Ubuntu 20.04-20.04.5 or 22.04.
- If the OS is RHEL, the linux Kernel version must be 3.10.0-123 or later.
- If the OS is Ubuntu, the linux kernel must be 5.4 or later.
- The following Linux packages must be installed:
  - `dkms` version 1.95 or later.
  - `gcc`
  - `kernel-headers` (RHEL)
  - `kernel-devel` (RHEL)
  - `linux-headers<kernel-version>` (Ubuntu)

  Important: The version of the Linux kernel must be the same as the version of the `kernel-headers` and `kernel-devel` packages. If you update the Linux kernel, you must also update the version of these packages. For details, see Updating the HTCrypt Kernel Dependencies.
  The Entrust Policy Agent includes a script that makes sure the required packages are installed and that they are all using the same version. You can run this script manually if you want to enable online encryption through the CLI, or you can let the Policy Agent take care of installing the required packages by enabling online encryption through the Cryptographic Security Platform Vault webGUI. For details, see Enabling Linux Online Encryption with the CLI or Enabling Linux Online Encryption with the CSP Vault for VM Encryption webGUI.

Considerations

- When you install the HTCrypt Driver for the first time on a VM, you will need to detach and then reattach all currently-attached block devices. If the root drive is already encrypted on the VM, the VM will need to be rebooted before Online Encryption is fully enabled for the VM.
- When you enter the `hcl encrypt`, `hcl rekey`, or `hcl decrypt` commands, the commands will return immediately and the encryption or decryption process will start running in the background. You can use the `hcl status` command to monitor the progress of these commands.
- Online Encryption does not support encrypting, rekeying, or decrypting only the allocated blocks on the VM. Therefore you cannot use the `-s` option with the `hcl encrypt`, `hcl rekey`, or `hcl decrypt` commands when Online Encryption is enabled.
- You cannot use Online Encryption if there is an Access Control Policy associated with the VM. If you enable the HTCrypt Driver and apply an Access Control Policy to the disk, online encryption will fail.
- If you are using Online Encryption on a VM and you want to encrypt a Linux system device (such as `/root`, `swap`, or `/home`), keep in mind that:
    - The VM will need to be rebooted before the Policy Agent can begin the encryption process. There will be no delay in the reboot process however. The VM will come back up and be available to users again before the Policy Agent starts encrypting it. After that intial reboot, the VM will remain available throughout the encryption process.
    - If you decrypt the system device, the VM will remain accessible to users during the entire process as long as the VM does not reboot. If the VM reboots, the VM will remain offline until the Policy Agent finishes decrypting the system device. Once the system device has been decrypted, you will need to reboot the VM before you perform any other administration functions, such as upgrading the kernel or re-encrypting the system device.
- After Online Encryption has been enabled, you can rekey all devices on the VM as a background process with no disruption to data disk access and minimal disruption to system device access.

Linux Encryption Prerequisites

The following prerequisites apply to all types of Linux encryption, including data drive encryption and root, swap, or system device encryption in online or offline mode. To enable Online Encryption for the VM, see Linux Online Encryption Prerequisites and Considerations for additional prerequisites.

- Make sure the Linux version you are using is supported.
- **Important:** Make sure that the /boot partition has at least 1GB of free space before starting root drive encryption.
- If you intend to use this VM with a BoundaryControl-enabled Cloud VM Set, you must install a VMware-supported version of VMware Tools on the VM. For all other VMs, installing VMware Tools is recommended but not required. In all cases, we recommend keeping VMware Tools up to date.
- If an entry for the Linux device you intend to encrypt already exists in the Filesystem Table (`/etc/fstab`), remove that entry until the encryption process is complete and the Entrust-created clear text path to the device is available. If you reboot the device after encryption with the `/etc/fstab` entry still pointing to the original device path, the system may hang because the encrypted version of the device will fail the filesystem check. For details, see Automatically Mounting Linux Filesystems.
- We recommend partitioning the disk before encrypting it. When Cryptographic Security Platform Vault for VM Encryption encrypts a disk, it writes a private region at the start of the disk that contains information that allows it to identify which keys are associated with which partition.
  For example, let's say you have 2 non-partitioned disks, `/dev/sdb` and `/dev/sdc`, where `/dev/sdc` is encrypted by Cryptographic Security Platform Vault for VM Encryption. If you remove `/dev/sdb` and reboot the VM, `/dev/sdc` will be renamed `/dev/sdb` and the association between the keys and the disk will become invalid. At that point, you will lose access to the encrypted data.

Now let's say you have the same setup as before, but you partition the disk `/dev/sdc` and then you encrypt the `/dev/sdc1` partition. Cryptographic Security Platform Vault for VM Encryption adds a UUID (Universally Unique Identifier) in the private area at the start of the `/dev/sdc` disk that associates the `/dev/sdc1` partition with its encryption keys. When you remove `/dev/sdb` and reboot the VM, the encrypted partition `/dev/sdc1` will be renamed `/dev/sdb1`, but the UUID does not change. In this case, Cryptographic Security Platform Vault for VM Encryption can use the UUID to match the encryption keys to the partition and the data remains accessible even after the partition name has changed.
Important: If you want to resize a partition after encrypting it with Cryptographic Security Platform Vault for VM Encryption, you must take additional steps. For more information, see Disk Size Management in Linux.

- Make sure the Linux VM has access to the following Linux packages and their dependencies:

Encryption type	Required packages	Note
All Linux encryption (data drives and system devices)	device-mapper OpenSSL Python 2.7 or Python 3	

Encryption type	Required packages	Note
Linux root, swap, or system device encryption	busybox cryptsetup or cryptsetup-luks dracut (RHEL) or initramfs-tools (Ubuntu) dracut-network dropbear EPEL-release hashalot OpenSUSE	If the server to be encrypted has external internet access, it will install any missing packages when you encrypt the root, swap, or system device. If the server is not connected to the internet, these packages must be fully installed before root/swap encryption begins, or the encryption request will fail.

Encryption type	Required packages	Note
Linux online encryption (data drives and system devices)	dkms gcc kernel-devel (RHEL) kernel-headers (RHEL) linux-headers-<kernel-version> (Ubuntu)	

- Cryptographic Security Platform Vault for VM Encryption supports disk encryption for disks formatted with btrfs. If the root file system or system mount (for example, /var, /usr, /etc) is btrfs and you have multiple storage disks, only the first disk can be encrypted. The first disk will have an entry in /etc/fstab.

  > ⚠ We recommend creating btrfs on an MBR or GPT partition, not on a RAW device. RAW devices are vulnerable to device name changes, which will render the encrypted device unusable.

- For a given client, you can have either online or offline encryption. You cannot mix them on the same client.

Data Encryption Overview

This chapter describes support for encryption within individual Virtual Machines (VMs) wherever they reside (data center, private, public, or hybrid clouds). For virtual machines, Entrust's encryption works independently of the type of hypervisor platform (Type 1, Type 2, etc.) as well as the hypervisor vendor (VMware, Microsoft, Citrix, Red Hat, etc.) and Cloud environment (Amazon AWS, ENKI, Microsoft Azure, etc.) or cloud frameworks such as OpenStack. Throughout the chapter, we will refer to the virtualized case and reference the agent being managed by Cryptographic Security Platform Vault as a "VM."

Once the VM has been registered, you can manage it through the Cryptographic Security Platform Vault webGUI or the `hicli`.

In order to encrypt a VM, complete the following tasks:

Step	Task	Description
1	Install Cryptographic Security Platform Vault and configure the Cryptographic Security Platform Vault cluster.	
2	If desired, create one or more custom Cloud Admin Groups in addition to the default Cloud Admin Group.	See Creating a Custom Cloud Admin Group. This step requires a Cryptographic Security Platform Vault account with Security Admin privileges.
3	Create one or more users with Cloud Admin privileges and assign them to the appropriate Cloud Admin groups.	
4	Create one or more Cloud VM Sets.	See Creating a Cloud VM Set for the CSP Vault for VM Encryption. This step requires an account with Cloud Admin privileges.
5	Install the Entrust Policy Agent on the VM you want to encrypt and register it with the Cryptographic Security Platform Vault.	For details, see the installation and administration guide at https://api.managed.entrust.com/vault/latest
6	Encrypt the data on the VM.	See one of the following: • Linux Encryption Overview. • Windows Encryption Prerequisites. • Linux Root, Swap, and System Device Encryption. • Windows Boot Drive Encryption.

Note:

- An encryption can be interrupted, but cannot be canceled or reversed. To reverse an encryption is to allow the encryption to complete, then to start a decryption.
- If an encryption, decryption, or rekey operation is interrupted, the following table describes the expected behavior.

Operating System	Mode	Disk Type	Behavior on Interrupted Operation
Linux	Offline	Root Drive	Automatically picks up from where it was interrupted.
Linux	Offline	Data Drive	You must reissue the command that was interrupted to resume the operation.

Operating System	Mode	Disk Type	Behavior on Interrupted Operation
Linux	Online	Root Drive	Automatically picks up from where it was interrupted.
Linux	Online	Data Drive	Automatically picks up from where it was interrupted.
Windows	Online	Boot Drive	Automatically picks up from where it was interrupted
Windows	Online	Data Drive	Automatically picks up from where it was interrupted

VM and Disk Management

- Decommissioning and Destroying a VM
- Removing a Disk from the CSP Vault for VM Encryption
- Removing a VM from the CSP Vault for VM Encryption
- Reactivating a Revoked Disk
- Revoking Access to a Disk
- Revoking VM Permissions
- Disk Size Management in Windows
- Disk Size Management in Linux
- Changing the Drive Letter for a Windows Disk
- Moving a VM to a Cloud VM Set
- Moving Disks Between VMs
- Viewing the Details for a Disk
- Using the Dashboard
- Backups, Clones, and Snapshots
- Re-Authenticating a Windows VM with the Entrust Policy Agent GUI
- Re-Authenticating a VM with an Encrypted Root Device or Boot Disk
- Re-Authenticating a Standard VM
- Access Control Policies
- VM Certificates
- Changing the Properties for a Specific VM
- Viewing the VM Status with the CLI
- Exporting VM Details
- Viewing the Details for a VM
- High Availability Between a VM and the CSP Vault Cluster
- Cloud VM Sets
- Effects of Encryption on Thin-Provisioned Disks

Decommissioning and Destroying a VM

The following procedure describes how to remove a VM from the Cryptographic Security Platform Vault for VM Encryption when you intend to destroy the VM without accessing any of the encrypted data. After you

remove the VM from the Cryptographic Security Platform Vault for VM Encryption, the VM no longer appears in the Cryptographic Security Platform Vault for VM Encryption webGUI and no longer counts against the Cloud VM Limit defined in your license.

If you want to remove the VM from the Cryptographic Security Platform Vault for VM Encryptionbut retain the data on the VM, see Removing a VM from the CSP Vault for VM Encryption.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab, then select the VM that you want to decommission.
4. Click **Actions > Revoke Authentication**.
5. Confirm the action at the prompt.
   The Cryptographic Security Platform Vault for VM Encryption revokes access to the VM and automatically displays the **Unauthenticated VMs** tab.
   Note: At this point, all of the encryption keys are still stored in the Cryptographic Security Platform Vault for VM Encryption, and you can restore the VM by selecting it and clicking **Actions > Rescue Authentication**. If you continue with this procedure, all access to any encrypted data on the VM will be lost when the VM is removed from the Cryptographic Security Platform Vault for VM Encryption.
6. Select the VM and click **Actions > Remove**.
   The Cryptographic Security Platform Vault for VM Encryption removes the VM from its inventory, returns the associated Cryptographic Security Platform Vault for VM Encryption license to the license pool, and destroys all encryption keys associated with that VM.
7. Use your hypervisor to delete the VM.

Removing a Disk from the CSP Vault for VM Encryption

The following procedure explains how to remove a disk from the Cryptographic Security Platform Vault for VM Encryption when you don't care about its contents. If you want to save the contents, you need to decrypt the disk before you remove it from the Cryptographic Security Platform Vault for VM Encryption. For details, see Decrypting a Disk Using the webGUI, Decrypting a Disk Using the Windows Policy Agent GUI, or Decrypting a Disk Using the CLI.

Important: This operation is destructive. You will lose all encrypted data that is stored on the disk.

Removing a Disk using the Policy Agent GUI

1. Log into the Windows system using an account with Administrator privileges.
2. Select **Start > All Programs > Entrust > Entrust DataControl** or start Windows PowerShell and enter the `hclGUI` command.
3. Right-click on the disk that you want to remove and select **Remove**.
4. Click **Yes** on the confirmation screen.

When the removal has finished, you will see a pop-up window stating that the disk has been removed. Click the Refresh button at the top to refresh the window.

Removing a Disk using the CLI

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. Unmount the disk you want to remove.
3. Enter the command `hcl rm [-y] <diskname | -a>`, where:
   - `-y` makes the command non-interactive.
   - *diskname* | `-a` is the name of the disk that you want to remove or `-a` to remove all disks on the VM that are registered with the Cryptographic Security Platform Vault for VM Encryption. For Linux, use

the short form of the disk name (for example, `sdb1` instead of `/dev/sdb1`). For Windows, specify the drive letter or folder mount associated with the disk.

The Cryptographic Security Platform Vault for VM Encryption issues an implicit `hcl detach` command and unregisters the disk(s) with the Cryptographic Security Platform Vault for VM Encryption. Any keys associated with the disk(s) are deleted and any encrypted data is now inaccessible.
For example:

```
# hcl rm sdd1
WARNING: Removal of devices will cause any data stored on them to be permanently lost.
Do you want to proceed? (y/n) y

Removed device sdd1
```

Removing a VM from the CSP Vault for VM Encryption

The following procedure describes how to decrypt the data on a VM and then remove it from the Cryptographic Security Platform Vault for VM Encryption so that it no longer appears in the Cryptographic Security Platform Vault inventory and it no longer counts against the Cloud VM Limit defined in your Cryptographic Security Platform Vault license. The data on the VM remains, however, and you can re-authorize the VM with Cryptographic Security Platform Vault at any time.

If you want to decommission a VM and destroy it immediately without ever accessing the data, see Decommissioning and Destroying a VM.

Before You Begin

You cannot decrypt a disk if it has an Access Control Policy associated with it. Make sure that no such policy association exists before you decrypt the disk. For details, see Viewing the Access Control Status for a Disk.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab and select the VM you want to work with from the list.
4. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
5. On the **Details** tab for the VM, make sure that:
   - The **Auto Encryption** property is either **Disabled** or the Automatic Data Encryption Policy does *not* include the disk you want to decrypt. If the Auto Encryption Policy Type is set to exclude, then the disks included as per policy can *not* be decrypted.
   - The **Decryption Allowed** property is set to **Yes**. If this field is set to **No**, click **No**, select **Yes** from the drop-down list, then click **Save**.

   Tip: If you want to decrypt the disks on multiple VMs in this Cloud VM Set, you can change these properties at the Cloud VM Set level and propagate the changes to all VMs in the Cloud VM Set. For more information, see Changing Cloud VM Set Properties.
6. Click the **Encrypted Disks** tab.
7. Select the encrypted disk. If more than one disk is encrypted:
   a. In the top right-hand corner, click **Multi-Select**.
   b. Click on the first encrypted disk.
   c. Shift+Click on the last encrypted disk.
8. Select **Actions > Decrypt Disk** from the VM-specific **Actions** menu.
   The Cryptographic Security Platform Vault for VM Encryption webGUI displays a message that the decrypt requests were successfully created and adds a **Decrypt Disk** task for the VM that will begin on the VM's next heartbeat. The length of time the operation will take depends on the amount of data present on the disk and the encryption settings configured for this system.

You can track the progress of the decrypt task on the Dashboard in the **Tasks** tile.
When the decrypt request begins processing, the Cryptographic Security Platform Vault for VM Encryption sets the state to **Active/Decrypt**. When the encryption process has finished, the Cryptographic Security Platform Vault for VM Encryption moves the disk back to the **Unencrypted Disks** tab and changes the state to **Available**.

9. Periodically check the **Encrypted Disks** tab for the VM until that tab shows that no encrypted disks remain in the VM. Do not proceed with this procedure until decryption is complete for all disks.
10. Select the VM you want to remove and click **Actions > Revoke Authentication** from the main **Actions** menu.
11. Confirm the action at the prompt.
    The Cryptographic Security Platform Vault for VM Encryption revokes access to the VM and automatically displays the **Unauthenticated VMs** tab.
12. Select the VM and click **Actions > Remove**.
    The Cryptographic Security Platform Vault for VM Encryption removes the VM from its inventory, returns the associated Cryptographic Security Platform Vault license to the license pool, and destroys all encryption keys associated with that VM.
13. Log into the VM as an administrator and uninstall the Entrust Policy Agent. For details, see Uninstalling the Policy Agent on Linux or Uninstalling the Policy Agent on Windows.

Reactivating a Revoked Disk

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab and select the VM you want to work with from the list.
4. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
5. Click the **Encrypted Disks** tab and select the disk that you want to reactivate.
6. Select **Grant Disk Access** from the VM-specific **Actions** menu. Cryptographic Security Platform Vault changes the disk state to **Active/Detached** until the action completes, at which time it changes the state to **Active/Attached**.
7. If this is a Linux disk, you need to manually remount the filesystem unless `auto_mount` is set to True. To verify which disks are currently accessible, use the `hcl status` command.

Revoking Access to a Disk

If you revoke access to a disk, it will be deactivated and detached on the next heartbeat. Any attempt to attach the disk using `hcl attach` will fail with the message stating that the key could not be fetched because the disk is not active.

If this is a Windows boot disk, the VM will be unable to boot. If this is a standard Windows disk, the associated drive will no longer be available through Windows Explorer or to any applications running on the Windows server. If this is a Linux disk, the filesystem will be unmounted and it will likewise be unavailable to any applications running on the server.

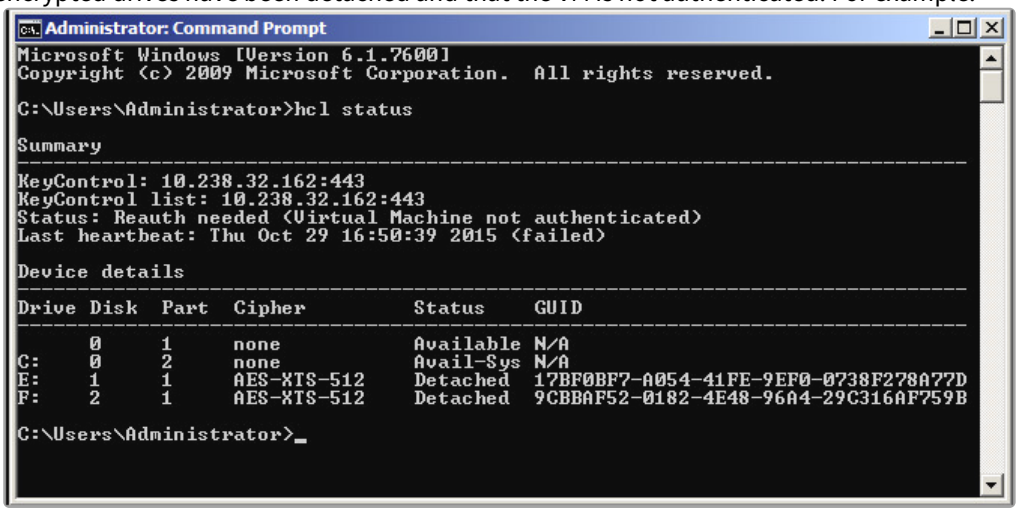
1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab and select the VM you want to work with from the list.
4. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
5. Click the **Encrypted Disks** tab and select the disk that you want to revoke.
6. Select **Revoke Disk Access** from the VM-specific **Actions** menu.
7. Click **Proceed** at the prompt to confirm the revoke request. Cryptographic Security Platform Vault changes the disk state to **Revoked/Attached** until the action completes, at which time it changes the state to **Detached**.

Revoking VM Permissions

f you revoke the permissions for an entire VM, all encrypted data on all the disks contained in the VM will become inaccessible until the VM is re-authenticated.

If you want to revoke individual disks within a VM, see Revoking Access to a Disk.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab.
4. Select the VM you want to revoke in the table.
5. Select **Actions > Revoke Authentication**.
6. Click **Proceed** at the prompt to confirm the revoke request. Cryptographic Security Platform Vault moves the VM to the **Unauthenticated VMs** tab and all future access requests will be denied until the VM is re-authorized. The operation is completed at the VM's next heartbeat.
   After the VM heartbeat, if you enter the `hcl status` command on the server, the result shows that the encrypted drives have been detached and that the VM is not authenticated. For example:



   To re-authenticate the VM, see Re-Authenticating a Standard VM.

Disk Size Management in Windows

How you increase the size of a Windows disk depends on whether the type of disk and whether or not the disk is encrypted.

- If the Windows disk has *not* been encrypted, you can extend or shrink that disk as desired using your hypervisor tools.
  - If the unencrypted disk is a Windows data disk or a GPT boot disk, you do not need to do anything in Cryptographic Security Platform Vault after you resize the disk, even if the Bootloader is already installed. Cryptographic Security Platform Vault will pick up the new disk size automatically.
  - If the unencrypted disk is an MBR boot disk with the Entrust Bootloader already installed, you need to move the boot partition as described in Resizing an Encrypted Windows Data Disk or GPT Boot Disk.
- If the disk is an encrypted Windows data disk or an encrypted GPT boot disk, you can extend or shrink that disk as desired using your hypervisor tools. After you resize the disk in your hypervisor, you need to update the size in Cryptographic Security Platform Vault using the `hcl extend` command. For details, see Resizing an Encrypted Windows Data Disk or GPT Boot Disk.

- If the disk is an encrypted Windows MBR boot disk, you must resize it as described in Extending an MBR Boot Partition After Installing the Bootloader.

Important:

- After you run the hcl extend operation to resize the drive, the new size may not be reflected in the Cryptographic Security Platform Vault for VM Encryption webGUI. If this happens, please execute the following commands:
  a. `hcl status`
  b. `hcl update_size_kc <disk #> <partition #>`
     where the disk # and partition # are for the drive in question, as reflected when you issue the hcl status command.
  c. `hcl heartbeat -u`

  Once the command execution is successful, the size should be displayed properly in the Cryptographic Security Platform Vault for VM Encryption webGUI.
- If the disk being extended is part of a **Microsoft Failover Cluster**, you must enable maintenance mode on the disk, extend the disk, and then disable maintenance mode on that disk.

Resizing an Encrypted Windows Data Disk or GPT Boot Disk

This is an online procedure, which means that the disk and its contents will remain available during the resize. However, you cannot resize a disk that is detached or that is in the process of being rekeyed.

Important: If you are using mount points instead of drive letters, you must use the Disk Management 'Change Drive letter and paths' option to temporarily assign a drive letter before you can change the size of the disk. After resizing, you can safely remove the drive letter.

Warning: If you resize the disk with Windows Disk Manager, you may be prompted to convert from a basic disk into a dynamic disk. Windows dynamic disks are *not* supported. If you select this option, you will not be able to access this disk through Cryptographic Security Platform Vault and all existing data will be lost.

1. Resize the underlying disk using your hypervisor tools.
2. Log into the VM as a System Administrator and open a Command Prompt or start Windows PowerShell.
3. Enter the command `hcl extend diskname`, where `diskname` is the drive letter or folder mount you want to resize. For example:
   C:\>hcl extend f:
   extending partition for f:
   extending filesystem for f:the new filesystem is 2146369536 bytes long

   Tip: If the `hcl extend` command fails with the message that there are too many partitions on the disk, see Detecting and Removing a Windows Snapshot Partition.

Extending an MBR Boot Partition After Installing the Boot loader

The Bootloader installation creates a new MBR partition labeled `HTBOOTLDR` immediately following the boot partition on the disk. If you want to extend the MBR boot partition at any time after you have installed the Bootloader, you need to make sure the unallocated space you want to use is immediately adjacent to the boot partition by extending the disk and then using the Entrust-provided PowerShell script that moves the `HTBOOTLDR` partition to the end of the disk and then extends the boot partition into the unallocated space. (For details about the Entrust Bootloader, see Windows Boot Drive Encryption.)

Important: The VM will need to be rebooted twice during this procedure.

1. Extend the MBR disk containing the boot partition using your hypervisor tools.
2. Log into PowerShell on the Windows VM.
3. Locate the main Policy Agent installation directory. The PowerShell scripts are located in the `bin` folder under this main directory. The default directory is `C:\Program Files\hcs`.

4. Run the PowerShell script `MoveHTBootloader.ps1` by entering the command `powershell -File "C:\entrust-install-dir\MoveHTBootloader.ps1"`.
   The script creates a new Bootloader partition at the end of the recently extended disk and reboots the virtual machine. On reboot, `MoveHTBootloader.ps1` will again be executed automatically and will delete the old Bootloader partition and then extend the boot partition to take up the available free space. The VM will be rebooted a second time to complete this process.
   Note: This operation changes the drive letter for the `HTBOOTLDR` drive. The original drive letter can be restored by either using the `htblconf.exe` GUI utility or the `ChangeHTBootloaderDrive.ps1` PowerShell script.
5. If desired, log into the Cryptographic Security Platform Vault webGUI and verify that the new boot drive size is displayed correctly. If it is not, go back to the Windows VM and enter the `hcl updateavail` command.

Disk Size Management in Linux

There are two methods for resizing an encrypted disk:

- **Online Resize Method**—The filesystem remains mounted and the clear text path for the device remains accessible during this process for most configurations. On some systems, the filesystem may need to be unmounted for when expanding or decreasing the disk size. Online resize is available for LVM (Logical Volume Manager) volumes.
  Important: Online resize is *not* available if Online Encryption is enabled on the LVM volume. If you are using Online Encryption, you must resize the volume while it unmounted and detached.
- **Offline Resize Method**—The filesystem must be unmounted. That means the data will not be available during this procedure. Offline resize is available for LVM volumes, root and swap devices, and data partitions.

Root, swap, and data partitions can both be expanded as required. Root partitions, however, cannot be reduced in size because they cannot be unmounted. If you need to grow the file system, run "resize / growfs".

Related Topics

- Decreasing the Size of an LVM Volume
- Decreasing the Size of a Linux Data Partition
- Expanding an LVM Swap Volume
- Expanding an LVM Data or Root Volume
- Expanding a Linux Data Partition
- Expanding a Swap Partition
- Expanding a Root Partition

Decreasing the Size of an LVM Volume

You can reduce the size of an LVM data volume only. You cannot reduce the size of a root volume.

The data volume must be detached during this procedure, which means that the data it contains will be inaccessible for a short period of time.

1. Unmount the disk and reduce the filesystem using your hypervisor tools. For example:
   # umount /dev/mapper/clear_myvg-myvol
   # e2fsck -f /dev/mapper/clear_myvg-myvol
   # resize2fs /dev/mapper/clear_myvg-myvol *<newsize>*
2. Detach the volume. For example:
   # hcl detach myvg-myvol
3. Shrink the underlying volume. For example:

```
# lvreduce -L<new size> /dev/myvg/myvol
```

4. Reattach the volume so that Cryptographic Security Platform Vault recognizes the new size.

```
# hcl attach myvg-myvol
```

Decreasing the Size of a Linux Data Partition

Note: Linux file systems like ext2/ext3/ext4/xfs do not allow you to reduce the filesystem size without unmounting the disk. This means that you cannot decrease the size of the root device because you cannot unmount it.

1. Unmount the disk and reduce the size of the disk using your hypervisor tools. For example:
   # umount /dev/mapper/clear_sdb1
   # e2fsck -f /dev/mapper/clear_sdb1
   # resize2fs /dev/mapper/clear_sdb1 <*newsize*>
2. Detach the disk using the command `hcl detach diskname`, where `diskname` is the short form of the disk name (for example, you would use `sdb1` instead of `/dev/sdb1`).
   `# hcl detach sdb1`
3. If this is a non-GPT data partition, decrease the underlying volume using the `fdisk` command. For example:
   # fdisk /dev/sdb
4. If the data partition is a GPT partition, you need to delete the partition and recreate it with the new size. To do so:
   a. Access the device using `gdisk`.
      `# gdisk /dev/sdb`
   b. Print all the information about the old partition using the `i partition-number` command and note the "Partition unique GUID".
      Important: You need to manually assign the current GUID to the resized partition or Cryptographic Security Platform Vault will not recognize the resized partition.
      Command (? for help): i 1
      Using 1
      Partition GUID code: EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 (Microsoft basic data)
      Partition unique GUID: 1390EA67-17AB-48F9-9851-8C8D54A9E454
      First sector: 2048 (at 1024.0 KiB)
      Last sector: 585727 (at 286.0 MiB)
      Partition size: 583680 sectors (285.0 MiB)
      Attribute flags: 0000000000000000
      Partition name: '1'
   c. Delete the old partition.
      `Command (? for help): d 1`
   d. Re-create the new partition with same start but different size when prompted.
      `Command (? for help): n 1`
   e. Switch to expert mode.
      `Command (? for help): x`
   f. Set the saved GUID for the partition.
      Expert command (? for help): c 1
      Using 1
      Enter the partition's new unique GUID ('R' to randomize):
      1390EA67-17AB-48F9-9851-8C8D54A9E454
   g. Save the changes to disk.

```
Expert command (? for help): w
```

5. Re-read the partition table using the `partprobe` command. For example:
   ```
   # partprobe /dev/sdb
   ```
   Note: `partprobe` may fail if the underlying device is busy, which can happen if LVM is configured for another partition on the same disk. If it fails, reboot the VM and continue with this procedure. The partition table will be correctly updated during the reboot.
6. Reattach the disk using the command `hcl attach diskname`, where *diskname* is the short form of the disk name.
   ```
   # hcl attach sdb1
   ```

Expanding an LVM Swap Volume

The following procedure applies to expanding an LVM swap volume only. If you want to expand a LVM root or data volume, see Expanding an LVM Data or Root Volume. If you want to expand a Linux root or data partition that is not managed by LVM, see Expanding a Root Partition and Expanding a Linux Data Partition.

Before You Begin

Make sure you know the name of the LVM swap volume and the Cryptographic Security Platform Vault clear text path to it. If you do not, use the `hcl status` command and look at the Registered Devices section. For example:

```
# hcl status
...

Registered Devices
------------------------------------------------------------------------------
Disk Name          Cipher      Status              Clear
------------------------------------------------------------------------------
cl_centos73-swap    AES-XTS-512  Attached            /dev/mapper/clear_htswap (swap)
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
cl_centos73-root      AES-XTS-512  Attached             /dev/mapper/clear_htroot (/)
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
```

Procedure

1. Log into the VM as `root`.
2. Get the UUID of the swap device by using the `blkid swap-clear-text-path` command. For example:
   ```
   # blkid /dev/mapper/clear_htswap
   /dev/mapper/clear_htswap: UUID="a949b636-1669-43cb-acc4-b1ed86e7f2f1 TYPE="swap"
   ```
3. Turn the swap off by entering the command `swapoff -a`.
   ```
   # swapoff -av
   swapoff on /dev/mapper/clear_htswap
   ```
   Tip: If the `swapoff` command does not work, applications are probably using the swap file. You can make a temporary swap space and move the swap there until this procedure is finished. For example:
   ```
   # fallocate --length 2GiB /swapfile
   # mkswap /swapfile
   # swapon /swapfile
   ```
   You can also try stopping all main applications and then dropping all caches from memory. For details, see your Linux documentation.

4. Increase the size the LVM swap volume as desired using the `lvresize diskname` command, where `diskname` is the name of the swap volume . For example, if you want to increase the swap volume `cl_centos73-swap` by 256M, you would enter:
   # lvm lvresize /dev/cl_centos73/swap -L +256M
   Size of logical volume cl_centos73/swap changed from 1.00 GiB (256 extents) to 1.25 GiB (320 extents).
   Logical volume cl_centos73/swap successfully resized.
5. Increase the size of the encrypted swap to match the new volume size. How you do this depends on whether Online Encryption is enabled or disabled for the volume.
   Tip: You can always use the Offline Resize Method for swap volumes regardless of whether they use Online Encryption. If you are not sure whether Online Encryption is enabled on the volume, use the Offline Resize Method.
   Select one of the following methods:
   - **Online Resize Method** — Usable for swap volumes only if Online Encryption is *disabled*.
     Use the command `hcl resize diskname` , where `diskname` is the name of the swap volume.
     # hcl resize cl_centos73-swap
     Warning: Resizing active device incorrectly can cause any data stored on them to become inaccessible
     Do you want to proceed? (y/n) y
     Device cl_centos73-swap was successfully resized
     Updating the KC with the size (1310720 KB) of the device
     Successfully updated the KC with size (1310720 KB) of the device cl_centos73-swap
   - **Offline Resize Method** — Usable for all swap volumes. This method is required for swap volumes on which Online Encryption is *enabled*.
     Reboot the VM.
     # reboot
6. Re-create swap on the swap volume using the `mkswap -U clear-text-path` command, where `clear-text-path` is the clear text path to the swap volume. For example, if the clear text path is `/dev/mapper/clear_htswap` , you would enter:
   # mkswap -U "a949b636-1669-43cb-acc4-b1ed86e7f2f1" /dev/mapper/clear_htswap
   mkswap: /dev/mapper/clear_htswap: warning: wiping old swap signature.
   Setting up swapspace version 1, size = 1310716 KiB
   no label, UUID=a949b636-1669-43cb-acc4-b1ed86e7f2f1
7. Turn the swap back on using the `swapon -va` command. For example:
   # swapon -va
   swapon /dev/mapper/clear_htswap
   swapon: /dev/mapper/clear_htswap: found swap signature: version 1, page-size 4, same byte order
   swapon: /dev/mapper/clear_htswap: pagesize=4096, swapsize=1342177280, devsize=1342177280

   # swapon --show
   NAME TYPE SIZE USED PRIO
   /dev/dm-4 partition 1.3G 0B -1

Expanding an LVM Data or Root Volume

How you expand an LVM data or root volume depends on whether you have enabled Online Encryption.

If you want to expand a LVM swap volume, see Expanding an LVM Swap Volume. If you want to expand a Linux root or data partition that is not managed by LVM, see Expanding a Root Partition and Expanding a Linux Data Partition.

Procedure

1. Expand the disk using your hypervisor tools.
2. Extend the underlying volume using your Linux management tools.
   For example, if the disk is an LVM volume called `myvg-myvol`, you would use:
   ```
   # lvextend -L<new size> /dev/myvg/myvol
   ```
3. Use the following command to resize the crypto mapping so that it matches the volume size:
   `hcl resize diskname`, where `diskname` is the short form of the disk name, as shown in the `hcl status` command. For example, `myvg-myvol`.
   ```
   # hcl resize myvg-myvol
   ```
   Important: The hcl resize command will fail if there is any ongoing encryption, rekey, or decryption. Please wait until the process is over before you run this command.
4. Expand the filesystem. How you do this depends on whether the volume uses the XFS or EXT filesystem. Both methods require you to specify the clear text path to the volume.
   Tip: The clear text path is shown in the `hcl status` command.
   XFS Filesystems
   Use the `xfs_growfs clear_path` command, where `clear_path` is the clear text path to the disk. For a data partition, the default path is `/dev/mapper/clear_diskname`. For a root partition, the clear text path is `/dev/mapper/clear_htroot`.
   ```
   # xfs_growfs /dev/mapper/clear_myvg_myvol
   meta-data=/dev/mapper/clear_myvg_myvol isize=512    agcount=8, agsize=65536 blks
            =                       sectsz=512   attr=2, projid32bit=1
            =                       crc=1        finobt=0 spinodes=0
   data     =                       bsize=4096   blocks=498688, imaxpct=25
            =                       sunit=0      swidth=0 blks
   naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
   log      =internal               bsize=4096   blocks=2560, version=2
            =                       sectsz=512   sunit=0 blks, lazy-count=1
   realtime =none                   extsz=4096   blocks=0, rtextents=0
   data blocks changed from 498688 to 524288
   ```
   EXT Filesystems
   Use the `resize2fs clear_path` command, where `clear_path` is the clear text path to the disk. For a data partition, the default path is `/dev/mapper/clear_diskname`. For a root partition, the clear text path is `/dev/mapper/clear_htroot`.
   ```
   # resize2fs /dev/mapper/clear_myvg-myvol
   # resize2fs /dev/mapper/clear_htroot
   ```

Expanding a Linux Data Partition

This procedure describes how to expand a data partition using the Offline Resize method. You must unmount the filesystem until the resizing is complete.

If you want to resize a boot partition or an LVM volume, Expanding a Root Partition or Expanding an LVM Data or Root Volume.

1. Unmount the file system. For example, if the target device is "sdb1", you would enter:
   `# umount /dev/mapper/clear_sdb1`

2. Detach the disk you want to expand using the command `hcl detach diskname`, where `diskname` is the short form of the disk name. For example, you would use `sdb1` instead of `/dev/sdb1`.
   ```
   # hcl detach sdb1
   ```
3. If the data partition is a non-GPT partition, extend the root partition using the `fdisk` or `partx` command.
   Warning: This is very critical operation. Make sure you do *not* change the starting offset of the partition while you are manipulating the partition table.
   ```
   # fdisk /dev/sdb
   ```
4. If the data partition is a GPT partition, you need to delete the partition and recreate it with the new size. To do so:
   a. Access the device using `gdisk`.
      ```
      # gdisk /dev/sdb
      ```
   b. Print all the information about the old partition using the `i partition-number` command and note the "Partition unique GUID".
      Important: You need to manually assign the current GUID to the resized partition or Cryptographic Security Platform Vault will not recognize the resized partition.
      ```
      Command (? for help): i 1
      Using 1
      Partition GUID code: EBD0A0A2-B9E5-4433-87C0-68B6B72699C7 (Microsoft basic data)
      Partition unique GUID: 1390EA67-17AB-48F9-9851-8C8D54A9E454
      First sector: 2048 (at 1024.0 KiB)
      Last sector: 585727 (at 286.0 MiB)
      Partition size: 583680 sectors (285.0 MiB)
      Attribute flags: 0000000000000000
      Partition name: '1'
      ```
   c. Delete the old partition.
      ```
      Command (? for help): d 1
      ```
   d. Re-create the new partition with same start but different size when prompted.
      ```
      Command (? for help): n 1
      ```
   e. Switch to expert mode.
      ```
      Command (? for help): x
      ```
   f. Set the saved GUID for the partition.
      ```
      Expert command (? for help): c 1
      Using 1
      Enter the partition's new unique GUID ('R' to randomize):
      1390EA67-17AB-48F9-9851-8C8D54A9E454
      ```
   g. Save the changes to disk.
      ```
      Expert command (? for help): w
      ```
5. Run the `partprobe` command to reread the partition table.
   ```
   # partprobe /dev/sdb
   ```
6. Reattach the disk using the command `hcl attach diskname`, where `diskname` is the short form of the disk name.
   ```
   # hcl attach sdb1
   ```
7. Check the files with the `e2fsck` command and then expand the filesystem using the `resize2fs clear_path` command where `clear_path` is the clear text path to the disk. The default path is `/dev/mapper/clear_diskname`.

```
# e2fsck -f /dev/mapper/clear_sdb1
# resize2fs /dev/mapper/clear_sdb1
```

8. Remount the filesystem.
   `# mount /dev/mapper/clear_sdb1`

Expanding a Swap Partition

Before You Begin

Make sure you know the name of the swap volume and the Cryptographic Security Platform Vault clear text path to it. If you do not, use the `hcl status` command and look at the Registered Devices section. For example:

```
# hcl status
...

Registered Devices
------------------------------------------------------------------------------
Disk Name     Cipher       Status                Clear
------------------------------------------------------------------------------
sda3          AES-XTS-512  Attached              /dev/mapper/clear_htswap (swap)
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
sda2            AES-XTS-512  Attached                 /dev/mapper/clear_htroot (/)
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
```

Procedure

1. Log into the VM as `root`.
2. Get the UUID of the swap device by using the `blkid swap-clear-text-path` command. For example:
   ```
   # blkid /dev/mapper/clear_htswap
   /dev/mapper/clear_htswap: UUID="62e5b7ca-cc50-409f-ba7d-5f0645c85588" TYPE="swap"
   ```
3. Turn the swap off by entering the command `swapoff -a`.
   ```
   # swapoff -av
   swapoff on /dev/mapper/clear_htswap
   ```

   Tip: If the `swapoff` command does not work, applications are probably using the swap file. You can make a temporary swap space and move the swap there until this procedure is finished. For example:
   ```
   # fallocate --length 2GiB /swapfile
   # mkswap /swapfile
   # swapon /swapfile
   ```

   You can also try dropping stopping all main applications and then dropping all caches from memory. For details, see your Linux documentation.
4. Increase the size of the swap device as desired. How you do this depends on the partition type.
   - If this is a GPT partition, you can use `partx` as long as you preserve the GUID assigned to the GPT partition. To determine the GUID, use the `i partition-number` command and look at the "Partition unique GUID" field. For an example of setting the GUID on a GPT partition, see Expanding a Linux Data Partition.

- If this is a non-GPT partition, you can use the `fdisk diskname` command, where `diskname` is the name of the swap device. An example of this process follows.
  Non-GPT Partition Example
  For example, if you want to increase the non-GPT swap partition `sda3` by 256M, you would enter:

```
# fdisk /dev/sda

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
        switch off the mode (command 'c') and change display units to
        sectors (command 'u').

Command (m for help): p

Disk /dev/sda: 17.2 GB, 17179869184 bytes
255 heads, 63 sectors/track, 2088 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000a3126

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1         131     1048576   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2             131        1828    13631488   83  Linux
/dev/sda3            1828        1980     1223262   82  Linux swap / Solaris

Command (m for help): d
Partition number (1-4): 3

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 3
First cylinder (1828-2088, default 1828):
Using default value 1828
Last cylinder, +cylinders or +size{K,M,G} (1828-2088, default 2088):
Using default value 2088

Command (m for help): t
Partition number (1-4): 3
Hex code (type L to list codes): 82
Changed system type of partition 3 to 82 (Linux swap / Solaris)

Command (m for help): p

Disk /dev/sda: 17.2 GB, 17179869184 bytes
255 heads, 63 sectors/track, 2088 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000a3126
```

```
   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1         131     1048576   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2             131        1828    13631488   83  Linux
/dev/sda3            1828        2088     2090772   82  Linux swap / Solaris

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

5. Run the `partprobe` command to reread the partition table. If this command fails because the device is busy, you need to reboot the VM.
   ```
   # partprobe /dev/sdb
   Warning: WARNING: the kernel failed to re-read the partition table on /dev/sda (Device or resource busy).  As a result, it may not reflect all of your changes until after reboot.

   # reboot
   ```
6. If you had to reboot the VM in the previous step, turn the swap off again by entering the command `swapoff -a`.
   ```
   # swapoff -av
   swapoff on /dev/mapper/clear_htswap
   ```
7. Recreate the swap device with the same UUID as the old device and turn it back on. For example:
   ```
   # mkswap -U "62e5b7ca-cc50-409f-ba7d-5f0645c85588" /dev/mapper/clear_htswap
   mkswap: /dev/mapper/clear_htswap: warning: don't erase bootbits sectors
           on whole disk. Use -f to force.
   Setting up swapspace version 1, size = 2090768 KiB
   no label, UUID=62e5b7ca-cc50-409f-ba7d-5f0645c85588
   # swapon -a

   # swapon -s
   NAME      TYPE      SIZE      USED PRIO
   /dev/dm-3 partition 2090768   0    -1
   ```

Expanding a Root Partition

This procedure describes how to expand a root partition using the Offline Resize method. You must unmount the filesystem and reboot the VM during this procedure.

If you want to resize a data partition or an LVM volume, see Expanding a Linux Data Partition or Expanding an LVM Data or Root Volume.

1. If necessary, use your hypervisor tools to expand the root disk so that there is sufficient room to resize it to the desired size. You might also have to push the "swap" partition forward, if it is immediately after the root partition.
2. Extend the root partition using the `fdisk` or `partx` command.

Warning: This is very critical operation. Make sure you do *not* change the starting offset of the partition while you are manipulating the partition table.

```
# fdisk /dev/sda
```

3. Reboot the VM to force the system to read the new partition table.

Changing the Drive Letter for a Windows Disk

Data Disks

At any time, you can use the Windows Disk Manager to change the drive letter for a data disk, even if that data disk is encrypted. The Cryptographic Security Platform Vault for VM Encryption automatically detects the change and displays the updated drive letter in the Cryptographic Security Platform Vault for VM Encryption webGUI after the next VM heartbeat.

If you want to force an immediate update, enter the `hcl heartbeat` command.

Boot Disk

If you have encrypted the boot disk, or if you plan to encrypt the boot disk in the future, Entrust Cryptographic Security Platform Vault requires that the boot disk must reside on `C:` or be mapped to `C:`.

If you are never going to encrypt the boot disk, you can use the Windows Disk Manager to change the drive letter as desired.

Entrust Bootloader Install Disk

If you want to change the drive letter for the disk on which the Entrust Bootloader is installed, you can use the Entrust Drive and Network Configuration utility or a PowerShell script.

To use the Entrust Drive and Network Configuration utility, run htblconf.exe and select the drive letter you want to use from the Select drive letter drop down. When you are finished, click Install.

To use the PowerShell script:

1. Log into the Windows VM as a System Administrator.
2. Start Windows PowerShell.
3. Enter the command `ChangeHTBootloadDrive.ps1 -drive new-drive:`, where `new-drive` is the drive letter that you want to use. For example:
   PS C:\Users\Administrator> ChangeBootLoadDrive.ps1 -drive s:
   HyTrust Bootloader is installed at E:, switching it to S:
   Success

Moving a VM to a Cloud VM Set

You can move any VM that does not have BoundaryControl enabled to a different Cloud VM Set.

Note: You must have access to both the original Cloud VM Set and the Cloud VM Set where you are moving the VM.

Movement will be blocked if:

- The source or the destination Cloud VM Set has one of the following configured:
  - Single Encryption Key (SEK)
  - Key Encryption Key (KEK)
- You exceed the max number of virtual machines registered for the destination Cloud VM Set.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab.
4. Select the VM that you want to move.
5. Select **Actions > Move VM to another Cloud VM Set**.
6. On the Move VM to another Cloud VM Set window, enter the following: . Select the Destination Group and the Destination CVM Set.

Field	Description
Destination Group	Select the name of the Cryptographic Security Platform Vault for VM Encryption Group that owns the destination Cloud VM Set.
Destination CVM Set	Select the Cloud VM Set set where you want to move the selected VM. The current Cloud VM Set will be listed, but cannot be selected.

7. Click **Migrate**.

Moving Disks Between VMs

Entrust supports the migration of disks between Linux VMs or between Windows VMs as long as:

- The original VM and the target VM are members of the same Cloud VM Set.
- The disk contains a GUID (Globally Unique Identifier) assigned by Cryptographic Security Platform Vault. The GUID is stored in a private area created when the disk is encrypted, added, or imported if there is enough space to do so.
- The disk is partitioned in such a way that Cryptographic Security Platform Vault for VM Encryption can add a private area for the GUID. For example, you cannot move a non-partitioned disk, a GPT partition, or a LVM (Logical Volume Manager) volume to another VM because Cryptographic Security Platform Vault for VM Encryption cannot add the private area to those entities. You can, however, move an MBR partition because Cryptographic Security Platform Vault for VM Encryption can add to that type of partition.
- There is no ongoing encryption.

Before You Begin

If you want to move a Linux disk that is protected by an Access Control Policy, you need to remove the policy from the disk before you can move the disk. For more information, see Access Control Policies.

If you want to move a Windows disk that is protected by an Access Control Policy, make sure that the policy's permissions list will be valid on the VM to which you want to move the disk. If any user currently in the permissions list does not exist on the new VM, the policy association will fail when the disk is rebooted.

Procedure

1. To verify that the disk you want to move has a GUID:
   a. Log into the original VM as `root` .
   b. Enter the command `hcl status -g` on Linux or `hcl status` on Windows.

   Linux Example

   ```
   # hcl status -g

   Device Discovery (Registered and Available)
   -------------------------------------------------
   Disk Name    PartLayout     GUID
   ```

```
-------------------------------------------------
sdb1        MBR          8AF3AF24-351A-2FD4-C1AE-44094D259B3F
sdb1        MBR          7AFFA524-459F-4F56-AC1E-5459E0259E3F
```

Windows Example

```
Device details
-------------------------------------------------
Drive Disk  Part  Cipher     Status      GUID
-------------------------------------------------
C:    0     2     none       Avail-Sys   N/A
E:    1     1     none       Available   A8E25AE9-7A75-471A-A1AA-7CAE1550B35C
F:    2     1     none       Available   583EB883-52D3-4B05-A482-FF113B5359DD
G:    3     1     none       Available   FF2A17F2-D7DE-404B-B977-018ADC611BCC
```

c. If the disk you want to move has a GUID, you can continue with this procedure. If it does not, then you cannot migrate the disk.

2. Move the disk to a target VM that is a member of the same Cloud VM Set as the original VM.
3. Log into the target VM as `root`.
4. Enter the command `hcl import [-y] diskname`, where:
   - `-y` specifies that the command should run without prompts.
   - `diskname` is the name of the disk that you just moved.

   The Cryptographic Security Platform Vault for VM Encryption recognizes the disk by the GUID and adds it back to the system in its new location. Because the disk was previously registered, the Cryptographic Security Platform Vault for VM Encryption does not need to re-encrypt the data or change the disk in any way. Therefore the data on the disk is immediately available to authorized clients.

Viewing the Details for a Disk

You can view the details for any disk on any VM that is registered with Cryptographic Security Platform Vault for VM Encryption. For each VM, the Cryptographic Security Platform Vault for VM Encryption webGUI displays separate tabs for encrypted and unencrypted disks.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab and select the VM you want to work with from the list.
4. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
5. To view the details for an encrypted disk, click the **Encrypted Disks** tab and select the disk from the list. the webGUI displays additional details for the selected disk below the table. For the selected disk you can do any of the following:
   - Revoke access to the disk by selecting **Actions > Revoke Disk Access**. For details, see Revoking Access to a Disk and Reactivating a Revoked Disk.
   - Decrypt the disk by selecting **Actions > Decrypt Disk**. For details, see Decrypting a Disk Using the webGUI.
     Note: This option is not available if there is an Access Control Policy associated with the disk.
   - Rekey the disk by selecting **Actions > Rekey Disk**. For details, see Encryption Key Maintenance.
   - Associate an Access Control Policy with the disk, or change the currently-associated Access Control Policy, by selecting **Actions > Set Policy on Disk**. For details, see Associating an Access Control Policy with a Disk.

- Edit the Access Control Policy associated with the disk by clicking the name of the policy in the **Policy Name** field. For details, see Changing a Linux Access Control Policy or Changing a Windows Access Control Policy.
- Change the expiry date or expiration option by clicking the value in the **Expiry Date** or On Expiration field. For details, see Setting the Key Expiration Date for a Disk.

6. To view the list of unencrypted disks, click the **Unencrypted Disks** tab. You can then select one or more disks and encrypt them using **Actions > Encrypt Disk**.

Using the Dashboard

The dashboard presents a graphical overview of your system, either for all your Cloud VM Sets or for a group of user-selected sets.

Procedure

1. In the top menu bar, click **Dashboard**.
2. To limit the number of Cloud VM Sets displayed, click the gear icon underneath the Entrust logo and select the sets you want to view, then select **Apply**. The webGUI displays a message next to the gear icon indicating how many Cloud VM Sets you are viewing.
3. To view additional details for any chart in the Dashboard, hover over it with the mouse. For all charts except VM Encryption and Disk Encryption, you can also click on a chart to view a pop-up dialog box with the details presented in tabular format.
4. To view the pending task list, click the **Expand** icon in the upper-right-hand corner of the **Tasks** box.

Backups, Clones, and Snapshots

If you want to backup an the Policy Agent on an encrypted disk, you need to make sure the entire disk is backed up (for example, the entire VMDK file in a VMware vSphere environment). This ensures that the Entrust GUIDs representing the keys are also backed up so the data can be decrypted if it is restored from the backup. Once the backup is reauthorized with Cryptographic Security Platform Vault, Cryptographic Security Platform Vault can use the restored GUIDs to determine which keys apply to the restored data.

To create the backup, see your hypervisor documentation. Entrust does not provide any tools for backing up a VM.

Warning: Before you back up your VM, make sure you check the expiration date for the data encryption keys on the disk. If you restore a backup with expired keys and the expiration option is set to SHRED, Cryptographic Security Platform Vault will destroy the keys immediately and the data will be inaccessible. If you set the expiration option to NO USE, the keys can be reactivated after the back up is restored. For more information, see Encrypting a Disk Using the CLI.

The Entrust Policy Agent identifies the VM on which it is running and uses this information and the certificate supplied during registration in order to authenticate the VM with Cryptographic Security Platform Vault. Cryptographic Security Platform Vault will not deliver keys to any VM that looks identical to one already in the system . While this is required from a security perspective, it presents challenges when dealing with VM snapshots and clones.

Snapshots

If you restore a VM using a snapshot, the hardware signature of the VM does not change. However, the restored VM may need to be re-authenticated with Cryptographic Security Platform Vault and should always be re-synchronized. For details, see Restoring a VM from a Snapshot.

Clones

If you want to add a clone of an existing VM while the original is still running, you must specifically register the clone VM with Cryptographic Security Platform Vault as an authorized clone of the existing VM.

For example, if you bring a clone of a VM online while the original VM is still running, the Policy Agent on the clone VM will attempt to communicate with Cryptographic Security Platform Vault on startup, but the check will fail authentication because the original VM is already registered.

If you enter the `hcl status` command on the clone VM, you will see messages similar to the following:

```
# hcl status
Summary
-------------------------------------------------
KeyControl: 192.168.140.151:443
KeyControl list: 192.168.140.151:443
Status: Reauth needed
```

For Windows, this would look like:

```
C:\>hcl status
Summary
-----------------------------------------------------------------------
KeyControl: 172.16.163.129:443
KeyControl list: 172.16.163.129:443
KeyControl Mapping: map1
Status: Reauth needed (Hardware signature verification failed)
```

Cryptographic Security Platform Vault does not know which VM is the original and which is the clone. In order to both VMs running at the same time, you need to register the clone as described in Registering a Cloned VM with Standard Authentication.

This section includes:

- Registering a Linux or Windows Root-Drive-Encrypted Cloned VM with Simplified Authentication
- Registering a Cloned VM with Simplified Authentication
- Registering a Cloned VM with Standard Authentication
- Restoring a VM from a Snapshot

Registering a Linux or Windows Root-Drive-Encrypted Cloned VM with Simplified Authentication

Backups, clones, and snapshots look identical to Cryptographic Security Platform Vault for VM Encryption. If you want both a VM and its clone running at the same time, you need to clone the VM certificate issued to the original VM and then register the clone using that certificate.

If the root drive is encrypted on a Linux or Windows VM, you must access the VM through your hypervisor and use the Entrust Debug Console as described below.

If only data drives are encrypted on the VM, there are two ways to register the certificate:

- Standard Authentication—The most secure authentication method. You create a certificate in the Cryptographic Security Platform Vault for VM Encryption webGUI which you then copy to the target system. For details, see Registering a Cloned VM with Standard Authentication.
- Simplified Authentication—The easiest method. It allows you to skip downloading a certificate from Cryptographic Security Platform Vault for VM Encryption webGUI, but it does require you to enter the Cryptographic Security Platform Vault for VM Encryption credentials on the command line. You should only use this method if the VM is secure. For details, see Registering a Cloned VM with Simplified Authentication.

Procedure

1. Power on the cloned Linux or Windows VM. The cloned VM's attempt to boot will fail because Cryptographic Security Platform Vault determines that the cloned VM has a different hardware signature than the original VM.
2. Open console access to the cloned VM through your hypervisor and wait for the VM to display the prompt asking if you want to use the Entrust Debug Console. When it does, type `y` and press **Enter** to launch the Debug Console.
3. From the Debug Console menu, select **Advanced Access**.
4. If you are using a static IP address for the cloned VM, do the following to change the IP address. (If you are using DHCP, the system automatically assigns a new IP address to the cloned VM.) In the following examples, the original VM's IP address is `10.238.66.240` and the clone's IP address is `10.238.66.100`.
   a. Add the new IP address you want to use for the cloned VM by entering the `ip addr add <clone IP address>/<netmask> dev <interface name>` command. For example:
   ```
   # ip addr add 10.238.66.100/24 dev eth0
   ```
   b. Delete the IP address being used by the original VM by entering the `ip addr del <original VM IP address>/<netmask> dev <interface name>` command. For example:
   ```
   # ip addr del 10.238.66.240/24 dev eth0
   ```
   c. If needed, add the clone IP address to the routing table with the `ip route add [default] <network/netmask> [via <gateway IP address>|dev <device>]` command.
5. Update the certificate on the cloned VM by entering the command `hcl updatecert -a [-u username -p password] [-e certificate expiration]` command, where:
   - `-a` tells `hcl` to contact Cryptographic Security Platform Vault to get the new certificate.
   - `-u` is a Cryptographic Security Platform Vault user account with Cloud Admin privileges. If you do not enter a user account name you will be prompted for one.
   - `-p` is the password for the Cryptographic Security Platform Vault user account. If you do not enter a password you will be prompted for one.
   - `-e` is the certificate expiration date in the format MM/DD/YYYY. If you do not enter an expiration date, Cryptographic Security Platform Vault uses the default date set in the **Certificate Expiration** option for the Cloud VM Set that this VM belongs to. The default is one year from the creation date.

   For example:
   ```
   # hcl updatecert -a -u CloudAdmin -p DogDays123! -e 06/30/2022
   ```
6. Register the cloned VM with Cryptographic Security Platform Vault by entering the following command:
   `hcl register -w -a -c [-h vm-name] [-d "vm-description"] [-u username [-s password]] [-z cvm-set] [-v vault-_id] kc-hostname[:port],kc-hostname2[:port],...`

   Important: For Windows systems, you must use the `-w` flag when registering cloned VMs.

   where:
   - `-a` indicates that hcl should download the VM certificate from Cryptographic Security Platform Vault and do the registration and authentication in one step.
   - `-c` indicates that this a cloned VM.
   - `-h` (optional)—The name of the clone VM that will be displayed in the Cryptographic Security Platform Vault webGUI (Default: hostname).
   - `-d` (optional)—A description of the clone VM that will be displayed in the Cryptographic Security Platform Vault webGUI.

- `-u` is a Cryptographic Security Platform Vault user account with Cloud Admin privileges. If you do not enter a user account you will be prompted for one.
- `-s` is the password for the Cryptographic Security Platform Vault user account. If you do not enter a password you will be prompted for one.
- `-z` (optional)—The name of the Cloud VM Set defined in the Cryptographic Security Platform Vault cluster to which you want to assign this VM. If you do not specify this parameter, the registration prompts you for the set name.
- `-v` —is the Vault ID of the Vault. This is displayed in the About section for each vault under the help icon (**?**) at the top right corner. If you do not enter a vault ID you will be prompted for one.
- `-w` —Required for Windows only. This option generates a HWSIG that is appropriate for the Windows bootloader.
- `kc-hostname[:port],kc-hostname2[:port],...` (required)—The list of IP addresses or hostnames for the Cryptographic Security Platform Vault nodes with which you want to register the VM. You must specify at least one Cryptographic Security Platform Vault node in this list. You must also specify a port if the Cryptographic Security Platform Vault nodes use anything other than the default port (443). On Windows, if you specify more than one IP address, enclose the list in double-quotes.

For example, if the clone VM name is "hq-vm-clone", the description is "Clone of HQ Server", and you want to register it with two Cryptographic Security Platform Vault nodes at 10.238.32.74 and 10.238.32.75, you would enter:
hcl register -a -c -v d84243e7-d359-4179-9530-3497434e3192 -h hq-vm-clone -d "Clone of HQ Server" 10.238.32.74,10.238.32.75

Please provide the Cryptographic Security Platform Vault login details
username: htcloudadmin
password: ********

Registered as hq-vm-clone with KeyControl node(s) 10.238.32.74,10.238.32.75

Completing authentication for hq-vm-clone on KeyControl node(s) 10.238.32.74,10.238.32.75
Authentication complete, machine ready to use

7. After the VM has been registered, exit from the Advanced Access shell and let the VM finish booting. After the VM has booted, log into the clone VM as `root` and set the clone VM's IP address using your standard networking tools.
8. Update the Entrust Bootloader network information with the `htroot update [-c params.conf]` command, where `-c` tells the command to run non-interactively.

Registering a Cloned VM with Simplified Authentication

Backups, clones, and snapshots look identical to the Cryptographic Security Platform Vault for VM Encryption. If you want both a VM and its clone running at the same time, you need to clone the VM certificate issued to the original VM and then register the clone using that certificate.

If the root drive is encrypted on the VM, you must register the certificate from the debug console or the VM console. For details, see Registering a Linux or Windows Root-Drive-Encrypted Cloned VM with Simplified Authentication.

If only data drives are encrypted on the VM, there are two ways to register the certificate:

- Standard Authentication—The most secure authentication method. You create a certificate in the Cryptographic Security Platform Vault for VM Encryption webGUI which you then copy to the target system. For details, see Registering a Cloned VM with Standard Authentication.

- Simplified Authentication—The easiest method. It allows you to skip downloading a certificate from the Cryptographic Security Platform Vault for VM Encryption webGUI, but it does require you to enter the Cryptographic Security Platform Vault for VM Encryption credentials on the command line. You should only use this method if the VM is secure. This method is described below.

Procedure

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. Update the certificate on the cloned VM by entering the command `hcl updatecert -a [-u username -p password] [-e certificate expiration]` command, where:
   - `-a` tells `hcl` to contact Cryptographic Security Platform Vault to get the new certificate.
   - `-u` is a Cryptographic Security Platform Vault user account with Cloud Admin privileges. If you do not enter a user account name you will be prompted for one.
   - `-p` is the password for the Cryptographic Security Platform Vault user account. If you do not enter a password you will be prompted for one.
   - `-e` is the certificate expiration date in the format MM/DD/YYYY. If you do not enter an expiration date, Cryptographic Security Platform Vault uses the default date set in the **Certificate Expiration** option for the Cloud VM Set that this VM belongs to. The default is one year from the creation date.

   For example:

   # hcl updatecert -a -u CloudAdmin -p DogDays123! -e 06/30/2022
3. Register the VM with Cryptographic Security Platform Vault by entering the following command:
   `hcl register -a -c [-h vm-name] [-d "vm-description"] [-u username [-v vault-id]] [-p password]] [-z cvm-set] kc-hostname[:port],kc-hostname2[:port],...`

   where:
   - `-a` indicates that hcl should download the VM certificate from Cryptographic Security Platform Vault and do the registration and authentication in one step.
   - `-c` indicates that this a cloned VM.
   - `-h` (optional) — The name of the clone VM that will be displayed in the Cryptographic Security Platform Vault for VM Encryption webGUI (Default: hostname).
   - `-d` (optional) — A description of the clone VM that will be displayed in the Cryptographic Security Platform Vault for VM Encryption webGUI.
   - `-u` is a Cryptographic Security Platform Vault user account with Cloud Admin privileges. If you do not enter a user account you will be prompted for one.
   - `-v` is the Vault ID of the Vault. This is displayed in the About section for each vault under the help icon (**?**) at the top right corner. If you do not enter a vault ID you will be prompted for one.
   - `-p` is the password for the Cryptographic Security Platform Vault user account. If you do not enter a password you will be prompted for one.
   - `-z` (optional) — The name of the Cloud VM Set defined in the Cryptographic Security Platform Vault cluster to which you want to assign this VM. If you do not specify this parameter, the registration prompts you for the set name.
   - `kc-hostname[:port],kc-hostname2[:port],...` (required)—The list of IP addresses or hostnames for the Cryptographic Security Platform Vault nodes with which you want to register the VM. You must specify at least one Cryptographic Security Platform Vault node in this list. You must also specify a port if the Cryptographic Security Platform Vault nodes use anything other than the default port (443). On Windows, if you specify more than one IP address, enclose the list in double-quotes.

For example, if the clone VM name is "hq-vm-clone", the description is "Clone of HQ Server", and you want to register it with two Cryptographic Security Platform Vault nodes at 10.238.32.74 and 10.238.32.75, you would enter:
hcl register -a -c -h hq-vm-clone -v "efe47ad3-26d7-49cf-b09d-538f0fc5db29" -d "Clone of HQ Server" 10.238.32.74,10.238.32.75
Please provide the KeyControl login details
username: htcloudadmin
password: ********

Registered as hq-vm-clone with KeyControl node(s) 10.238.32.74,10.238.32.75

Completing authentication for hq-vm-clone on KeyControl node(s) 10.238.32.74,10.238.32.75
Authentication complete, machine ready to use

Registering a Cloned VM with Standard Authentication

Backups, clones, and snapshots look identical to Cryptographic Security Platform Vault for VM Encryption. If you want both a VM and its clone running at the same time, you need to clone the VM certificate issued to the original VM and then register the clone using that certificate.

If the root drive is encrypted on the VM, you must register the certificate from the debug console or the VM console. For details, see Registering a Linux or Windows Root-Drive-Encrypted Cloned VM with Simplified Authentication.

If only data drives are encrypted on the VM, there are two ways to register the certificate:

- Standard Authentication—The most secure authentication method. You create a certificate in the Cryptographic Security Platform Vault for VM Encryption webGUI which you then copy to the target system. This method is described below.
- Simplified Authentication—The easiest method. It allows you to skip downloading a certificate from the Cryptographic Security Platform Vault for VM Encryption webGUI, but it does require you to enter the Cryptographic Security Platform Vault for VM Encryption credentials on the command line. You should only use this method if the VM is secure. For details, see Registering a Cloned VM with Simplified Authentication.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab.
4. Select the VM that you want to clone from the list.
5. Select **Actions > Clone Certificate**.
6. Optionally enter a passphrase for the certificate. If you enter one here, you will be required to enter the same passphrase when you register the cloned VM.
7. If you want to change the date on which the certificate expires, enter a new date in the **Date** field.
8. When you are done, click **Clone**. Cryptographic Security Platform Vault creates a cloned certificate and copies it to your browser's default download location.
9. Copy the certificate to the cloned VM.
10. Register the cloned VM using the command `hcl register -c [-h myname] [-d description] [-v vault-id]][-p certificate_password] [-o one_time_passphrase] kc_hostname[:port],kc_hostname2[:port2],... /path/to/certificate.cert`, where:
    - `-c` indicates that this is a cloned VM.
    - `-h` specifies the name associated with this VM. This name is visible in the webGUI and through APIs.

- `-d` is an optional description for the VM.
- `-v` is the Vault ID of the Vault. This is displayed in the About section for each vault under the help icon (**?**) at the top right corner. If you do not enter a vault ID you will be prompted for one.
- `-p` is the password for the certificate if one was entered when the certificate was created. If you omit this option and a password is required, you will be prompted for the password when you execute the command.
- `-o` is a one-time passphrase that will be used to authenticate the VM with the Cryptographic Security Platform Vault for VM Encryption through the webGUI. If you do not specify a passphrase, you will be prompted for one when you execute the command. The passphrase must contain at least 16 alphanumeric characters.
- `kc-hostname[:port],kc-hostname2[:port],...` (required)—The list of IP addresses or hostnames for the Cryptographic Security Platform Vault nodes with which you want to register the VM. You must specify at least one Cryptographic Security Platform Vault node in this list. You must also specify a port if the Cryptographic Security Platform Vault nodes use anything other than the default port (443). On Windows, if you specify more than one IP address, enclose the list in double-quotes.
- The final option is the fully-qualified name of the certificate that you downloaded from the Cryptographic Security Platform Vault for VM Encryption webGUI.

For example:

```
# hcl register -c -h "ubuntu-12.10" -d "My 12.10 VM" 192.168.140.15\
  -v "efe47ad3-26d7-49cf-b09d-538f0fc5db29" bbd7d0c7-*_130415215216.cert

Certificate passphrase might be required
Certificate successfully unpacked

You need to specify a passphrase which will be used for authentication with KeyControl
Enter passphrase (min 16 characters): onetimepassword16chrs

Registered as ubuntu-12.10 with KeyControl(s) 192.168.140.15
Please log on to any KeyControl to complete the authentication of this node
```

11. Return to the webGUI and authenticate the VM:
    a. Click the **Unauthenticated VMs** tab.
    b. Select the clone VM you just registered.
    c. Select **Actions > Authenticate**.
    d. Enter the one-time passphrase at the prompt.
12. If you want to change the Cryptographic Security Platform Vault for VM Encryption node IP addresses the clone VM will use, see Updating CSP Vault Node IP Addresses on an Individual VM. If you want to associate a Cluster Node Mapping with the clone VM, see Managing the Cluster Node Mapping on a VM.

Restoring a VM from a Snapshot

1. Use your hypervisor tools to restore the VM from the snapshot.
2. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
3. Enter the `hcl status` command and determine if the grace period has expired.
4. If required, re-authenticate the VM with Cryptographic Security Platform Vault for VM Encryption as described in Re-Authenticating a Standard VM or Re-Authenticating a VM with an Encrypted Root Device or Boot Disk.
5. After the VM has been authenticated, re-synchronize the device using the `hcl devicesync reason` command, where `reason` is a user-defined reason for the re-sync. This text string is logged in the Cryptographic

Security Platform Vault for VM Encryption audit log and added to the alert message sent during sync processing.

```
# hcl devicesync "restored hq-4-linux from snapshot"
```

6. Make sure the device list in configuration file on the VM is accurate using the `hcl updateconfig` command. This updates the list in real time without requiring a VM reboot.

```
# hcl updateconfig
```

Re-Authenticating a Windows VM with the Entrust Policy Agent GUI

1. Log into the VM as a System Administrator.
2. Select **Start > All Programs > Entrust > Entrust DataControl** or start Windows PowerShell and enter the `hclGUI` command.
3. Click **Authenticate** and specify the options you want to use.

Field	Description
Username	The login name of a Cryptographic Security Platform Vault account with Cloud Admin privileges.
Password	The password for the Cryptographic Security Platform Vault account.

4. When you are done, click **Authenticate**.

Re-Authenticating a VM with an Encrypted Root Device or Boot Disk

Because encryption keys are never stored locally, a VM with an encrypted boot partition requires access to Cryptographic Security Platform Vault when booting or the attempt will fail. If Cryptographic Security Platform Vault is not available when the system is booted, the VM repeatedly attempts to contact Cryptographic Security Platform Vault for 30 seconds. If contact cannot be established after that time, the VM presents a console menu with a number of options.

This procedure describes how to re-authenticate a Linux VM with an encrypted root device or a Windows VM with an encrypted boot disk using the console menu on the VM. If you want to re-authenticate a regular VM, see Re-Authenticating a Standard VM.

> Note: The following procedure only works with root or boot-encrypted VMs because they continually try to reach Cryptographic Security Platform Vault until they are authenticated. Regular VMs stop trying to contact Cryptographic Security Platform Vault after a small number of attempts.

Procedure

1. Access the VM through your hypervisor.
   If you are unable to view the console directly, for example in environments such as Amazon Web Services (AWS), you can access the console using an SSH client. This requires the `id_rsa` key file generated during the Policy Agent installation. Copy the `id_rsa` file to the server and then reboot.

   Tip: If you need another copy of the `id_rsa` key file, you can download it from the Cryptographic Security Platform Vault for VM Encryption webGUI by selecting the VM on the **Workloads > VMs** tab and then selecting **Actions > Download Bootloader SSH Key**.
2. The Policy Agent should automatically display the console when it has failed to authenticate with Cryptographic Security Platform Vault for at least 30 seconds. From this console menu, select **Authenticate** for Linux or **Reauthenticate** for Windows.

3. When prompted, enter a one time passphrase of exactly 16 alphanumeric characters that you can use to validate the reauthentication request in the Cryptographic Security Platform Vault for VM Encryption webGUI.
4. Reauthenticate the VM using the Cryptographic Security Platform Vault for VM Encryption webGUI.
    a. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
    b. In the top menu bar, click **Workloads**.
    c. Select the VM in the table and then select **Actions > Authenticate**.
    d. Enter the one-time passphrase at the prompt.
5. Return to the VM and make sure that it can now communicate with Cryptographic Security Platform Vault and the boot process succeeds.
6. If reauthenticating the VM from the console does not work, you can try to rescue the authentication from the Cryptographic Security Platform Vault for VM Encryption webGUI. Rescue authentication can only be used on encrypted boot drives and it should only be used after you have tried reauthenticating from the console menu on the VM.
   To use rescue authentication, make sure the VM is selected in the Cryptographic Security Platform Vault for VM Encryption webGUI then select **Actions > Rescue Authentication**. At the VM's next heartbeat, Cryptographic Security Platform Vault authenticates the VM.

Re-Authenticating a Standard VM

The way you re-authenticate a VM depends on the operating system and whether the boot drive is encrypted on the VM. The following procedure describes how to re-authenticate a standard VM. If you want to re-authenticate a VM with an encrypted boot drive, see Re-Authenticating a VM with an Encrypted Root Device or Boot Disk.

When you re-authenticate a VM you can either create a one-time passphrase on the VM that you must then enter in the Cryptographic Security Platform Vault for VM Encryption webGUI, or you can enter the credentials of a Cryptographic Security Platform Vault for VM Encryption user account with Cloud Admin privileges on the command line or in the Policy Agent GUI.

Using the Policy Agent GUI

1. Log into the Windows system using an account with Administrator privileges.
2. Select **Start > All Programs > Entrust > Entrust DataControl** or start Windows PowerShell and enter the `hclGUI` command.
3. Click the **Authenticate** button.
4. In the pop-up window, enter the credentials and click **Authenticate**.
5. When the status update window appears, click **OK**.
6. Refresh the window to confirm that the VM was re-authenticated.

Using the CLI

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. If you want to enter a one-time passphrase that you will confirm in the :
    a. Enter the command `hcl auth [-o one_time_passphrase]` , where `-o` is the one-time passphrase that you will use in the Cryptographic Security Platform Vault for VM Encryption webGUI. The passphrase must contain exactly 16 alphanumeric characters.
    b. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
    c. In the top menu bar, click **Workloads**.
    d. Click the **VMs** tab.
    e. Select the VM in the table and then select **Actions > Authenticate**.

f. Enter the one-time passphrase at the prompt.
g. Return to the VM and enter the command `hcl attach -a` to reattach all registered disks on the VM.

3. If you want to enter your Cryptographic Security Platform Vault for VM Encryption user account credentials on the command line, enter the command `hcl auth -a [-u user [-s password]]`, where:
   - `-u` is a Cryptographic Security Platform Vault for VM Encryption user account name with Cloud Admin privileges.
   - `-s` is the password for the Cloud Admin account.

Access Control Policies

An Access Control Policy determines who can access the files and data blocks on the Cryptographic Security Platform Vault for VM Encryption-encrypted data disks associated with the policy. The default permission is "Deny", so as soon as you associate an Access Control Policy with an encrypted disk, the data on that disk is inaccessible to everyone except the users and groups who have explicit "Allow" permissions in the policy rules.

The first time you associate an Access Control Policy with a disk, Cryptographic Security Platform Vault for VM Encryption sends the policy information to the VM at the VM's next heartbeat. At that time, the Policy Agent verifies that all local user account entries in the policy's permissions list are valid. If they are, the Policy Agent enables the Access Control Policy on the disk. If not, the Policy Agent raises an alert describing the problem and does not enable *any* access controls on the disk.

> Note: For Windows, the permissions list can also contain Active Directory (AD) users and groups which are validated when the AD accounts are added to the permissions list. If a policy's permissions list contains AD accounts that have since been removed from AD, the Policy Agent ignores the non-existent accounts and implements the rest of the Access Control Policy.

The permissions lists for an Access Control Policy are stored in the Access Control Rules defined for that policy. For details, see Access Control Rule Types.

Linux Access Control Policy Maintenance

Whenever you change a Linux Access Control Policy in Cryptographic Security Platform Vault for VM Encryption, the Cryptographic Security Platform Vault for VM Encryption sends the changes to each associated Linux VM on the VM's next heartbeat. At that time, the Policy Agent verifies the new permissions list. If any local user account entries are not found, the Policy Agent raises an alert and continues to use the old permissions list for the VM.

The old permissions list remains in effect until a Cloud Admin changes the Access Control Policy in the Cryptographic Security Platform Vault for VM Encryption webGUI and the new permissions list is validated by the Policy Agent.

Windows Access Control Policy Maintenance

Whenever you change a Windows Access Control Policy in Cryptographic Security Platform Vault for VM Encryption, the Cryptographic Security Platform Vault for VM Encryption sends the changes to each associated VM on the VM's next heartbeat. At that time, the Policy Agent verifies the new permissions list. If any local users account entries are not found, the Policy Agent raises an alert and continues to use the old permissions list until the VM reboots. At that time, if the permissions list still contains invalid local accounts, the Policy Agent raises an alert and does not enable *any* access controls on the disk.

Whenever a Windows VM reboots, regardless of whether there have been any changes to the associated Access Control Policies, the Policy Agent re-verifies the entries in the each policy's permissions list on each protected disk. If all of the local user account entries are still valid for an individual disk, the Policy Agent enables the Access Control Policy on the disk. Otherwise, the Policy Agent raises an alert and does not enable *any* access controls on the disk.

As with the initial policy application, if a policy's permissions list contains AD accounts that have since been removed from AD, the Policy Agent ignores the non-existent accounts and implements the rest of the Access Control Policy.

This section includes:

- Deleting an Access Control Policy
- Removing Access Controls from a Disk
- Viewing the Access Control Status for a Disk
- Associating an Access Control Policy with a Disk
- Enabling Access Controls on a Linux VM
- Viewing the Change History for an Access Control Policy
- Changing a Windows Access Control Policy
- Changing a Linux Access Control Policy
- Creating a Windows Access Control Policy
- Creating a Linux Access Control Policy
- Changing the AD Server Configuration
- Managing Active Directory Server Associations
- Associating an AD Server with a Cloud Administration Group
- Windows Access Control Rule Recommendations and Considerations
- Windows Access Control Rule Processing
- Access Control Rule Types
- Implementation Differences Between Linux and Windows
- Access Control Requirements and Considerations

Deleting an Access Control Policy

You can delete an Access Control Policy as long as that policy is not currently associated with a disk.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Navigate to the **Access Control Policies** tab.
4. Click the policy that you want to delete and select **Actions > Remove Policy**.
   The Cryptographic Security Platform Vault webGUI displays a message indicating whether the policy was successfully deleted.

Removing Access Controls from a Disk

You need to remove the Access Control Policy from a disk if you want to decrypt that disk. For Linux, you also need to remove the policy if you want to move the disk from one VM to another or if you want to back up your Cryptographic Security Platform Vault configuration.

For Windows, you can remove an Access Control Policy from an individual Windows disk while leaving the others protected. In Linux, removing the Access Control Policy from one disk removes it from all disks on the VM. In addition, a Linux VM must be rebooted in order for to fully remove the access controls. This reboot happens automatically at the VM's next heartbeat after you complete this procedure.

Important: For Linux, it is essential that you use this procedure to cleanly remove the Access Control Policy from the VM. Do not simply revoke the authentication or remove the VM from Cryptographic Security Platform Vault without first removing the Access Control Policy and rebooting the VM. Doing so may cause erroneous alerts and audit log messages.

Before You Begin

Make sure password-based SSH login is enabled for the VM. If it is not, the process will fail and the Access Control Policy will not be removed from the disks on the VM.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab.
4. Click the **Expand** button (**>**) at the end of the row associated with the VM whose disks you want to change. Cryptographic Security Platform Vault displays the details for the VM along with a VM-specific **Actions** button that allows you to manage the selected VM without affecting other VMs registered with Cryptographic Security Platform Vault.
5. In the Details area, click the **Encrypted Disks** tab.
6. Click on the data disk from which you want to remove the Access Control Policy and select **Actions > Remove Policy from Disk** from the VM-specific **Actions** button.
   At the selected VM's next heartbeat, the Entrust Policy Agent removes the Access Control Policy from the selected Windows disk or Linux VM. If it is a Linux VM, the Policy Agent also reboots the VM to complete the removal process.

What to Do Next

If you want to force an update so that the Access Control Policy is removed before the next scheduled heartbeat, you can log into the VM as an administrator and use the `hcl heartbeat` command.

Important: For a Linux disk, the `hcl heartbeat` command may take a few minutes to complete while the policy is being removed. If you use this command, make sure you wait for it to complete because interrupting the policy removal process may cause issues on the VM. The Policy Agent automatically reboots the VM as soon as the `hcl heartbeat` command has finished.

Viewing the Access Control Status for a Disk

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab and select the VM that contains the disk.
4. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
5. Click the **Encrypted Disks** tab and select the disk whose Access Control Policy you want to see. Cryptographic Security Platform Vault displays the **Policy Name** and **Policy Status** properties for the selected disk below the table.
   The policy status can be:
   - **Enabled**—The policy has been successfully associated with the disk and all entries in the permissions list have been validated by the Entrust Policy Agent.
   - **Update Pending**—The policy shown in the **Policy Name** field is either being associated with the disk for the first time or there is a new version of the policy that has not yet been applied to the disk. If the process completes successfully, a message appears in the Cryptographic Security Platform Vault Audit Log and the status changes to **Enabled**. If it fails, Cryptographic Security Platform Vault displays an Alert and does not change the policy status until the issue is fixed.
   - **Disabled**—No policy is currently associated with the disk.

Associating an Access Control Policy with a Disk

You can enable access controls on any Windows or Linux data disk that has been encrypted by Cryptographic Security Platform Vault. Access controls are not supported on Windows boot disks, Linux root or swap disks, or unencrypted data disks.

Before You Begin

- Make sure the disk meets the requirements described in Access Control Policies.

- Make sure you know what Access Control Policy you want to associate with the disk. For Windows, you can use any Windows Access Control Policy for any disk. For Linux, if one Access Control Policy has been applied to another disk on this VM, you must use the same Access Control Policy for this disk.
- If this is a Linux disk:
  - Make sure access controls have been enabled on the VM as described in Enabling Access Controls on a Linux VM.
  - Make sure password-based SSH login is enabled for the Linux VM. If it is not, the process will fail and the Access Control Policy will not be associated with the disk.
  - If this is the first time you are associating an Access Control Policy with the disk, make sure that any currently-active users accessing that disk know that they will lose access as soon as the Policy Agent validates the Access Control Policy. The first time an Access Control Policy is successfully associated with a disk, all Allowed users must log out and log back in before they can continue to access the files and data blocks on the disk.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab.
4. Click the **Expand** button (**>**) at the end of the row associated with the VM whose disks you want to protect. Cryptographic Security Platform Vault displays the details for the VM along with a VM-specific **Actions** button that allows you to manage the selected VM without affecting other VMs registered with Cryptographic Security Platform Vault.
5. In the Details area, click the **Encrypted Disks** tab.
6. In the list of disks, click on the data disk that you want to associate with an Access Control Policy and select **Actions > Add Policy to Disk** from the VM-specific **Actions** button.
   Tip: If the **Add Policy to Disk** option is not available for a Linux disk, make sure access controls have been enabled on the VM as described in Enabling Access Controls on a Linux VM.
7. In the Available Policies dialog box, select the policy that you want to use and click **Add Policy**.
   At the selected VM's next heartbeat, the Entrust Policy Agent attempts to associate the Access Control Policy with the selected disk. At this time, the Policy Agent verifies the permissions specified in the associated policy rules. If all permission entries are valid, the association is successful and access controls are enabled for that disk. The Policy Agent records the successful application of the policy in the Audit Log.
   Important: If any of the permissions list entries are invalid, the Policy Agent issues an alert and does *not* apply the Access Control Policy. If this is an update to an existing policy, what happens next depends on the type of disk. For Linux disks, the Policy Agent continues to use the previous version of the policy. For Windows disks, the Policy Agent continues to use the previous policy settings *until* the VM reboots. If the permissions list contains invalid entries when the Windows VM reboots, the Policy Agent disables *all* access controls for the disk.

What to Do Next

If you want to force an update so that the Access Control Policy is applied before the next scheduled heartbeat, you can log into the VMs as an administrator and use the `hcl heartbeat` command.

> Note: For a Linux disk, the `heartbeat` command may take a few minutes to complete the first time an Access Control Policy is associated with the disk. If you use this command, make sure you wait for it to complete because interrupting the policy association process may cause issues on the VM.

Enabling Access Controls on a Linux VM

Before you can associate an Access Control Policy with an encrypted Linux data disk, you need to enable access controls on the VM that contains the disk. This process must be done once for each VM that contains

a disk you want to protect, but after it has been set up you can associate an Access Control Policy with any number of encrypted data disks on that VM.

> Note: The following procedure is for Linux only. Access controls are automatically enabled for Windows disks.

Before You Begin

Make sure your Linux VM meets the requirements specified in Access Control Policies.

Procedure

1. Log into the VM as `root`.
2. Make sure that the following required packages are installed:
   - setools-console
   - selinux-policy-devel
   - sshpass

   If any of the required packages are not there, install them using the `yum install pkg-name` command.
3. Enter the command `rpm -ivh /opt/hcs/rpms/hytrust_accesscontrols-relnum-buildnum.noarch.rpm`, where `relnum-buildnum` is the rpm release and build number that you are using.
   For example:
   # rpm -ivh /opt/hcs/rpms/hytrust_accesscontrols-10.5.3-13239M.noarch.rpm

Viewing the Change History for an Access Control Policy

After you create an Access Control Policy, Cryptographic Security Platform Vault tracks the changes made to the policy details, rules, and permission lists. You can access the change history in for any policy in the Cryptographic Security Platform Vault webGUI.

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI on any node in the cluster using an account with Cloud Admin privileges in the Cloud Administration group under which you want to add the policy.
2. In the top menu bar, click **Workloads**.
3. Navigate to the **Access Control Policies** tab.
4. Select the policy whose change history you want to view in the list.
5. In the Policy Details area below the table, look at the **Version** field. If changes have been made since the policy was created, the Cryptographic Security Platform Vault webGUI displays the **View Change List** link. Click this link to view the Change Version History dialog box.
   Note: If the version number is higher than 1 but there is no **View Change List** link, that means the changes were made while the policy was being created. Cryptographic Security Platform Vault does not begin logging the changes until after the policy has been saved for the first time.
6. To view the details of a particular change, click any of the fields for that change. The Cryptographic Security Platform Vault webGUI displays the old version and the new version side by side.
   For Windows rules, the Changes in Version dialog box also contains a Rule Type field that identifies which kind of rule was changed. The Rule Type can be:
   - 1—Filesystem-Level Access Rule
   - 2—Block-Level Access Rule
   - 3—Filesystem-Level and Block-Level Access Rule
   - 4—Folder-Level Access Rule

   Note: In order to keep the changes easy to identify, Cryptographic Security Platform Vault creates a new version each time you click **Save** during the process. For example, if you add a permission for the user `fred` and click **Save**, that becomes a new version. If you then edit the permissions list again and add `martha`, that becomes a different version. If, however, you edit the permissions list and add `fred`, then

you click **Add Another** and add `martha` then you click **Save**, the addition of `fred` and `martha` are both part of the same version.

Changing a Windows Access Control Policy

You can change the name, description, or permissions lists associated with an existing Access Control Policy, but you cannot change the OS Type or Cloud Administration Group for the policy. You also cannot change the Rule Type associated with a Windows Access Control Rule.

If a VM contains one or more disks associated with the policy you are changing, Cryptographic Security Platform Vault communicates the changes at the VM's next heartbeat. If the policy is associated with disks on more than one VM, this means that policy changes may not take effect on all associated disks at the same time because the VMs may be on different heartbeat schedules. If you want to force the update on a particular VM immediately, you can use the `hcl heartbeat` command on that VM.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Navigate to the **Access Control Policies** tab.
4. Click on the policy you want to change. The Cryptographic Security Platform Vault webGUI displays details about the policy and its associated rules in the Details area under the Policy table.
5. Select **Actions > Edit Policy**.
6. On the Details tab in the Edit Policy Wizard Details wizard, you can change the policy name or description if desired. You cannot change the OS Type or the Cloud Administration Group specified for the policy.
7. If you want to edit the rules associated with the policy, click the **Rules** tab and do any of the following:
    - To add a new rule type, click **Add**. You can specify one filesystem-level rule, one block-level access rule, and any number of folder-level rules per policy.
    - To delete an existing rule, click the associated selection check box and click **Delete**.
      Note: The rule list cannot be empty, so you can only delete a rule if a second rule already exists in the list.
    - To change an existing rule, click the associated selection check box and click **Edit**. On the **Details** tab you can change the rule name or description, but you cannot change the rule type. If you want to change the rule's permissions list, click the **Permissions** tab and make the desired changes. Make sure that any entries you add contain a valid local VM user or group name, an NT service name, or a valid Active Directory (AD) user or group name.
      Important: If any of the local users in the permissions list are invalid, the Policy Agent issues an alert and does *not* apply the Access Control Policy. If access controls were already enabled for the disk, the Policy Agent continues to use the previous access control settings until the VM reboots. If the permissions list contains invalid entries when the VM reboots, the Policy Agent disables *all* access controls for the disk.
      We strongly recommend that you *only* specify AD users and groups so that the removal of a local user account cannot invalidate the entire Access Control Policy. If the Policy Agent encounters an invalid AD account entry, it simply ignores that entry and enables the rest of the Access Control Policy.
      For security reasons, we also recommend that you do not add SYSTEM as a whitelisted user.
      For the domain, you can select one of the following:
        - Local—This account is local to the Windows VM.
        - NT Service—This is a virtual account under which a Windows Service is running on the VM.
        - *AD-Domain-Name*—This account comes from the selected domain in the AD defined for the Cloud Admin Group associated with this policy.

      Note: The permissions list for a filesystem-level rule or a folder-level rule cannot be empty, so you cannot select all entries and click **Delete**. You must first de-select at least one entry before you can delete the others.

If any of the entries in the permissions list are groups, make sure the order of the entries is correct. When the Policy Agent receives an access request, it processes the permissions list in order, from top to bottom. As soon as it finds an entry that matches the account that requested the data, it assigns that permission level to the user and stops processing the permissions list. If you have added an entry to deny a particular user access but the user is part of a group that was granted permission higher in the list, that user's request for access will be granted. For details, see Windows Access Control Rule Processing.

8. When you are finished changing the policy, click **Done**. Cryptographic Security Platform Vault applies the changes to the associated disks the next time the VMs containing those disks heartbeat with Cryptographic Security Platform Vault.

What to Do Next

If you want to force an update on one or more VMs so that the Access Control Policy changes are applied before the next scheduled heartbeat, you can log into the VMs as an administrator and use the `hcl heartbeat` command.

Changing a Linux Access Control Policy

You can change the name, description, or permissions list associated with an existing Access Control Policy, but you cannot change the OS Type or Cloud Administration Group for the policy.

If a VM contains one or more disks associated with the policy you are changing, Cryptographic Security Platform Vault communicates the changes at the VM's next heartbeat. If the policy is associated with disks on more than one VM, this means that policy changes may not take effect on all associated disks at the same time because the VMs may be on different heartbeat schedules.

Before You Begin

Make sure password-based SSH login is enabled for the VM. If it is not, the process will fail and the Access Control Policy will not be updated on the VM. For details, see Access Control Requirements and Considerations.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Navigate to the **Access Control Policies** tab.
4. Click on the policy you want to change. The Cryptographic Security Platform Vault webGUI displays details about the policy and its associated rules in the Details area under the Policy table.
5. If you want to change the policy name or description, select **Actions > Edit Policy**. In the Edit Policy Wizard Details page, change the policy name or description if desired. You cannot change the OS Type or the Cloud Administration Group specified for the policy.
6. To edit the existing rule, select **Actions > Edit Rule** and make the desired changes. Make sure that any entries you add contain a valid local VM username. Cryptographic Security Platform Vault does not support domain-qualified usernames in Linux.
7. When you are finished, click **Done**. Cryptographic Security Platform Vault saves the rule changes immediately and applies them to the associated disks the next time the VMs containing those disks heartbeat with Cryptographic Security Platform Vault.

What to Do Next

If you want to force an update on one or more VMs so that the Access Control Policy changes are applied before the next scheduled heartbeat, you can log into the VMs as an administrator and use the `hcl heartbeat` command.

Important: The `heartbeat` command may take a few minutes to complete the first time an Access Control Policy is associated with the disk. If you use this command, make sure you wait for it to complete because interrupting the policy association process may cause issues on the VM.

Creating a Windows Access Control Policy

Windows Access Control Policies can control who can access the files and folders on a disk, who can access the data blocks on a disk, or both. The rules are independent, which means that you create one list of users who have filesystem-level access, another list who have folder-level access, and a third list who have block-level access. You can specify both local and Active Directory (AD) users and groups in the rule permission lists.

We recommend that you create a least a filesystem-level access rule and a block-level access rule in all Windows Access Control Policies so that your data disks are fully protected. We also recommend that you include only AD users and groups in your permissions lists. For more information, see Windows Access Control Rule Recommendations and Considerations.

The following procedure describes how to create a Windows Access Control Policy. For Linux, see Creating a Linux Access Control Policy.

Before You Begin

- Make sure you have reviewed the requirements and recommendations described in Access Control Policies.
- Make sure you know the Cloud Administration group under which you want to add the Access Control Policy. Each policy can be associated with one and only one Cloud Administration group.
- If you intend to include AD users or groups, make sure an AD server has been associated with the Cloud Admin Group under which you intend to add the policy. For details, see Managing Active Directory Server Associations and Associating an AD Server with a Cloud Administration Group.
- If you intend to add Active Directory groups to your permissions lists, make sure you know what order the groups should be in. For details, see Windows Access Control Rule Processing and Windows Access Control Rule Recommendations and Considerations.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI on any node in the cluster using an account with Cloud Admin privileges in the Cloud Administration group under which you want to add the policy.
2. In the top menu bar, click **Workloads**.
3. Navigate to the **Access Control Policies** tab.
4. **Select Actions > Create Policy**.
5. In the Create Policy Wizard Details page, enter the following information:

Field	Description
Name	Enter a name for the Access Control Policy (1-256 characters). The name can include special characters and spaces.
OS Type	Select Windows. Note: You cannot change the OS Type after the policy has been saved.
Cloud Administrator Group	Select the Cloud Admin Group with which this policy should be associated. Note: You cannot change the group after the policy has been saved.

Field	Description
Description	Enter an optional description for the policy. This description is displayed in the Cryptographic Security Platform Vault webGUI when a user selects the Access Control Policy to associate with the disk.

6. When you are done, click **Next**.
7. In the Rules page, click **Add rule now**.
8. In the Create Rule Wizard Details page, enter the following information:

Field	Description
Name	Enter a name for the Access Control Rule (1-256 characters). The name can include special characters and spaces and it does not need to be unique.
Description	Enter an optional description for the rule.
Rule Type	Select the rule type. • **Filesystem-level Access** controls who can access the files and folders on the disk as long as those folders are not protected by a specific folder-level rule. This type of rule covers the majority of users. You can have one filesystem-level rule per policy. • **Folder-level Access** controls who can see the files and subfolders in a specific folder on the disk. All subfolders in the specified folder automatically inherit the same access permissions unless they are protected by their own folder-level rule. You can have as many folder-level rules as needed. • **Block-level Access** controls who can access the blocks on the disk. Generally, only a few applications, such as backup utilities, require block-level access. You can have one block-level rule per policy.
Folder	If the rule type is Folder-level Access, enter the path to the folder you want to protect in this field. You can enter only one folder path per rule. If the specified folder contain subfolders, those subfolders inherit the same access permissions list as the parent folder. To override the default inheritance, enter a separate rule for both the parent folder and the subfolder. For example, you could restrict the folder `\HR` to only those users who are in the HR department but you could make the subfolder `\HR\employee_public` accessible to all employees in the company.

9. When you are finished, click **Next**.
10. In the Permissions page, click **Add permission now**.
    Note: If this is a block-level access rule, you do not have to add a user to the permission list if you do not want anyone to be able to access the data blocks on the disk. If this is a filesystem-level or folder-level access rule, you must add at least one user to the permissions list.
11. In the Create Permission dialog box, enter the following information:

Field	Description
User or Group Name	Enter a user or group name. The user or group can be local or can come from Active Directory. Important: If any of the local users in the permissions list are invalid, the Policy Agent issues an alert and does *not* apply the Access Control Policy. If access controls were already enabled for the disk, the Policy Agent continues to use the previous access control settings until the VM reboots. If the permissions list contains invalid entries when the VM reboots, the Policy Agent disables *all* access controls for the disk. We strongly recommend that you *only* specify AD users and groups so that the removal of a local user account cannot invalidate the entire Access Control Policy. If the Policy Agent encounters an invalid AD account entry, it simply ignores that entry and enables the rest of the Access Control Policy. For security reasons, we also recommend that you do not add SYSTEM as a whitelisted user.
Domain	You can select: • Local—This account is local to the Windows VM. • NT Service—This is a virtual account under which a Windows Service is running on the VM. • *AD-Domain-Name*—This account comes from the selected domain in the AD defined for the Cloud Admin Group associated with this policy.
Permission	Specify whether the user should be allowed or denied access to the data on the disk. The default permission is "Deny" for all users not explicitly allowed or not included in an explicitly-allowed group.

12. If you want to add another user to the permissions list, click **Add Another**. Otherwise, click **Save**.
13. If any of the entries in the permissions list are groups, make sure the order of the entries is correct. When the Policy Agent receives an access request, it processes the permissions list in order, from top to bottom. As soon as it finds an entry that matches the account that requested the data, it assigns that permission level to the user and stops processing the permissions list. If you have added an entry to deny a particular user access but the user is part of a group that was granted permission higher in the list, that user's request for access will be granted. For details, see Windows Access Control Rule Processing.
14. After you have added all of the required permissions and verified the order, click **Add Rule**.
15. If you want to add another rule, click the blue **+** (Plus sign) above the table and repeat the steps above.
16. When you have added all of the necessary rules, click **Create Policy**.

What to Do Next

Associate the Access Control Policy with one or more Windows data disks as described in Associating an Access Control Policy with a Disk.

Creating a Linux Access Control Policy

Linux Access Control Policies determine which local user accounts can access the data files and blocks on the associated Linux data disks. Each policy contains one rule with one permissions list, so you cannot differentiate between filesystem-level controls and block-level controls. The default permission is "Deny" for

all accounts, so the permissions list is a whitelist of the accounts that are allowed to access the data on the disk.

The permission list can contains local VM users only. You cannot specify a domain-qualified user account. This means that any protected disk will block all remote access user requests.

The following procedure describes how to create a Linux Access Control Policy. For Windows, see Creating a Windows Access Control Policy.

Before You Begin

Make sure you have reviewed the requirements and recommendations described in Access Control Policies.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI on any node in the cluster using an account with Cloud Admin privileges in the Cloud Administration group under which you want to add the policy.
2. In the top menu bar, click **Workloads**.
3. Navigate to the **Access Control Policies** tab.
4. Select **Actions > Create Policy**.
5. In the Create Policy Wizard Details page, enter the following information:

Field	Description
Name	Enter a name for the Access Control Policy (1-256 characters). The name can include special characters and spaces.
OS Type	Select Linux. Note: You cannot change the OS Type after the policy has been saved.
Cloud Administrator Group	Select the Cloud Administration Group with which this policy should be associated. Note: You cannot change the Group after the policy has been saved.
Description	Enter an optional description for the group. This description is displayed in the Cryptographic Security Platform Vault webGUI when a user selects the Access Control Policy to associate with the disk, so we recommend that you use this field so other Cloud Admins can be sure that they are selecting the correct policy.

6. When you are done, click **Next**.
7. In the Rules page, click **Add rule now**.
8. In the Create Rule Wizard Details page, enter a name and description for the Access Control Rule. For Linux, you can only create one rule that applies to both filesystem-level access and block-level access.
9. When you are finished, click **Next**.
10. In the Permissions page, click **Add permission now**.
    You must add at least one user to the permissions list before you can save the Access Control Policy.
11. In the Create Permission dialog box, enter a local VM account name that will be allowed to access the data on the disk. Cryptographic Security Platform Vault does not support domain-qualified usernames for Linux.
    For security reasons, you cannot add `root` to the permissions list.

Important: If any of the permissions list entries are invalid, the Policy Agent does *not* apply the Access Control Policy. If access controls were already enabled for the disk, the Policy Agent continues to use the previous access control settings.

12. If you want to add another user to the permissions list, click **Add Another**. Otherwise, click **Save**.
    Note: A Linux Access Control Policy can only contain one rule, and only one Access Control Policy can be associated with a specific Linux VM, so this permissions list must include all users who are authorized to access the files and data blocks on all protected disks on the VM.
13. After you have added all of the required permissions, click **Add Rule**.
14. Click **Create Policy**.

What to Do Next

Associate the Access Control Policy with one or more Linux data disks as described in Associating an Access Control Policy with a Disk.

Changing the AD Server Configuration

You can change all AD server properties except for the associated Cloud Admin group. Once an AD server has been associated with a group, it cannot be re-associated with a different group. If you are using LDAPS or LDAP with the STARTTLS option, you do not need to re-upload the AD server's CA certificate unless you change the server URL or you enable STARTTLS for an LDAP server connection.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Navigate to the **Active Directory** tab.
4. Click on the AD server you want to edit and select **Actions > Edit Active Directory**.
5. In Edit Add Active Directory Server dialog box, specify the options you want to use.

Field	Description
Cloud Admin Group	The Cloud Administration group with which this AD server is associated. You cannot change the group association.
Server URL	The AD domain controller IP address or hostname. Select `LDAP://` or `LDAPS://` from the drop-down list and enter the controller's URL in the text field. To include a port number, specify `:port` after the name. For example, `10.238.66.33:389`. Cryptographic Security Platform Vault does *not* support multiple AD domain controllers defined in the same Server URL field. If you want to use multiple domain controllers, you need to add a separate entry for each controller. Important: Enter the URL of your AD domain controller, not the URL of a specific AD domain. If you use a specific AD domain, you may encounter authorization issues the next time you upgrade Cryptographic Security Platform Vault.

Field	Description
STARTTLS	Enable this option if you want Cryptographic Security Platform Vault to use Transport Layer Security (TLS) protocol when communicating with the AD server. If you select this option, you must upload a CA certificate for the AD server. Note: This option is only available if the Server URL starts with `LDAP://`.
Service Account	The AD account that Cryptographic Security Platform Vault should use when logging into the AD server. Specify the account using one of the following formats: • Distinguished Name (DN). For example, `CN=Administrator,CN=users,DC=<company-name>,DC=com` • User Principal Name (UPN). For example, `administrator@<company-name>.com`. • Account username. For example, `administrator`. The AD account is usually an administrative user and it can have read only permissions on the AD server.
Service Account Password	The password for the Service Account.
CA Certificate	If you changed the Server URL and you are using `LDAPS://` or have selected the STARTTLS option for `LDAP://`, click Load File and select the CA certificate for the AD server.

6. When you are done, click **Save**.

Managing Active Directory Server Associations

To view the AD server associations defined for the Cloud Administration groups that your Cryptographic Security Platform Vault user account is a member of, do the following:

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Navigate to the **Active Directory** tab.

From this tab, if you want to:

- Create a new AD server association, select **Actions > Add Active Directory**. For details, see Associating an AD Server with a Cloud Administration Group.
- Edit an existing AD server association, click on the AD association and select **Actions > Edit Active Directory**. For details, see Changing the AD Server Configuration.
- Delete an existing AD server association, click on the AD association and select **Actions > Remove Active Directory**, then confirm the deletion at the prompt.

Associating an AD Server with a Cloud Administration Group

If you want to add AD users and groups to the permissions lists for your Windows Access Control Policies, you need to associate at least one AD server with each Cloud Administration group in which you plan to create these policies. After you have associated the AD server with the Cloud Administration group, Cloud Admins can select the appropriate AD domain for each user from a drop-down list.

If you want to use the same AD server for multiple groups, you need to associate the server with each one of the groups individually. There is no default AD server association.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Navigate to the **Active Directory** tab.
4. Select **Actions > Add Active Directory**.
5. In the Add Active Directory Server dialog box, specify the options you want to use.

Field	Description
Cloud Admin Group	Select the Cloud Administration group with which this AD server should be associated. Note: You cannot change the group name after you save the AD server.
Server URL	The AD domain controller IP address or hostname. Select `LDAP://` or `LDAPS://` from the drop-down list and enter the controller's URL in the text field. To include a port number, specify `:port` after the name. For example, `10.238.66.33:389`. Cryptographic Security Platform Vault does *not* support multiple AD domain controllers defined in the same Server URL field. If you want to use multiple domain controllers, you need to add a separate entry for each controller. Important: Enter the URL of your AD domain controller, not the URL of a specific AD domain. If you use a specific AD domain, you may encounter authorization issues the next time you upgrade Cryptographic Security Platform Vault.
STARTTLS	Enable this option if you want Cryptographic Security Platform Vault to use Transport Layer Security (TLS) protocol when communicating with the AD server. If you select this option, you must upload a CA certificate for the AD server. Note: This option is only available if the Server URL starts with `LDAP://`.

Field	Description
Service Account	The AD account that Cryptographic Security Platform Vault should use when logging into the AD server. Specify the account using one of the following formats: • Distinguished Name (DN). For example, `CN=Administrator,CN=users,DC=<company-name>,DC=com` • User Principal Name (UPN). For example, `administrator@<company-name>.com`. • Account username. For example, `administrator`. The AD account is usually an administrative user and it can have read only permissions on the AD server.
Service Account Password	The password for the Service Account.
CA Certificate	If you are using `LDAPS://` or have selected the STARTTLS option for `LDAP://`, click Load File and select the CA certificate for the AD server.

6. When you are done, click **Add**.

Windows Access Control Rule Recommendations and Considerations

- Due to security issues that can arise when using local accounts, we recommend that you only add users and groups from Active Directory (AD). If a System Administrator removes a local account that has been included in the permissions list for an Access Control Policy and reboots the VM, the Policy Agent disables access controls but leaves the encrypted disk attached. This cannot happen if all users and groups in the permissions list come from AD, because if the Policy Agent finds an invalid AD account in the permissions list it just ignores that account and implements the rest of the Access Control Policy.
- If your rule definition includes AD groups, we recommend that you:
  - Put all of the individual local and AD user permissions first. The order of the individual users does not matter as long as the entries are unique.
  - Put all of the AD group permissions after the individual users, making sure that you have the correct order of precedence so that users are not being granted permission to access data they should not access or being denied permission to access data they need.
  - Make sure you allow access to the smallest AD groups possible. For example, if you have a group that includes all the developers in your company and smaller sub-groups that are specific to each product line, try to use the product-specific groups unless everyone in development truly needs access to the data.
- If an AD account that is included in one or more permissions lists is deleted and later re-added to AD, you need to delete that account and re-add it to any relevant permissions lists as well.

Windows Access Control Rule Processing

The permissions list for a Windows Access Control Rule can contain both individual users as well as user groups. For each entry, you can also specify whether the user or group is to be Allowed or Denied access to the associated disk or folder. This allows you to give access permission to an entire AD group while denying access to specific members in that group.

When determining a user's permission level, the Entrust Policy Agent uses the order of the entries in the Access Control Rule. As soon as it finds a match for the user requesting access, it allows or denies access to that user based on the matching entry and stops processing the permissions list. If the first entry is "Allow", it allows the user access even if there is a rule further down the list that denies the user access.

For example, let's say you want to give access permissions to the AD group `development-all` but deny access to the sub-group `development-interns` and the individual users Joe Smith (`jsmith`) and Mary Carson (`mcarson`) because they are both temporary contractors. In order to do this, you would specify the following permissions in the rule:

User or Group Name	Domain	Permission
jsmith	mycompany.com	Deny
mcarson	mycompany.com	Deny
development-interns	mycompany.com	Deny
development-all	mycompany.com	Allow

If the AD user `jsmith` , `mcarson` , or one of the users listed in `development-interns` logs in, they will be denied access even if they are a member of the group `development-all` because the Deny entries come before `development-all` in the list. If someone signs into the VM locally, access to the data will be denied because no local users are defined in the permissions list.

However, let's say the permissions list looked like this:

User or Group Name	Domain	Permission
development-all	mycompany.com	Allow
jsmith	mycompany.com	Deny
mcarson	mycompany.com	Deny
development-interns	mycompany.com	Deny

Now if the AD user `jsmith` , `mcarson` , or one of the users listed in `development-interns` logs in, the Policy Agent will *grant them access* if they are a member of the group `development-all` , because the `development-all` group comes first in the list and all members of that group are automatically allowed access regardless of the other entries in the permissions list.

Access Control Rule Types

Linux Access Control Rule Type

Linux only allows one type of Access Control Rule, and it controls local user access to both the files and blocks on the associated disks. Because the default is to deny access to the disk, the Linux policy rule is basically a "whitelist" of the users who can access the files and data blocks on the encrypted disk.

Entrust supports only local Linux users. You cannot add domain-qualified user names to the access control rule.

Windows Access Control Rule Types

For Windows, there are three types of Access Control Rules that you can create:

- **Filesystem-Level Access Rules** control which local VM users, local VM groups, Active Directory (AD) users, and AD groups can access the files on the encrypted disk. This is the standard type of disk access and a majority of users will be covered by these rules. You can have one filesystem-level rule per disk.
- **Folder-Level Access Rules** control which local VM users, local VM groups, Active Directory (AD) users, and AD groups can access the files and subfolders in a specific folder on the encrypted disk. As soon as you apply one or more folder-level access rules to a disk, the folders protected by those rules can only be seen by those users who have been granted specific permission to view those folders. You can have as many folder-level rules per disk as you need.
- **Block-Level Access Rules** control which local VM users, local VM groups, AD users, and AD groups can access the individual blocks on the encrypted disk. We highly recommend that you create a block-level access rule in every Windows Access Control Policy that you create and that you make sure the permissions list is kept up to date because block-level access can be used by hackers to bypass filesystem-level restrictions. Only those programs that legitimately require block-level access (such as back up utilities) should be included on the permissions list. You can have one block-level access rule per disk.

Each rule you include in an Access Control Policy functions independently with its own permissions list. Adding a filesystem-level or folder-level access rule does *not* turn on block-level restrictions, and adding a block-level rule does *not* turn on filesystem-level or folder-level restrictions. In addition, users with filesystem-level access to the disk will *not* be able to see the folders protected by a folder-level access rule unless they are included in *both* the filesystem-level rule and in the folder-level access rule.

> Note: We recommend that you include only AD users and groups in the permissions list for all three rule types. If you specify an invalid local user account, or if a local user account on the permissions list is deleted after the Access Control Policy has been applied, the next time the Policy Agent validates the permissions list the entire Access Control Policy will fail validation and the Policy Agent will disable *all* access controls on the disk. For more information, see Windows Access Control Rule Recommendations and Considerations.

For all rules, the order of the entries in the rule determines how permission conflicts are resolved. For details, see Windows Access Control Rule Processing.

Implementation Differences Between Linux and Windows

Linux and Windows allow different types of access controls. The following topic summarizes the differences in how access controls behave on these two platforms.

Access Control Rule Types

Windows supports three types of access control rules: folder-level access, filesystem-level access, and block-level access. Folder-level access determines who can see the files and subfolders in specific folders on a disk. Filesystem-level access controls who can see all of the files and folders on the disk as long as those folders are not protected by a specific folder-level access rule. Block-level access determines who can

access the data blocks on the disk. Windows allows you to have one permission list for each rule type, so users who have filesystem-level access may not be able to see certain folders that are protected by a folder-level rule, and users who have folder-level access may not be able to see any of the other files on the disk.

Linux only supports one type of access control rule, and that rule determines who can have access to the both the files and the data blocks on the disk.

For details, see Access Control Rule Types.

Remote Users and User Groups

For Windows, you can include remote users and groups from Active Directory (AD) as well as local users and groups defined on the Windows VM. Because you can include groups, Windows also allows you to specify to whom access should be denied as well as to whom it should be granted.

For example, you could allow access to the group `development-all` but deny access to the sub-group `development-interns`. Permission conflicts are resolved using the order of precedence defined in the rule. For details, see Windows Access Control Rule Processing and Windows Access Control Rule Recommendations and Considerations.

For Linux, you can only include local user accounts in the permissions list. Local groups or remote users and groups are not supported. Therefore, the permission list for an Access Control Policy is a simple whitelist of local user accounts that can access the files and data blocks on the associated disks.

Access Control Policy Application and Re-Verification

If a Windows Access Control Policy contains invalid local user accounts when the Policy Agent verifies the Access Control Policy, the Policy Agent raises an alert and does one of the following:

- If this is the first time a policy is being associated with the disk, or if the Windows VM has just rebooted, the Policy Agent does not apply *any* access controls to the disk.
  Note: During policy validation, the Policy Agent ignores non-existent Active Directory accounts. It only disables access controls if there are invalid local accounts.
- If the Policy Agent is verifying a new version of the policy that it received from the Cryptographic Security Platform Vault for VM Encryption, the Policy Agent does *not* apply the new version. Instead, it continues to use the previous version of the policy until the VM reboots. On reboot, the application of the policy is always all-or-nothing. If the current version of the policy contains invalid local accounts on reboot, the Policy Agent always disables all access controls, even if a previous version of the policy exists.

If a Linux Access Control Policy contains invalid local user accounts when the Policy Agent verifies the Access Control Policy, the Policy Agent raises an alert. If this is the first time a policy is being associated with the disk, the Policy Agent does not apply *any* access controls to the disk. If a previous version of the policy has been successfully verified for the disk, the Policy Agent uses that version of the policy. The Policy Agent only verifies the permissions list when an Access Control Policy is first associated with the VM or when changes to the Access Control Policy are communicated to the VM from Cryptographic Security Platform Vault. The Policy Agent does not re-verify the permissions list when the Linux VM reboots.

Associating Access Control Policies with Multiple Disks on a VM

Windows allows you to associate different Access Control Policies with different disks and different folders on the same VM. You can also remove an Access Control Policy from one disk or folders without affecting any of the other disks or folders on the VM.

Linux requires you to use the same Access Control Policy for all disks on the same VM. In addition, if you remove the Access Control Policy from one disk, the Policy Agent removes it from all disks on the VM.

Access Control Requirements and Considerations

Platform Requirements

Platform	Supported Versions
Linux	RHEL 8 and above. Oracle Linux 8 and above.
Windows	All Windows platforms supported by Cryptographic Security Platform Vault.

General Requirements and Considerations

- You can only associate an Access Control Policy with a data disk encrypted by Cryptographic Security Platform Vault for VM Encryption.
  You cannot associate a policy with an unencrypted data disk, a data disk encrypted by some application other than Cryptographic Security Platform Vault for VM Encryption, or with a boot disk (even if the boot disk is encrypted by Cryptographic Security Platform Vault for VM Encryption).
- If a disk is associated with an Access Control Policy, system administrators can still perform basic disk management functions such as creating mount points or adding, expanding, or shrinking partitions. They cannot, however, decrypt the disk until they remove the Access Control Policy.
- If you want to protect a disk accessed by Application Services (such as a web server), make sure all Application Services and Programs run under specific user accounts that you can add to the permissions list.
- The Access Control Policy creates a user "htadmin". Before associating a policy, make sure you don't already have a predefined user named "htadmin" in the VM.

Linux-Only Requirements and Considerations

- With Linux, you can create only one Access Control Rule per policy that provides a "whitelist" of local VM user accounts that can access both files and blocks on the disk. You can't grant file access while denying block access to a particular user, nor can you grant access to a domain-qualified user name.
- If you want to use an Access Control Policy on a Linux VM, you need to install three SELinux packages and an Entrust-supplied rpm package. For details, see Enabling Access Controls on a Linux VM.
- For security reasons, you cannot enable an Access Control Policy on a VM with any custom SELinux configuration settings or modules. If the Policy Agent finds any such customizations, the policy association will fail.
  Important: After you associate an Access Control Policy with a Linux VM, do *not* customize any SELinux configuration settings or modules. If you do so, the interaction between the SELinux customizations and the access controls could cause data loss.
  In addition, if the Policy Agent determines that any Entrust SELinux policies have been removed or that SELinux has been disabled or tampered with in any way (as could be done with a custom SELinux policy), the Policy Agent prevents the disk from being attached and access to the data will be lost.
- The `hcld` daemon must be run by the `root` user.
- One of the supported Linux filesystems must already exist on the disk before you can associate it with an Access Control Policy.
- You can associate one and only one Access Control Policy with one or more data disks on a specific VM. Linux does not support using different Access Control Policies for different disks on the same VM.
- Once the Policy Agent enables access controls on a disk, users on that disk operate in a custom SELinux environment, which can restrict certain sudo actions.

In addition, users with root privileges are blocked from performing operations such as file system checks or data backup for any access-controlled disks on the VM.

- If you apply an Access Control Policy for the first time while users are actively using the disk, all logged-in users will immediately lose access to the disk, even if they are included in the permissions list. Allowed users must log out and log back in before they can continue accessing the files and data blocks on the disk.
  If you apply a valid update to an existing Access Control Policy, the Policy Agent verifies that all active users are still included in the permissions list. If they are, those users can continue to access the disk as normal. If any currently active users have been removed from the permissions list, the Policy Agent automatically logs them out as soon as it validates the new version of the Access Control Policy.
  In either case, if the Access Control Policy contains invalid users, the Policy Agent does *not* apply that version and does not validate currently active users. This means that if you want to block a currently active user from accessing the disk, the Access Control Policy version you apply must be valid before the Policy Agent logs off the now-unauthorized user.
- If you want to move a disk to another registered VM in the same Cloud VM Set, you must first remove the Access Control Policy from the Linux disk before you move it. Access Control Policies do not move with the Linux disk.
- If you import a disk into a VM that is already associated with an Access Control Policy, the Access Control Policy is not automatically associated with the new disk. You must explicitly associate the Access Control Policy with the imported disk.
- If the Linux VM has multiple disks protected by the Access Control Policy, you cannot remove the Access Control Policy from only one of those disks. Policy removal is an all-or-nothing operation, so if you remove the Access Control Policy from one disk, the Policy Agent removes it from all disks and reboots the VM. You must then re-associate the policy with the disks that you want to protect.
- The VM must support creating local user accounts, as some access control functions require the Policy Agent to create (and then delete) a temporary local user account as needed.
- Enable password-based SSH login on the VM if you want to add, change, or remove an Access Control Policy, because setting and enforcing SELinux policies requires SSH login as an Entrust-admin. The superuser cannot perform these activities. After you successfully associate the policy, you can disable password-based SSH login until you need to associate the policy with a different disk or change or remove the existing policy.
  If you attempt to add, change, or remove an Access Control Policy and password-based SSH login is not enabled, the attempt will fail, and the following message will be displayed in the Cryptographic Security Platform Vault Audit Log:
  `Error enforcing policy <policy name>, version <version no> on VM <vmname>. Check if password-based SSH login is enabled on the VM.`
  Note: Password-based SSH login is enabled by default for most Linux systems, but it is *disabled* by default for VMs in an Amazon Web Services (AWS) or Microsoft Azure environment. For details about enabling it for those VMs, see your AWS or Azure documentation.
- To remove the VM from Cryptographic Security Platform Vault for VM Encryption, first remove the Access Control Policy associated with the VM by following the procedure described in Removing Access Controls from a Disk. This procedure also removes the Entrust SELinux customizations from the VM. If you remove the VM from the Cryptographic Security Platform Vault for VM Encryption without following this procedure, you may encounter issues accessing the data on the disk or with normal VM behavior because of these SELinux customizations. For this reason, the `hcl unregister` command will fail if an Access Control Policy is associated with the disk.
- To back up your Cryptographic Security Platform Vault for VM Encryption configuration, first remove any Linux Access Control Policies applied to your Linux disks. If you create the backup with any Linux Access Control Policies still active, you may be unable to access those VMs when you restore your Cryptographic Security Platform Vault for VM Encryption configuration from the backup file.
- When Access Control Policy is enabled on a Linux system, do not set up auto-mount on the access-controlled disk using hcl (for example, `hcl set mntpt=/mnt/sdd1 sdd1`), as the mount will fail on VM reboot, because

root is not allowed to access the disk. The workaround is to create a script to mount the access-controlled disk after the VM is rebooted, rather than using HCL commands to set up auto-mount.

Windows-Only Requirements and Considerations

- With Windows, you can protect the disk at the folder level, the file level, the data block level, or any combination of the three. Each protection type has a separate policy rule with its own permissions list. Each permissions list can contain users and groups that are either local to the VM or defined in Active Directory (AD). You can grant access to some users or groups while denying access to others so that you can grant access to an entire group but then deny access to selected members within the group. For details, see Windows Access Control Rule Processing and Windows Access Control Rule Recommendations and Considerations.
- Because local accounts can introduce security issues, we recommend adding only users and groups from Active Directory. If a System Administrator removes a local account included in the permissions list for an Access Control Policy and reboots the VM, the Policy Agent disables access controls but leaves the encrypted disk attached. This cannot happen if all users and groups in the permissions list come from AD, because the Policy Agent ignores non-existent AD accounts during policy verification and applies the rest of the Access Control Policy to the disk.
- Windows System Administrators can still use most Windows Disk Management Tools on access-controlled disks to perform basic disk management functions such as managing partitions, creating shadow volumes, and monitoring disk performance. However, they *cannot*:
  - Check for or fix errors on a disk by any means other than `chkdsk.exe`. Error checking is blocked for the Windows Disk Manager and the Windows Explorer Tools UI.
  - Format a volume with Windows Explorer. Instead, System Administrators need to format volumes with Windows Disk Manager, the `diskpart` CLI command, or `format.com`.
- If the data on the Windows disk is accessed by Windows Services, you need to add the Windows Service Accounts or the SYSTEM account under which the Services are running to the Access Control Policy permissions list. If you add SYSTEM, be aware that System Administrators will be able to run programs under the SYSTEM account.
  This is especially important for Active Directory disks, because AD will not boot if it cannot access the data through the SYSTEM account. For other applications, check the appropriate documentation to see if the program can run under a specific user account instead of using SYSTEM.
  Note: Most antivirus programs require that scheduled antivirus scans run under the SYSTEM account. This means that scheduled scans will be blocked on a disk protected by an Access Control Policy that does not allow access to SYSTEM. However, when an authorized user accesses a file on the protected disk, the on-access antivirus scan will work for most antivirus software, as that scan does not run under SYSTEM.
- An Access Control Policy is associated with a Windows disk, not a VM. You can associate different Access Control Policies with different disks on the same VM. If you move any of the disks from one VM to another, the associated Access Control Policy moves with the disk.
  The only caveat is if the disk was originally imported from another VM before you applied an Access Control Policy. In this case, if you move the disk back to the original VM after applying an Access Control Policy, the Access Control Policy does *not* move with the disk.
- If an unauthorized user attempts to access a protected disk, the Policy Agent adds an entry to the Cryptographic Security Platform Vault for the VM Encryption Audit Log. The log message specifies the file that the user tried to access, the login account associated with the request, the process name that made the request, and the name of the Access Control Rule that blocked the request.
- When you apply a valid Access Control Policy version to a disk while users are actively using that disk, the access controls take effect immediately. Active users with Allow permissions can continue accessing the disk as normal. Active users not listed in the permissions list, or those with Deny permissions, will immediately lose access to the files and data blocks on the disk.
- Do not apply an Access Control Policy to a parent volume that contains one or more folder mount points of access controlled volumes, because applying an Access Control Policy to the parent volume would flood

the Cryptographic Security Platform Vault for VM Encryption Audit Log. For example, if an Access Control Policy has been applied to `G:`, mounted on `N:` (`N:\GDrive`), no Access Control Policy must be applied to `N:`.

VM Certificates

When you first install the Policy Agent on a VM, you register the VM with Cryptographic Security Platform Vault using a certificate created by Cryptographic Security Platform Vault for VM Encryption for that VM. If the certificate is about to expire, you need to re-authenticate the VM with a new certificate. If you do not re-authenticate the VM and the certificate expires, Cryptographic Security Platform Vault for VM Encryption waits for a given amount of time and then detaches the encrypted drives from the VM so that they can no longer be accessed. The drives will remain detached until the certificate is renewed.

> Note: The amount of time Cryptographic Security Platform Vault for VM Encryption waits before detaching the drives is determined by the Grace Period set for the VM. For details, see Changing the Properties for a Specific VM.

By default, Cryptographic Security Platform Vault for VM Encryption automatically renews the certificate for a VM based on the setting of the Certificate Auto Renewal Period option on both the Cloud VM Set and the VM itself. For details, see Creating a Cloud VM Set for the CSP Vault for VM Encryption and Changing the Properties for a Specific VM.

If you have elected to disable auto-renewal, you need to reauthenticate the VM with a new certificate through the webGUI or `hicli` before the old certificate expires in order to avoid an interruption in service. For details, see Renewing a VM Certificate.

Cryptographic Security Platform Vault for VM Encryption generates alerts with increasing frequency when the certificate expiration date nears. If the certificate expiration date is:

- More than three months away, no alert is generated.
- Three months away, Cryptographic Security Platform Vault for VM Encryption generates one alert.
- Two months away, Cryptographic Security Platform Vault for VM Encryption generates one alert.
- Between four weeks to one week, Cryptographic Security Platform Vault for VM Encryption generates an alert once a week.
- In the final week and for the next week after expiration, Cryptographic Security Platform Vault for VM Encryption generates an alert every day.
- After the first week, Cryptographic Security Platform Vault for VM Encryption generated an alert every week for the next month.
- For the second and third months after expiration, Cryptographic Security Platform Vault for VM Encryption generates one alert each month.
- After the third month, no alert is generated.

This section includes:

- Revoking a Client Certificate
- Viewing Client Certificates
- Renewing a VM Certificate

Revoking a Client Certificate

You can revoke a certificate using the Cryptographic Security Platform Vault for VM Encryption webGUI.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Navigate to the Client Certificates tab.

4. Select the VM for which you want to revoke the certificate.
5. Select **Actions > Revoke Certificate**.

Important: If a certificate is revoked, you must reauthenticate the VM with a new certificate. See Renewing a VM Certificate.

Viewing Client Certificates

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Navigate to the Client Certificates tab.
   The Client Certificates page displays the following:

Field	Description
Name	The name of the certificate. If you hover over the tool tip after the name with the mouse, the certificate fingerprint will be displayed.
Registered	Whether the certificate is currently associated with a VM.
Used	Whether the certificate has ever been associated with a VM.
Revoked	Whether the certificate has been revoked.
Expiration Time	The date and time that the certificate will expire.
VM Name	The VM associated with the certificate. This field will be empty if the certificate has never been used.
VM Set Name	The name of the VM Set to which the certificate belongs.

4. Use the filter to narrow down your choices.

Renewing a VM Certificate

If you have disabled the Cryptographic Security Platform Vault for VM Encryption auto-certificate renewal feature, you can reauthenticate a VM with a new certificate manually through the CLI or the Cryptographic Security Platform Vault for VM Encryption webGUI.

Note: This procedure updates the VM's certificate with Cryptographic Security Platform Vault for VM Encryption. If you need to update the Cryptographic Security Platform Vault for VM Encryption certificate stored on the VM,

Renewing the Certificate with the CLI

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. Enter the command `hcl updatecert -a [-u username -p password] [-e certificate expiration]`, where:
   - `-a` tells `hcl` to contact Cryptographic Security Platform Vault to get the new certificate.
   - `-u` is a Cryptographic Security Platform Vault user account with Cloud Admin privileges. If you do not enter a user account name you will be prompted for one.
   - `-p` is the password for the Cryptographic Security Platform Vault user account. If you do not enter a password you will be prompted for one.
   - `-e` is the certificate expiration date in the format MM/DD/YYYY. If you do not enter an expiration date, Cryptographic Security Platform Vault uses the default date set in the **Certificate Expiration** option for the Cloud VM Set that this VM belongs to. The default is one year from the creation date.

   For example:

```
# hcl updatecert -a -u CloudAdmin -p password -e 06/30/2025
```

Renewing the Certificate with the CSP Vault for VM Encryption webGUI

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select the VM for which you want to renew the certificate.
   Important: If the VM is located in the Unauthenticated VMs tab, then you will need to run the Rescue Authentication command in the Cryptographic Security Platform Vault Management webGUI before you can renew the certificate. This command resets the authentication and will move the VM back to the VMs tab. For more details, see Re-Authenticating a VM with an Encrypted Root Device or Boot Disk.
4. Select **Actions > Renew Certificate**.
5. In the **Renew Certificate** dialog box, enter the passphrase for the certificate. This passphrase is optional but recommended for added security.
6. If desired, change the default certificate expiration date.
7. When you are done, click **Renew**. Cryptographic Security Platform Vault for VM Encryption generates a new certificate with the .cert extension and downloads it to your browser's default download location.
   Important: Do not change the name of the certificate file. If you do, the reauthorization will fail.
8. Copy the certificate to the VM.
9. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
10. Enter the command `hcl updatecert [-p certificate_passphrase] /path/to/cert.cert`, where:
    - `-p` is the passphrase for the certificate you specified in the Cryptographic Security Platform Vault for VM Encryption webGUI. If you do not enter a passphrase and the certificate requires one, you will be prompted for the passphrase.
    - `/path/to/cert.cert` is the fully-qualified name of the certificate file you copied to the VM.

    For example:

```
# hcl updatecert -p onetimepassphrase16chars /entrust/cert.cert
```

Changing the Properties for a Specific VM

When you add a VM to a Cloud VM Set, the VM inherits the settings for most of its property settings from the global defaults specified for the associated Cloud VM Set. (The only exception is the Description, which is set when you register the VM with Cryptographic Security Platform Vault.) You can override the global

defaults for individual VMs as required. For details about setting the global defaults, see Creating a Cloud VM Set for the CSP Vault for VM Encryption.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select the VM whose properties you want to set and click the **Expand** button (**>**) at the end of the row.
4. On the **Details** tab, specify the options you want to use.

Option	Description
Description	A user-defined string identifying this VM.
Certificate Valid Until	The date on which the certificate for this VM will expire. To have Cryptographic Security Platform Vault automatically renew the certificate, set the Certificate Auto Renewal Period option, described below.
Heartbeat	The length of time between the heartbeats each VM in the set sends to the Cryptographic Security Platform Vault for VM Encryption to verify that the connection between them is functioning normally. You can specify seconds, minutes, hours, or days. The default is 5 minutes. This value should be set to a minimum of 10 seconds. If changes have been made to the VMs through the Cryptographic Security Platform Vault for VM Encryption webGUI, those changes are communicated to the VMs during the heartbeat. That means if the heartbeat is set to 5 minutes, then it can take up to 5 minutes for any changes made in the Cryptographic Security Platform Vault for VM Encryption webGUI to be applied to the VMs in the set. If a VM cannot reach the Cryptographic Security Platform Vault for VM Encryption during the heartbeat, the VM continues to run but any changes made are not picked up by the VM until the next successful heartbeat. Cryptographic Security Platform Vault for VM Encryption sets the status of the VM to Unreachable, but it takes no further action unless the heartbeat continues to fail after the Grace Period has expired.
Grace Period	The length of time that can pass without a successful heartbeat. The default is 1 day. You can specify the grace period in seconds, minutes, hours, or days. If a VM remains unresponsive past the grace period, access to the data on the VM will be unavailable until the VM is re-authenticated with Cryptographic Security Platform Vault for VM Encryption.
OS	The operating system running on the VM.
Policy Agent Version	The version of the Entrust Policy Agent running on the VM.

Option	Description
Rekey Interval	If you specify any value other than 0 (zero) for this option, Cryptographic Security Platform Vault periodically creates a rekey task for every encrypted disk in the VM. You can select any number of days, weeks, months, or years and the Cryptographic Security Platform Vault for VM Encryptionwill automatically rekey the encrypted disks on that schedule. To disable Auto Rekey, enter 0 in this field. By default, Auto Rekey is disabled. Note: For Linux VMs, Auto Rekey only works if the online encryption driver has been configured and is active on the Linux VM.
Certificate Auto Renewal Period	If you want Cryptographic Security Platform Vault for VM Encryption to automatically renew the certificate for a VM in this Cloud VM Set, enter an integer greater than zero in this field. Cryptographic Security Platform Vault for VM Encryption will renew the certificate that many days before the old one expires. For example, if you enter a value of 5 in this field and a VM certificate is set to expire on June 12, 2022, Cryptographic Security Platform Vault for VM Encryption will renew the license on June 7, 2022. The default is 10 days. The expiry date is always 1 year from the date the certificate was created or renewed. To change the renewal period, click the existing value and enter a new value in the text field, then select days/weeks/months/years from the drop-down list. When you are finished, click Save. If you want to disable certificate auto-renewal, enter 0 (zero) in this field. Note: If you have auto-renewal set, but the renewal fails, Cryptographic Security Platform Vault for VM Encryption will continue to retry until the certificate is valid. When the certificate is no longer valid, the admin password will be required.
Mapping	The Cluster Node Mapping associated with this VM, if any. For details, see Creating a Cluster Node Mapping.
Single Encryption Key State	Whether the Single Encryption Key (SEK) option is enabled or disabled for the Cloud VM Set with which this VM is registered. For details, see Data Deduplication with Cloud VM Sets.

Option	Description

Auto Encryption	If this option is enabled, whenever Cryptographic Security Platform Vault for VM Encryption detects a new Windows drive or Linux device has been added to this VM, Cryptographic Security Platform Vault for VM Encryption immediately checks the Auto Encryption Policy. If the new drive or device is covered by the policy, Cryptographic Security Platform Vault for VM Encryptionautomatically tells the Policy Agent to encrypt that drive or device.
	
	To enable this option, click Disabled, select Enabled from the drop-down list, then click Save. When you do so, the webGUIdisplays the Encryption Policy fields:
	
	• **Auto Encryption Policy Type**. This can be:
	  • **Exclude**—The Windows drives and Linux devices listed in the **Auto Encryption Policy Path(s)** field will *not* be automatically encrypted, although they can be encrypted manually at any time. This is the default.
	  • **Include**—The Windows drives and Linux devices listed in the **Auto Encryption Policy Path(s)** field *will be*automatically encrypted. All other drives or devices on the VM must be encrypted manually.
	  • **Encrypt All Devices**—All Windows drives and Linux devices will be automatically encrypted.
	• **Auto Encryption Policy Path(s)**—If the policy type is Include or Exclude, enter a path that should be included or excluded. To add additional paths, click the + (Plus sign) in this field. You can enter either a Windows drive a Linux device name. For example, any of the following would be valid path names: `C:` , `C:\data` , or `sdb1` .
	Important: Each path *must* be on its own line.
	For more information, see Automatic Data Encryption.

Decryption Allowed	If this option is set to Yes, the drives and devices in this VM can be decrypted. If it is set to No, any decryption request will fail.
Policy Agent Uninstallation Allowed	If this option is set to Yes, the Policy Agent can be uninstalled on this VM. If it is set to No, the Policy Agent cannot be uninstalled.

5. On the **Reauthentication Settings** tab, you can change any of the following options by clicking the entry in the field, setting the new value, and then clicking **Save**. You must click **Save** after each change or your changes will be lost when you select a different field.

Option	Description
Reauthentication on IP Change	Whether the VM must be re-authenticated when the VM's IP address changes. The default is No. If your system configuration uses DHCP or multiple NICs, do *not* set this option to Yes. If you do so, the VM may go into a reboot loop if the boot partition is encrypted and any encrypted drives may be detached.
Reauthentication on H/W Signature Change	Whether the VM must be re-authenticated if its MAC address or UUID changes. The options are: • **Yes**—If *either* the MAC address *or* the UUID changes, the VM requires reauthentication. This is the default. We recommend that you do not change this option. • **Permissive**—Both the MAC address *and* the UUID must change before the VM requires reauthentication. • **No**—The Cryptographic Security Platform Vault for VM Encryption does not require reauthentication if VM's MAC address or UUID changes. We strongly recommend that you do **not** select this option. If you do, a cloned or misconfigured VM could gain access to the keys associated with the original VM. If you do select this option, you must confirm the selection before you can proceed. If Cryptographic Security Platform Vault for VM Encryption detects multiple VMs with the same MAC address and UUID combination when hardware validation is off, Cryptographic Security Platform Vault for VM Encryption generates an alert every 8 hours until the cloned VMs stop heartbeating or hardware authentication is set to **Yes** or **Permissive**. In addition, Cryptographic Security Platform Vault for VM Encryption generates an alert when client operations, such as key access or device registration, occur on the cloned VMs. Note: If this VM is a Master vSphere VDI VM, this option should always be Yes. If it is set to No, Cryptographic Security Platform Vault for VM Encryption may not be able to tell the Master VM from its clones. For details, see Combining VMware vSphere VDI with CSP Vault.
Reauthentication on Reboot	Whether the VM must be re-authenticated every time it reboots. The default is No. Setting this value to Yes is similar to requiring a boot-time password before the VM can come up completely.

Viewing the VM Status with the CLI

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. Run the `hcl status` command.

Example:
hcl status

```
Summary
--------------------------------------------------------------------------------
KeyControl: 10.1.228.10:443
KeyControl list: 10.1.228.10:443
Vault ID: 6971c6a2-48c5-4dfa-9234-198ffcaa3999
Status: Connected
Last heartbeat: Fri Feb 16 13:00:28 2024 (successful)
AES_NI: enabled
Certificate Expiration: Feb 15 18:51:17 2025 GMT
HTCRYPT: enabled

Registered Devices
--------------------------------------------------------------------------------
Disk Name       Cipher      Status              Clear
--------------------------------------------------------------------------------
sdb1            AES-XTS-512-FIPS Attached (RK 15.67%)    /dev/mapper/clear_sdb1
'--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT,

Available Devices
--------------------------------------------------------------------------------
Disk Name       Device Node             Size (in MB)
--------------------------------------------------------------------------------
sde7            /dev/sde7               580
sdc1            /dev/sdc1               118

Other Devices
--------------------------------------------------------------------------------
Disk Name       Device Node             Status
--------------------------------------------------------------------------------
sda2            /dev/sda2               Mounted (/)
```

Note: In this example, sbd1 is currently being encrypted.
The VM status can be one of the following:

- **Not registered** — The Policy Agent software is installed but the VM has not yet been registered with Cryptographic Security Platform Vault.
- **Connected** — The VM can communicate with the Cryptographic Security Platform Vault for VM Encryption and everything is running normally.
- **Could not connect** — The Cryptographic Security Platform Vault for VM Encryption is not reachable. If this condition continues, the VM will need to be re-authenticated with the Cryptographic Security Platform Vault for VM Encryption when communication is re-established.
- **Need to update certificate** — The certificate for the is VM is no longer valid and should be updated.
- **Reauth needed** — The VM needs to be re-authenticated.
- **Virtual Machine not authenticated** — VM permissions have been revoked from the Cryptographic Security Platform Vault for VM Encryption. To fix this issue, see Reactivating a Revoked Disk.
- **Identity verification failed** — Permissions are not available because the VM heartbeat has timed out or its IP address or hardware signature has changed. This can occur if you have changed the IP address on a VM or copied the VM to a new server.
- **Unknown error from KeyControl cluster** — An unknown error has occurred. Please contact Support if you see this message.

Exporting VM Details

You can export the details for all VMs registered with Cryptographic Security Platform Vault, or for all VMs registered with selected Cloud VM Sets, to a CSV (comma separated value) file. The CSV file includes information about the VM's status, IP address, operating system, Policy Agent version, certificate expiration date, and the basic VM option settings.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. If you want to download the details for all VMs registered with the Cloud VM Sets to which your account has access, click **Actions > Download All CVM Set Info**. If you want to download the details for specific Cloud VM Sets, select those sets and click **Actions > Download Selected CVM Set Info**.
   Cryptographic Security Platform Vault generates and downloads a file called `htdc-cvmsetinfo-yymmddhhmm.csv`, where `yymmddhhmm` is the year, month, day, hour, and minute server time at which the export file was created.
   Note: This option is only available for Cloud VM Sets that have at least one registered VM. If you select a Cloud VM Set and **Download Selected CVM Set Info** does not appear in the **Actions** menu, then the selected set does not have any registered VMs.

Viewing the Details for a VM

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab.
4. To view the details for a VM, click the **Expand** button (**>**) at the end of the row.
   Cryptographic Security Platform Vault displays the details for the VM along with a VM-specific **Actions** button that allows you to manage the selected VM without affecting other VMs registered with Cryptographic Security Platform Vault.

VM Status Information

The VM Status can be one of the following:

- **Not registered** — The Policy Agent software is installed but the VM has not yet been registered with Cryptographic Security Platform Vault.
- **Connected** — The VM can communicate with the Cryptographic Security Platform Vault for VM Encryption and everything is running normally.
- **Could not connect** — The Cryptographic Security Platform Vault for VM Encryption is not reachable. If this condition continues, the VM will need to be re-authenticated with the Cryptographic Security Platform Vault for VM Encryption when communication is re-established.
- **Need to update certificate** — The certificate for the is VM is no longer valid and should be updated.
- **Reauth needed** — The VM needs to be re-authenticated.
- **Virtual Machine not authenticated** — VM permissions have been revoked from the Cryptographic Security Platform Vault for VM Encryption. To fix this issue, see Reactivating a Revoked Disk.
- **Identity verification failed** — Permissions are not available because the VM heartbeat has timed out or its IP address or hardware signature has changed. This can occur if you have changed the IP address on a VM or copied the VM to a new server.
- **Unknown error from KeyControl cluster** — An unknown error has occurred. Please contact support if you see this message.

VM Details Area

The VM Details area contains the following tabs:

- **Details** — Shows the basic information about the VM including its certificate status, rekey interval, and the version of the Entrust Policy Agent installed on the VM.
- **Reauthentication Settings** — Shows whether Cryptographic Security Platform Vault requires you to reauthenticate the VM when its IP address changes, its hardware signature changes, or it reboots.
- **Encrypted Disks** — Shows the status of the VM's encrypted disks, including both regular disks and Windows folder mounts.
- **Unencrypted Disks** — Shows the disks and Windows folder mounts available for encryption.
- **User Tasks** — Shows the tasks that were started by a Cryptographic Security Platform Vault user. This list includes any manually-initiated disk encryption or decryption tasks and the status of any changes to the Cluster Node Mapping assigned to the VM.
- **System Tasks** — Shows the tasks that were started automatically by Cryptographic Security Platform Vault. This list includes any auto encryption tasks for the VM.

High Availability Between a VM and the CSP Vault Cluster

When you register a VM with Cryptographic Security Platform Vault for VM Encryption, you must provide at least one Cryptographic Security Platform Vault for VM Encryption node IP address. If that is all you do, then that is the *only* Cryptographic Security Platform Vault for VM Encryption node that the VM will communicate with, even if that Cryptographic Security Platform Vault for VM Encryption node is part of a cluster. If that Cryptographic Security Platform Vault for VM Encryption node becomes unreachable, then the VM's heartbeat will fail and access to the VM may be disrupted.

If you have a cluster of Cryptographic Security Platform Vault for VM Encryption nodes, you can solve this issue by configuring High Availability between the VM and all the nodes in the Cryptographic Security Platform Vault for VM Encryption cluster. To do this, Entrust recommends associating the VM with a Cluster Node Mapping, which is a list of Cryptographic Security Platform Vault for VM Encryption nodes maintained in Cryptographic Security Platform Vault for VM Encryption. If you add or remove a Cryptographic Security Platform Vault for VM Encryption node from the cluster, or if any of the Cryptographic Security Platform Vault for VM Encryption node IP addresses change, you can update the Node Mapping and Cryptographic Security Platform Vault for VM Encryption will automatically disseminate those updates to all associated VMs at their next heartbeat.

> Tip: You can create a Cluster Node Mapping even if you have a standalone Cryptographic Security Platform Vault for VM Encryption node. That way, if you ever decide to add additional nodes to form a Cryptographic Security Platform Vault for VM Encryption cluster, you just need to add the new nodes to your existing Node Mapping and the changes will be disseminated to the VMs automatically.

Alternatively, you can configure High Availability on an individual VM-by-VM basis. If you do this, however, you must manually update the list of available Cryptographic Security Platform Vault for VM Encryption nodes on every VM any time you add or remove a Cryptographic Security Platform Vault for VM Encryption node from the cluster.

High Availability Through a Global Cluster Node Mapping

A Cluster Node Mapping is a list of Cryptographic Security Platform Vault for VM Encryption nodes maintained in Cryptographic Security Platform Vault for VM Encryption. Each Cluster Node Mapping is assigned to a specific Cloud Admin Group, and it can be associated with any number of VMs registered with that group. If you add or remove a Cryptographic Security Platform Vault for VM Encryption node from the cluster, you only need to edit the Node Mapping and the changes will be disseminated to the associated VMs at their next heartbeat.

For each Cryptographic Security Platform Vault for VM Encryption node in the Node Mapping, you can specify an externally-visible IP address or hostname. This allows you to connect the VMs with the Cryptographic Security Platform Vault for VM Encryption nodes across a firewall or in an environment such

as Amazon Web Services (AWS) or Microsoft Azure, where the node is assigned an internal IP address as well as an external IP address.

You can create as many Cluster Node Mappings for each Cloud Admin Group as you need. The first node in each Node Mapping will always be the preferred Cryptographic Security Platform Vault for VM Encryption node for the associated VMs. So if you have some Cryptographic Security Platform Vault for VM Encryption nodes in the US and some in Europe, you can create one Node Mapping with the US nodes listed first and another mapping with the European nodes listed first. Then you can assign the appropriate Node Mapping to each VM based on its location.

You cannot, however, associate the same Node Mapping with multiple Cloud Admin Groups. Even if you want to use the same list of Cryptographic Security Platform Vault for VM Encryption nodes for every registered VM, you must still create a unique Cluster Node Mapping for each Cloud Admin Group.

Failover with a Cluster Node Mapping

The order of the IP addresses in the list determines the order of precedence. The first node in a Cluster Node Mapping is considered the preferred node, and all VMs will use that node as long as it is available. If the preferred node is offline when a VM heartbeats, the VM will try the other IP addresses in the Node Mapping, starting with the second IP address in the list and working downwards. Once the VM finds an available Cryptographic Security Platform Vault for VM Encryption node, it will use that node to complete the current heartbeat, and it will continue to use that node until the cluster returns to a healthy state. After the cluster becomes healthy, the VM will resume using the preferred node at its next heartbeat.

If you want to change the preferred Cryptographic Security Platform Vault for VM Encryption node, you can change the order of the nodes in the Node Mapping, and, the next time the VM heartbeats with a healthy Cryptographic Security Platform Vault for VM Encryption cluster, it will begin using the new preferred node immediately.

Important: If you remove the preferred Cryptographic Security Platform Vault for VM Encryption node from the cluster, you will need to remove the node from the Cluster Node Mapping as well. See Changing a Cluster Node Mapping . Cryptographic Security Platform Vault for VM Encryption automatically gives you the option of removing the Cryptographic Security Platform Vault for VM Encryption node from the Node Mapping as well. Doing this by itself, however, is *not* enough to make the registered VMs fail over to a different node in the Node Mapping. Instead, you must *also* shut down or destroy the old node so that it is no longer reachable by the VMs. As soon at it is no longer reachable, the VMs will fail over to one of the other Cryptographic Security Platform Vault for VM Encryption nodes in the Node Mapping. At that point Cryptographic Security Platform Vault for VM Encryption will communicate the updated Node Mapping to the VMs and they will begin to use the Cryptographic Security Platform Vault for VM Encryption node that is listed first in the updated Node Mapping.

High Availability on Individual VMs

You can maintain the list of available Cryptographic Security Platform Vault for VM Encryption node IP addresses on individual VMs using the `hcl updatekc` command on each VM. In this case, if the list of Cryptographic Security Platform Vault for VM Encryption IP addresses changes in any way, those changes must be manually disseminated to each VM by re-running the `hcl updatekc` command on each VM.

This method also requires that the VM and all of your Cryptographic Security Platform Vault for VM Encryption nodes be on the same network so that they can ping each other directly, or that you have set up a Domain Name Server (DNS) server with entries that map each Cryptographic Security Platform Vault for VM Encryption IP address to a single domain name. With a DNS server, if you add or remove Cryptographic Security Platform Vault for VM Encryption nodes from the cluster, the Policy Agents can continue to use the same domain name but you must update the DNS entries on the DNS server.

For details on the `hcl updatekc` command, see Updating CSP Vault Node IP Addresses on an Individual VM. For details about setting up a DNS server, see your DNS server documentation.

Related Topics

- Updating CSP Vault Node IP Addresses on an Individual VM
- Managing the Cluster Node Mapping on a VM
- Changing a Cluster Node Mapping
- Creating a Cluster Node Mapping

Updating CSP Vault Node IP Addresses on an Individual VM

If the Cryptographic Security Platform Vault nodes in a cluster change, you need to update the IP address list on each Policy Agent unless you have specified a Cluster Node Mapping for the VMs. Cluster Node Mapping changes are done through Cryptographic Security Platform Vault and are communicated to each associated VM on the VM's next heartbeat. For more information, see High Availability Between a VM and the CSP Vault Cluster.

Procedure

For each VM registered with this Cryptographic Security Platform Vault cluster:

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. Enter the `hcl updatekc kc_hostname[:port],kc_hostname[:port],kc_hostname[:port],...` command
   where `kc_hostname,kc_hostname,kc_hostname...` is a comma-separated list of the Cryptographic Security Platform Vault node IP addresses or hostnames and `port` is an optional port number (the default is port 443). If you are entering the command on Windows, use quotes around the list of hostnames.
   The first Cryptographic Security Platform Vault node in the list will be considered the primary node, and the VM will always attempt to reach Cryptographic Security Platform Vault through that node first. If that node is unavailable, the VM will try the other nodes in the list in order until it finds a Cryptographic Security Platform Vault node that it can communicate with.
   For example, if you want to specify the Cryptographic Security Platform Vault node named `kc-chicago` as your primary node and the nodes `10.238.66.234` and `kc-bangalore` on port 447 as your second and third nodes, you would specify:
   Linux: `# hcl updatekc kc-chicago,10.238.66.234,kc-bangalore:447`
   Windows: `C:\> hcl updatekc "kc-chicago,10.238.66.234,kc-bangalore:447"` (Note the `""` around the hostname list for Windows.)

Important: The list you specify overwrites any existing list on the Policy Agent. So if the Policy Agent is currently connected to three Cryptographic Security Platform Vault nodes and you remove one, you must specify the two remaining nodes with the `updatekc` command. The third node will be removed automatically. Similarly, if you add a fourth Cryptographic Security Platform Vault node, you must specify all four IP addresses with the `updatekc` command. If you only specify the new Cryptographic Security Platform Vault node, then that becomes the *only* node that the Policy Agent will communicate with.

To verify the connection status, enter the `hcl status` command, as shown. The first line shows the Cryptographic Security Platform Vault that the VM is currently communicating with and the second line shows the three Cryptographic Security Platform Vault nodes available to the VM.

```
C:\> hcl status
Summary
-------------------------------------------------
KeyControl: kc-chicago:443
KeyControl list: kc-chicago:443,10.238.66.234:443,kc-bangalore:447
Status: Connected
```

Managing the Cluster Node Mapping on a VM

You can associate a Cluster Node Mapping with a VM at any time. The same procedure can also be used to change the Node Mapping currently associated with a VM. This can be done either through the Cryptographic Security Platform Vault for VM Encryption webGUI or through the CLI or Policy Agent GUI on the VM itself.

If you use the Cryptographic Security Platform Vault for VM Encryption webGUI, you can also use the Multi-Select option to set the Node Mapping for multiple VMs at the same time.

Managing the Node Mapping Through the webGUI

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click on the VM whose Node Mapping you want to set and select **Actions > Set Mapping**.
   Tip: If you want to set the same Node Mapping for multiple VMs, enable the **Multi-Select** option and then click on each of the VMs whose Node Mapping you want to set.
4. Select the Node Mapping you want to use from the drop-down list, then click **Set Mapping**.
   Cryptographic Security Platform Vault for VM Encryption automatically communicates the new Node Mapping information to the VM. After that, the VM will connect to Cryptographic Security Platform Vault for VM Encryption using the first node in the Node Mapping. If that node is unavailable, the VM will automatically fail over to the next node in the Node Mapping. For details, see High Availability Between a VM and the CSP Vault Cluster.
   You can view the progress of the Node Mapping assignment on the **User Tasks** tab for the VM. You can also view the currently-assigned Node Mapping on the VM's **Details** tab in the **Mapping** field.

Managing the Node Mapping Through the CLI

Log into each VM you want to associate with the Cluster Node Mapping and enter the command `hcl updatekc –a [-u username [-s password]]` , where:

- `-u` is a Cryptographic Security Platform Vault for VM Encryption user account with Cloud Admin privileges. If you do not enter a user account name you will be prompted for one.
- `-s` is the password for the Cryptographic Security Platform Vault for VM Encryption user account. If you do not enter a password you will be prompted for one.

The Policy Agent then queries Cryptographic Security Platform Vault for VM Encryption for the list of available Cluster Node Mappings. Type the number corresponding to the Node Mapping you want to use and press Enter. For example:

```
# hcl updatekc -a
Getting Mapping information
Please provide the login details
username: cloudadmin
password: ********

This VM can be added to one of the following Mappings
-----------------------------------------------------
1 : San Francisco Datacenter
2 : AWS VMs
-----------------------------------------------------
Please select Mapping (0 to skip): 1

Mapping
```

server description KC-1, ip 192.168.140.151, port 443
server description KC-2, ip 192.168.140.152, port 443
Updated list with nodes 192.168.140.151:443,192.168.140.152:443

> Note: If you select 0, no changes are made to the current IP addresses or Cluster Node Mapping associated with the VM.

Managing the Node Mapping Through the Policy Agent GUI

1. Log into the Windows system using an account with Administrator privileges.
2. Select **Start > All Programs > Entrust > Entrust DataControl** or start Windows PowerShell and enter the `hclGUI` command.
3. Click the **Update Mapping** button.
4. In the Mapping window, update the Mapping Name, Vault User, and the Password.
5. Click **Update Mapping**.
6. When the status update window appears, click **OK**.
7. Click the **Refresh** button to refresh the window and see the changes.

Changing a Cluster Node Mapping

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **Mappings** tab.
4. Select the Node Mapping you want to change in the list.
5. If you want to change the Node Mapping name, associated Cloud Admin Group, or description, do the following:
    a. In the Details tab below the table, click the text in the field you want to change.
    b. Make your changes and click **Save**.
6. If you want to change the Cryptographic Security Platform Vault for VM Encryption nodes in the Node Mapping or the order of the node in the Node Mapping, do the following:
    a. Select **Actions > Edit Mapping**.
    b. If you want to add a new IP address, click the **+** (Plus sign) on the right-hand side of the dialog box to add a new row, then enter the following information:

Field	Description
External IP	The externally-visible hostname or IP address to which this node should be mapped. Each node in the cluster can be associated with one and only one externally-visible IP address. Note: If the VMs will be communicating with the Cryptographic Security Platform Vault for VM Encryption node through a firewall or in an environment like Amazon Web Services or Microsoft Azure, the externally-visible IP address may not be the same as the internal Cryptographic Security Platform Vault for VM Encryption node IP address. Make sure that all VMs that will use this Node Mapping can communicate with the Cryptographic Security Platform Vault for VM Encryption node via the specified IP address/port number combination.

Field	Description
Port	The port number for the specified Hostname or IP address. The default is 443.
CSP Vault Server	Select the appropriate Cryptographic Security Platform Vault for VM Encryption node in the drop-down list. You can only have one entry for each CSP Vault for VM Encryption node.
State	Select Enabled if the node is available to the VMs associated with this Cluster Node Mapping. If you want to use this as a placeholder until you bring the node online, select Disabled. The default is Enabled.
Description	Enter a description for this node that lets you distinguish it from other nodes in the Cluster Node Mapping.

c. If you want to delete an existing entry, click the – (Minus sign) at the end of the row you want to delete.
d. When you are done changing the list of nodes, make sure that the order is correct because the order of the IP addresses in the list determines the order of precedence. The first node in a Cluster Node Mapping is considered the preferred node, and all VMs will use that node as long as it is available. If the preferred node is offline when a VM heartbeats, the VM will try the other IP addresses in the Node Mapping, starting with the second IP address in the list and working downwards. Once the VM finds an available Cryptographic Security Platform Vault for VM Encryption node, it will use that node to complete the current heartbeat, and it will continue to use that node until the cluster returns to a healthy state. After the cluster becomes healthy, the VM will resume using the preferred node at its next heartbeat.
   If you need to change the order, click and hold on the arrow icon at the beginning of the line to drag the entry to the proper position. Release the mouse to drop the entry in the new location.
   You can view the Preferred Node in the Details section of the selected mapping.
e. When you are done, click **Update**. Cryptographic Security Platform Vault for VM Encryption communicates the changes to the associated VMs on their next heartbeat.

Creating a Cluster Node Mapping

A Cluster Node Mapping lets you create a list of Cryptographic Security Platform Vault for VM Encryption IP addresses that you maintain in Cryptographic Security Platform Vault for VM Encryption. Each Cryptographic Security Platform Vault for VM Encryption node in the Node Mapping is associated with an externally visible IP address or hostname that VMs can use to access that node. If you ever change the list of Cryptographic Security Platform Vault for VM Encryption nodes in the Node Mapping, Cryptographic Security Platform Vault for VM Encryption automatically disseminates the changes to each associated VM at its next heartbeat.

Associating a Node Mapping with a VM enables High Availability between the VM and Cryptographic Security Platform Vault for VM Encryption by enabling failover among the Cryptographic Security Platform Vault for VM Encryption nodes, and it means you do not need to update the individual VMs when Cryptographic Security Platform Vault for VM Encryption nodes are added to, or removed from, the cluster.

For more information on High Availability and failover, see the installation and administration guide at https://api.managed.entrust.com/vault/latest

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **Mappings** tab.
4. Select **Actions > Create Mapping**.
5. On the **Mapping** tab, specify the options you want to use.

Field	Description
Name	Enter the name for this Cluster Node Mapping. You can use - (hyphen) and _ (underscore) as well as any alphanumeric characters.
Cloud Admin Group drop-down list	Select the Cloud Admin Group associated with this Node Mapping. The Node Mapping will be available to all VMs that are registered with the Cloud VM Sets assigned to the selected Cloud Admin Group.
Description	Enter a description for the Cluster Node Mapping. This description will be displayed on the VMs when they are associated with the Cluster Node Mapping.

6. When you are done, click **Next**.
7. On the **Servers** tab, create an entry for the first Cryptographic Security Platform Vault for VM Encryption node by specifying the options you want to use.

Field	Description
External IP	The externally-visible hostname or IP address to which this node should be mapped. Each node in the cluster can be associated with one externally visible IP address. Note: If VMs will communicate with the Cryptographic Security Platform Vault for VM Encryption node through a firewall or in an environment like Amazon Web Services or Microsoft Azure, the externally visible IP address may not match the internal Cryptographic Security Platform Vault for VM Encryption node IP address. Make sure that all VMs that will use this Node Mapping can communicate with the Cryptographic Security Platform Vault for VM Encryption node via the specified IP address/port number combination.
Port	The port number for the specified Hostname or IP address. The default is 443.
Cryptographic Security Platform Vault Server	Select the appropriate Cryptographic Security Platform Vault for VM Encryption node in the drop-down list. You can only have one entry for each Cryptographic Security Platform Vault for VM Encryption node.

Field	Description
State	Select Enabled if the node is available to the VMs associated with this Cluster Node Mapping. If you want to use this as a placeholder until you bring the node online, select Disabled. The default is Enabled.
Description	Enter a description for this node that lets you distinguish it from other nodes in the Cluster Node Mapping.

8. To add another node, click the **+** button and enter the appropriate information.
9. When you are done adding nodes, make sure that the order is correct because the order of the IP addresses in the list determines the order of precedence. The first node in a Cluster Node Mapping is considered the preferred node, and all VMs will use that node as long as it is available. If the preferred node is offline when a VM heartbeats, the VM will try the other IP addresses in the Node Mapping, starting with the second IP address in the list and working downwards. Once the VM finds an available Cryptographic Security Platform Vault for VM Encryption node, it will use that node to complete the current heartbeat and continue using it until the cluster returns to a healthy state. After the cluster becomes healthy, the VM will resume using the preferred node at its next heartbeat.
   To change the order, click and hold the arrow icon at the beginning of the line, then drag the entry to the correct position. Release the mouse to drop the entry in the new location.
10. When you include all nodes and the order is correct, click **Create**.
11. At the Mapping Successfully Created message, click **Close**.
12. If you want to associate the Cluster Node Mapping with an existing VM that already has the Policy Agent installed:
    a. Log into the VM as an administrator.
    b. Enter the command `hcl updatekc -a` and enter the credentials for a Cryptographic Security Platform Vault for VM Encryption user account with Cloud Admin privileges at the prompt. Cryptographic Security Platform Vault for VM Encryption displays a list of available Cluster Node Mappings that you can use with the VM.
    c. Select the Cluster Node Mapping you want to use from the list. Cryptographic Security Platform Vault for VM Encryption echoes the IP addresses in the list for confirmation.

```
# hcl updatekc -a
Getting Mapping information
Please provide the login details
username: cloudadmin
password: ********

This VM can be added to one of the following Mappings
-----------------------------------------------------
1 : San Francisco Datacenter
2 : AWS VMs
-----------------------------------------------------
Please select Mapping (0 to skip): 1

Mapping
server description KC-1, ip 192.168.140.151, port 443
server description KC-2, ip 192.168.140.152, port 443
Updated list with nodes 192.168.140.151:443,192.168.140.152:443
```

Note: For details about specifying a Cluster Node Mapping when you install the Policy Agent, see the installation and administration guide at https://api.managed.entrust.com/vault/latest

Cloud VM Sets

A Cloud VM Set is a logical grouping of related VMs, such as "Amazon EC2 VMs," "Azure VMs," and "Legal Dept VMs". When you register a new VM with Cryptographic Security Platform Vault, you must assign that VM to a Cloud VM Set before the data can be encrypted.

When you create a Cloud VM Set, you can specify default properties that are inherited by every VM that is registered with that set. These default properties can be overridden at the individual VM level if required.

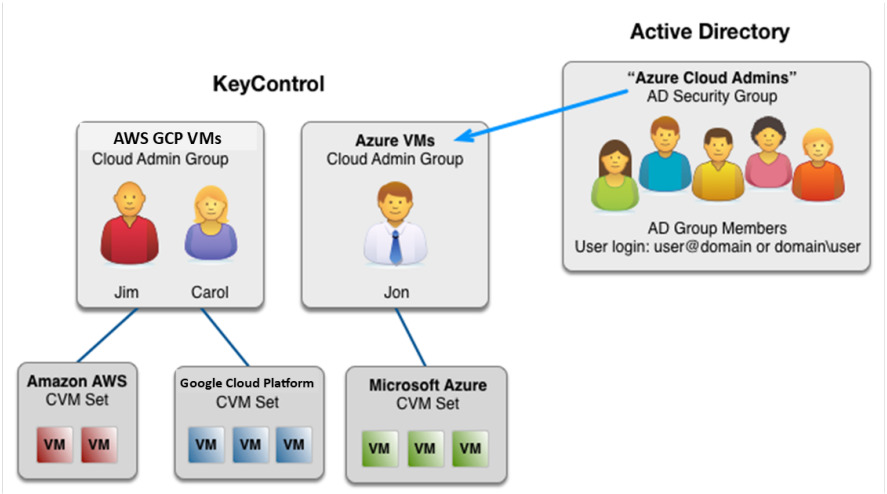
If Cryptographic Security Platform Vault has access to a hardware security module (HSM), the Cloud VM Set can also be associated with a Key Encryption Key (KEK) that provides an extra layer of security and that can be used to expire or revoke access to all VMs in the set automatically. For more information, see KEKs with Cloud VM Sets.

Each Cloud VM Set is associated with a specific Cloud Admin group, and that group is, in turn, associated with one or more Cryptographic Security Platform Vault accounts with Cloud Admin privileges.

This structure allows you to create boundaries between your VM groups so that Cloud Admins from one group cannot see the VMs assigned to a different group.

The following figure shows an example of the relationship between Cryptographic Security Platform Vault users, Cloud Admin Groups, and Cloud VM Sets. In this example:

- Jim and Carol both have Cryptographic Security Platform Vault-managed user accounts assigned to the Cloud Admin Group "AWS GCP VMs". They are responsible for the VMs in the Cloud VM Sets "Amazon AWS" and "Google Cloud Platform". When they log in, they cannot see any of the VMs that have been registered with the "Microsoft Azure" Cloud VM Set.
- Jon has a Cryptographic Security Platform Vault-managed user account, and both his account and the Active Directory Security group "Azure Cloud Admins" have been assigned to the Cloud Admin Group "Azure VMs". Jon and all the members of the AD Security group are responsible for the VMs in the Cloud VM Set "Microsoft Azure". When Jon or any of the AD Security group members log into Cryptographic Security Platform Vault, they can only see the VMs in the "Microsoft Azure" Cloud VM Set.



For more information about Cloud Admin groups and user accounts, see Cloud Admin Groups and CSP Vault User Accounts.

Related Topics

- Changing Cloud VM Set Properties
- Adding KEK to an Existing Cloud VM Set
- Creating a Cloud VM Set for the CSP Vault for VM Encryption
- Setting Default Cloud VM Set Properties
- Data Deduplication with Cloud VM Sets
- KEKs with Cloud VM Sets

Changing Cloud VM Set Properties

Note: Changes to the Cloud VM Set properties are applied to any new VMs that are registered with the Cloud VM Set. If you want to change the properties for an existing VM, see Changing the Properties for a Specific VM.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. On the **VM Sets** tab, select the Cloud VM Set whose properties you want to change. The Cryptographic Security Platform Vault webGUI displays the Cloud VM Set properties below the list of Cloud VM Sets.
4. On the **Details** tab, you can change any of the following options by clicking the entry in the field, setting the new value, and then clicking **Save**. You must click **Save** after each change or your changes will be lost when you select a different field.

Option	Description
Name	The name of the Cloud VM Set.
Description	A user-defined description of the Cloud VM Set.
Group	The Cloud Admin group to which this Cloud VM Set belongs.
VMs	The number of VMs registered to this set. Click the link in this field to view details about the individual VMs.

Option	Description
Heartbeat	The length of time between the heartbeats each VM in the set sends to the Cryptographic Security Platform Vault for VM Encryption to verify that the connection between them is functioning normally. You can specify seconds, minutes, hours, or days. The default is 5 minutes. This value should be set to a minimum of 10 seconds. If changes have been made to the VMs through the Cryptographic Security Platform Vault for VM Encryption webGUI, those changes are communicated to the VMs during the heartbeat. That means if the heartbeat is set to 5 minutes, then it can take up to 5 minutes for any changes made in the Cryptographic Security Platform Vault for VM Encryption webGUI to be applied to the VMs in the set. If a VM cannot reach the Cryptographic Security Platform Vault for VM Encryption during the heartbeat, the VM continues to run but any changes made are not picked up by the VM until the next successful heartbeat. Cryptographic Security Platform Vault for VM Encryption sets the status of the VM to Unreachable, but it takes no further action unless the heartbeat continues to fail after the Grace Period has expired.
Grace Period	The length of time that can pass without a successful heartbeat. The default is 1 day. You can specify the grace period in seconds, minutes, hours, or days. If a VM remains unresponsive past the grace period, access to the data on the VM will be unavailable until the VM is re-authenticated with Cryptographic Security Platform Vault for VM Encryption.
Max Parallel Rekey Operations	The number of concurrent Auto Rekey operations that can be performed for VMs in the Cloud VM Set. The default is 1.
Rekey Interval	If you specify any value other than 0 (zero) for this option, Cryptographic Security Platform Vault periodically creates a rekey task for every encrypted disk in every VM that is registered with this Cloud VM Set. You can select any number of days, weeks, months, or years and the Cryptographic Security Platform Vault for VM Encryptionwill automatically rekey the encrypted disks on that schedule. To disable Auto Rekey, enter 0 in this field. By default, Auto Rekey is disabled.

Option	Description
Certificate Auto Renewal Period	If you want Cryptographic Security Platform Vault for VM Encryption to automatically renew the certificate for a VM in this Cloud VM Set, enter an integer greater than zero in this field. Cryptographic Security Platform Vault for VM Encryption will renew the certificate that many days before the old one expires. For example, if you enter a value of 5 in this field and a VM certificate is set to expire on June 12, 2022, Cryptographic Security Platform Vault for VM Encryption will renew the license on June 7, 2022. The default is 10 days. The expiry date is always 1 year from the date the certificate was created or renewed. To change the renewal period, click the existing value and enter a new value in the text field, then select days/weeks/months/years from the drop-down list. When you are finished, click Save. If you want to disable certificate auto-renewal, enter 0 (zero) in this field. Note: If you have auto-renewal set, but the renewal fails, Cryptographic Security Platform Vault for VM Encryption will continue to retry until the certificate is valid. When the certificate is no longer valid, the admin password will be required.
Certificate Expiration	The length of time for which a VM certificate will be valid when it is first registered with Cryptographic Security Platform Vault for VM Encryption or when it is auto-renewed by Cryptographic Security Platform Vault for VM Encryption. The default is 1 year. To change the expiation, click the existing value and enter a new value in the text field, then select days/weeks/months/years from the drop-down list. When you are finished, click Save. Note: If you change this value for an existing Cloud VM Set, the certificate expiration date is not changed for any of the VMs that are currently part of the set. This value only takes effect for new VMs or when the certificates for the existing VMs are renewed.
Single Encryption Key State	Whether the VMs in this Cloud VM Set are encrypted with the same Single Encryption Key (SEK) key. For information about changing the SEK properties, see Changing SEK Properties. For details about SEK usage with Cryptographic Security Platform Vault for VM Encryption, see Data Deduplication with Cloud VM Sets.
Single Encryption Key Cipher	The cipher used for all SEK keys. This value cannot be changed. Note: This field is only displayed if the SEK state is Enabled.

Option	Description
Single Encryption Key Version	The highest version number among the SEK keys that have been created for this Cloud VM Set. To fully enable data deduplication, you should make sure that all encrypted disks on all VMs in the Cloud VM Set are using the same version of the SEK key. For details, see Generating a New SEK Key. Note: This field is only displayed if the SEK state is Enabled.

Auto Encryption	If this option is enabled, whenever a new VM is registered with this Cloud VM Set, Cryptographic Security Platform Vault for VM Encryption will automatically instruct the Policy Agent to encrypt one or more of the drives on that VM.
	To enable this option, click Disabled, select Enabled from the drop-down list, then click Save. When you do so, the webGUI displays the Encryption Policy fields:
	• **Auto Encryption Policy Type**. This can be:
	  • **Exclude**—The Windows drives and Linux devices listed in the **Auto Encryption Policy Path(s)** field will *not* be automatically encrypted, although they can be encrypted manually at any time. This is the default.
	  • **Include**—The Windows drives and Linux devices listed in the **Auto Encryption Policy Path(s)** field *will be*automatically encrypted. All other drives or devices on the VM must be encrypted manually.
	  • **Encrypt All Devices**—All Windows drives and Linux devices will be automatically encrypted.
	• **Auto Encryption Policy Path(s)**—If the policy type is Include or Exclude, enter a path that should be included or excluded. To add additional paths, click the + (Plus sign) in this field. You can enter either a Windows drive a Linux device name. For example, any of the following would be valid path names: `C:` , `C:\data` , or `sdb1` .
	Important: Each path *must* be on its own line.
	For more information, see Automatic Data Encryption.

Decryption Allowed	If this option is set to Yes, the drives and devices in the VMs registered with this Cloud VM Set can be decrypted. If it is set to No, any decryption request will fail. If you change this option, you can also propagate the change to all of the VMs that are currently registered with the Cloud VM Set. If you do not propagate the change, then this setting will be inherited only by new VMs registered with the Cloud VM Set.

Option	Description
Policy Agent Uninstallation Allowed	If this option is set to Yes, the Policy Agent can be uninstalled on the VMs registered with this Cloud VM Set. If it is set to No, the Policy Agent cannot be uninstalled. If you change this option, you can also propagate the change to all of the VMs that are currently registered with the Cloud VM Set. If you do not propagate the change, then this setting will be inherited only by new VMs registered with the Cloud VM Set.

5. On the **Reauthentication Settings** tab, you can change any of the following options by clicking the entry in the field, setting the new value, and then clicking **Save**. You must click **Save** after each change or your changes will be lost when you select a different field.

Option	Description
Reauthentication on IP Change	Whether a VM in the set must be re-authenticated when the VM's IP address changes. The default is No. If your system configuration uses DHCP or multiple NICs, do *not* set this option to Yes. If you do so, the VMs in the set may go into a reboot loop if their boot partitions are encrypted and any encrypted drives may be detached.

Option	Description
Reauthentication on H/W Signature Change	Whether a VM in the set must be re-authenticated if its MAC address or UUID changes. The options are: • **Yes**—If *either* the MAC address *or* the UUID changes, the VM requires reauthentication. This is the default. We recommend that you do not change this option. • **Permissive**—Both the MAC address *and* the UUID must change before the VM requires reauthentication. You can use this option if your system administrators are performing maintenance on the VMs in this Cloud VM Set that require changes to the network cards and hence to the MAC addresses of the VMs in the set. We recommend you reset this value to **Yes** once maintenance is finished. • **No**—The Cryptographic Security Platform Vault for VM Encryption does not require reauthentication if VM's MAC address or UUID changes. We strongly recommend that you do **not** select this option. If you do, a cloned or misconfigured VM could gain access to the keys associated with the original VM. If you do select this option, you must confirm the selection before you can proceed. If Cryptographic Security Platform Vault for VM Encryption detects multiple VMs with the same MAC address and UUID combination when hardware validation is off, Cryptographic Security Platform Vault for VM Encryption generates an alert every 8 hours until the cloned VMs stop heartbeating or hardware authentication is set to **Yes** or **Permissive**. In addition, Cryptographic Security Platform Vault for VM Encryption generates an alert when client operations, such as key access or device registration, occur on the cloned VMs.
Reauthentication on Reboot	Whether a VM in the set must be re-authenticated every time it reboots. The default is No. Setting this value to Yes is similar to requiring a boot-time password before the VM can come up completely.

Revoking KEK Access

If you specified a Key Encryption Key (KEK) when you created the Cloud VM Set, you can revoke access to all of the VMs in the Cloud VM Set by revoking access to the KEK. When you do so, Cryptographic Security Platform Vault for VM Encryption immediately deactivates and detaches all encrypted disks for all VMs in the Cloud VM Set regardless of the KEK expiration date.

The Revoke KEK action can be performed with base64-encoded KEK.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select the Cloud VM Set for which you want to revoke access.

4. Select **Actions > Revoke Key Encryption Key**.
5. Click **Revoke**.
6. To verify that the KEK was revoked, click on the **Key Encryption Key** tab and look at the **Key Encryption Key State** field. While the operation is proceeding, the state is REVOKE_PENDING. When the process is finished, the state changes to REVOKED.

While the key is revoked, you will not be able to add a new VM to the Cloud VM Set or access, encrypt, or decrypt any of the existing VMs in the set. These operations are only available when the KEK state is ACTIVE.

To restore access to the VMs, select the Cloud VM Set then select Actions > Unrevoke Key Encryption Key. Cryptographic Security Platform Vault for VM Encryption restores access to the VMs as long as the KEK has not expired.

Viewing the SEK Key Version for a Disk

When a Cloud Admin generates a new version of the SEK key, Cryptographic Security Platform Vault for VM Encryption does *not* automatically launch a rekey task for all the disks in the Cloud VM Set. It does, however, provide the new version of the SEK key to the Entrust Policy Agent when the Policy Agent needs to encrypt a new disk or rekey an previously encrypted disk.

This gives the Cloud Admin full control over when rekeys take place, but it does mean that some disks in the Cloud VM Set may be using different versions of the SEK key. If data deduplication stops working for some of the VMs in the Cloud VM Set, use this procedure to verify that the encrypted disks are using the most recent version of the SEK key. If there are discrepancies, you can rekey the appropriate disks.

1. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
2. Enter the `hcl keyversion diskname` command, where `diskname` is the name of the disk that you want to check. For Linux, use the short form of the disk name. (For example, `sdb1` instead of `/dev/sdb1`.) For Windows, specify the drive letter or folder mount associated with the disk. (For example, `f:` or `g:\data`). The command returns the key version being used by the disk as well as the current SEK key version. The following example shows a disk that is currently encrypted with an older version of the SEK key:
   # hcl keyversion sdb1
   keyversion: 2 SEKversion: 4

   In this case, you should rekey the disk to bring it up to date. For details, see Rekeying a Disk using the CLI and Rekeying a Disk Using the webGUI.

Changing the SEK Key Expiration Options

You can change the expiry date and expiration option for the version of the SEK key associated with any disk in the Cloud VM Set. When you do so, Cryptographic Security Platform Vault for VM Encryption applies the changes to all disks on all VMs in the Cloud VM Set using the same version of the SEK key as the selected disk.

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI on any node in the cluster using an account with Cloud Admin privileges for the Cloud VM Set you want to modify.
2. In the top menu bar, click **Workloads**.
3. Click the **VMs** tab and select the VM you want to work with from the list.
4. Click the **Expand** button (**>**) at the end of the row to access the details for the specific VM.
5. Click the **Encrypted Disks** tab and select the disk whose expiration date you want to set. Cryptographic Security Platform Vault for VM Encryptiondisplays the **Expiry Date** and **On Expiration** properties for the selected disk below the table.
6. If the **Expiry Date** field displays:

- **Never**, click **Never** and enter a date in the format mm/dd/yyyy or click the calendar icon and select the day from the pop up calendar.
- A date, change the date using the field or the calendar icon. To set the key expiration back to **Never**, click **Clear**.

If the date is valid, Cryptographic Security Platform Vault for VM Encryption displays a confirmation dialog letting you know that these changes will affect all disks on all VMs in the Cloud VM Set that use the same version of the SEK key as the selected disk. Confirm your changes at the prompt.
Cryptographic Security Platform Vault for VM Encryption changes the date and updates the information for the affected disks in the Disk table. If there is a problem, check whether the Cloud VM Set to which this VM belongs has an associated KEK. If it does, you cannot change the key expiration date for the disk beyond the date specified for the KEK.

7. If desired, change what happens when the expiration date arrives for all disks on all VMs in the Cloud VM Set that use the same version of the SEK key as the selected disk. You can select:
   - **No Use**—The key is deactivated but retained. It can be reactivated by setting a future expiration date, or by setting the expiration date to "Never". At that point, all access to the encrypted data will be restored. This is the default.
   - **Shred**—The key is destroyed and cannot be retrieved. You should only use this option if you are absolutely certain that you will never again need to access the data encrypted by this key. If a key is shredded, any data encrypted by this key *cannot* be decrypted.

   When you are finished, click **Save**. At the prompt, confirm that you want to set the expiration option for all disks in the Cloud VM Set using the same version of the SEK key as the selected disk.

Changing SEK Properties

After you create the Cloud VM Set, you can enable or disable the use of SEK for the set as long as there are no VMs registered with the set. If one or more VMs are registered with the Cloud VM Set, you can no longer change these properties.

> Tip: If you want to change the cipher Cryptographic Security Platform Vault uses for the SEK keys, disable SEK for the Cloud VM Set then re-enable it. You can only set the cipher when you first enable SEK.

If you want to change the expiration date or expiration option for a SEK key, see Changing the SEK Key Expiration Options.

Enabling SEK for the Cloud VM Set

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI on any node in the cluster using an account with Cloud Admin privileges for the Cloud VM Set you want to modify.
2. In the top menu bar, click **Workloads**.
3. On the **VM Sets** tab, select the Cloud VM Set for which you want to enable SEK.
4. On the Details tab, click **Enable** in the **Single Encryption Key** field.
5. In the Enable Single Encryption Key dialog box, specify the options you want to use.

Option	Description
Single Key Encryption Expiration	The date on which the SEK key will expire or "Never" if the SEK never expires. If you specify a date and the SEK key expires, access to every encrypted disk on every VM in the Cloud VM Set will be denied. What happens to the SEK key depends on the setting in the Expiration Action field.

Option	Description
Single Key Encryption Expiration Action	• **No Use**—The key is deactivated but retained. It can be reactivated by setting a future expiration date, or by setting the expiration date to "Never". At that point, all access to the encrypted data will be restored. This is the default. • **Shred**—The key is destroyed and cannot be retrieved. You should only use this option if you are absolutely certain that you will never again need to access the data encrypted by this key. If a key is shredded, any data encrypted by this key *cannot* be decrypted.

6. When you are done, click **Enable**. Cryptographic Security Platform Vault creates a SEK key that it will use to encrypt all disks in all VMs registered with this Cloud VM Set until you generate a new SEK key. For details, see Generating a New SEK Key.

Disabling SEK for the Cloud VM Set

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI on any node in the cluster using an account with Cloud Admin privileges for the Cloud VM Set you want to modify.
2. In the top menu bar, click **Workloads**.
3. On the **VM Sets** tab, select the Cloud VM Set for which you want to disable SEK.
4. On the Details tab, click **Disable** in the **Single Encryption Key** field.
5. Confirm that you want to disable SEK at the prompt.

Generating a New SEK Key

When you want to rekey the disks in the Cloud VM Set or you have the Auto Rekey option turned on and you want to have a new SEK key available, you need to manually generate one. When you do, Cryptographic Security Platform Vault for VM Encryption:

- Generates and stores a new version of the SEK key.
- Increments the version number shown in the Single Key Encryption Version field and assigns that version number to the new version of the SEK key.
- Uses the new SEK key version when you tell Cryptographic Security Platform Vault for VM Encryption to encrypt a disk in the Cloud VM Set for the first time.

Cryptographic Security Platform Vault for VM Encryption does *not* automatically rekey any of the previously-encrypted disks. This means that, if you generate a new key and then you encrypt a disk without rekeying the other disks in the Cloud VM Set, data deduplication will not work with the newly-encrypted disk because the data blocks on the new disk will use a different offset from the data blocks on the disks using the older version of the SEK key.

After you rekey the older disks, however, data deduplication will again work for all of the disks in the Cloud VM Set.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. On the **VM Sets** tab, select the Cloud VM Set for which you want to generate a new key.
4. In the **Single Encryption Key State** field, click **Add New Key**.
5. In the Generate New Single Encryption Key dialog box, specify the options you want to use.

Option	Description
Single Key Encryption Expiration	The date on which the SEK key will expire or "Never" if the SEK never expires. If you specify a date and the SEK key expires, access to every encrypted disk on every VM in the Cloud VM Set will be denied. What happens to the SEK key depends on the setting in the Expiration Action field.
Single Key Encryption Expiration Action	• **No Use**—The key is deactivated but retained. It can be reactivated by setting a future expiration date, or by setting the expiration date to "Never". At that point, all access to the encrypted data will be restored. This is the default. • **Shred**—The key is destroyed and cannot be retrieved. You should only use this option if you are absolutely certain that you will never again need to access the data encrypted by this key. If a key is shredded, any data encrypted by this key *cannot* be decrypted.

6. When you are finished, click **Generate**.

What to Do Next

Rekey the disks in the Cloud VM Set or make sure that Auto Rekey is enabled for the Cloud VM Set. For details, see Rekeying a Disk Using the webGUI, Rekeying a Disk using the CLI, and Configuring Auto Rekey for a Cloud VM Set.

Changing KEK Properties

If you want to use a KEK with a Cloud VM Set, you can either specify it during Cloud VM Set creation or add it later.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select the Cloud VM Set whose KEK properties you want to change.
4. Click the **Key Encryption Key** tab. The options you can change are displayed as blue links in the Cryptographic Security Platform Vault for VM Encryption webGUI.
5. Change any available option by clicking on the current value and then entering a new value in the field. When you are finished with each field, click **Save** in that field or your changes will be lost. Cryptographic Security Platform Vault for VM Encryption applies each change as soon as you click **Save**. While the change is in process, the **Key State** changes to ACTIVE_PENDING. When the change has been completed, the **Key State** returns to ACTIVE.

Option	Description
Key Expiration Period	The length of time for which the KEK and all data encryption keys on the VMs will be valid. To indicate that the KEK should never expire, set this field to 0 (zero). If you change the Key Expiration Period, the new expiration period begins from the day you make the change, not from the day the Cloud VM Set was created. When this time period expires: • All disks on all VMs in the Cloud VM Set are automatically detached. What happens to the keys depends on the setting in the **Key Expiration Action** field. • Any attempt to register a new VM with the Cloud VM Set will fail. • Any encrypt or decrypt operation on any of the associated VMs will fail. Note: If the Key Expiration Option field is set to Change, you can shorten the expiration period but you cannot lengthen it beyond the original date.
Key Expiration Action	The options are: • **No Use**—The KEK and all data encryption keys are deactivated but retained. The keys can be reactivated and the expiration date extended if the **Key Expiration Option** field is set to **Extend**. This is the default. • **Shred**—The KEK and all data encryption keys are destroyed and cannot be retrieved. In addition, all VMs in the set are removed from Cryptographic Security Platform Vault for VM Encryption and the Cloud VM Set itself is deleted. **Shred** is a destructive action that cannot be undone. Make sure you have set the correct **Key Expiration Period** when using this option.
Key Expiration Option	The options are: • **No Change**—None of the KEK properties can be changed. The only thing you can do is revoke access to all VMs in the Cloud VM Set by selecting **Actions > Revoke Key Encryption Key**. • **Change**—You can change the expiration options but you cannot set an expiration date beyond the date originally specified when the Cloud VM Set was created. This is the default. • **Extend**—You can change any of the expiration options as desired.
VM Set Retention Period	If Key Expiration Action is set to No Use, this field determines the period of time for which Cloud VM Set objects will be retained after the expiration date is reached. After this period passes, Cryptographic Security Platform Vault for VM Encryption permanently deletes all cloud VMs, the Cloud VM Set, and the associated KEK.

Adding KEK to an Existing Cloud VM Set

You can add a Key Encryption Key (KEK) to an existing Cloud VM Set that contains VMs. A KEK provides an extra layer of security by encrypting the individual data encryption keys on the VMs associated with this Cloud VM Set. It also controls the expiration and revocation of those data encryption keys. When you add the KEK, all existing KeyIDs, disk encryption keys, and any new VM keys created will be encrypted using the KEK. A rekey process will be started to encrypt the existing encryption keys. An alert will be generated when the encryption of all keys has completed successfully.

To protect the KEK, Cryptographic Security Platform Vault for VM Encryption requires that the KEK be stored in a hardware security module (HSM) that is associated with this Cryptographic Security Platform Vault for VM Encryption cluster. For more information, see KEKs with Cloud VM Sets.

After the KEK has been added, you cannot change whether the Cloud VM Set uses a KEK, or what type of KEK is used. The HSM must be available before you can encrypt keys with KEK. Keys will remain accessible by clients when the rekey is in progress.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select the Cloud VM Set to which you would like to add the KEK.
4. Select **Actions > Add KEK**.
5. In the Add KEK to Cloud VM Set window, choose **Use KEK** from the drop-down list and click **Save** to view the Key Encryption Key properties.
6. Complete the required information:

Option	Description
Key Expiration Period	The length of time for which the KEK and all data encryption keys on the VMs will be valid. To indicate that the KEK should never expire, set this field to 0 (zero). This is the default. If you change the Key Expiration Period, the new expiration period begins from the day you make the change, not from the day the Cloud VM Set was created. When this time period expires: • All disks on all VMs in the Cloud VM Set are automatically detached. What happens to the keys depends on the setting in the **Key Expiration Action** field. • Any attempt to register a new VM with the Cloud VM Set will fail. • Any encrypt or decrypt operation on any of the associated VMs will fail. To change the expiration period, click the existing value and enter a new value in the text field, then select days/weeks/months/years from the drop-down list. When you are finished, click Save. Note: If the Key Expiration Option field is set to Change, you can shorten the expiration period but you cannot lengthen it beyond the original date.

Option	Description
Key Expiration Action	The options are: • **No Use**—The KEK and all data encryption keys are deactivated but retained. The keys can be reactivated and the expiration date extended if the **Key Expiration Option** field is set to **Extend**. This is the default. • **Shred**—The KEK and all data encryption keys are destroyed and cannot be retrieved. In addition, all VMs in the set are removed from Cryptographic Security Platform Vault for VM Encryption and the Cloud VM Set itself is deleted. **Shred** is a destructive action that cannot be undone. Make sure you have set the correct **Key Expiration Period** when using this option.
Key Expiration Option	The options are: • **No Change**—The KEK expiration options cannot be changed after the Cloud VM Set has been created. This is the default. Selecting this option means that once the top-level key expires it cannot be reactivated and all VMs will be automatically detached from Cryptographic Security Platform Vault when the expiration date is reached. • **Change**—The KEK expiration options can be changed after the Cloud VM Set has been created, but the **Key Expiration Period** cannot be extended beyond the original date. This is the default. • **Extend**—All KEK expiration options can be changed after the Cloud VM Set has been created.

7. Click **Add**.

Creating a Cloud VM Set for the CSP Vault for VM Encryption

A VM must be part of a Cloud VM Set before you can encrypt it. The set controls global options for the VMs it contains. It also lets you enable the BoundaryControl feature, which uses Policy Rules and constraints in Entrust CloudControl to authenticate and authorize delivery of encryption keys for data encrypted by the Entrust Policy Agent and managed by Cryptographic Security Platform Vault for VM Encryption.

Before You Begin

If you want to use a Key Encryption Key (KEK) with the Cloud VM Set, Cryptographic Security Platform Vault for VM Encryption must have access to a hardware security module (HSM) in which it can store the KEK. For more information, see KEKs with Cloud VM Sets.

Procedure

1. Log in to the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Create New Cloud VM Set**.
4. On the **VM Set** tab:
    a. Enter a name for the Cloud VM Set.
    b. Select the group to which this set should belong, or accept the default.
    c. Optionally enter a description for the set.

5. To specify additional options, click the Additional Properties tab and select the options you want to use.

Option	Description
Heartbeat	The length of time between the heartbeats each VM in the set sends to the Cryptographic Security Platform Vault for VM Encryption to verify that the connection between them is functioning normally. You can specify seconds, minutes, hours, or days. The default is 5 minutes. Set this value to at least 10 seconds. If you make changes to the VMs through the Cryptographic Security Platform Vault for VM Encryption webGUI, those changes are communicated to the VMs during the heartbeat. That means if the heartbeat is set to 5 minutes, then it can take up to 5 minutes for any changes made in the Cryptographic Security Platform Vault for VM Encryption webGUI to be applied to the VMs in the set. If a VM cannot reach the Cryptographic Security Platform Vault for VM Encryption during the heartbeat, the VM continues to run, but it does not pick up any changes until the next successful heartbeat. Cryptographic Security Platform Vault for VM Encryption sets the VM status to Unreachable, but takes no further action unless the heartbeat continues to fail after the Grace Period has expired.
Grace Period	The length of time that can pass without a successful heartbeat. The default is 1 day. You can specify the grace period in seconds, minutes, hours, or days. If a VM remains unresponsive past the grace period, access to the VM's data will be unavailable until the VM is re-authenticated with Cryptographic Security Platform Vault for VM Encryption.
Max Parallel Rekey Operations	The number of concurrent Auto Rekey operations that can be performed for VMs in the Cloud VM Set. The default is 1.
Rekey Interval	If you specify any value other than 0 (zero) for this option, the Cryptographic Security Platform Vault periodically creates a rekey task for every encrypted disk in every VM registered with this Cloud VM Set. You can select any number of days, weeks, months, or years, and the Cryptographic Security Platform Vault for VM Encryption will automatically rekey the encrypted disks on that schedule. To disable Auto Rekey, enter 0 in this field. By default, Auto Rekey is disabled.
Maximum VMs allowed	The maximum number of cloud VMs allowed to register in this Cloud VM Set. The default is unlimited.

Option	Description
Certificate Auto Renewal Period	If you want Cryptographic Security Platform Vault for VM Encryption to automatically renew the certificate for a VM in this Cloud VM Set, enter an integer greater than zero in this field. Cryptographic Security Platform Vault for VM Encryption will renew the certificate that many days before the old one expires. For example, if you enter 5 in this field and a VM certificate is set to expire on June 12, 2022, Cryptographic Security Platform Vault for VM Encryption will renew the license on June 7, 2022. The default is 10 days. The expiry date is always 1 year from the date the certificate was created or renewed. To change the renewal period, click the existing value and enter a new value in the text field, then select days/weeks/months/years from the drop-down list. When you are finished, click Save. If you want to disable certificate auto-renewal, enter 0 (zero) in this field. Note: If you have auto-renewal enabled but the renewal fails, Cryptographic Security Platform Vault for VM Encryption will keep retrying until the certificate is valid. When the certificate is no longer valid, the admin password will be required.
Certificate Expiration	The length of time for which a VM certificate will be valid when it is first registered with Cryptographic Security Platform Vault or when it is auto-renewed by Cryptographic Security Platform Vault. The default is 1 year. To change the expiration, click the existing value and enter a new value in the text field, then select days/weeks/months/years from the drop-down list. When you are finished, click Save. Note: If you change this value for an existing Cloud VM Set, the certificate expiration date does not change for any VMs currently in the set. This value applies only to new VMs or when the certificates for existing VMs are renewed.

Option	Description

Auto Encryption	If this option is enabled, whenever a new VM is registered with this Cloud VM Set, Cryptographic Security Platform Vault for VM Encryption will automatically instruct the Policy Agent to encrypt one or more of the drives on that VM.
	To enable this option, click Disabled, select Enabled from the drop-down list, then click Save. When you do so, the webGUI displays the Encryption Policy fields:
	• **Auto Encryption Policy Type**. This can be:
	  • **Exclude**—The Windows drives and Linux devices listed in the **Auto Encryption Policy Path(s)** field will *not* be automatically encrypted, although they can be encrypted manually at any time. This is the default.
	  • **Include**—The Windows drives and Linux devices listed in the **Auto Encryption Policy Path(s)** field *will be* automatically encrypted. You must encrypt all other drives or devices on the VM manually.
	  • **Encrypt All Devices**—Automatically encrypts all Windows drives and Linux devices.
	• **Auto Encryption Policy Path(s)**—If the policy type is Include or Exclude, enter a path that should be included or excluded. To add additional paths, click the + (Plus sign) in this field. You can enter either a Windows drive or a Linux device name. For example, any of the following would be valid path names: `C:`, `C:\data`, or `sdb1`.
	Important: Each path *must* be on its own line.
	For more information, see Automatic Data Encryption.

Decryption Allowed	If this option is set to Yes, the drives and devices in the VMs registered with this Cloud VM Set can be decrypted. If it is set to No, any decryption request will fail.
Policy Agent Uninstallation Allowed	If this option is set to Yes, you can uninstall the Policy Agent on the VMs registered with this Cloud VM Set. If it is set to No, you cannot uninstall the Policy Agent.

6. To specify when VMs in the Cloud VM Set need to be re-authenticated, click the Reauthentication Settings tab and select the options you want to use.

Option	Description
Reauthentication on IP Change	Whether a VM in the set must be re-authenticated when the VM's IP address changes. The default is No. If your system configuration uses DHCP or multiple NICs, do *not* set this option to Yes. If you do, the VMs in the set may enter a reboot loop if their boot partitions are encrypted and any encrypted drives may be detached.
Reauthentication on H/W Signature Change	Whether a VM in the set must be re-authenticated if its MAC address or UUID changes. The options are: • **Yes**—If *either* the MAC address *or* the UUID changes, the VM requires reauthentication. This is the default. We recommend that you do not change this option. • **Permissive**—Both the MAC address *and* the UUID must change before the VM requires reauthentication. You can use this option if your system administrators perform maintenance on the VMs in this Cloud VM Set that requires changes to the network cards and, therefore, to the VMs' MAC addresses. We recommend you reset this value to **Yes** once maintenance is finished. • **No**—The Cryptographic Security Platform Vault for VM Encryption does not require reauthentication if a VM's MAC address or UUID changes. We strongly recommend that you do **not** select this option. If you do, a cloned or misconfigured VM could gain access to the keys associated with the original VM. If you do select this option, you must confirm the selection before you can proceed. If Cryptographic Security Platform Vault for VM Encryption detects multiple VMs with the same MAC address and UUID combination when hardware validation is off, it generates an alert every 8 hours until the cloned VMs stop heartbeating or hardware authentication is set to **Yes** or **Permissive**. In addition, Cryptographic Security Platform Vault for VM Encryption generates an alert when client operations, such as key access or device registration, occur on the cloned VMs.
Reauthentication on Reboot	Whether a VM in the set must be re-authenticated every time it reboots. The default is No. Setting this value to Yes is similar to requiring a boot-time password before the VM can fully start.

7. If you want to specify a key encryption key (KEK), click the **Key Encryption Key** tab, choose the type of Key Encryption Key Association, and then specify the required information.
   A KEK provides an extra layer of security by encrypting the individual data encryption keys on the VMs associated with this Cloud VM Set. It also controls the expiration and revocation of those data encryption keys. To protect the KEK, Cryptographic Security Platform Vault requires that you store the KEK in the hardware security module (HSM) associated with this Cryptographic Security Platform Vault cluster. For more information, see KEKs with Cloud VM Sets.
   You can add the KEK during Cloud VM Set creation or later.
   a. Determine whether Cryptographic Security Platform Vault for VM Encryption creates a KEK for this Cloud VM Set. To use a KEK, select **Use KEK** from the drop-down list and click **Save** to view the KEK properties.

If you do not make a selection, then the default value is **No KEK Association** is used, and the tab is not populated. If you decide you want to use a KEK, you can add the KEK to the Cloud VM Set later.

b. If you selected USE KEK, complete the following:

Option	Description
Key Expiration Period	The length of time for which the KEK and all data encryption keys on the VMs will be valid. To indicate that the KEK should never expire, set this field to 0 (zero). This is the default. If you change the Key Expiration Period, the new expiration period begins from the day you make the change, not from the day the Cloud VM Set was created. When this time period expires: • All disks on all VMs in the Cloud VM Set are automatically detached. What happens to the keys depends on the setting in the **Key Expiration Action** field. • Any attempt to register a new VM with the Cloud VM Set will fail. • Any encrypt or decrypt operation on any of the associated VMs will fail. To change the expiration period, click the existing value and enter a new value in the text field, then select days/weeks/months/years from the drop-down list. When you are finished, click Save. Note: If the Key Expiration Option field is set to Change, you can shorten the expiration period, but you cannot lengthen it beyond the original date.
Key Expiration Action	The options are: • **No Use**—The KEK and all data encryption keys are deactivated but retained. You can reactivate the keys and extend the expiration date if the **Key Expiration Option** field is set to **Extend**. This is the default. • **Shred**—The KEK and all data encryption keys are destroyed and cannot be retrieved. In addition, all VMs in the set are removed from Cryptographic Security Platform Vault for VM Encryption and the Cloud VM Set itself is deleted. **Shred** is a destructive action that cannot be undone. Make sure you have set the correct **Key Expiration Period** when using this option.
Key Expiration Option	The options are: • **No Change**—You cannot change the KEK expiration options after the Cloud VM Set has been created. This is the default. Selecting this option means that once the top-level key expires, it cannot be reactivated, and all VMs will be automatically detached from Cryptographic Security Platform Vault for VM Encryption when the expiration date is reached. • **Change**—You can change the KEK expiration options after the Cloud VM Set has been created, but you cannot extend the Key Expiration Period beyond the original date. This is the default. • **Extend**—You can change all KEK expiration options after the Cloud VM Set has been created.

8. To use a Single Encryption Key (SEK) for the VMs in this Cloud VM Set, click the **Single Encryption Key** tab and enter the required information.
   If you enable this option, all the VMs registered with the Cloud VM Set will be encrypted with the same encryption key, and the key's expiry date and expiration option will be set at the Cloud VM Set level instead of at the disk level. Using a SEK enables data deduplication because identical blocks at the same offset are encrypted with the same key and therefore remain identical after encryption. For details, see Data Deduplication with Cloud VM Sets.

Option	Description
Single Key Encryption State	This feature is Disabled by default. To enable it, click Disabled, select Enabled from the drop-down list, then click Save. After you click Save, the Cryptographic Security Platform Vault for VM Encryption webGUI displays the remaining SEK option fields.
Single Key Encryption Expiration	The date the SEK key will expire, or "Never" if it never expires. If you specify a date and the SEK key expires, access to every encrypted disk on every VM in the Cloud VM Set will be denied. What happens to the SEK key depends on the setting in the Expiration Action field.
Single Key Encryption Expiration Action	• **No Use**—The key is deactivated but retained. You can reactivate it by setting a future expiration date or by setting the expiration date to "Never". At that point, all access to the encrypted data will be restored. This is the default. • **Shred**—The key is destroyed and cannot be retrieved. Use this option only if you are absolutely certain you will never need to access data encrypted by this key again. If you shred a key, you cannot decrypt any data encrypted with it.

9. After you finish specifying the **Cloud VM Set** options, click **Create**.
10. When you see the **Cloud VM Set Successfully Created** message, click **Close**.

What to Do Next

Install the Policy Agent on the VM(s) you want to encrypt and register it with Cryptographic Security Platform Vault. For details, see the installation and administration guide at:

https://api.managed.entrust.com/vault/latest

Setting Default Cloud VM Set Properties

You can set defaults for some of the Cloud VM Set properties so that, when you create a new Cloud VM Set, those defaults are automatically populated. Changes to these properties are only applied to Cloud VM Sets created after the changes are saved. The changes do *not* affect any existing Cloud VM Sets.

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **Cloud Settings** section, click **Cloud Settings** and specify the options you want to use.

Option	Description
Heartbeat	The length of time between the heartbeats each VM in the set sends to the Cryptographic Security Platform Vault for VM Encryption to verify that the connection between them is functioning normally. You can specify seconds, minutes, hours, or days. The default is 5 minutes. This value should be set to a minimum of 10 seconds. If changes have been made to the VMs through the Cryptographic Security Platform Vault for VM Encryption webGUI, those changes are communicated to the VMs during the heartbeat. That means if the heartbeat is set to 5 minutes, then it can take up to 5 minutes for any changes made in the Cryptographic Security Platform Vault for VM Encryption webGUI to be applied to the VMs in the set. If a VM cannot reach the Cryptographic Security Platform Vault for VM Encryption during the heartbeat, the VM continues to run but any changes made are not picked up by the VM until the next successful heartbeat. Cryptographic Security Platform Vault for VM Encryption sets the status of the VM to Unreachable, but it takes no further action unless the heartbeat continues to fail after the Grace Period has expired.
Grace Period	The length of time that can pass without a successful heartbeat. The default is 1 day. You can specify the grace period in seconds, minutes, hours, or days. If a VM remains unresponsive past the grace period, access to the data on the VM will be unavailable until the VM is re-authenticated with Cryptographic Security Platform Vault for VM Encryption.

4. When you are finished, click **Close**.

Data Deduplication with Cloud VM Sets

Data deduplication (dedupe) eliminates redundant copies of identical data blocks by replacing those data blocks with a pointer to a single "master copy". Dedupe is especially effective across a large number of VMs running the same operating system because most of the OS data blocks are identical on every VM.

When you encrypt those VMs, however, the data blocks are no longer the same because each virtual disk has a different encryption key that changes the content of the encrypted data blocks.

In order to support dedupe, Cryptographic Security Platform Vault for VM Encryption provides the Single Encryption Key (SEK) option for a Cloud VM Set. When enabled, Cryptographic Security Platform Vault for VM Encryption encrypts all VMs in the Cloud VM Set with the same encryption key. This means that, if dedupe found identical data blocks across the VMs *before* they were encrypted, dedupe will find approximately 90% of the same identical data blocks *after*they are encrypted.

You can enable the SEK option when you create the Cloud VM Set, and you can change that option up until you register a VM with Cloud VM Set. After one or more VMs are registered with the set, you cannot change the SEK option for that set.

Considerations

- Using the same key for all VMs in the Cloud VM Set makes the VMs slightly less secure because if a hacker gains access to the SEK key on one VM, they can use that key to access all VMs in the Cloud VM Set.

- The SEK key expiration date and expiration option become global values set when you generate a new SEK key. If you change those options for any disk on any VM in the Cloud VM Set, Cryptographic Security Platform Vault applies the changes to all disks on all VMs in the Cloud VM Set.
- If you generate a new SEK key, you must rekey the encrypted disks in the VMs manually or use the Auto Rekey feature. Cryptographic Security Platform Vault does *not* automatically schedule a rekey task for the VMs when you generate a new SEK key. In addition, the benefits of dedupe will be reduced until all encrypted disks in the VMs in the Cloud VM Set have been rekeyed.
- If you are using the Auto Rekey feature for the Cloud VM Set, a Cloud Admin should manually generate a new SEK key before an automatic rekey operation is about to start. Auto Rekey rekeys the disks using the latest version of the SEK key available. It does not automatically generate a new SEK key before it begins the rekey operation. For more information, see Generating a New SEK Key.
- Before the Policy Agent rekeys a disk it checks to make sure that there is a new version of the SEK key available. If there is not, it raises an alert stating that there is no new SEK key to use and it does not rekey the disk.
- Entrust recommends that you always upgrade your Policy Agents when you upgrade Cryptographic Security Platform Vault for VM Encryption. However, if a VM in the Cloud VM Set is using a version of the Policy Agent older than 4.2, the following caveats apply:
    - The older Policy Agent will always rekey a disk when requested, even if there is no new version of the SEK key. While this does not harm anything, it is a waste of time and resources. It will also adversely impact deduplication while the rekey is in process.
    - If you add or encrypt a Linux disk, or if you add a Windows disk, the older Policy Agent will use the first version of the SEK key. If new SEK keys have been generated in the meantime, the Cloud Admin must rekey the disk after it has been added or encrypted in order for that disk to use the current version of the SEK key. (When you first encrypt a Windows disk, the older Policy Agent correctly uses the current version of the SEK key.)

Related Topics

Creating a Cloud VM Set for the CSP Vault for VM Encryption

Changing SEK Properties

Changing the SEK Key Expiration Options

Generating a New SEK Key

KEKs with Cloud VM Sets

A Key Encryption Key (KEK) provides an extra layer of security by encrypting the individual data encryption keys on the VMs associated with a Cloud VM Set. Both the KEK and the individual data encryption key must be available before the information on the VM can be accessed.

To protect the KEK, Cryptographic Security Platform Vault for VM Encryption requires that the KEK be stored in the hardware security module (HSM) associated with this Cryptographic Security Platform Vault for VM Encryption cluster. If the HSM is not available, then the VMs protected by the KEK cannot be accessed or rebooted. If you decide to associate a KEK with a Cloud VM Set, it is imperative that the HSM be available to Cryptographic Security Platform Vault for VM Encryption at all times.

The KEK also provides a way to control the accessibility of all the associated VMs with a single command. If the KEK expires or is revoked, then all associated VMs become inaccessible at the next heartbeat regardless of the state of their individual data encryption keys.

As the KEK expiration date nears, Cryptographic Security Platform Vault for VM Encryption issues an alert notifying the Domain Admins associated with the Cloud VM Set that the KEK is about to expire. When the expiration date is reached, the KEK state changes from ACTIVE to EXPIRED_PENDING. What happens at that point depends on the Key Expiration Action defined for the KEK. For more information, see Changing KEK Properties.

Considerations

- The HSM must be available before you can encrypt any virtual disk on any VM associated with a Cloud VM Set that uses a KEK.
- After you encrypt the virtual disk, the HSM must be available any time that VM is booted or rebooted, or the boot operation will fail.
- The Cloud Admin user can specify the Cloud VM Set to be associated with a KEK either during the Cloud VM Set creation or at a later time.
- If a Cloud VM Set is associated with a KEK, no VMs can be registered with the Cloud VM Set until Cryptographic Security Platform Vault for VM Encryption has successfully stored the KEK in the HSM.

Effects of Encryption on Thin-Provisioned Disks

Many virtual disks are thin-provisioned so physical storage is only created when the Linux or Windows filesystem allocates and writes new blocks. Encrypting disk partitions can increase the amount of storage required and can, at times, essentially convert thin-provisioned disks to thick-provisioned. The following table describes what will happen for Windows and Linux depending on the disk type and the filesystem that uses it.

Linux Disks

The effect of encryption, decryption, and rekeying on Linux data disk provisioning depends on whether you used the `-s` option with the `hcl encrypt` , `hcl decrypt` , or `hcl rekey` commands. The `-s` option tells `hcl` to only encrypt, decrypt, or rekey the allocated blocks on the disk, and it retains thin-provisioning where possible.

> Note: The `-s` option is *not* supported for root drives, data drives that use the XFS filesystem, or any Linux data drives that have the Online Encryptionfeature enabled. For more information, see Encrypting a Disk Using the CLI.

Filesystem Type	Root Drives	Data Drives with -s Option	Data Drives without -s Option
ext2	Always become thick-provisioned (`-s` not supported).	Thin-provisioned disks remain thin after encryption.	Always become thick-provisioned.
ext3	Always become thick-provisioned (`-s` not supported).	Thin-provisioned disks remain thin after encryption.	Always become thick-provisioned.
ext4	Always become thick-provisioned (`-s` not supported).	Thin-provisioned disks remain thin after encryption.	Always become thick-provisioned.
XFS	Always become thick-provisioned (`-s` not supported).	Always become thick-provisioned (`-s` not supported).	Always become thick-provisioned.

Windows Disks

The effect of data encryption, decryption, or rekeying on Windows disk provisioning depends on the filesystem type and whether the target is a boot drive or a data drive. For each filesystem, the results are the same for MBR and GPT partitions.

Filesystem Type	Boot Drives	Data Drives
NTFS	Always become thick-provisioned as all blocks on the boot drive are encrypted.	Data drive encryption, decryption, and rekeying preserves thin disks. We have measured around 5% increase in thin volume space utilization when the drive is first encrypted.
ReFS	Boot drive encryption is not supported for ReFS.	Data drive encryption, decryption, and rekeying preserves thin disks. We have measured around 5% increase in thin volume space utilization when the drive is first encrypted.

Configuring Vault Authentication for CSP Vault for VM Encryption

By default each vault is configured for local authentication. You can change the authentication method as required. In the current release, you can choose between local authentication, Active Directory, OpenID Connect (OIDC) with AD, or OIDC without AD.

> Note: You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users.

For details on configuring each authentication option, see:

- Configuring Active Directory for the CSP Vault for VM Encryption
- Configuring Local Authentication for CSP Vault for VM Encryption

Configuring Active Directory for the CSP Vault for VM Encryption

By default the vault is configured for local authentication. You can change the authentication method as required.

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. On the Authentication page, select **LDAP** as the Authentication Type.
5. On the Domain tab, enter:

Field	Description
Domain Name	Enter the domain name for the service account.
Directory Service Type	If you plan to use Microsoft AD directory services, select Microsoft AD. Select OpenLDAP for all non-Microsoft AD directory services.

Field	Description
Service Account Name	Enter the name of the service account for given domain. For example: Administrator. The service account needs read-only access for users and groups on the domain and any subdomain that is used. Note: The service account name and password is required.
Service Account Password	Enter the password for the service account.
UID Attribute	Enter the Security Manager Account Name (sAMAccountName) for the user. This is the attribute of the user or group object that would be queried during search.

6. Click **Apply** to save the changes.
7. Click the Domain Controllers tab.
   To add a controller, select **+**. The Add Domain Controller window appears.
   Add the following details:

Field	Description
Server URL	Select LDAP:// or LDAPS://, then enter the domain name or IP address. To include a port number, enter `<ip-address>:<port>`.
STARTTLS	If you selected LDAP, check the checkbox if you want to use LDAP over TLS. Note: This is not available if you selected LDAPS.
CA Certificate	The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller. The CA certificate must be in Base64-encoded pem format. If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates. Click Load File to select the CA certificate that you want to use.

Field	Description
User Search Context (Base DN)	Enter the Distinguished Name (DN) of the node where the search for users should start. This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP. For performance reasons, the base DN should be as specific as possible. For example, `dc=ldapserver,dc=com`.
Group Search Context (Base DN)	Enter the Distinguished Name (DN) of the node where the search for Security groups should start. This option applies to AD Security groups being associated with a Cloud Admin Group.
Timeout	Set the timeout in seconds before connecting to an alternate domain controller. If multiple domain controllers are specified, this is the amount of time Cryptographic Security Platform Vault waits for a response before it re-sends the request to another domain controller. This option only applies to the TCP/LDAP request. It does not apply to the DNS request before the LDAP server has been successfully contacted. If the DNS server is down, Cryptographic Security Platform Vault may take longer than the length of time specified here before it fails over to the next domain controller in the list or it considers the authentication request to have failed.

8. Click **Save and Close**.

If you want to add an Active Directory Group, complete the following:

1. From the Cryptographic Security Platform Vault for VM Encryption webGUI, in the top menu bar, click **Security**.
2. Click the Groups tab.
3. Select **Actions > Create Group**.
4. On the Group tab, enter the name of the group and click **Next**.
5. On the Active Directory Groups tab, type the first three letters of the group to fetch the group name from the AD server.
6. Click **Next**.
7. On the KeyControl Managed User Members tab, select the managed users that you want to assign and click the right arrow icon.
8. Click **Create**.

For information on using Cloud Admin groups with this Cryptographic Security Platform Vault, see Cloud Admin Groups and CSP Vault User Accounts.

Configuring Local Authentication for CSP Vault for VM Encryption

Local authentication is enabled by default when you create a vault. If using local authentication, no further authentication configuration is required. The next step is to configure your access policies and users.

> Note: You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users.

Managing Authentication for Vault for VM Encryption

By default each vault is configured for local authentication. You can change the authentication method as required. In the current release, you can choose between local authentication, Active Directory, OpenID Connect (OIDC) with AD, or OIDC without AD.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users.

For details on configuring each authentication option, see:

- Configuring local authentication for Vault for VM Encryption
- Configuring Active Directory for the Vault for VM Encryption
- Configuring OIDC with Active Directory for Vault for VM Encryption
- Configuring OIDC for Vault for VM Encryption
- Managing two-factor authentication in Vault for VM Encryption

Configuring local authentication for Vault for VM Encryption

Local authentication is enabled by default when you create a vault. If using local authentication, no further authentication configuration is required. The next step is to configure your access policies and users.

> You can change the authentication method as required. If you change the authentication method, local authentication will still be available. For example, you can configure LDAP or OIDC for all of your users, but have local authentication available for admin users

Configuring Active Directory for the Vault for VM Encryption

See below for configuring Active Directory for the Vault for VM Encryption.

> By default, the vault uses local authentication. You can change the authentication method as required.

To configure Active Directory

1. Log in to the CSP Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. On the Authentication page, select **LDAP** as the Authentication Type.
5. On the **Domain** tab, enter:
    - Domain Name—Enter the domain name for the service account.
    - Directory Service Type—Select **Microsoft AD** if you plan to use Microsoft AD directory services, or **OpenLDAP** for all non-Microsoft AD directory services.

- Service Account Name—Enter the name of the service account for the given domain (for example, Administrator).

  > The service account needs read-only access to users and groups on the domain and any subdomain used.

- Service Account Password —Enter the password for the service account.
- UID Attribute—Enter the Security Manager Account Name (sAMAccountName) for the user.

  > This is the attribute of the user or group object that would be queried during search.

6. Click **Apply** to save the changes.
7. Click the **Domain Controllers** tab.
8. Click **+**
9. Add the following details in the **Add Domain Controller** window.
   - Server URL
   - STARTTLS
   - CA Certificate
   - User Search Context (Base DN)
   - Group Search Context (Base DN)
   - Timeout
10. Click **Save and Close**.

Server URL

Select LDAP or LDAPS and enter the domain name or IP address. To include a port number, use the following syntax:

```
<ip>:<port>
```

STARTTLS

If you selected LDAP, check the checkbox if you want to use LDAP over TLS.

CA Certificate

The certificate chain of all the Trusted Certificate Authorities that can verify the SSL certificate used by the domain controller.

- The CA certificate must be in Base64-encoded PEM format.
- If the CA certificate file you are uploading contains just the certificate of the root certificate authority, make sure that the SSL certificate used by the Domain Controller contains the entire chain of intermediate CA certificates.

Click Load File to select the CA certificate that you want to use.

User Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the user search should start. For performance reasons, make the base DN as specific as possible. For example:

```
dc=ldapserver,dc=com
```

This option applies to Cryptographic Security Platform Vault-managed account names that are authenticated through LDAP.

Group Search Context (Base DN)

Enter the Distinguished Name (DN) of the node where the search for Security groups should start.

This option applies to AD Security groups being associated with an admin group.

Timeout

Set the timeout in seconds before connecting to an alternate domain controller.

- If multiple domain controllers are specified, this is how long the Cryptographic Security Platform Vault waits for a response before re-sending the request to another domain controller.
- If the DNS server is down, Cryptographic Security Platform Vault may take longer than the time specified here before it fails over to the next domain controller in the list or considers the authentication request failed.

This option only applies to the TCP/LDAP request. It does not apply to the DNS request before the LDAP server has been successfully contacted.

Configuring OIDC with Active Directory for Vault for VM Encryption

By default, the vault uses local authentication. You can change the authentication method as required, and you can have multiple authentication modes active at the same time. However, OIDC without Active Directory cannot be used with Active Directory, and OIDC with Active Directory cannot be used without Active Directory.

You cannot disable OIDC authentication once it is configured. After you enable OIDC, you can no longer sign in with AD credentials. However, you can sign in using local authentication credentials without any issues.

To configure OIDC

1. Log in to the Vault web GUI.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Authentication**.
4. In the **Choose Authentication Type** drop-down menu, select:
    - **OpenID Connect** to configure OIDC without Active Directory
    - **OpenID Connect (with AD)** to configure OIDC with Active Directory
5. Click the **Learn more about configuring the OIDC Provider** link to view the OIDC provider's login redirect URL and logout redirect URL.
6. Specify the OpenID Connect Configuration settings:
    - Name
    - Client ID
    - Client Secret
    - Base URL
7. Optionally, click **Load File** to upload the CA certificate in base64-encoded PEM format.
8. Click **Apply**.

9. Select **Verify and Enable**. After verification, a message appears confirming OpenID Connect has been successfully enabled. Vault is set for OIDC authentication.
10. Sign out from the vault and sign in to the vault as an OIDC user by selecting **Sign in with IDAAS** and entering your OIDC credentials.

Name

A user-defined name for the OpenID Connect provider.

> Cryptographic Security Platform Vault displays this name on the button in the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

> This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Configuring OIDC for Vault for VM Encryption

By default, the KeyControl Vault Management application is configured for local authentication. You can change the authentication method as required, but you can use only one type of authentication per vault at a time.

- If you want to use OIDC without AD, you can only change to that mode from the local authentication mode.
- If you have configured AD or OIDC with AD, you cannot change to OIDC without AD.

Each vault can be configured with a separate OIDC server or a separate application from same server.

> OIDC without AD is the recommended mode of OIDC authentication method where the OIDC provider independently manages identity and authentication. For new OIDC setups, this is the preferred option.

To configure OIDC

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **Authentication**.
5. In the **Choose Authentication Type** drop-down list, select **OpenID Connect**.
6. Specify the OpenID Connect Configuration settings:
    - Name
    - Client ID
    - Client Secret

- Base URL

7. Optional. Click **Browse** to upload the CA Certificate.

   The certificate needs to be in base64 encoded pem format.

8. Enter the Admin Name and Admin Email for OIDC user. This user will be created and will act as the Vault Administrator. They will be assigned to the admin policy and receive the email with the registration URL.
9. Click **Apply**. The OpenID Connect Configuration window appears showing the current configuration.
10. Click **Verify and Enable**. The OpenID Connect Successfully Configured window displays the new login URL.
11. Copy the URL, and click **Log Out and Sign in with IDP**.
12. After you are logged out, paste the URL into the browser window.
13. Log in to the Identity Provider using the name and password that you created.

Name

A user-defined name for the OpenID Connect provider. Cryptographic Security Platform Vault displays this name on the button on the login dialogs.

Client ID

The organizational identity assigned by the OpenID Connect provider when you sign up for the service.

Client Secret

A cryptographic component used to secure the organization's access to the OpenID Connect provider.

This field is write-only. It will never be displayed again after it has been initially created. It can be reentered if necessary.

Base URL

The URL that Cryptographic Security Platform Vault will use to contact the OpenID Connect provider to present the login page.

Managing two-factor authentication in Vault for VM Encryption

Two-factor authentication requires you to enter two forms of identification before you can access your CSP Vault.

- The first form is your standard username and password combination,
- The second is a one-time password (OTP) generated by an authorization app. The OTP is appended to your existing password.

See below for how to enable and manage it.

- Requirements for enabling two-factor authentication in Vault for VM Encryption
- Enforcing two-factor authentication in Vault for VM Encryption
- Disabling two-factor authentication in Vault for VM Encryption

Two-factor authentication is supported with local authentication only. If you want to use two-factor authentication for non-local users, we recommend enabling it in your remote authentication provider.

Requirements for enabling two-factor authentication in Vault for VM Encryption

Make sure you have access to an authentication app that can generate HOTP or TOTP passwords. For example:

- For TOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. These applications continuously generate passwords valid for 30 seconds. If the current password expires before you can submit the login request, you must wait for it to generate a new password, then use that to log in.
- For HOTP authentication, you can use an app such as Google Authenticator or Microsoft Authenticator. A password generated through the application is valid from the time you create it until you use it to log in. To log in again, click **Next** in the app to generate a new password.

Enforcing two-factor authentication in Vault for VM Encryption

See below for enforcing two-factor authentication in Vault for VM Encryption.

- Enforcing two-factor authentication for the current user
- Enforcing two-factor authentication for all users

Enforcing two-factor authentication for the current user

See below for enforcing two-factor authentication for the current user.

To enforce two-factor authentication for the current user

1. Log in to the Cryptographic Security Platform Vault for VM Encryption webGUI.
2. In the top menu bar, click **Settings**.
3. In the **Two-Factor Authentication** field, click **Set up Two-Factor Authentication**.
4. In the **Enable Two-Factor** dialog box, select the HOTP or TOTP radio button.
5. Scan the generated barcode with your authorization app.
6. Enter the six-digit verification code from your app in the dialog box.
7. Click **Continue**. Cryptographic Security Platform Vault verifies the code and displays a message indicating success or failure. If the code is not correct, re-enter it.
8. After the code has been accepted, click **Done**.
9. When you log into the Vault web GUI:
    - Enter a valid OTP along with your standard account password on the login page. Do not add any characters or spaces between your account password and the one-time password generated by your authorization app. For example, if your password is `XyZ123$`, and your OTP is `32325`, you enter `XyZ123$32325` in the password field.
    - If you use TOTP, make sure your password doesn't expire before you submit the login request.

Enforcing two-factor authentication for all users

See below for enforcing two-factor authentication for all Vault users

To enforce two-factor authentication for all users

1. Log into the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the **Two-Factor Authentication Settings** page, select **ENFORCED**.
5. Click **Apply**.

Disabling two-factor authentication in Vault for VM Encryption

See below for disabling two-factor authentication in Vault for VM Encryption.

- Disabling two-factor authentication for a user
- Disabling two-factor authentication for all users

Disabling two-factor authentication for a user

See below to disable two-factor authentication for a single Vault user.

To disable two-factor authentication

1. Log in to the Vault web GUI using an account with Security Admin privileges.
2. In the top menu bar, click **Security**.
3. Select the **Users** tab
4. Select the user for whom you want to disable two-factor authentication.
5. In the **Details** tab below the table, click the **Enabled** link for the **Two-Factor Authentication** row.
6. In the **Disable Two-Factor Authentication** window, click **Proceed**.

Disabling two-factor authentication for all users

See below to disable two-factor authentication for all Vault users.

To disable two-factor authentication for all users

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section, click **Two-Factor Authentication Settings**.
4. On the Two-Factor Authentication Settings page, select **NOT ENFORCED**.
5. Click **Apply**.

External Authentication Provider Examples

- Example: Configuring Azure OIDC to use with CSP Vault
- Example: Configuring Entrust Identity as a Service

Example: Configuring Azure OIDC to use with CSP Vault

The following example shows how to configure Azure OIDC to use with Cryptographic Security Platform Vault for External Authentication using Open ID Connect. You will need to register Entrust Cryptographic Security Platform as a Microsoft Azure application, then copy the following information from Azure and paste it into Cryptographic Security Platform Vault:

- the Client Secret
- the Application (client) ID
- the base URL

Procedure

1. In Microsoft Azure, click **App Registrations** in the sidebar.
2. Click **New Registration**.
3. In the Register an application page, enter the name to use for the application and enter the following redirect URIs:
    - Set the Login Redirect URIs for all nodes in the cluster to: `https://<IP or FQDN of Cryptographic Security Platform Vault node>/v5/oidc/callback`
    - Set the Logout Redirect URIs for all nodes in the cluster to: `https://<IP or FQDN of Cryptographic Security Platform Vault node>/v5/kc/oidc/logout`
4. Click **Register**.

After the application is created, you will be taken to the new application page.

5. Copy the Application (client) ID to a text window for later use.
   Important: This will be the application (client) ID that you will paste into Cryptographic Security Platform Vault.
6. Click **Certificates & secrets** in the sidebar to create a client secret.
7. In the Client secrets section, click **New client secret**.
8. In the Add a client secret window, enter a description, set the expiration date, and click **Add**.
   The new client secret appears in the Client secrets section.
9. Copy the client secret value to a text window for later use.
   Important: This will be the client secret that you will paste into Cryptographic Security Platform Vault.
10. Click **Token configuration** in the sidebar and then click **Add optional claim**.
11. In the Add optional claim window, select 'ID' for the token type and 'upn' and 'sid' for the claim.
12. Click **Add**.
13. In the pop-up window, check the 'Turn on the Microsoft Graph profile permission (required for claims to appear in token) checkbox.
14. Click **Overview** in the sidebar, and then click **Endpoints**.
15. In the Endpoints window, copy the OpenID Connect metadata document (up to and including the v2.0) to a text window to find the OpenID Connect URI or Issuer URI. This is the only URL in the Endpoints window that ends with /.well-known/openid-configuration.
    For example, if the OpenID Connect metadata document field has the URL https://login.microsoftonline.com/<GUID>/2.0/.well-known/openid-configuration, you will need to ignore everything after the /2.0 and copy this section to a text window for later use: https://login.microsoftonline.com/<GUID>/2.0.
    Important: This will be the base URL that you will paste into Cryptographic Security Platform Vault.
16. Close the Endpoints window to return to the Overview page.

Example: Configuring Entrust Identity as a Service

The following example shows how to configure Entrust Identity as a Service (IDaaS) to use with CSP Vault for External Authentication using Open ID Connect.

1. Log into Entrust IDaaS with your user name and one time password (OTP).
2. After you have logged in, click **Applications**.
3. Click the + icon to create a new Generic OpenID Connect and OAuth Cloud Integration.
4. Create a Generic Web Application using the following:
   Note: Use the default for all other settings.
   - General Settings:
     - Copy and paste the Client ID and the Client Secret to a safe location. These will be used when configuring OIDC in Entrust CloudControl.
     - Set the Token / Revocation Endpoint Client Authentication Method to Client Secret Post.
     - Set the Login Redirect URIs for all nodes in the cluster to: `https://<IP or FQDN of Cryptographic Security Platform Vault node>/v5/oidc/callback`
     - Set the Logout Redirect URIs for all nodes in the cluster to: `https://<IP or FQDN of Cryptographic Security Platform Vault node>/v5/kc/oidc/logout`
   - Authentication Settings:
     - Check the Require Consent checkbox.
     - Under Grant Types Supported, check the Authorization Code checkbox.
   - Supported Scopes
     - Select the Your unique identifier checkbox.
     - Select the Email address checkbox.

5. Add a resource rule to the AD Group so that the AD group and users from that AD group can access the application.

Personal Access Tokens

Personal Access tokens allow you to use automation scripts and CLI commands in your Cryptographic Security Platform Vaults that are using OIDC for authentication.

The following vaults must have OIDC without AD configured:

- Cryptographic Security Platform Vault for Cryptographic APIs
- Cryptographic Security Platform Vault for KMIP
- Cryptographic Security Platform Vault for Secrets

The following vaults support using OIDC, AD or local authentication at the same time. For these vaults, only users with the OIDC authentication type (OIDC without AD) can use personal access tokens.

- Cryptographic Security Platform Vault for Cloud Keys
- Cryptographic Security Platform Vault for Databases
- Cryptographic Security Platform Vault for VM Encryption

Each user can have one personal access token. The tokens act like passwords, and are not stored in Cryptographic Security Platform Vault. You must keep track of your own personal access token and keep it safe. If the personal access token is lost, there is no way to retrieve it. You will need to delete the existing token and create a new one.

Once created, you can use your personal access token when you login by providing it as a password. This allows your scripts and CLI to function seamlessly.

This section includes:

- Creating a Personal Access Token
- Deleting a Personal Access Token

Creating a Personal Access Token

Depending on your Cryptographic Security Platform Vault, the creation process differs.

Creating a Personal Access Token with the Application Security, KMIP, and Secrets Vaults:

1. Log into one of the following vaults:
   - Cryptographic Security Platform Vault for Cryptographic APIs
   - Cryptographic Security Platform Vault for KMIP
   - Cryptographic Security Platform Vault for Secrets
2. In the top right of the webGUI, click the Account icon drop-down and select **Personal Access Token**.
3. In the Generate Personal Access Token window, enter your name, the description, and the expiration date for the token.
4. Click **Generate Token**.
   CSP Vault generates the token, and displays it in the Personal Access Token Successfully Generated window. Copy the token and keep it in a safe place.
   Important: If you do not save the token now, you will need to create a new personal access token.

Creating a Personal Access Token with the Cloud Keys, Databases, and VM Encryption Vaults:

1. Log into one of the following vaults:
   - Cryptographic Security Platform Vault for Cloud Keys
   - Cryptographic Security Platform Vault for Databases
   - Cryptographic Security Platform Vault for VM Encryption

2. In the top right of the webGUI, click the account name drop-down and select **Personal Access Token**.
3. Click **Generate Token**.
   CSP Vault generates the token, and displays it in the Personal Access Token Successfully Generated window. Copy the token and keep it in a safe place.
   Important: If you do not save the token now, you will need to create a new personal access token.

Deleting a Personal Access Token

You can delete your personal access tokens from the Edit Personal Access Token window.

Deleting a Personal Access Token with the Application Security, KMIP, and Secrets Vaults:

1. Log into one of the following vaults:
   - Cryptographic Security Platform Vault for Cryptographic APIs
   - Cryptographic Security Platform Vault for KMIP
   - Cryptographic Security Platform Vault for Secrets
2. In the top right of the webGUI, click the Account icon drop-down and select **Personal Access Token**.
3. In the Edit Personal Access Token window, click **Delete Token**.
4. In the confirmation window, click **Delete**.

Deleting a Personal Access Token with the Cloud Keys, Databases, and VM Encryption Vaults:

1. Log into one of the following vaults:
   - Cryptographic Security Platform Vault for Cloud Keys
   - Cryptographic Security Platform Vault for Databases
   - Cryptographic Security Platform Vault for VM Encryption
2. In the top right of the webGUI, click the account name drop-down and select **Personal Access Token**.
3. In the Edit Personal Access Token window, click **Delete Token**.
4. In the confirmation window, click **Delete**.

Cloud Admin Groups and CSP Vault User Accounts

Cloud Admin Groups and Cryptographic Security Platform Vault User Accounts apply to the following Cryptographic Security Platform Vaults only:

- Cryptographic Security Platform Vault for Cloud Keys
- Cryptographic Security Platform Vault for Databases
- Cryptographic Security Platform Vault for VM Encryption

This section includes:

- Cloud Admin Groups
- Cloud Admin Groups Overview

Cloud Admin Groups

Every VM that you register with Cryptographic Security Platform Vault must be assigned to a specific Cloud VM Set. A Cloud VM Set is a logical grouping of related VMs, such as "Amazon EC2 VMs," "Azure VMs," and "Legal Dept VMs". The configuration settings specified for a specific Cloud VM Set apply to all VMs registered with that set.

Every Cloud VM Set must be associated with a Cloud Admin Group that determines the list of Cryptographic Security Platform Vault users and Active Directory (AD) Security groups that can see and managed the VMs in that Cloud VM Set. All Cryptographic Security Platform Vault users that have access to a specific Cloud Admin Group can see all of the VMs registered with all of the Cloud VM Sets in that group.
Likewise, Cryptographic Security Platform Vault alerts and audit log entries that pertain to the VMs in a Cloud Admin Group can be seen by all members of that group, but they cannot be seen by the members of other Cloud Admin Groups.

When you install Cryptographic Security Platform Vault, the installer creates a default group called `Cloud Admin Group` and assigns the default user account, `secroot`, to that group. You can change the name of the default Cloud Admin Group or remove `secroot` from that group, but you cannot delete that group.

In order to be associated with one or more Cloud Admin Groups, a Cryptographic Security Platform Vault user account must have Cloud Admin privileges. If you assign an Active Directory (AD) Security group to a Cloud Admin Group, then every individual user who is a member of that Security group in Active Directory will be given Cloud Admin access to all of the VMs registered with all of the Cloud VM Sets that are associated with the Cloud Admin Group. (For more information, see Considerations When Using AD Security Groups.)

If you want to limit the access to the VMs registered with Cryptographic Security Platform Vault, you can create multiple Cloud Admin Groups and Cloud VM Sets. Then you can distribute the Cloud VM Sets among the Cloud Admin Groups and create a different membership list for each Cloud Admin Group.

For example, let's say you have 5 VMs in the Midwestern US and another 10 VMs in India. You want the US VMs to be managed by one group of users and the Indian VMs to be managed by another. In addition, you have a small set of superusers who can manage all aspects of Cryptographic Security Platform Vault as well as any VM anywhere in the world.

To achieve this configuration, you could:

1. Create two Cloud Admin Groups, one called **US-MidWest** and the other called **India-Bangalore**.
2. Create a Cryptographic Security Platform Vault-managed Cloud Admin user account for *each* Midwestern user, or create an AD Security group on your AD server and then assign the relevant Midwest AD user accounts to that AD Security group. When you are done, add the Cryptographic Security Platform Vault user accounts or the AD Security group as members of the **US-MidWest** Cloud Admin Group.
3. Create a Cryptographic Security Platform Vault-managed Cloud Admin user account for *each* Indian user, or create an AD Security group on your AD server and then assign the relevant Indian AD user accounts to that AD Security group. When you are done, add the Cryptographic Security Platform Vault user accounts or the AD Security group as members of the **India-Bangalore** Cloud Admin Group.
4. Create two Cloud VM Sets, one called **US-MidWest-VMs** associated with the US-MidWest Cloud Admin Group and the other called **India-Bangalore-VMs** associated with the India-Bangalore Cloud Admin Group.
5. Add the Midwest VMs to the **US-MidWest-VMs** Cloud VM Set.
6. Add the Indian VMs to the **India-Bangalore-VMs** Cloud VM Set.
7. Create a Cryptographic Security Platform Vault-managed user account for each superuser with all three user roles (Security Admin, Domain Admin, and Cloud Admin), and assign them to the **US-MidWest** Cloud Admin Group and the **India-Bangalore** Cloud Admin Group.
   Note: These superuser accounts must be created in and managed by Cryptographic Security Platform Vault so that they can be assigned Security Admin and Domain Admin privileges. Users from an AD Security group can only be assigned Cloud Admin privileges.

This section includes:

- Deleting a Cloud Admin Group
- Changing a Cloud Admin Group
- Creating a Custom Cloud Admin Group
- Considerations when using AD Security Groups

Deleting a Cloud Admin Group

You can only delete a Cloud Admin Group if there a no Cloud VM Sets registered with the group and no Cryptographic Security Platform Vault-managed users or Active Directory (AD) groups associated with the group.

To verify that there are no associated Cloud VM Sets or AD groups, you can look at the KeyControl User Members, AD Group Members, and Number of VM Sets columns on the Security > Groups tab. All three of these columns must show 0 (zero) members before you can delete the group.

> Note: You cannot delete the Cloud Admin Group created when Cryptographic Security Platform Vault was installed. The default name for this group is Cloud Admin Group.

Procedure

1. If there are Cloud VM Sets still associated with this Cloud Admin Group:
    a. Log into the Cryptographic Security Platform Vault webGUI using an account with Cloud Admin privileges. This account must be a member of the Cloud Admin Group that you intend to delete. In addition, if you want to transfer the Cloud VM Sets to another Cloud Admin Group instead of deleting them, this account must also be a member of the Cloud Admin Groups to which you want to transfer the Cloud VM Sets.
    b. In the top menu bar, click **Workloads**.
    c. On the **VM Sets** tab, look at the **Group** column. For each Cloud VM Set that is registered with the Cloud Admin Group you want to delete, either delete that Cloud VM Set or associate that Cloud VM Set with a new Cloud Admin Group.
2. If necessary, log into the Cryptographic Security Platform Vault webGUI on any node in the cluster using an account with Security Admin privileges.
3. In the top menu bar, click **Users**.
4. Click the **Groups** tab.
5. Select the group you want to delete.
6. Click the **Members** tab and remove any AD groups or Cryptographic Security Platform Vault-managed users.
7. Click **Actions > Delete Group**.
8. Click **Proceed** at the prompt.

Changing a Cloud Admin Group

Before You Begin

If you want to associate one or more AD Security groups with this Cloud Admin Group, make sure that:

- You have reviewed the considerations described in Considerations When Using AD Security Groups.
- The Security groups you want to add already exist in the AD server and contain only the users who require access to Cryptographic Security Platform Vault.
- Cryptographic Security Platform Vault can communicate with your AD authentication server.

Procedure

1. Log in to the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Security**.
4. Click the **Groups** tab.
5. Select the group you want to modify.
6. On the **Group** tab, click the **Name** or **Description** to change that field.
7. Click **Save** in the field to save your changes.
8. To change the users in a group, click the **Members** tab.

- To assign an AD Security group, start typing the name of the Security group in the **Active Directory Groups** field. Cryptographic Security Platform Vault automatically searches the associated AD server and displays a list of Security groups matching what you have typed. Select the Security group you want to add from the list. As soon as you select the Security group name, all members of that Security group can immediately access Cryptographic Security Platform Vault with Cloud Admin privileges and see all of the VMs registered to all of the Cloud VM Sets that are assigned to this Cloud Admin Group.
  Note: If the text you enter matches many AD groups, the AD server may return the message "Size Limit Exceeded". If this happens, enter a longer search string to limit the number of matches the AD server returns.
- To assign a Cryptographic Security Platform Vault-managed user to the group, move them to the **Assigned Users** list box. To remove a Cryptographic Security Platform Vault-managed user from the group, move them to the **Available Users** list box.

Your changes are saved automatically.

Creating a Custom Cloud Admin Group

This applies to the following vaults only:

- Cryptographic Security Platform Vault for Cloud Keys
- Cryptographic Security Platform Vault for Databases
- Cryptographic Security Platform Vault for VM Encryption

Cloud Admin Groups can contain Cryptographic Security Platform Vault-managed user accounts with Cloud Admin privileges or Active Directory (AD) Security groups whose members are automatically granted Cloud Admin privileges when they log into Cryptographic Security Platform Vault.

Users with Cloud Admin privileges:

- Can manage the encryption of virtual machines that have the Entrust Policy Agent installed.
- Can create and manage Cloud VM Sets, which separate the encrypted VMs into logical groups such as "VMs running in AWS" or "UK Data Center VMs". The configuration settings selected for a Cloud VM Set are automatically applied to all VMs in that set.
- Can set options for specific VMs that override the default options specified in the Cloud VM Set.
- Can create certificates for VMs and specify key expiration dates.
- Can revoke access to individual encrypted disks/filesystems, or the whole VM. When access to disks is revoked, filesystems are forcibly unmounted, thus removing access to clear-text data.
- Can create encryption keys to securely move encrypted data between specified VMs in the same Cloud VM Set.
- Can view audit records and alerts generated from the all VMs in the Cloud VM Sets to which they have access.

Before You Begin

If you want to associate one or more AD Security groups with this Cloud Admin Group, make sure that:

- You have reviewed the considerations described in Considerations When Using AD Security Groups.
- The Security groups you want to add already exist in the AD server and that they contain only those users who require access to Cryptographic Security Platform Vault.
- Cryptographic Security Platform Vault can communicate with your AD authentication server. For details, see the appropriate link:
  -

Procedure

1. Log into the appropriate Cryptographic Security Platform Vault webGUI using an account with Security Admin privileges.
   This can be one of the following vaults:

- Cryptographic Security Platform Vault for Cloud Keys
- Cryptographic Security Platform Vault for Databases
- Cryptographic Security Platform Vault for VM Encryption

2. From the Home tab, select **Security > Access Policies**.
3. On the Manage Access Policies page, you can create a new policy or use an existing policy. The policy must have admin permissions.
   By default, when you configure AD, it will add the AD group and rescue user to the default policy.
4. On the About tab of the Create Access Policy dialog box, complete the following:

Field	Description
Name	Enter the policy name.
Description	Optionally enter a description for the policy.
Role	This is set to User for all policies other than the admin policy.
Users	Select the required users to be added to the policy. If the vault is configured for Active Directory authentication, select User or Group and search for the required AD user or AD group.

5. Click **Continue**.
6. On the Permissions tab of the Create Access Policy dialog box, select whether to grant All Permissions or Specific Permissions to the users.
7. If you selected Specific Permissions, check the checkboxes for each permission that you want to assign.
8. Click **Apply**.
9. Click the **Groups** tab.
10. Click **Actions > Create Group**.
11. In the **Add New Group** dialog box on the **Group** tab, specify the options you want to use.

Option	Description
Group Name	The name of the new Cloud Admin Group.
Description	An optional description of the group.

12. Click **Next**.
13. To add Cryptographic Security Platform Vault users to the group, click the **Members** tab.
    - To assign an AD Security group, start typing the name of the group in the **Active Directory Groups** field. Cryptographic Security Platform Vault automatically searches the associated AD server and displays a list of Security groups matching what you have typed. Select the group you want to add from the list. All members of the selected AD Security group will be able to access Cryptographic Security Platform Vault with Cloud Admin privileges and see all of the VMs registered to all of the Cloud VM Sets that are assigned to this Cloud Admin Group.
      Note: If the text you enter matches a large number of AD groups, the AD server may return the message "Size Limit Exceeded". If this happens, enter a longer search string to limit the number of matches returned from the AD server.

- To assign a Cryptographic Security Platform Vault-managed user to the group, move that user from the **Available Users** list box to the **Assigned Users** list box.

14. Click **Create**.

Considerations when using AD Security Groups

- Cryptographic Security Platform Vault only supports Active Directory (AD) Security groups. You cannot assign an AD Distribution group to a Cloud Admin Group.
- Cryptographic Security Platform Vault evaluates only a user's Secondary AD group memberships when determining the user's privileges. It does *not* evaluate the user's Primary AD group membership. Therefore, all privileges must come from Secondary AD Security groups.
- Cryptographic Security Platform Vault supports one AD domain for account authentication. If your system configuration includes Cryptographic Security Platform Vault-managed user accounts authorized using an LDAP server, the AD Security groups must be in the same AD domain as those Cryptographic Security Platform Vault-managed accounts.
- If Cryptographic Security Platform Vault sends an email alert to a Cloud Admin Group that is associated with one or more AD Security groups, every member of the associated AD Security groups receives the email alert at the email address listed for them in Active Directory. Individual AD users cannot turn off alert notifications.
- The relationship between AD Security groups and Cloud Admin Groups is many-to-many. You can associate any number of AD Security groups with a Cloud Admin Group, and you can associate any number of Cloud Admin Groups with an AD Security group.
- If you assign an AD Security group to a Cloud Admin Group, every user who is a member of that AD Security group in Active Directory will get Cloud Admin access to all VMs registered in all Cloud VM Sets associated with the Cloud Admin Group.
  You cannot exclude specific members of the AD group, nor can you grant automatic access to any AD groups nested inside the parent group. Every AD group you want to include must be directly associated with the Cloud Admin Group, and every individual member of every associated AD group will automatically get access to Cryptographic Security Platform Vault and the VMs associated with that Cloud Admin Group.
  For details about what Cloud Admins can do in Cryptographic Security Platform Vault.
- We recommend creating separate AD Security groups that contain only those users who require access to Cryptographic Security Platform Vault. Cloud Admins can decrypt any VM registered with any Cloud Admin Group of which they are a member, so it is critical to restrict access to a very small set of trusted users.
- When an AD user logs into the Cryptographic Security Platform Vault webGUI, the system evaluates their privileges only during the initial login. If an AD user is removed from, or added to, a Security group in Active Directory while logged into the webGUI, the changes to their account privileges will not take effect until the user logs out of their current session and then logs back into the webGUI.
  Tip: Any Cryptographic Security Platform Vault-managed user account with Security Admin privileges can view the Audit log to determine which users are currently logged into the Cryptographic Security Platform Vault webGUI.
- When an AD user logs into the Cryptographic Security Platform Vault webGUI, Cryptographic Security Platform Vault Security Admins can see the exact AD group memberships that Cryptographic Security Platform Vault used when it assigned privileges to that AD user.

Cloud Admin Groups Overview

When a user logs into the Cryptographic Security Platform Vault webGUI, the options displayed in the webGUI depend on two things: the privileges associated with the user's account and the *Cloud Admin Groups* to which the user account has been assigned.

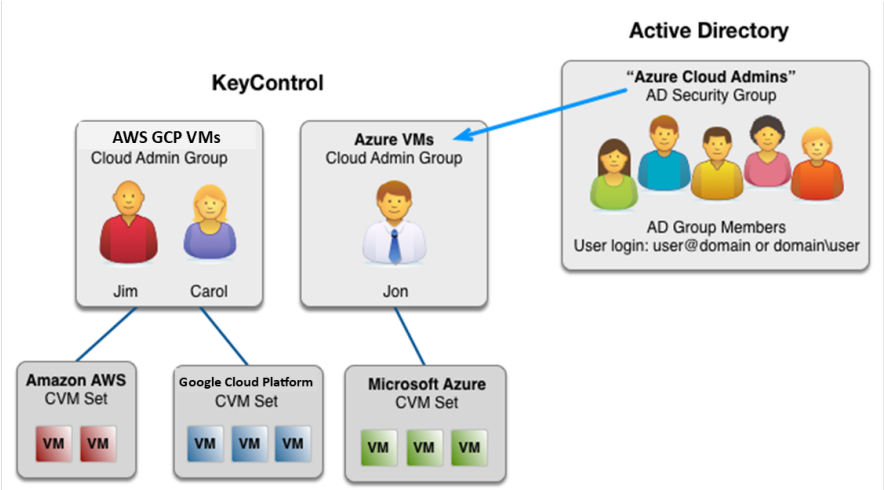
When you register a VM with Cryptographic Security Platform Vault, you must assign that VM to a *Cloud VM Set*. In turn, every Cloud VM Set must be assigned to a *Cloud Admin Group* that defines which users can see and maintain the VMs assigned to the Cloud VM Set.

The relationship between Cloud Admin Groups and Cloud VM Sets is one to many. While each Cloud VM Set can only be associated with one Cloud Admin Group, each Cloud Admin Group can contain any number of Cloud VM Sets.

When you create a Cloud Admin Group, you can associate any number of Cryptographic Security Platform Vault user accounts or Active Directory (AD) Security groups with that Cloud Admin Group. As soon as you assign a Cloud VM Set to that group and you register a VM with that Cloud VM Set, all the Cryptographic Security Platform Vault users and AD Security group members associated with the Cloud Admin Group can see and manage that VM.

The following figure shows an example of the relationship between Cryptographic Security Platform Vault users, Cloud Admin Groups, and Cloud VM Sets. In this example:

- Jim and Carol both have Cryptographic Security Platform Vault-managed user accounts assigned to the Cloud Admin Group "AWS GCP VMs". They are responsible for the VMs in the Cloud VM Sets "Amazon AWS" and "Google Cloud Platform". When they log in, they cannot see any of the VMs that have been registered with the "Microsoft Azure" Cloud VM Set.
- Jon has a Cryptographic Security Platform Vault-managed user account, and both his account and the Active Directory Security group "Azure Cloud Admins" have been assigned to the Cloud Admin Group "Azure VMs". Jon and all the members of the AD Security group are responsible for the VMs in the Cloud VM Set "Microsoft Azure". When Jon or any of the AD Security group members log into Cryptographic Security Platform Vault, they can only see the VMs in the "Microsoft Azure" Cloud VM Set.



9 Upgrading CSP Vault

- CSP Vault Upgrade Paths
- CSP Vault Upgrade Requirements
- Upgrading CSP Vault to 10.6.1

CSP Vault Upgrade Paths

Important: Beginning with version 10.4.7, you will no longer be allowed to upgrade if your license is not current. If you see an error message, please contact support at https://trustedcare.entrust.com.

If your Cryptographic Security Platform Vault nodes are running version 10.4.3 or later, you can upgrade the entire cluster from any node in the cluster using the Cryptographic Security Platform Vault Management webGUI. Cryptographic Security Platform Vault automatically applies the upgrade to all nodes in the cluster sequentially so that the Cryptographic Security Platform Vault cluster remains available for key requests from the registered VMs throughout the entire upgrade process.

You can only upgrade between successive versions. Supported upgrade paths are:

Initial Release	Available Upgrade Paths
10.5.1	10.6.1
10.4.7	10.5.1, 10.6.1
10.4.5	10.4.7, 10.5.1, 10.6.1
10.4.3	10.4.5, 10.4.7, 10.5.1, 10.6.1

Important: You must upgrade the Cryptographic Security Platform Compliance Manager before you upgrade Cryptographic Security Platform Vault.

You can upgrade from Cryptographic Security Platform Vault 5.5.1 to 10.6.1. To do so, you upgrade from 5.5.1 to 10.0, then upgrade from 10.0 to 10.1.1, then from 10.1.1 to 10.2, then from 10.2 to 10.3.1, then to 10.4.1, 10.4.1.1, or 10.4.3, and then to 10.6.1.

For details on upgrading earlier versions, please see the version of the documentation that you are upgrading to. For example, if you need to upgrade from 5.5.1 to 10.0, see the KeyControl 10.0 documentation.

> Note: Because the OS for Cryptographic Security Platform Vault was changed in 10.4.1, if you upgrade from 10.3.3 or earlier, the process is a migration method rather than the standard upgrade procedure. Please be sure to review the Installation and Upgrade Guide for 10.4.3 before you start the upgrade. We recommend that you migrate to version 10.4.3 and then upgrade directly to 10.6.1.

CSP Vault Upgrade Requirements

Important:

- **You must upgrade the Cryptographic Security Platform Compliance Manager before you upgrade Cryptographic Security Platform Vault.**

- The CSP Vault Management Appliance and all CSP Vaults must be connected to the CSP Compliance Manager and must have a valid unexpired license, as well as usage within the limits for each category, before you start the upgrade.
  Note:
  - If your vaults are not connected to the CSP Compliance Manager, you can connect them after you have upgraded CSP Compliance Manager to 10.5.1. For versions 10.4.5 and above, follow the directions in Connecting CSP Vault and CSP Compliance Manager. For CSP Vault version 10.4.3, you will need to download the JSON file and then copy the Compliance Manager ID and the App Link Token from the JSON file. To do this:
    i. Download the JSON file from the CSP Compliance Manager webGUI.
    ii. Open the JSON file with a text editor. The beginning will look similar to the following text:
    "appLinkToken":
    "NkFGNDM0MUMzRDI4NEExNzQ5NDYzMDlENjE4QjZGREQ0Q0Y5NjlEQzg5MDgxRUJDRDBBQzY1RTFBQjU2OTZGREEwNzc0NjhERjVCRDQwOEZBRDc0ODM4QTlBRjFCRkY5NTVGMjNDMkUwNDA4QkQ3NTc1MzQ3MDk3QjVBMTU1MDZCQkQ4QUFCNTA4QzJBQkMxMTlBQ0U2MTQyRTRCQUIwRkZDOTc4ODY0QjRCRDM1NDgyRjcwMUM4MDcyQjg5Q0IwREMyMDk5NkM4NjZFQjRGQkYzN0M1MUFCOEUwRjMxMzBGRkQ2MUNGRDQ0QTY2NkRBMjhENzA4RDQzQjMwMTJBNkMyQjA5QkZCRTIzRkJERUE5QjUxMjcyRUU1QThBMUVB",
    "kcmId": "10.1.232.31",
    "sslVerify": true,
    "applicationId": "cbe4d5a1-a25c-4721-a95f-5981522b7ef5",
    "rootCertificate": "-----BEGIN CERTIFICATE-----\nMIIGATCCA+mgAwIBAgIEaYuG/jANBgkqhkiG9w0BAQsFADBbMQswCQYDVQQGEwJV\n
    iii. Copy the text for the `appLinkToken` and paste it in the Token field in the KeyControl webGUI.
    iv. Copy the `applicationId` and paste it in the KeyControl Compliance Manager ID field in the KeyControl webGUI.
    v. Click **Connect**.
  - If you are using BYOK or TDE, you may encounter an error message during the upgrade process similar to: The upgrade can not be started: ["Cloud Keys Vault 'BYOK_Dev_Vault' Cloud Key(s) license entitlement above limit (count: 479, limit: 0)."]. The message text will vary, but the count will be non-zero and the limit zero.
    If this happens, open your Cryptographic Security Platform Compliance Manager to the collection that contains the Vault where you received the error messages. Navigate to the Licenses page and remove all but one license file (CSP Compliance Manager will not let you remove all licenses). Add those licenses back in, then remove and add back the last license file.
    After you complete that step, restart the upgrade.
- If you have a multi-node cluster with passphrase-based startup authentication, you cannot upgrade directly to 10.5.1. You must either disable the startup authentication or reduce the cluster to a standalone node before you upgrade.
- If you have just upgraded from a previous version, and want to upgrade to a newer version, you may see a message that reads: Ongoing Encrypt on Cryptographic Security Platform Vault system device - Try again later. In this case, the internal processing will take about 30 minutes to complete before you can continue.

After you upgrade your Cryptographic Security Platform Vault nodes, we strongly recommend that you also upgrade the Policy Agents running on all VMs registered with Cryptographic Security Platform Vault. For details, see Policy Agent Upgrade Requirements.

Upgrading CSP Vault to 10.6.1

If your Cryptographic Security Platform Vault nodes are running version 10.4.3 or later, you can use the Cryptographic Security Platform Vault Management webGUI to upgrade any node in the cluster and Cryptographic Security Platform Vault will automatically upgrade the other nodes one at a time until all nodes have been upgraded. By doing sequential upgrades, Cryptographic Security Platform Vault ensures that at least one node in the cluster remains available during the entire upgrade process.

Important: If you are using HSM Root-of-Trust mode with password, you must enter the password on each node during upgrade.

You can use this procedure for all installations of Cryptographic Security Platform Vault, including AWS, Azure, and GCP.

> Note: Any new features in the Cryptographic Security Platform Vault release will *not* be available until all nodes in the cluster have been upgraded.

Before You Begin

- Make sure that the Cryptographic Security Platform Vault nodes can communicate with one another on port `TCP/8443` and `TCP/5432`. For details, see Network requirements.
- Entrust recommends that you back up your Cryptographic Security Platform Vault cluster before you upgrade it. For details, see Backing Up CSP Vault Through the webGUI
- Please download your Admin Key and store it in a safe place before you upgrade. If Cryptographic Security Platform Vault prompts for an admin key to recover your Cryptographic Security Platform Vault system, you must provide this admin key to proceed. If you do not have your admin key, you may lose your data. For details, see Downloading Your Admin Key Part.
- We recommend that you enable the support login on all cluster nodes before you start the upgrade. For details, see Enabling or Disabling the Support Login .
- Make sure your internet connection to the Cryptographic Security Platform Vault node is as fast and as stable as possible. To begin the upgrade, you need to upload the upgrade ISO image to the Cryptographic Security Platform Vault node in one continuous session. If the upload times out or if connectivity to the Cryptographic Security Platform Vault node is lost during the upload, you will see error messages in Cryptographic Security Platform Vault and you must re-upload the file from scratch. Cryptographic Security Platform Vault *cannot* resume the upload from where it left off during a previous session.

Procedure

1. Sign on to the Cryptographic Security Platform Vault Management webGUI with Domain and Security Admin privileges.
2. In the top right, click the **Appliance Management** link.
3. In the top menu bar, click **Cluster** and make sure the **Status** of the cluster is **Healthy**. If it is not, you must resolve those issues before you can upgrade the cluster.
4. In the top menu bar, click **Settings**.
5. In the **System Settings** section, click **System Upgrade**.
6. Click **Browse**, navigate to the Entrust ISO upgrade file, and click **Open**.
   Important: Cryptographic Security Platform Vault now has separate ISO files for installation and upgrade. Please ensure that you use the ISO upgrade file.
7. Click **Upload File**. If the **Upload File** button is not active, make sure that you have selected an ISO file and that the cluster is healthy.
   After Cryptographic Security Platform Vault uploads and validates the ISO file, Cryptographic Security Platform Vault begins the automatic upgrade process by copying the ISO file from the current node to all of the other Cryptographic Security Platform Vault nodes in the cluster. After the ISO file has been copied, Cryptographic Security Platform Vault displays a Success message. Click **Close** to continue with the upgrade.

Cryptographic Security Platform Vault displays a status message stating that the upgrade is in process along with a **Cancel Upgrade** button in case you want to stop the process.
During this time you can continue to use Cryptographic Security Platform Vault as normal, including changing all configuration options and adding or removing VMs. When Cryptographic Security Platform Vault is ready to upgrade all nodes in the cluster, it displays the **Finish Upgrade** button.

8. Click **Finish Upgrade**.
   Note: Ensure you are still on the same node where you clicked **Upgrade File**.
   Cryptographic Security Platform Vault displays a message stating that the cluster will be put into maintenance mode during this procedure and that all nodes will be rebooted. While in maintenance mode, Cryptographic Security Platform Vault can still service key requests from the registered VMs, but no Cryptographic Security Platform Vault configuration changes can be made and no new VMs can be added.
9. Click **Proceed**.
   Cryptographic Security Platform Vault displays a status message stating that the cluster nodes are being rebooted. It may take a while for this process to run on all nodes except for the current node. When all of the other nodes have been upgraded and are back online, Cryptographic Security Platform Vault reboots the current node to finish the upgrade process on that node. At this point, you will be automatically logged out of the Cryptographic Security Platform Vault Management webGUI on that node. You can monitor the progress on the Cryptographic Security Platform Vault Management webGUI of the other nodes. This again may take a while to complete.
   When any node is being upgraded, if you have access to the Cryptographic Security Platform Vault System Console, you can view the upgrade messages.
   Note: When Cryptographic Security Platform Vault reboots the current node, you may see a message that the application cannot connect to the server, then browser page may display a "connection refused" message. Wait a few moments for the node to finish rebooting, then refresh your browser page. You should see the Cryptographic Security Platform Vault Login page.
   Beginning with 10.2, Cryptographic Security Platform Vault has changed the login experience. You can now switch between the Cryptographic Security Platform Vault Management webGUI and the Cryptographic Security Platform Vault Appliance Management webGUI in the same browser with one login. When you log in, click the Switch to **Appliance Management** link at the top right side of the web page to switch.
10. To verify the upgrade, return to **Settings > System Upgrade** and verify the settings for **Current Version** and **Previous Version**.

10 Installing Policy Agent

- Preparing to Install the Policy Agent
- Linux Policy Agent Installation
- Windows Policy Agent Installation

Preparing to Install the Policy Agent

Before you can install the Policy Agent on Linux or Windows, you must complete the following:

1. Determine whether you want to use the Cryptographic Security Platform Vault for Databases or the Cryptographic Security Platform Vault for VM Encryption.
2. In the Cryptographic Security Platform Vault Management webGUI select **Create Vault** and follow the steps in Creating a Vault.
   You must create either the Cryptographic Security Platform Vault for Databases or the Cryptographic Security Platform Vault for VM Encryption.
3. Create a Cloud Admin Group. For more information, see Cloud Admin Groups.
4. Create a Cloud VM Set for your vault. For more information, see see Creating a Cloud VM Set for the CSP Vault for Databases or Creating a Cloud VM Set for the CSP Vault for VM Encryption.

Linux Policy Agent Installation

- Linux Policy Agent Installation Overview
- Linux Installation Prerequisites
- Installing the Policy Agent on Linux
- Authenticating a New VM

Linux Policy Agent Installation Overview

The Entrust Policy Agent is a software module that runs inside Windows and Linux operating systems that provides encryption of virtual disks and individual files. All VMs that have the Policy Agent installed can also securely share encrypted files and disks. When a user attempts to access an encrypted disk, the Policy Agent queries Cryptographic Security Platform Vault to validate the request, and returns the information to the user if Cryptographic Security Platform Vault authorizes the request.

You must install a copy of the Policy Agent in each VM you want to encrypt with Cryptographic Security Platform Vault.

Linux Installation Prerequisites

- Make sure the version of Linux running on the target system is supported for data encryption. For details, see Platform requirements.
- Make sure the default language for the Linux operating system is English. The Entrust Policy Agent uses scripts that parse the output of Linux commands, and those scripts may give unexpected results if the command output is in a language other than English.
- Make sure that the `tar` utility is installed. If you see this error, then `tar` is not installed:
  `Uncompressing hcs-client-agent-10.5.1-550001852.run ... Extraction failed.`
- Make sure that Entrust Cryptographic Security Platform Vault is installed and the cluster is configured properly as described in Initializing the web GUI. The cluster must be healthy. You cannot register the Policy Agent with a degraded Cryptographic Security Platform Vault cluster.
- Have the following information available:

    - The IP addresses of all Cryptographic Security Platform Vault nodes with which you want to register the Policy Agent, or one IP address and the name of the Cluster Node Mapping you want to use on this VM. Registering the Policy Agent with multiple Cryptographic Security Platform Vault nodes provides a failover mechanism in case one of the Cryptographic Security Platform Vault nodes is unreachable.
    - The credentials for a Cryptographic Security Platform Vault webGUI user account with Cloud Admin privileges.
    - The name of the Cryptographic Security Platform Vault Cloud VM Set with which you want to associate the VM. You cannot encrypt the disks or drives until the VM has been registered with a Cloud VM Set in Cryptographic Security Platform Vault. For details, see the Administration Guide.
- Select an authentication method. The options are:
    - **Standard Authentication** — This is the most secure authentication method. You create a certificate in the Cryptographic Security Platform Vault webGUI which you then copy to the target system. After you install the Policy Agent software, you specify the name and location of the certificate file during registration. You also create a passphrase during the Policy Agent registration that you must then enter in the Cryptographic Security Platform Vault webGUI.
    - **Simplified Authentication** — This method involves authenticating the VM with Cryptographic Security Platform Vault through the VM itself. It allows you to skip downloading a certificate and logging into Cryptographic Security Platform Vault during the authentication process, but it does require you to enter the Cryptographic Security Platform Vault credentials directly into the VM and to have a Cloud VM Set already created. You should only use this method if your VM is secure.
    - **Automated Authentication** — This method involves adding the Cryptographic Security Platform Vault username and password on the `hcl` command line using the `hcl register -a` command. This method is the least secure and should be used with caution due to the fact that the Cryptographic Security Platform Vault username and password must be included on the command line or in the script.
- **RHEL 10 Caveats**—If you plan to use RHEL 10 with the Linux Policy Agent, please be aware of the following:
    - The 'htroot setup' job will fail if network is set to DHCP. This is because system device encryption is not supported with DHCP. To fix this issue, please use static IP configuration during setup.
    - The 'htdrv prepare' job may fail to install the EPEL package. To fix this issue, run the following command manually:
      `rpm -Uvh "https://dl.fedoraproject.org/pub/epel/epel-release-latest-10.noarch.rpm"`
      Then you can rerun the 'htdrv prepare' job.
    - The upgrade process using Leaap will fail if the root disk is encrypted. To fix this issue, boot into RHEL 9 from the GRUB menu to rescue the VM.
      To avoid this issue do the following:
        i. Decrypt the root disk before upgrading.
        ii. Perform a clean upgrade to RHEL 10.
        iii. Re-encrypt the root disk after the upgrade is complete.

Installing the Policy Agent on Linux

See below for installing the Policy Agent on Linux.

- Downloading the installation file
- Creating a certificate for the registration process
- Copying the installer
- Running the installer
- Registering the virtual machine into Vault.

Make sure you have completed the prerequisites described in Linux Installation Prerequisites.

Downloading the installation file

See below for installing the Policy Agent installation file.

To download the Policy Agent installation file

1. Log in to the Cryptographic Security Platform Vault for VM Encryption webGUI or the Cryptographic Security Platform Vault for Databases webGUI with Cloud Admin privileges.
2. Click **Workloads**.
3. Click **Actions > Download Policy Agent**.
4. Click the **Download** link associated with the following file:

```
hcs-client-agent-rel.number-build.number.run
```

Creating a certificate for the registration process

Create a certificate that you can install on the VM and use during the registration process.

Skip this section if you want to use Simplified or Automated Authentication.

To create a certificate for the registration process

1. Select the Cloud VM Set with which you want to associate the VM.
2. Click **Actions > Create New Certificate**.
3. If desired, enter a passphrase for the certificate. If you enter a passphrase here, you will need to enter that passphrase when you install the certificate on the VM.
4. Enter a date on which this certificate should expire.
5. Click **Create**. Cryptographic Security Platform Vault downloads a `.cert` file to the default download location.

   Do not rename the downloaded certificate. The certificate name includes additional information, and a renamed certificate will fail.

Copying the installer

Copy the `hcs-client-agent-rel.number-build.number.run` installation file to the Linux machine.

Running the installer

Log in to the target Linux system as `root`, and run the following command in the directory containing the installation file.

```
$ sh ./hcs-client-agent-rel.number-build.number.run install [-y] [-P
<installation_path>]
```

Where:

- `-y` tells the installer to use the `/opt/hcs` default installation directory without prompting.
- `-P` specifies the installation directory.

Make sure that you have executable permissions to `/tmp` because the installer extracts itself to the `/tmp` directory. If you get the following error:

```
./install.sh: Permission denied
```

Use the `TMPDIR` variable to select a different temporary directory. For example:

```
$ TMPDIR=$HOME
```

⚠ When uninstalling the Linux Policy Agent, you will also need to use a different directory.

The following example prompts the user for the installation directory.

```
$ sh ./hcs-client-agent-10.5.1-12345.run
Verifying archive integrity... All good.
Uncompressing hcs-client-agent.run.............
HyTrust Agent will be installed in /opt/hcs
Specify location for installing HyTrust Agent (/opt/hcs): <Enter>
Run once hcld
Starting hcld... done

You can now install online encryption driver, the process is described in the Admin
Guide
Please see the following section of Admin Guide for details
  – Administration Guide > Data Encryption > Linux Encryption Overview

Installation successful
```

The following example installs the Policy Agent in the `/opt/hcs` default directory.

```
$ sh ./hcs-client-agent-10.5.1-12345.run install -y
Verifying archive integrity... All good.
Uncompressing hcs-client-agent.run.............
HyTrust Agent will be installed in /opt/hcs
Run once hcld
Starting hcld... done

You can now install online encryption driver, the process is described in the Admin
Guide
Please see the following section of Admin Guide for details
  – Administration Guide > Data Encryption > Linux Encryption Overview
```

```
Installation successful
```

The following example installs the Policy Agent in the specified directory `/opt/test` without prompting:

```
$ sh ./hcs-client-agent-10.5.3-12345.run install -y -P /opt/test
Verifying archive integrity... All good.
Uncompressing hcs-client-agent.run.............
HyTrust Agent will be installed in /opt/test
Run once hcld
Starting hcld... done

You can now install online encryption driver, the process is described in the Admin
Guide
Please see the following section of Admin Guide for details
  – Administration Guide > Data Encryption > Linux Encryption Overview

Installation successful
```

Registering the virtual machine into Vault.

Run the following command to register the virtual machine with Cryptographic Security Platform Vault.

```
hcl register [-a] [-h vm-name] [-d "vm-description"] [-p cert-passphrase] [-o one-
time-passphrase] [-z cvm-set] [-v vault_id] [-n mapping-name] [-N] kc-
hostname[:port],kc-hostname2[:port],... [cert-file.cert]
```

Where:

- `-a` —Indicates that you want to authenticate the VM through the command line or the script instead of through a certificate file. Use this option if you are using Simplified or Automated Authentication. If you created a certificate in Cryptographic Security Platform Vault, omit this option and specify the certificate name in *cert-file*.cert.
- `-c` —Allows you to register this VM as a clone of the original VM.
- `-h` —The name of the VM that will be displayed in the Cryptographic Security Platform Vault webGUI (Default: hostname).
- `-d` —A description of the VM that will be displayed in the Cryptographic Security Platform Vault webGUI.
- `-p` —The passphrase assigned to the certificate when it was created. If you do not specify this parameter and the certificate has an associated passphrase, the registration process prompts you for the passphrase. Applies to Standard Authentication only.
- `-v` —The Vault ID of the Vault that will be displayed in Vault Management. If you do not specify the vault_id, you will be asked to enter vault_id.
- `-o` —The one-time passphrase that will be used to encrypt the initial communication between this VM and the existing Cryptographic Security Platform Vault cluster. If you do not specify this parameter, the registration process prompts you for the one-time passphrase. Applies to Standard Authentication only.

> The passphrase is valid for 15 minutes from the time it is created. Authenticate the VM in the Cryptographic Security Platform Vault during this time. Authentication will fail after the passphrase has expired.

- `-z` —The name of the Cloud VM Set defined in the Cryptographic Security Platform Vault cluster to which you want to assign this VM. Applies to Simplified or Automated Authentication only (the `-a` option must be specified on the `hcl register` command).
- `-n` —The name of the Cluster Node Mapping that you want to associate with this VM. If you do not specify this option and one or more Cluster Node Mappings have been configured, the Policy Agent prompts you to select a Node Mapping from the list. If you do not want to use a Node Mapping, you must manually respond to this prompt. This option is mutually exclusive with the `-N` option, described below, and it requires that the `-a` option must be specified on the `hcl register` command.
- `-N` —Tells the Policy Agent that you do *not* want to use a Cluster Node Mapping, even if one is available. If you specify both `-N` and `-n`, the Policy Agent ignores the `-n` option and does *not* assign a Node Mapping to the VM. Applies to Simplified or Automated Authentication only (the `-a` option must be specified on the `hcl register` command).
- `kc-hostname[:port],kc-hostname2[:port],...` (required) — The list of IP addresses or hostnames for the Cryptographic Security Platform Vault nodes with which you want to register the VM. You must specify at least one Cryptographic Security Platform Vault node in this list. You must also specify a port if the Cryptographic Security Platform Vault nodes use anything other than the default port (443).

  > If you are using the `-n` option to specify a Cluster Node Mapping, this IP address will be the Cryptographic Security Platform Vault node that the VM contacts to retrieve the Node Mapping information. After the Node Mapping has been retrieved, the Policy Agent ignores any other IP addresses in this list and only registers the VM with the Cryptographic Security Platform Vault nodes contained in the Node Mapping.

- *cert-file*`.cert` —The name of the certificate file you copied to the target system if you are using Standard Authentication. If you are running the `hcl register` command from a directory other than the one where the `.cert` file resides, specify the full path to the `.cert` file as part of this option. If you did not create a certificate file in Cryptographic Security Platform Vault, omit this option and use the `-a` option instead.

The following command registers a VM with the "hq-vm-4" name, the "HQ Linux Server Alpha" description, and two nodes.

```
$ hcl register -h hq-vm-4 -d "HQ Linux Server Alpha" 10.238.32.74,10.238.32.75
 ad85837b-9862-11e1-afd5-000c29de5d41_120507163538.cert
You need to specify a passphrase that will be used for authentication
Enter passphrase (min 16 characters):

Registered as hq-vm-4 with node(s) 10.238.32.74,10.238.32.75
Please login to the node to complete the authentication of this node
```

The following command registers a VM without prompting the user.

```
$ hcl register -h hq-vm-4 -d "HQ Linux Server Alpha" -p <certpassphrase> -o
<onetimepassword> 10.238.32.74,10.238.32.75 ./install/hytrust/cert/
ad85837b-9862-11e1-afd5-000c29de5d41_120507163538.cert

Registered as hq-vm-4 with node(s) 10.238.32.74,10.238.32.75
Please login to the node to complete the authentication of this node
```

The following command registers a VM with the "hq-vm-4" name, the "HQ Linux Server Alpha" description, and prompts the user for the admin account information, the cloud VM Set, and the cluster node mapping.

```
$ hcl register -a -h hq-vm-4 -d "HQ Linux Server Alpha" 10.238.66.250

Do you want to register into a Vault?  (y/n) y
Please provide the vaultID
vaultid: d84243e7-d359-4179-9530-3497434e3192
Please provide the login details
username: CloudAdmin
password:

Available Cloud VM Sets
--------------------------------------------------------------------------------
SF-Datacenter
--------------------------------------------------------------------------------

Please specify Cloud VM Set to which this VM should be added: SF-Datacenter
Registered as hq-vm-4 with node(s) 10.238.66.250

Completing authentication for hq-vm-4 on node(s) 10.238.66.250

Authentication complete, machine ready to use
Getting Mapping information


This VM can be added to one of the following Mappings
--------------------------------------------------------------------------------
1 : SF-Datacenter-Map
2 : West-Coast-Map
--------------------------------------------------------------------------------

Please select a numeric Mapping ID (0 to skip): 1
Mapping: SF-Datacenter-Map
server description First Node, ip 10.238.66.250, port 443
server description Second Node, ip 10.238.66.251, port 443
Updated list with nodes 10.238.66.250:443,10.238.66.251:443
```

The following command sets the name, description, cloud VM set, and cluster node mapping without prompting user.

```
$ hcl register -a -h hq-vm-4 -v d84243e7-d359-4179-9530-3497434e3192 -d "HQ Linux
Server Alpha" -z SF-Datacenter -n SF-Datacenter-Map 10.238.66.250
```

```
Please provide the login details
username: CloudAdmin
password:
Registered as hq-vm-4 with node(s) 10.238.66.250

Completing authentication for hq-vm-4 on node(s) 10.238.66.250

Authentication complete, machine ready to use
Getting Mapping information

Mapping: SF-Datacenter-Map
server description First Node, ip 10.238.66.250, port 443
server description Second Node, ip 10.238.66.251, port 443
Updated list with nodes 10.238.66.250:443,10.238.66.251:443
```

Authenticating a New VM

1. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Click the **Unauthenticated VMs** tab.
4. Select the VM you want to authenticate.
5. Click **Actions > Authenticate**.
6. Enter the system passphrase at the prompt and click **Authenticate**. This passphrase must exactly match the passphrase that was specified when the new VM was registered. The passphrase is case-sensitive.
7. Click on the VM to verify that the VM is reachable and the VM details match what you expect.

Windows Policy Agent Installation

- Windows Installation Prerequisites
- Windows Boot Drive Installation Prerequisites
- Installing Interactively on Windows
- Installing Silently on Windows
- Registering the Policy Agent Using the Entrust Policy Agent GUI
- Registering the Policy Agent from the Windows command line
- Uninstalling Silently on Windows

Windows Installation Prerequisites

- Make sure the version of Windows running on the target system is supported for data encryption. If you want to encrypt the boot drive, make sure the Windows version is supported for boot drive encryption as well. For details, see Platform requirements.
- Make sure the default language for the Windows operating system is English. The Entrust Policy Agent uses scripts that parse the output of Windows commands, and those scripts may give unexpected results if the command output is in a language other than English.
- Make sure that the Cryptographic Security Platform Vault for VM Encryption or Cryptographic Security Platform Vault for Databases is installed and the cluster is configured properly as described in the Administration Guide. The cluster must be healthy. You cannot register the Policy Agent with a degraded cluster.

- Make sure the target system is partitioned correctly and you know which partition you want to encrypt. In addition, the partition must be assigned a drive letter or folder mount through the Windows Disk Manager. For details, see your Windows documentation.
- Make sure that the Microsoft .NET framework 4.8.0 or higher is installed on the target system. For more information, see https://dotnet.microsoft.com/en-us/download/dotnet-framework/net481.
  Note: The Microsoft .NET framework is required to use the Policy Agent GUI. If not installed, you will need to use the CLI.
- If you want to encrypt the boot drive, see the prerequisites in Windows Boot Drive Installation Prerequisites.

Windows Boot Drive Installation Prerequisites

The Entrust Policy Agent supports encryption for Windows MBR and GPT boot disks, including any GPT boot disks that use UEFI Secure Boot, as long as those boot disks meet the following requirements.

Important: UEFI and Secure Boot is only supported with VMware ESXi. It is not supported on AWS, Azure, or GCP.

For details on boot drive encryption, see Windows Boot Drive Encryption.

- The encrypted boot partition must be on the Windows `C:` drive. Although Windows itself can boot from alternate drive letters, the boot volume can only be encrypted if it is the `C:` drive or if it is mapped to `C:`. The Bootloader is automatically assigned a drive letter during installation. This default drive letter can be changed using the Windows Disk Manager after the Bootloader has been installed.
- The Bootloader requires a Windows System Reserved Partition (SRP). We will create an SRP if one does not already exist.
  The Bootloader SRP requires roughly 350 MB on Windows 2016 and above, and roughly 100 MB on Windows 10. As part of the installation process, the boot drive will shrink to free up space for the Bootloader (and Windows SRP if one does not already exist). If there is insufficient space on the boot drive, the Bootloader will fail to install.
  Note: If the Bootloader SRP has less than 50 MB free space, Cryptographic Security Platform Vault generates an alert every six hours until the issue is resolved.
- The SRP and the boot partition must both reside on `Harddisk0` (Disk 1). You cannot encrypt a boot partition that resides on any other disk, or split the SRP and the boot partition across disks.
- The boot disk must have at least 1 MB of free space at the beginning of the disk that Cryptographic Security Platform Vault can use to store encryption metadata. If this free space is not available, boot drive encryption will fail.
- If the VM is associated with a Cloud VM Set that is controlled by a Key Encryption Key (KEK), the HSM must be available before you can encrypt the root drive on the VM. For more information, see KEKs with Cloud VM Sets.
- The Disk Defragmenter service on the target server must be enabled before installing the Policy Agent software.
- The user account used for installing the software must have **SeRestorePrivilege** and **SeTakeOwnershipPrivilege**.
- For GPT boot disks:
  - The GPT disk must be running Windows Server 2016, Windows Server 2019, Windows Server 2022, or Windows 10.
  - The boot partition must be one of the first four partitions on the disk.
    Tip: If you try to encrypt the boot disk and the boot partition is not one of the first four partitions, the encryption will fail with the error "Maximum supported encrypted partition limit exceeded."
  - If you want to extend the boot partition, you must use the `hcl extend` command. For details, see Disk Size Management in Windows.

Installing Interactively on Windows

This procedure described how to install the Entrust Policy Agent by interacting with the installer on the Windows system. For details about installing the Policy Agent silently, see Installing Silently on Windows.

Before You Begin

- Make sure you have completed the prerequisites in Windows Installation Prerequisites.
- Make sure you have the credentials for a Windows user account with Administrator privileges.
- If you plan to download the Policy Agent installation file on Windows 10 from the Microsoft Edge browser while logged in with the BUILTIN\Administrator account, make sure that User Account Control (UAC) is enabled for the BUILTIN\Administrator account. Alternatively, you can set the integrity level for the installer to high after you have downloaded it. For details, see the Microsoft Windows 10 documentation.

Procedure

1. Sign in to the Cryptographic Security Platform Vault for Databases webGUI or Cryptographic Security Platform Vault for VM Encryption webGUI with Cloud Admin privileges.
2. Click **Workloads**.
3. Click **Actions > Download Policy Agent**.
4. Click the **Download** link associated with the file `hcs-client-agent-rel.number-build.number.exe`. Cryptographic Security Platform Vault downloads the file to your browser's default download location.
5. Copy `hcs-client-agent-rel.number-build.number.exe` to the Windows system that you want to encrypt.
6. Log into the target Windows system as an Administrator.
7. Navigate to the directory in which you placed the `hcs-client-agent-rel.number-build.number.exe` file and run the installer.
8. On the **Welcome** page of the Setup Wizard, click **Next**.
9. On the **License Agreement** page, review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
10. On the **Choose Install Location** page, select the folder in which Policy Agent will be installed.
    Note: You must install Policy Agent in a folder on the `C:` drive.
11. In the **Choose Components** page, review the setting of the **HT Bootloader** option.
    If you want to encrypt the boot drive on this system now or in the future, make sure this option is selected. If you do not need to encrypt the boot drive, make sure this check box is cleared. The Bootloader is only supported for the Cryptographic Security Platform Vault for VM Encryption.
    Note: If you do not install the Entrust Bootloader now, you can do so later if needed. For details, see Installing the Bootloader After the Policy Agent Is Installed.
12. If the **HT Bootloader** option is *not* selected:
    a. Click **Install**.
    b. On the Completing the Entrust Setup Wizard page, select **Reboot Now** and click **Finish**.
13. If the **HT Bootloader** option *is* selected:
    a. Click **Next**.
    b. On the Drive and Network Configuration page, select the drive letter and the network that the Entrust Bootloader should use when connecting to Cryptographic Security Platform Vault. By default, this dialog box shows the current DeviceID (a unique integer) and ConnectionID from `WMI class Win32_NetworkAdapter` for the selected network interface.
    c. When you are finished, click **Install**.
    d. If prompted, click **Yes** to remove any existing Bootloader partitions.
    e. On the Completing the Setup Wizard page, select **Reboot Now** and click **Finish**.

f. The machine will reboot several times to finish the installation. After the machine has finished booting, copy the `id_rsa` key file to another location in case you ever need to access the Entrust Bootloader Debug Console using SSH.
Tip: You can download the `id_rsa` key file using the Cryptographic Security Platform Vault for VM Encryption webGUI after the boot drive has been encrypted. To do so, log into the Cryptographic Security Platform Vault for VM Encryption webGUI, click **Workloads** and go to the **VMs** tab. Select the appropriate VM, then select **Actions > Download Bootloader SSH Key**.

What to Do Next

Register the VM as described in Registering the Policy Agent Using the Entrust Policy Agent GUI or Registering the Policy Agent from the Windows command line.

Installing Silently on Windows

This procedure describes how to install the Entrust Policy Agent silently on Windows using a command line script. For details about installing the Policy Agent through an interactive GUI, see Installing Interactively on Windows.

Note: The Policy Agent can only be installed on the Windows system (C:) drive, not a data drive.

Before You Begin

- Make sure you have completed the prerequisites in Windows Installation Prerequisites.
- Make sure you have the credentials for a Windows user account with Administrator privileges.
- If you plan to download the Policy Agent installation file on Windows 10 from the Microsoft Edge browser while logged in with the BUILTIN\Administrator account, make sure that User Account Control (UAC) is enabled for the BUILTIN\Administrator account. Alternatively, you can set the integrity level for the installer to high after you have downloaded it. For details, see the Microsoft Windows 10 documentation.

Procedure

1. Sign in to the Cryptographic Security Platform Vault for Databases webGUI or Cryptographic Security Platform Vault for VM Encryption webGUI with Cloud Admin privileges.
2. Click **Workloads**.
3. Click **Actions > Download Policy Agent**.
4. Click the **Download** link associated with the file `hcs-client-agent-rel.number-build.number.exe`. Cryptographic Security Platform Vault downloads the file to your browser's default download location.
5. Copy `hcs-client-agent-rel.number-build.number.exe` to the Windows system that you want to encrypt.
6. If your system contains multiple network adapters and you want to specify the adapter that Cryptographic Security Platform Vault should use, do the following:
   a. Enter the command `hcs-client-agent-rel.number-build.number.exe /NLIST`. Cryptographic Security Platform Vault writes the list to the file `HTIfaceList` in the same directory as the installer executable.
   b. Open `HTIfaceList` and determine the index of the adapter you want to use.
   c. Specify that index using the `/NET` switch as described in the next step.
7. Run `hcs-client-agent-rel.number-build.number.exe` using the following switches. All switches are case-sensitive and must be entered in upper-case. The installer ignores any unsupported switches.

Switch	Description
/S	Required. Tells Windows to run the installer silently.
/NORB	Do not reboot automatically. Required if you want to check the final state of installation, which is explained in the following step.
Windows Bootloader Switches	
/NOBL	Do not install the Windows Bootloader. The default is to install the Bootloader.
/NLIST	List of network adapters with an index that can be used with the `/NET` switch. This does not cause actual installation.
/NET=*n*	Use adapter *n* with its current settings as the primary network interface for the Entrust Bootloader, where *n* is the DeviceID of any of the network adapters listed by `/NLIST`. If this switch is not specified, the first network adapter is used by default. This is equivalent to specifying `/NET=1`.
/DRIVE=*d*	Assign drive letter *d* to the Bootloader partition. The drive letter is not case-sensitve.
/NORM	Do not delete HTBOOTLDR partition left by an older installation. By default, old HTBOOTLDR partitions are deleted.

For example, if you want to run `hcs-client-agent-10.5.1-12345.exe` silently, assign the drive letter D to the Bootloader, and not reboot automatically after the install runs, you would enter:
`C:\hytrust\installer\dir> hcs-client-agent-10.5.1-12345.exe /S /DRIVE=D /NORB`

8. If you specified the /NORB switch and you want to check the success of the installation, look at the files generated by the installer. These files will be placed in the same directory as the `.exe` file. The files are:
   - `HTDone` —This indicates the installation ended. You should poll for creation of this file to ensure that the installer process finished. If no other file is created, it means that the installation completed successfully.
     Note: Boot drive encryption is not available until AFTER a successful installation and reboot.
   - `HTError` —The installation failed. This file contains the error string.
   - `HTBLError` —Entrust Bootloader installation failed, but the rest of the installation succeeded. This file contains the error string.
   - `HTRetryOnReboot` —If this file is present, the installation was not a failure, but it needs a reboot. To complete the installation, reboot and run the installer again.
9. If you specified the /NORB switch, reboot the Windows system to complete the installation.

What to Do Next

Register the VM with Cryptographic Security Platform Vault as described in Registering the Policy Agent Using the Entrust Policy Agent GUI or Registering the Policy Agent from the Windows command line.

Registering the Policy Agent Using the Entrust Policy Agent GUI

Before You Begin

Make sure that you know:

- The IP address of the Cryptographic Security Platform Vault for VM Encryption or Cryptographic Security Platform Vault for Databases node with which you want to register the Policy Agent.
- The login credentials for a Cryptographic Security Platform Vault for VM Encryption webGUI or Cryptographic Security Platform Vault for Databases webGUI account with Cloud Admin privileges.
- The name of the Cryptographic Security Platform Vault for VM Encryption or Cryptographic Security Platform Vault for Databases Cloud VM Set with which you want to associate the VM. You cannot encrypt the drive until it has been associated with a Cloud VM Set. For details, see Creating a Cloud VM Set for the CSP Vault for Databases or Creating a Cloud VM Set for the CSP Vault for VM Encryption.

Procedure

1. Log into the Windows system using an account with Administrator privileges.
2. Select **Start > All Programs > Entrust > Entrust DataControl** or start Windows PowerShell and enter the `hclGUI` command.
3. Click **Register**.
4. In the **Register with a KeyControl Server** dialog box, enter the following information:

Field	Required ?	Description
KeyControl Name / IP	Yes	The IP address of the Cryptographic Security Platform Vault for VM Encryption or Cryptographic Security Platform Vault for Databases node with which you want to register this system. Only the IP address is required. Do not enter the full URL.
KeyControl Port	Yes	The Cryptographic Security Platform Vault for VM Encryption or Cryptographic Security Platform Vault for Databases node port. The default is 443.
Username	Yes	The user name for a Cryptographic Security Platform Vault for VM Encryption webGUI or Cryptographic Security Platform Vault for Databases webGUI account with Cloud Admin privileges.
Password	Yes	The password for the specified Cryptographic Security Platform Vault for VM Encryption webGUI or Cryptographic Security Platform Vault for Databases webGUI account.
Vault ID	Yes	The Vault ID of the Cryptographic Security Platform Vault for VM Encryption webGUI or Cryptographic Security Platform Vault for Databases webGUI. The Vault ID is located on the About page. Click on your account name in the top right-hand corner or the vault, then select About.

Field	Required ?	Description
Cloud VM Set	Yes	The name of the Cloud VM Set to which you want to add this VM.
VM Name	Yes	The name for the system that will be displayed in the Cryptographic Security Platform Vault for VM Encryption webGUI or Cryptographic Security Platform Vault for Databases webGUI. The default is VM hostname.
Description	No	A description for the VM that will be displayed in the Cryptographic Security Platform Vault webGUI or Cryptographic Security Platform Vault for Databases webGUI.

Note: The VM name, description, and Cloud VM Set can also be set in the CSP Vault for VM Encryption webGUI or CSP Vault for Databases webGUI.

5. When you are finished, click **Register**.
6. Click **OK** at the Registration Successful prompt.

What to Do Next

Encrypt the drive as described in Data Encryption and Windows Boot Drive Encryption.

Registering the Policy Agent from the Windows command line

See below for registering the Policy Agent from the Windows command line

- Required information
- Creating the cloud VM set of certificates
- Running the registration command

Required information

Before registering the Policy Agent from the Windows command line, make sure you know:

- The VM Encryption vault details. This is the vault you configured during the initial setup.
- The IP addresses of the Cryptographic Security Platform Vault for VM Encryption node with which you want to register the Policy Agent.
- The login credentials for a Cryptographic Security Platform Vault for VM Encryption account with Cloud Admin privileges.
- The name of the Cryptographic Security Platform Vault for VM Encryption Cloud VM Set with which you want to associate the VM. You cannot encrypt the drive until it has been associated with a Cloud VM Set in Cryptographic Security Platform Vault for VM Encryption. For details, see the Administration Guide.

Creating the cloud VM set of certificates

When you register the VM, you can either specify the Cloud VM Set you want to use interactively during registration, or create a certificate for that Cloud VM Set in the Cryptographic Security Platform Vault for VM Encryption web GUI and use that certificate during registration.

To create the cloud VM set of certificates

1. Log in to the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. On the **VM Sets** tab, select the Cloud VM Set with which you want to associate the VM.
4. Click **Actions > Create New Certificate**.
5. If desired, enter a passphrase for the certificate. If you enter a passphrase here, you will need to enter that passphrase when you use the certificate on the VM.
6. Enter a date on which this certificate should expire.
7. Click **Create**. The Cryptographic Security Platform Vault for VM Encryption downloads a `.cert` file to the default download location.

   > ⚠ Do not rename the downloaded certificate. The certificate name includes additional information, and a renamed certificate will fail.

8. If necessary, copy the `.cert` file to the Windows VM.

Running the registration command

Log into the VM using an account with administrator privileges, open a Windows command prompt run the following command.

```
hcl register [-a] [-h vm-name] [-d "vm-description"] [-p cert-passphrase] [-o one-time-passphrase] [-z cvm-set] [-v vault_id] [-n mapping-name] [-N] kc-hostname[:port],kc-hostname2[:port],... [cert-file.cert]
```

Where:

- `-a` — Indicates that you want to authenticate the VM through the command line or the script instead of through a certificate file. Use this option if you are using Simplified or Automated Authentication. If you created a certificate in Cryptographic Security Platform Vault, omit this option and specify the certificate name in *cert-file*`.cert`.
- `-h` —The name of the VM that will be displayed in the Cryptographic Security Platform Vault for VM Encryption (Default: hostname).
- `-d` —A description of the VM that will be displayed in the Cryptographic Security Platform Vault for VM Encryption.
- `-p` —The passphrase assigned to the certificate when it was created. If you do not specify this parameter and the certificate has an associated passphrase, the registration process prompts you for the passphrase. Applies to Standard Authentication only.
- `-v` (optional)—The Vault ID of the Vault that will be displayed in Vault Management. If you do not specify vault_id, you will be asked whether you want to enter vault_id.
- `-o` —The one-time passphrase that will be used to encrypt the initial communication between this VM and the existing Cryptographic Security Platform Vault for VM Encryption cluster. If you do not specify this parameter, the registration process prompts you for the one-time passphrase. Applies to Standard Authentication only.

  > ℹ The passphrase is valid for 15 minutes from the time it is created. Make sure you authenticate the VM in Cryptographic Security Platform Vault during this time. Authentication will fail after the passphrase has expired.

- `-z` —The name of the Cloud VM Set defined in the Cryptographic Security Platform Vault for the VM Encryption cluster to which you want to assign this VM. Applies to Simplified or Automated Authentication only (the `-a` option must be specified on the `hcl register` command).
- `-n` — The name of the Cluster Node Mapping that you want to associate with this VM. If you do not specify this option and one or more Cluster Node Mappings have been configured, the Policy Agent prompts you to select a Node Mapping from the list. If you do not want to use a Node Mapping, you must manually respond to this prompt. This option is mutually exclusive with the `-N` option, described below, and it requires that the `-a` option must be specified on the `hcl register` command.
- `-N` —Tells the Policy Agent that you do *not* want to use a Cluster Node Mapping, even if one is available. If you specify both `-N` and `-n`, the Policy Agent ignores the `-n` option and does *not* assign a Node Mapping to the VM. Applies to Simplified or Automated Authentication only (the `-a` option must be specified on the `hcl register` command).
- `kc-hostname[:port],kc-hostname2[:port],...` (required)—The list of IP addresses or hostnames for the Cryptographic Security Platform Vault nodes with which you want to register the VM. You must specify at least one Cryptographic Security Platform Vault node in this list. You must also specify a port if the Cryptographic Security Platform Vault nodes use anything other than the default port (443).

  > If you are using the `-n` option to specify a Cluster Node Mapping, this IP address will be the Cryptographic Security Platform Vault for VM Encryption node that the VM contacts to retrieve the Node Mapping information. After the Node Mapping has been retrieved, the Policy Agent ignores any other IP addresses in this list and only registers the VM with the Cryptographic Security Platform Vault for VM Encryption nodes contained in the Node Mapping.

- *cert-file*.cert —The name of the certificate file you copied to the target system if you are using Standard Authentication. If you are running the `hcl register` command from a directory other than the one where the `.cert` file resides, specify the full path to the `.cert` file as part of this option. If you did not create a certificate file in Cryptographic Security Platform Vault for VM Encryption, omit this option and use the `-a` option instead.

The following command registers a VM with the "hq-vm-3" and the "HQ Windows 2022 Server" description, using standard authentication and a node at 10.238.32.74.

```
C:\> hcl register -h hq-vm-3 -d "HQ Windows 2022 Server" 10.238.32.74
ad85837b-9862-11e1-afd5-000c29de5d41_120507163538.cert
You need to specify a passphrase that will be used for authentication with KeyControl
Enter passphrase (min 16 characters): passphrase16chars

Registered as hq-vm-3 with KeyControl node(s) 10.238.32.74
Please login to the KeyControl node to complete the authentication of this node
```

The following command line registers the VM without prompting the user.

```
C:\> hcl register -h hq-vm-3 -d "HQ Linux Server Alpha" -p <certpassphrase> -o
 <onetimepassword> 10.238.32.74 ./install/entrust/cert/ad85837b-9862-11e1-
afd5-000c29de5d41_120507163538.cert
```

```
Registered as hq-vm-3 with KeyControl node(s) 10.238.32.74
Please login to the KeyControl node to complete the authentication of this node
```

The following command registers a VM named "hq-vm-3" with the "HQ Windows 2022 Server" description and prompts the user for the account information, the cloud VM set, and the cluster node mapping.

```
C:\> hcl register -a -h hq-vm-3 -d "HQ Windows 2022 Server" 10.238.66.250

Do you want to register into a Vault?  (y/n) y
Please provide the vaultID
vaultid: d84243e7-d359-4179-9530-3497434e3192
Please provide the login details
username: CloudAdmin
password:

Available Cloud VM Sets
-------------------------------------------------------------------------------
SF-Datacenter
-------------------------------------------------------------------------------

Please specify Cloud VM Set to which this VM should be added: SF-Datacenter
Registered as hq-vm-3 with KeyControl node(s) 10.238.66.250

Completing authentication for hq-vm-3 on KeyControl node(s) 10.238.66.250

Authentication complete, machine ready to use
Getting KeyControl Mapping information


This VM can be added to one of the following KeyControl Mappings
-------------------------------------------------------------------------------
1 : SF-Datacenter-Map
2 : West-Coast-Map
-------------------------------------------------------------------------------

Please select a numeric KeyControl Mapping ID (0 to skip): 1
KeyControl Mapping: SF-Datacenter-Map
server description First Node, ip 10.238.66.250, port 443
server description Second Node, ip 10.238.66.251, port 443
Updated KeyControl list with KeyControl nodes 10.238.66.250:443,10.238.66.251:443
```

Uninstalling Silently on Windows

Before You Begin

Ensure that the Windows Policy Agent is installed.

Procedure

1. Start Windows command prompt with administrator-level privileges.
2. Run the uninstaller using the following command:
   C:\Program Files\hcs\uninstall.exe "/S _?=c:\Program Files\hcs"
   Note: This command assumes that the Policy Agent is installed in the default location. If you used a different location for your installation directory, please replace the folder paths.

The Windows Policy Agent is uninstalled silently.

11 Upgrading Policy Agent

- Policy Agent Upgrade Requirements
- Upgrading Policy Agent with the webGUI
- Upgrading the Policy Agent on Linux
- Upgrading the Policy Agent on Windows

Policy Agent Upgrade Requirements

The supported upgrade paths for the Policy Agent are listed below.

Important: You may be able to upgrade from an unsupported version, but those versions are not tested. We recommend you only use the supported upgrade paths.

Initial Release	Available Upgrade Paths
10.5.1	10.6.1
10.4.7	10.5.1, 10.6.1
10.4.5	10.4.7, 10.5.1, 10.6.1
10.4.3	10.4.5, 10.4.7, 10.5.1, 10.6.1

Upgrading Policy Agent with the webGUI

Important: You can upgrade the Policy Agent using the Cryptographic Security Platform Vault for VM Encryption webGUI or the Cryptographic Security Platform Vault for Databases webGUI. This procedure is written using the Cryptographic Security Platform Vault for VM Encryption webGUI, but the steps are the same as for the Cryptographic Security Platform Vault for Databases webGUI.

In order to complete the upgrade, the VM must be rebooted. You can either have this happen automatically during the upgrade procedure or you can tell Cryptographic Security Platform Vault that you want to reboot the VM manually. After you submit the upgrade request, the actual upgrade process will begin the next time that VM heartbeats with Cryptographic Security Platform Vault.

Important: Do not attempt to encrypt your system devices while the Policy Agent upgrade is in process. You can encrypt after the upgrade is complete and you have rebooted the VM where the Policy Agent is installed.

For older Policy Agents or other upgrade options, see Upgrading the Policy Agent on Linux and Upgrading the Policy Agent on Windows.

Procedure

1. Sign in to the Cryptographic Security Platform Vault for VM Encryption webGUI with Cloud Admin privileges.
2. In the top menu bar, click **WORKLOADS**.
3. Select the VM whose Policy Agent you want to upgrade and click the **Expand** button (**>**) at the end of the row.
4. If the Cryptographic Security Platform Vault for VM Encryption webGUI displays a message stating that an updated agent version is available, select **Actions > Upgrade Agent** from the main **Actions** menu.
5. Confirm that you want to upgrade the Policy Agent at the prompt.

6. If you want to have the Policy Agent automatically reboot the VM after the upgrade, click **Yes**. If you want to manually reboot the VM later to finish the upgrade, click **No**.
   Cryptographic Security Platform Vault creates an upgrade task that it communicates to the VM at the VM's next heartbeat. You can view the status of this task on the Dashboard in the Tasks tile. If you want the upgrade to begin immediately, log into the VM as an administrator and use the `hcl heartbeat` command.
7. If you selected No when prompted about automatic reboot, wait until the upgrade task has completed and then reboot the VM to finish the Policy Agent upgrade. The Cryptographic Security Platform Vault for VM Encryption webGUI will continue to display the informational message stating that an updated Policy Agent is available in the VM Details area until the VM is rebooted.
   Note: In some cases, the upgrade might not require a reboot. If the Cryptographic Security Platform Vault for VM Encryption webGUI simply displays the new version, then you do not need to reboot the VM.

Upgrading the Policy Agent on Linux

Before You Begin

- Make sure that you have upgraded your Cryptographic Security Platform Vault nodes before you upgrade your Policy Agents. Registration will fail if the version of the Policy Agent is higher than that of the Cryptographic Security Platform Vault node and your encrypted data may become unavailable.
- Make the upgrade path from your current version to the new version is supported. For details, see Policy Agent Upgrade Requirements.

Important: Do not attempt to encrypt your system devices while the Policy Agent upgrade is in process. You can encrypt after the upgrade is complete and you have rebooted the VM where the Policy Agent is installed.

Procedure

1. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI or the Cryptographic Security Platform Vault for Databases webGUI with Cloud Admin privileges.
2. Click **Workloads**.
3. Click **Actions > Download Policy Agent**.
4. Click the **Download** link associated with the file `hcs-client-agent-rel.number-build.number.run`. Cryptographic Security Platform Vault downloads the file to your browser's default download location.
5. Copy `hcs-client-agent-rel.number-build.number.run` to the Linux system that you want to upgrade.
6. Log into the target system as `root`.
7. Run the installer by navigating to the directory containing `hcs-client-agent-rel.number-build.number.run` and entering the command `sh ./hcs-client-agent-rel.number-build.number.run [install -y]`, where `[install -y]` tells the installer to upgrade the agent without prompting.
   For example:

```
# sh ./hcs-client-agent-10.5.1-12345.run
Creating directory hcs-agent-agent
Verifying archive integrity... All good.
Uncompressing hcs-agent-agent.run.....
HyTrust Agent version 4.1 already installed
Upgrade existing install? (y/n): y
Stopping hcld... done
Run once hcld
Starting hcld... done

You can now install online encryption driver, the process is described in the Admin Guide
Please see the following section of Admin Guide for details
```

— Administration Guide > Data Encryption > Linux Encryption Overview

Installation successful

```
# sh ./hcs-client-agent-10.5.1-12345.run install -y
Creating directory hcs-agent-agent
Verifying archive integrity... All good.
Uncompressing hcs-agent-agent.run.....
HyTrust Agent version 4.1 already installed
Stopping hcld... done
Run once hcld
Starting hcld... done

You can now install online encryption driver, the process is described in the Admin Guide
Please see the following section of Admin Guide for details
  — Administration Guide > Data Encryption > Linux Encryption Overview

Installation successful
```

8. If you want to verify the version of Policy Agent, enter the following command:
   # hcl version

Upgrading the Policy Agent on Windows

Before You Begin

- Make sure that you have upgraded your Cryptographic Security Platform Vault nodes before you upgrade your Policy Agents. Registration will fail if the version of the Policy Agent is higher than that of the Cryptographic Security Platform Vault node and your encrypted data may become unavailable.
- Make the upgrade path from your current version to the new version is supported. For details, see Policy Agent Upgrade Requirements.
- Make sure that any outstanding encryption or decryption operations are complete on the target system by checking the Cryptographic Security Platform Vault webGUI Dashboard.

Important: Do not attempt to encrypt your system devices while the Policy Agent upgrade is in process. You can encrypt after the upgrade is complete and you have rebooted the VM where the Policy Agent is installed.

Procedure

1. Sign in to the Cryptographic Security Platform Vault for Databases webGUI or Cryptographic Security Platform Vault for VM Encryption webGUI with Cloud Admin privileges.
2. Click **Workloads**.
3. Click **Actions > Download Policy Agent**.
4. Click the **Download** link associated with the file `hcs-client-agent-rel.number-build.number.exe` . Cryptographic Security Platform Vault downloads the file to your browser's default download location.
5. Copy `hcs-client-agent-rel.number-build.number.exe` to the Windows system that you want to upgrade.
6. Log into the target system as an Administrator.
7. Navigate to the directory in which you placed the `hcs-client-agent-rel.number-build.number.exe` file and run the installer.
8. On the Welcome page of the Entrust Setup Wizard, click **Next**.
9. On the License Agreement page, review the EULA (end user license agreement) and click **I Agree**.
10. In the **Choose Components** page, review the setting of the **HT Bootloader** option.
    If you want to encrypt the boot drive on this system now or in the future, make sure this option is selected.

If you are certain that you will never need to encrypt the boot drive, you can clear this check box.

11. If the **HT Bootloader** option is *not* selected:
    a. Click **Install**.
    b. The installer displays a prompt that the system is going to be upgraded and will require a reboot. Click **Yes** to continue with the upgrade.
12. If the **HT Bootloader** option *is* selected:
    a. Click **Next**.
    b. On the Drive and Network Configuration page, select the drive letter and the network that the Entrust Bootloader should use when connecting to Cryptographic Security Platform Vault. By default, this dialog box shows the current DeviceID (a unique integer) and ConnectionID from `WMI class Win32_NetworkAdapter` for the selected network interface.
    c. When you are finished, click **Install**.
    d. If prompted, click **Yes** to remove any existing Bootloader partitions.
    e. The installer displays a prompt that the system is going to be upgraded and will require a reboot. Click **Yes** to continue with the upgrade.
    f. If this is the first time the Entrust Bootloader has been installed on this VM, after the machine has finished booting, copy the `id_rsa` key file to another location in case you ever need to access the Entrust Bootloader Debug Console using SSH. If you are upgrading an existing Bootloader installation, the `id_rsa` key file is not changed during the upgrade.

12 CSP Vault Appliance Management

Appliance Management is part of the Cryptographic Security Platform Vault Management webGUI. Click the Appliance Management link to switch views. When you are on the Appliance Management page, click the Manage Vaults link to return.

- CSP Vault System Configuration
- CSP Vault Cluster Maintenance
- CSP Vault System Maintenance and Troubleshooting
- CSP Vault Management webGUI Page Reference

CSP Vault System Configuration

- Enabling an HTTP Proxy Server in CSP Vault
- Network Interface Configuration Options
- Configuring TLS
- Uploading an OIDC CA Certificate
- Setting Email Server Preferences
- Setting CSP Vault Console Settings
- Syslog Server Settings
- CSP Vault Certificates
- Admin Keys
- KMIP Server Configuration
- Hardware Security Modules with CSP Vault
- SNMP Traps in Cryptographic Security Platform Vault
- Setting CSP Vault Management webGUI Alert Settings
- Using the Entrust CSP Vault System Console

Enabling an HTTP Proxy Server in CSP Vault

If Cryptographic Security Platform Vault does not have direct access to the internet, you can configure an HTTP proxy server to use for BYOK.

Note: The proxy settings affect the entire Cryptographic Security Platform Vault and also apply to all the vaults that you create.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **Proxy Settings**.
5. On the Proxy Settings page, specify the following:
    - On the Basic tab, enter the IP/Hostname and the port number for the HTTP proxy server.
    - On the Advanced tab, optionally enter the username and password for the HTTP proxy server.

   Note: If your HTTP proxy server is configured without authorization, then you do not need to enter a username and password. We recommend that you use authentication.
6. When you are finished, click **Apply**.

Network Interface Configuration Options

When you install Cryptographic Security Platform Vault, you have to specify a valid network connection to make sure the Cryptographic Security Platform Vault node can communicate with other Cryptographic Security Platform Vault nodes and with associated VMs. If your network changes or if you want to use

multiple NICs (Network Interface Cards), you can update your settings using Manage Network Settings from the Entrust Cryptographic Security Platform Vault System Console on the node whose network settings you want to change.

The Manage Network Settings menu includes the following options:

Option	Description
Show Current Network Configuration	Lets you view the current network configuration for the node. If the node has multiple NICs, this option allows you to select which NIC configuration you want to view.
Manage IP Address Settings	Lets you change the current network configuration. If the node has multiple NICs, this option allows you to select which NIC configuration you want to change. For details, see Multi-NIC Node Configuration.
Disable a Network Interface	If the node is configured with multiple NICs, this option lets you remove one or more NICs from the configuration. For details, see Removing a NIC from the Configuration. Note: You cannot remove the management interface.
Manage DNS Settings	Lets you view and update your current DNS Settings. For details, see Configuring DNS Settings.
Manage NTP Settings	Lets you view and update your current NTP Settings. For details, see Configuring NTP Settings.
Manage Static Routes	Lets you add static routes for the Cryptographic Security Platform Vault node for environments where dynamic routing is not the optimal solution. For details, see Configuring Static Routes.
Network Diagnostic Tools	Lets you troubleshoot network issues. For details, see Troubleshooting Network Issues.

Multi-NIC Node Configuration

If you want to segregate the communication traffic across multiple channels, you can configure a Cryptographic Security Platform Vault node to use multiple virtual NICs (Network Interface Cards). For example, you may want one NIC to handle the communication between the Cryptographic Security Platform Vault webGUI and the Cryptographic Security Platform Vault nodes on `TCP/443` while a second NIC handles the cluster traffic and the internal node management traffic on `TCP/8443`. Multi-NIC configuration is only supported with the Cryptographic Security Platform Vault for Databases and the Cryptographic Security Platform Vault for VM Encryption for policy agent communication.

With multiple NICs, one NIC must be designated as the "management interface", and this interface must be able to communicate on port `TCP/8443`. Cryptographic Security Platform Vault uses the internal node management interface to:

- Determine the administrative MAC address for the node.
- Initializes the communication traffic between the nodes in the cluster.
- Handle any authentication requests that come into the cluster.

All management interface communication must take place on the management interface. You *cannot* split management communication across multiple interfaces.

Considerations

When you are configuring multiple NICs on a node, keep the following things in mind:

- Cryptographic Security Platform Vault supports a maximum of four virtual NICs. One NIC must be the management interface, as described above. In addition to the management interface, you can specify up to three additional NICs that can be used for inbound and outbound traffic. This includes inbound client and Cryptographic Security Platform Vault webGUI traffic as well as outbound syslog, NFS, and email traffic.
- All NICs must be of the same interface adapter type. For example, if the first NIC specified uses the adapter type VMXNET, all other NICs must be of type VMXNET.
- All NICs use global values for their DNS settings, NTP settings, default gateway, and DNS server list. Any change made to those settings on one NIC affects all NICs.
- When you deploy a new Cryptographic Security Platform Vault node through an OVA template or an ISO image, you must specify basic network information such as an IP address, domain, gateway, and DNS server list. When you do so, Cryptographic Security Platform Vault automatically designates that IP address as the management interface on port `TCP/8443`. We strongly recommend that you do not change this interface if the node is already part of a cluster or if any VMs have already been registered with the node.
  If you want to select the management interface during deployment, you must install Cryptographic Security Platform Vault from the ISO image on an existing VM that already has all of the required NICs configured. In this case, Cryptographic Security Platform Vault will prompt you to select the management interface during the installation.
- Adding additional NICs to the VM after deployment requires you to shut down the Cryptographic Security Platform Vault node while you add the NICs. You cannot add NICs to a running system.
  If the node is part of a cluster, the cluster will become degraded if the node is unreachable for too long. If the node is a standalone node, any VMs registered with the node will be unable to retrieve their keys while the network services are offline, and any VM heartbeats will fail.
- Cryptographic Security Platform Vault automatically restarts the network services on the node every time you change the configuration for a NIC. The node will be unavailable for a brief period until this process has finished.

Related Topics

- Configuring Multiple NICs on an Existing CSP Vault
- Removing a NIC from the Configuration

Configuring Multiple NICs on an Existing CSP Vault

When you deploy a new Cryptographic Security Platform Vault node, you configure the management interface during that process. We strongly recommend that you do not change this interface after you have deployed the node if the node is part of a cluster or if there are VMs registered with the node.

The following procedure describes how to add and configure additional NICs on an already-deployed node. For details about deploying a new Cryptographic Security Platform Vault node, see Installing CSP Vault from an OVA Template or Installing the First CSP Vault Node from an ISO Image.

Warning: During the following procedure, the node will be unavailable at certain points. If the node is part of a cluster, the cluster will become degraded if the node is unreachable for too long. If the node is a standalone node, any VMs registered with the node will be unable to retrieve their keys while the node is offline.

In addition, if the node is part of a cluster and you want to change the management interface, you must remove the node from the cluster first.

1. If the additional NICs you want to use have not yet been configured on the VM in which the Cryptographic Security Platform Vault node is running, do the following:
    a. If the Cryptographic Security Platform Vault node is powered on, shut it down using your hypervisor or the node's Entrust Cryptographic Security Platform Vault System Console. For details, see Using the Entrust CSP Vault System Console.
    b. In your hypervisor, add the new NICs to the Cryptographic Security Platform Vault VM and configure them using your corporate standards.
    Note: Make sure that the new NICs use the same adapter type as the existing NICs. For example, if the management interface NIC is of type VMXNET, the new NICs must be of type VMXNET as well.
    c. Make a note of the MAC address you are using for each NIC. When the NICs are displayed in Cryptographic Security Platform Vault, they are identified by their MAC address. Therefore, when you go to configure the NIC in Cryptographic Security Platform Vault later in this procedure, you will need to know its MAC address.
    d. Power on the Cryptographic Security Platform Vault VM.
2. Log in as `htadmin` on the Cryptographic Security Platform Vault node whose NICs you want to configure.
Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
3. Select **Manage Network Settings**.
4. Select **Manage IP Address Settings**.
5. On the **Interfaces** screen, select the NIC you want to configure and press **Enter**.
The NIC that is the current management interface has 'Current management interface' listed after the name. We strongly recommend that you do not change this interface after deployment if this node is part of a Cryptographic Security Platform Vault cluster or any VMs are registered with this node. If you select the management interface, acknowledge the configuration request at the prompt.
6. On the **Secondary Network Configuration** screen, specify the static IP address and netmask for the Cryptographic Security Platform Vault node.
Note:
    - Changing the hostname on one NIC changes it for all NICs, including the management interface NIC. If this node is part of a cluster, you should not change the hostname for the node.
    - All NICs must use the same default gateway and DNS server list.
    - Make sure you specify a static IP address and netmask for the Cryptographic Security Platform Vault node.
7. When you have finished specifying the network information, select **OK** and press **Enter**.
Cryptographic Security Platform Vault restarts the network services using the new configuration. Contact with the node via the Cryptographic Security Platform Vault webGUI or by any VMs registered with the node will be unavailable until the restart is finished.
When the network finishes restarting, Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console.
8. Repeat the proceeding steps for any other NICs you want to configure. Cryptographic Security Platform Vault will restart the network services and the node will be unreachable for a short time after each configuration change.
9. If you want to verify the configuration information, select **Manage Network Settings**. From there, select **Show Current Network Configuration** to view a list of the configured NICs with their IP addresses and netmasks. The management interface IP address is shown as the main interface. Any additional interfaces that are configured are shown below.

Removing a NIC from the Configuration

If you want to remove a NIC that you have previously configured, you should use the Entrust Cryptographic Security Platform Vault System Console to disable that NIC in Cryptographic Security Platform Vault before you remove it from the VM.

In addition, if this node is part of a cluster we recommend that you remove it from the cluster before you remove the NIC. You can then re-join it with the cluster after the network configuration is complete.

Warning: This option is not reversible and it requires the node to reboot.

1. Log in as `htadmin` on the VM whose NIC you want to remove.
   Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Manage Network Settings**.
3. Select **Disable Network Configuration**.
4. Select the interface you want to disable.
   Note: You cannot disable the management interface, so Cryptographic Security Platform Vault does not show that interface in the list.
5. Confirm at the prompt.
6. Press **Enter** to reboot the node.
7. If desired, select **Shutdown System** and then use your hypervisor to remove the NIC from the VM.

Configuring DNS Settings

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. From the Entrust Cryptographic Security Platform Vault System Console, select **Manage Network Settings > Manage DNS Settings**.
3. On the **Modify DNS Settings** page, you can view your existing DNS settings. Select one of the following:
   - **No**—Exits the screen and returns to the Manage Network Settings page.
   - **Yes**—Opens the Network Configuration screen. Enter a comma-separated list of DNS addresses. Select **Ok** to save and then **Yes** on the confirmation screen. If you decide not to make changes, select **Cancel** to return to the Manage Network Settings page.

Configuring NTP Settings

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. From the Entrust Cryptographic Security Platform Vault System Console, select **Manage Network Settings > Manage NTP Settings**.
3. On the **Modify NTP Network Settings** page, you can view your existing NTP settings. Select one of the following:
   - **No**—Exits the screen and returns to the Manage Network Settings page.
   - **Yes**—Opens the Network Configuration screen. Enter a comma-separated list of NTP addresses. Select **Ok** to save and then **Yes** on the confirmation screen. If you decide not to make changes, select **Cancel** to return to the Manage Network Settings page.

Configuring Static Routes

In some network environments, it may be necessary to add static routes to Cryptographic Security Platform Vault rather than relying on dynamic routing.

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. From the Entrust Cryptographic Security Platform Vault System Console, select **Manage Network Settings > Manage Static Routes**.
3. From the **Static Routes** page, you can:
    - View a list of the defined routes by selecting **List Current Static Routes**.
    - Add a new route by selecting **Add Static Route** and entering the route network address and gateway in the Add Static Route page. Cryptographic Security Platform Vault displays a message that the route has been successfully added.
    - Delete a previously-defined static route by selecting **Delete Static Route** and specifying the network address and gateway of the route you want to delete. Cryptographic Security Platform Vault displays a message that the route has been deleted.

Configuring TLS

Because each node hosts a standalone webserver, if you want to configure TLS for a node you must log into the webGUI for that specific node.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **General Settings** section, click **TLS Configuration**.
5. On the **Protocol** tab, select the TLS authentication modes that you want to use:
    - TLSv1.2, TLSv1.3
    - TLSv1.3 only
6. Optionally, on the **Cipher Suite** tab, review the detailed list of available ciphers. If you want to remove ciphers from this list, click the **X** following the cipher name that you do not want to use. If you want to add a cipher, click in the bottom of the list box and enter a valid cipher name, then click **Reload**.
   The following ciphers are supported:
    - ECDHE-ECDSA-AES256-GCM-SHA384
    - ECDHE-RSA-AES256-GCM-SHA384
    - ECDHE-ECDSA-AES256-CCM
    - ECDHE-ECDSA-AES128-GCM-SHA256
    - ECDHE-RSA-AES128-GCM-SHA256
    - ECDHE-ECDSA-AES128-CCM
    - DHE-RSA-AES256-GCM-SHA384
    - DHE-RSA-AES256-CCM
    - DHE-RSA-AES128-GCM-SHA256
    - DHE-RSA-AES128-CCM
    - PSK-AES256-GCM-SHA384
    - PSK-AES256-CCM
    - PSK-AES128-GCM-SHA256
    - PSK-AES128-CCM
    - DHE-PSK-AES256-GCM-SHA384
    - DHE-PSK-AES256-CCM

- DHE-PSK-AES128-GCM-SHA256
- DHE-PSK-AES128-CCM

7. On the **TLS Extended Master Secret** tab, select whether or not to enforce EMS. We highly recommend that you enable EMS.
   Important:
   - The EMS setting applies to the entire cluster. Changing the EMS will automatically reboot all nodes in the cluster. After rebooting, it may take the nodes several minutes to restart.
   - If you have EMS configured on your Cryptographic Security Platform Vault Appliance, you must disable it before you can connect to Cryptographic Security Platform Compliance Manager.
   - If you plan to use Double Key Encryption (DKE), TLS must be set to **TLSv1.2, TLSv1.3** and EMS must be set to **Do not enforce EMS**.
8. When you are finished, click **Apply**.

Uploading an OIDC CA Certificate

Because the Cryptographic Security Platform Vault certificate store is shared between the appliance and all individual vaults, if a vault using OIDC is locked out because the OIDC certificate expired, you can upload it here to restore access to the vault.

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar click **Settings**.
4. In the General Settings section, click **OIDC CA Cert**.
5. On the OIDC CA Cert page, click **Load File** and locate the certificate that you want to upload.
   Note: Certificates must be in base 64 encoded .pem format.
6. Click **Upload**.

Setting Email Server Preferences

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Mail Server**.
4. On the **Mail** tab, specify the options you want to use.

Option	Description
Disable E-mail Notifications check box	If checked, no alert emails are sent to the user accounts in the system. If the Admin Key is regenerated, all security admins must manually download their key parts from the Settings tab. If this option is not selected, Cryptographic Security Platform Vault only sends alerts and new Admin Key parts through email. Security Admins can still download their Admin Key parts from the webGUI. For details about the Admin Key, see Admin Keys.

Option	Description
Server	The IP address or fully qualified domain name (FQDN) of the SMTP server. If your domain has an MX record configured, you can use Cryptographic Security Platform Vault to relay mail by setting the IP address to `127.0.0.1`. This is the default behavior.
Port	The mail server port.
Login	If required, the user account with which Cryptographic Security Platform Vault should log into the email server.
Password	The password for the login account.
Sender	The sender that Cryptographic Security Platform Vault should use when sending email.
SMTPS	If this option is set to On, Cryptographic Security Platform Vault uses SMTP Secure (SMTPS). Note: • If you disable SMTPS, and the server supports StartTLS, then when the connection is made StartTLS will be used. SMTPS is not compatible with StartTLS, and only one can be used. • Important information such as alerts and admin keys are shared by email. We highly recommend you set this option to use encryption with SMTP.

5. To test the email settings, click **Send Test Email**.

Setting CSP Vault Console Settings

If you do not remember the credentials of any user with the Security Administrator (`secroot`) privilege, or if you are locked out of the Cryptographic Security Platform Vault webGUI, Cryptographic Security Platform Vault provides a self-service option using the Cryptographic Security Platform Vault System Console to reset the `secroot`) user credentials with a temporary password. You can disable this option if you do not want this feature.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **Console Settings**.
5. On the Cryptographic Security Platform Vault Console Settings page, select one of the following:
   - Select **YES** to allow the `htadmin` user to reset the `secroot` password.
   - Select **NO** if you do not want to allow the `htadmin` user to reset the `secroot` password.

6. Click **Apply**.

Syslog Server Settings

The Syslog Server Settings page allows you to view the settings of your Syslog Server, or enable or disable the server. When enabled, you can set the protocol to TCP or UDP, set the type of TLS authentication, the log format (RFC 5424 or CEF), and enter a list of syslog servers and their corresponding ports. You can also generate a certificate signing request, and, if required by your authentication mode, upload a CA certificate or client certificate. You can also reset the Syslog Server settings to the default values.

- Configuring Syslog Server Settings
- Resetting Syslog Server Settings

Configuring Syslog Server Settings

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. Click the Switch to Appliance Management link at the top right.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **Syslog Server**.
5. On the **Syslog Server Settings** page, specify the options you want to use.

Option	Description
State	Select ENABLED to use a syslog server.
Protocol	Select the protocol that you want to use. You can use TCP or UDP for syslog.
TLS Authentication List	Select one of the following: • No validation • x509/certvalid—Requires server certificate validation. • x509/name—Requires server certificate validation and hostname validation. • x509/fingerprint—Requires server certificate fingerprint. The fingerprint is a SHA1 hash of the server certificate, for example: "SHA1:00:11:22:33:44:55:66:77:88:99:00:11:22:33:44:55:66:77:88:99".
Server List	Enter the list of syslog servers and their corresponding ports. For the port, enter an outbound port between 25 and 65535.
Log Format	Select one of the following: • RFC 5424 • CEF
CA Certificate	Upload a CA certificate if you are using x509/certvalid or x509/name.

Option	Description
Client Certificate	Upload a client certificate if you are using x509/certvalid, x509/name, or x509/fingerprint.

6. Click **Apply**.

Important: If you plan to use an external syslog server for your audit logs, you must also complete the following:

1. Configure your syslog server to receive messages from each of the Cryptographic Security Platform Vault nodes in the cluster. The `syslogd` flags that specify the Cryptographic Security Platform Vault nodes should contain names that are resolvable. Make sure that your `/etc/hosts` file is set up correctly, with either IP addresses or hostnames. If you use hostnames, make sure that reverse lookups work on the syslog server.
2. Add the tag `hcs_audit` to your `syslog.conf` file. The FreeBSD example below directs all `hcs_audit` messages to go to the log file `/var/log/hcs_audit.log`:
   ```
   ! hcs_audit *.* /var/log/hcs_audit.log
   ! -hcs_audit
   ```
3. Make sure the audit log file is only writeable by `root`. For example:
   ```
   # touch /var/log/hcs_audit.log
   # chmod 0600 /var/log/hcs_audit.log
   ```
4. Configure your `rc.conf` file. For example, the following should be set prior to changing to `syslog.conf`:
   ```
   syslogd_enable="YES"
   syslogd_flags="-a kps1.domain -a kps2.domain -v"
   ```
5. Restart the syslog daemon and verify that audit records generated by every Cryptographic Security Platform Vault node are being written to the `hcs_audit.log` file by logging out and then log back in on each of the Cryptographic Security Platform Vault nodes in the cluster. When you are done, examine the audit log to make sure those logins were properly recorded.
   If messages are not being added, use **tcpdump** to make sure that packets are arriving at the syslog server. If the packets are arriving, check the documentation for your syslog server to make sure the configuration is correct.

Resetting Syslog Server Settings

You can reset the Syslog server settings to the default values.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, select **Syslog Server**.
5. Select **Actions > Reset to Default**.
6. At the prompt, select **Proceed**.

CSP Vault Certificates

- About CSP Vault Certificates
- Viewing the Expiration Date for the Current CSP Vault SSL Certificate

- Creating a Certificate Signing Request
- Using Self-Signed Certificates for All Nodes in a Cluster
- Generating and Installing a Custom Self-Signed Certificate
- Installing External Certificates for Internal and External Webservers
- CSP Vault Certificate Expiration Notification
- Installing a New Self-Signed Certificate for a Node
- Downloading a CSP Vault CA Certificate
- Troubleshooting Certificate Issues
- Manually Updating the CA Certificate on a Linux Root Drive Encrypted VM
- Manually Updating the CA Certificate on a Data Encrypted VM
- Manually Updating the CA Certificate on a Windows Boot Drive Encrypted VM

About CSP Vault Certificates

Cryptographic Security Platform Vault requires that an SSL certificate be installed on each Cryptographic Security Platform Vault node in a cluster. Each Cryptographic Security Platform Vault instance is installed with two web servers:

- An internal web server that manages the CSP Vault node to node cluster communication on port 8443.
- An external web server that manages the CSP Vault Web UI, the REST API interface, and the Policy agent communication on port 443.

By default, Cryptographic Security Platform Vault includes a component for creating a Root Certificate Authority (CA) that can generate digital certificates. When the first Cryptographic Security Platform Vault node is installed, it creates a Private and Public CA that it also stores in the Cryptographic Security Platform Vault object store.

The first Cryptographic Security Platform Vault node then uses the Private CA to create an SSL certificate that contains the hostname (FQDN) as well as the IP address of the Cryptographic Security Platform Vault node for the internal web server and Public CA to create an SSL certificate that contains the hostname, both short and FQDN, as well as the IP address of the Cryptographic Security Platform Vault node for the external web server. When the node reboots, Cryptographic Security Platform Vault checks the IP address and recreates the SSL certificate if the IP address has changed.

Cryptographic Security Platform Vault node to node communication is on a TLS channel and it uses SSL certificates issued by Private CA to secure communication. When additional Cryptographic Security Platform Vault nodes are added to the cluster, the first Cryptographic Security Platform Vault node shares the Private and Public CA through the Cryptographic Security Platform Vault object store over an HTTPS connection.

In addition to creating an SSL certificate on each Cryptographic Security Platform Vault node, the Public CA also creates a matching CA certificate that is copied to a VM when the VM is registered with Cryptographic Security Platform Vault. The VM uses the CA certificate to verify Cryptographic Security Platform Vault's identity every time it receives a communication from Cryptographic Security Platform Vault. If the CA certificate on the VM cannot verify the SSL certificate that signed the communication, the VM rejects the communication.

The VM also has its own certificate that it uses to sign any communication it sends to Cryptographic Security Platform Vault. If Cryptographic Security Platform Vault determines that the VM's certificate is invalid or has expired, Cryptographic Security Platform Vault rejects the communication.

Because both the VM and Cryptographic Security Platform Vault verify any incoming communication, a "man in the middle" attack is not possible. The VM must be able to verify Cryptographic Security Platform Vault's identity and Cryptographic Security Platform Vault must be able to verify the VM's identity before any information is exchanged.

In this scenario, the Public CA installed on all the Cryptographic Security Platform Vault nodes is the same, ensuring that every Cryptographic Security Platform Vault node is able to verify SSL certificates generated by every other Cryptographic Security Platform Vault node in the cluster. However, this default SSL certificate is considered self-signed, which can lead to trust issues.

Cryptographic Security Platform Vault Certificate Options

You can replace the default SSL certificate configured on external and internal web server with an externally signed SSL certificate at any time by uploading the externally signed SSL certificate and its associated CA certificate to one of the Cryptographic Security Platform Vault nodes in the cluster.

If an externally signed SSL certificate is uploaded to be installed on internal web server, Cryptographic Security Platform Vault automatically distributes an updated CA certificate to all other nodes in the cluster.

If an externally signed SSL certificate is uploaded to be installed on external web server, Cryptographic Security Platform Vault automatically distributes an updated CA certificate to all registered VMs. The VMs can then use the updated CA certificate to validate any communication coming from Cryptographic Security Platform Vault. You can either use the same external SSL certificate on all Cryptographic Security Platform Vault nodes or you can use a different SSL certificate on each node. If you use different certificates, however, Entrust recommends that those certificates all be signed by the same certificate authority. For more information, see Installing External Certificates for Internal and External Webservers.

> Note: If you are generating an SSL certificate from openssl or other third-party tool, make sure you use a template designed for a web server certificate. Cryptographic Security Platform Vault registration may fail for some VMs if the SSL certificate is generated using a template designed for a Certificate Authority certificate.

You can also replace the current SSL certificate with a new self-signed certificate that will be automatically distributed to all Cryptographic Security Platform Vault nodes. If a new signed certificate is generated for external web server, Cryptographic Security Platform Vault does not need to communicate with the VMs because the default CA certificate is always copied to the VM during the registration process, even when Cryptographic Security Platform Vault is using an externally signed certificate. For more information, see Installing a New Self-Signed Certificate for a Node.

Viewing the Expiration Date for the Current CSP Vault SSL Certificate

It is critical to keep the Cryptographic Security Platform Vault certificate current. If it expires, Cryptographic Security Platform Vault will be unable to send keys to the registered VMs and data access will be denied until a valid certificate is installed.

Use the following procedure to view the expiration date for the current Cryptographic Security Platform Vault certificate on the selected Cryptographic Security Platform Vault node.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Servers** tab and select a Cryptographic Security Platform Vault node.
5. To view the SSL certificate configured for the internal web server, click the link next to **Internal Web server** in the Certificate detail.
   The link name is **Default** if the internal web server is using the default self-signed certificate and **Custom** if it is using a custom SSL certificate.
6. To view the SSL certificate configured for the external web server, click the link next to **External Web server** in the Certificate detail.
   The link name is **Default** if the external web server is using the default self-signed certificate and **Custom** if it is using a custom SSL certificate.

7. When you are done, click **Close**.
8. If you want to check the expiration date for the certificate on another Cryptographic Security Platform Vault node, select that node and repeat this procedure.

Creating a Certificate Signing Request

A certificate signing request (CSR) tells an external Certificate Authority (CA) that you want an SSL certificate generated and signed by that CA. The SSL certificate can then be uploaded to Cryptographic Security Platform Vault and used in place of the default self-signed certificate.

When you use Cryptographic Security Platform Vault to create the CSR, Cryptographic Security Platform Vault creates a key pair and uses that key pair in conjunction with the information you specify to create the CSR. Cryptographic Security Platform Vault then encrypts the key pair and stores it for later use.

You can use the resulting CSR to generate an SSL certificate from the external CA you want to use. After you receive the SSL certificate from that external CA, you can upload it to Cryptographic Security Platform Vault. Because the key pair already exists on the system, you do not need to upload anything else.

If you create the CSR to generate an SSL certificate to be installed for internal web server, you must include the IP address of the Cryptographic Security Platform Vault node in Subject Alternative Name.

If you create the CSR outside of Cryptographic Security Platform Vault, you need to upload both the SSL certificate and the matching private key file when you install the certificate on Cryptographic Security Platform Vault.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Servers** tab and select a Cryptographic Security Platform Vault node.
5. Select **Actions > Create CSR**.
6. In the Generate Certificate Signing Request dialog box, specify the options you want to use.

Field	Description
Common Name	The name to associate with this request. By default, Cryptographic Security Platform Vault enters the selected server name in this field. You can edit the default name as needed.
Locality	The locale to associate with this request.
State	The state to associate with this request.
Subject Alternative Names	The host names that will be protected by this certificate. If you want to use the same certificate on multiple Cryptographic Security Platform Vault nodes in the system for the external web server, add all of the Cryptographic Security Platform Vault URLs to this list. By default, Cryptographic Security Platform Vault adds the URL of the selected Cryptographic Security Platform Vault node. You can change or delete the default URL as long as you end up specifying at least one Cryptographic Security Platform Vault node in this field.

Field	Description
Key Size	Select the key size that you want to use. The default is 4096 bytes.
Country	The ISO 3166-1 alpha-2 code of country to associate with this request. The default is US.
Organization	The organization to associate with this request.
Organization Unit	The organizational unit associate with this request.

7. Click **Generate**.
8. When you receive the message that Cryptographic Security Platform Vault has created the CSR, click **Download** to save a copy of the CSR to your browser's default download directory or click **Preview** to view the CSR in a pop-up window. You can copy the CSR from the Preview window to the clipboard if desired.
9. Use the CSR to request an SSL certificate from the external Certificate Authority you want to use. How you do this depends on the CA you are using.

What to Do Next

After you receive the SSL certificate from the external CA, install it on Cryptographic Security Platform Vault as described in Installing External Certificates for Internal and External Webservers.

Using Self-Signed Certificates for All Nodes in a Cluster

If you plan to use self-signed certificates, we recommend that you use them for all nodes in the cluster. You can now set the entire cluster to accept self-signed certificates.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Cluster** tab and select **Actions > Use Self-Signed Certificate**.
5. Click **Proceed** at the prompt.
   Cryptographic Security Platform Vault generates a new self-signed certificate for all nodes in the cluster, and then restarts the server. You will need to log back into Cryptographic Security Platform Vault after the restart.
   Tip: If you are using IE, you may receive an alert stating that revocation information for the certificate is not available. Click **Yes** to acknowledge the alert and restart the web service. If you are using Chrome and you receive a series of connection errors when the web service restarts, open the webGUI login page in a new tab.
   To view the certificates, click the Servers tab, select a node, and then click the links next to **Internal/ External web server**.

Generating and Installing a Custom Self-Signed Certificate

Use this procedure to generate and install a custom self-signed certificate for all nodes in your cluster. If you are using a KMIP server you can choose to use this certificate for the KMIP server as well.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Cluster** tab and select **Actions > Generate and Install Self-Signed Certificate**.
5. Complete the following:

Field	Description
Common Name	The name to associate with this certificate. This field is required.
Locality	Optional. The locale to associate with this certificate.
State	Optional. The state to associate with this certificate.
Subject Alternative Names	Optional. The host names that will be protected by this certificate. If you want to use the same certificate on multiple Cryptographic Security Platform Vault nodes in the system for the external web server, add all of the Cryptographic Security Platform Vault URLs to this list. By default, Cryptographic Security Platform Vault adds the URL of the selected Cryptographic Security Platform Vault node. You can change or delete the default URL as long as you end up specifying at least one Cryptographic Security Platform Vault node in this field.
Key Size	Optional. Select the key size that you want to use. The default is 4096 bytes.
Country	The ISO 3166-1 alpha-2 code of country to associate with this certificate. This field is required.
Organization	Optional. The organization to associate with this request.
Organization Unit	Optional. The organizational unit associate with this request.
Validity (Days)	Optional. The number of days this certificate will be valid. The default is 365 days.
Use this certificate for KMIP	Select Yes if you are using a KMIP server along with the Cryptographic Security Platform Vault for KMIP and want to use this certificate for the KMIP server as well. The default is No.

6. Click **Generate and Install**.

Installing External Certificates for Internal and External Webservers

Use this procedure to replace the current Cryptographic Security Platform Vault SSL certificate with a new externally-signed SSL certificate. If you want to use a new, self-signed SSL certificate generated by the Public CA or Private CA included with Cryptographic Security Platform Vault, see Installing a New Self-Signed Certificate for a Node.

Before You Begin

- If you generated external certificates using Microsoft Active Directory Certificate Services, then the certificates will be in .p7b format. Because Cryptographic Security Platform Vault only accepts certificates in base64-encoded PEM format, you will need to convert the file using the following:
    a. Run `openssl pkcs7 -in cert.p7b -inform p7b -print_certs -out cert.pem`, where cert.p7b is the input certificate in .p7b format and cert.pem is the converted certificate in .pem format.
    b. If you have a certificate chain with no separate server certificate and CA certificate/chain, the first certificate in the chain is generally used as the server certificate, and all other certificates would be the CA certificate chain. In this case, you can break up the chain into two files, with server.pem containing the server certificate (the first certificate) and cacert.pem containing the remaining certificates.
    If this occurs, verify that the separation is correct by running `openssl verify -verbose -CAfile server.pem cacert.pem`, where server.pem is the server certificate and and cacert.pem are is the CA certificate/chain.
- If you generated the Certificate Signing Request (CSR) through Cryptographic Security Platform Vault, you need to make sure you have the resulting SSL certificate and the CA certificate in Base64-encoded pem format files accessible to the Cryptographic Security Platform Vault node that you are logged into. If you generated the CSR through some other means, make sure you have both of the Base64-encoded pem format certificates and the Base64-encoded pem format private key file that goes with the certificates. Cryptographic Security Platform Vault supports only RSA private keys. For more information, see Creating a Certificate Signing Request.
- If you generated the SSL certificate from openssl or other third-party tool, make sure the certificate is formatted as a web server certificate. Cryptographic Security Platform Vault registration may fail for some VMs if the SSL certificate is formatted as a Certificate Authority certificate.
- The SSL certificate generated for the internal web server should be able to function as the Client and Server certificate.
- SSL certificates that contain an intermediate CA certificate chain are not supported for the internal web server. If there is a certificate chain, it must be specified in the CA certificate for the internal web server.
- We strongly recommend that you verify all VMs registered with Cryptographic Security Platform Vault are online and accessible before you install a new SSL certificate on Cryptographic Security Platform Vault for the external web server. During the installation process, Cryptographic Security Platform Vault sends an updated version of the CA certificate to each of the registered VMs at their next heartbeat. If all VMs are online, this process is fairly simple and ensures that there is no interruption in the communication between the VMs and Cryptographic Security Platform Vault. If any VMs are inaccessible, however, the CA certificate may need to be manually updated on those VMs after the SSL certificate installation on Cryptographic Security Platform Vault is complete because the old CA certificate installed on the VMs will no longer be able to verify Cryptographic Security Platform Vault's identity and all communication coming from Cryptographic Security Platform Vault will be rejected by the VMs.
- Externally signed custom certificates must have the "Key Usage" extension set to "Digital Signature" and "Key Encipherment".

Procedure

1. Sign in to the Cryptographic Security Platform Vault Management webGUI with domain admin privileges.
2. In the top menu bar, click **Cluster**.
3. Click the **Servers** tab and select a Cryptographic Security Platform Vault node.

Note: You can use SSL certificates signed by different certificate authorities on individual Cryptographic Security Platform Vault nodes. However, Entrust recommends that all of the SSL certificates be signed by the same Certificate Authority so that only one CA certificate is required on the VMs registered with Cryptographic Security Platform Vault.

4. Select **Actions > Install Certificate**.
5. In the **Certificate** tab of the Certificate Installation dialog box, specify the options you want to use.

Field	Description
SSL Certificate	The SSL certificate file in Base64-encoded pem format. This certificate must be valid for the installation to succeed.
CA Certificate	The certificate of the CA that issued the SSL certificate in Base64-encoded pem format. The VMs registered with Cryptographic Security Platform Vault use the CA certificate to verify communication with Cryptographic Security Platform Vault.
Web Server	Choose which web server (External for port 443 or Internal for Port 8443) to install the custom certificate. You can select both if you wish to install the same SSL certificate for the internal and the external web server. If the SSL certificate is used for both web servers, it should be able to function as a Client and Server certificate and it should have the Cryptographic Security Platform Vault IP address specified in SAN.

Important: Before Cryptographic Security Platform Vault installs the certificate, it checks with the certificate authority to make sure that the SSL certificate can be validated.
If using a CA Certificate Chain, where the Server Certificate is signed by Intermediate CA, Entrust recommends:

- The Server Certificate (SSL Certificate) should be a separate SSL Certificate file.
- The CA Certificate of the intermediate CA and its chain leading to self-signed root CA certificate should be in a single CA certificate file and arranged as shown below:

```
-----BEGIN CERTIFICATE-----
Intermediate CA Certificate that signed Server Certificate
-----END CERTIFICATE-----
.
.
. there can be a chain of intermediate CA certificates here
.
.
-----BEGIN CERTIFICATE-----
Root CA Certificate signed by itself (self-signed root CA Certificate)
-----END CERTIFICATE-----
```

Ensure the Server has a purpose set. You configure this using the External Key Usage property of the Server Certificate accordingly.
a. If using the certificate for External Web Server, Server Authentication must be enabled.
b. If using the certificate for Internal Web Server, both Server & Client Authentication must be enabled.

This would be `extendedKeyUsage = serverAuth, clientAuth` in openssl.cnf (OpenSSL config) of the Certificate Authority issuing Server Certificate. It can be verified by running `openssl x509 -purpose -noout -in server.pem` on the server Certificate. as shown in the example below:

```
# openssl x509 -purpose -noout -in server.pem
Certificate purposes:
SSL client : Yes
SSL client CA : No
SSL server : Yes
SSL server CA : No
Netscape SSL server : Yes
Netscape SSL server CA : No
S/MIME signing : Yes
S/MIME signing CA : No
S/MIME encryption : Yes
S/MIME encryption CA : No
CRL signing : No
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
Time Stamp signing : No
Time Stamp signing CA : No
```

`SSL server : Yes` (the SSL server line) indicates Server authentication is enabled. `SSL client : Yes` (the SSL client line) indicates Client authentication is enabled.

6. If you did *not* create the certificate signing request with Cryptographic Security Platform Vault:
   a. Click the **Private Key** tab and click **Load File**, then navigate to the private key file you want to use. Cryptographic Security Platform Vault never stores the private key in clear text.
   b. If the private key file is encrypted, enter the user-specified password for the key file in the **Password** field. This password is not stored in the Cryptographic Security Platform Vault object store or on the local file system.
7. Click **Install Certificate**.
   If an SSL certificate is to be installed for the external web server and if there are any VMs already registered with the system, Cryptographic Security Platform Vault automatically distributes the new CA certificate to those VMs on their next heartbeat and tracks the progress of the install in the **Certificate State** field. Cryptographic Security Platform Vault updates the installation status shown in the webGUI every 5 minutes. The state can be:
   - IN PROGRESS—The install is in progress. The table displays one line for each Cryptographic Security Platform Vault node showing the total number of VMs, the number of VMs that timed out and could not be reached, and the number that are waiting for the web service to restart.
     If a new VM is added to Cryptographic Security Platform Vault or a previously-inaccessible VM comes back online during this phase, Cryptographic Security Platform Vault automatically sends the appropriate CA certificate to that VM as soon as there is a successful VM heartbeat.

The length of time this phase takes depends on heartbeat duration configured for the registered VMs and whether all of those VMs are accessible. Cryptographic Security Platform Vault polls for responses once every 5 minutes. If all VMs have had a successful heartbeat during that time, Cryptographic Security Platform Vault completes this phase and changes the installation status to RESTART PENDING. If one or more VMs have not yet been contacted or if their heartbeat has failed, Cryptographic Security Platform Vault waits another 5 minutes and polls again.
This process continues until all registered VMs have either been successfully contacted or have failed 4 consecutive heartbeats. If even one VM is inaccessible, the entire installation process remains in this phase until that VM either comes back online or has failed the fourth scheduled heartbeat. In the latter case, Cryptographic Security Platform Vault considers the installation request to have timed out for that VM and it sets the installation status to TIMED OUT.
For example, If you are using the default heartbeat duration of 5 minutes, that means Cryptographic Security Platform Vault will wait at least 20 minutes until it considers the request to have timed out. If you have increased the heartbeat duration for any of the VMs registered with Cryptographic Security Platform Vault, then this step will take longer. If you have increased the heartbeat for a particular VM to 1 day, Cryptographic Security Platform Vault may have to wait up to 24 hours before the next scheduled VM heartbeat occurs and it can update the status of the installation request to RESTART PENDING. If that VM is inaccessible, Cryptographic Security Platform Vault has to wait for 4 days before it stops trying to update that VM. It is only when the last VM has been contacted or has timed out that Cryptographic Security Platform Vault concludes this phase.
Tip: If you do not want to wait for the next scheduled heartbeat on a particular VM, log into that VM as an administrator and issue the `hcl heartbeat` command on that VM. This allows Cryptographic Security Platform Vault to update the certificate information on the VM immediately.

- RESTART PENDING—The install is completed and the new certificate will be used as soon as the web service is restarted. Cryptographic Security Platform Vault has successfully sent the new CA certificate to all registered VMs, so there should be no interruption in service once the web service restarts.
- TIMED OUT—At least one of the VMs associated with the Cryptographic Security Platform Vault node could not be reached and the new CA certificate could not be sent to those VMs. When a VM times out, Cryptographic Security Platform Vault sends an alert to the Cloud Admins associated with that VM. The Cloud Admins are responsible for updating the Cryptographic Security Platform Vault CA certificate on the unreachable VMs. For more information, see Troubleshooting Certificate Issues.

8. If you install the SSL certificate for the internal web server, the web server automatically restarts.
   If you install the SSL certificate for the external web server, when the installation is complete, click **Restart Web Service** or select **Actions > Restart Web Service** and confirm the request at the prompt.
   After the web service restarts, Cryptographic Security Platform Vault will use the new certificate. Cryptographic Security Platform Vault restarts the web server which may interrupt the browser connection to the webGUI. When the restart is finished you are returned to the webGUI login page.
   Tip: If you are using Chrome, the connection status in your browser may still show as insecure. To fix this, open the Cryptographic Security Platform Vault Management webGUI login page in a new tab.
9. If you want to verify that the new certificate was properly installed, select the node and click the link next to **Internal/External web server**.
   If you already have a custom certificate installed for external web server and the Cryptographic Security Platform Vault internal web server uses a default self signed SSL certificate, Cryptographic Security Platform Vault automatically detects and provides an option to use the same custom SSL certificate for internal web server if it meets the certificate requirements of the internal web server. Select **Use external Web server SSL certificate for internal Web server** and click **Save** to install the same custom SSL certificate for the internal web server.
   If you already have a custom certificate installed for the internal web server and the Cryptographic Security Platform Vault external web server uses a default self signed SSL certificate, Cryptographic Security Platform Vault automatically detects it and provides an option to use the same custom SSL certificate for the external

web server if it meets the certificate requirements of the external web server. Select **Use internal Web server SSL certificate for external Web server** and click **Save** to install the same custom SSL certificate for internal web server. When the installation is complete, click **Restart Web Service** or select **Actions > Restart Web Service**, then confirm the request at the prompt. After the web service restarts, Cryptographic Security Platform Vault will use the custom SSL certificate for external web server.
You can also use the `openssl verify` command to ensure that you are using the correct server certificate and CA certificate combination:

```
$ openssl verify -verbose -CAfile cacert.pem server.crt

server.crt: OK
```

CSP Vault Certificate Expiration Notification

Cryptographic Security Platform Vault checks internal and external web server certificates for expiration starting 21 days before the expiration date. The alerts are sent once per day until the certificate is replaced.

- If email notification is enabled, you will receive alert notifications by email.
- In the audit log, you will see alerts for the following:
    - 249 - External web server certificate has expired.
- 250 - External web server certificate will expire within x amount of time in days and hours.
- 467 - Internal web server certificate has expired.
- 468 - Internal web server certificate will expire within x amount of time in days and hours.

Installing a New Self-Signed Certificate for a Node

Use this procedure to replace the current Cryptographic Security Platform Vault certificate on configured on an internal or external web server with a new self-signed certificate generated by the certificate authority that is included with Cryptographic Security Platform Vault.

Note:

- This procedure is for an individual node only.
- If you want to install an externally-signed SSL certificate from a Base64-encoded pem format file, see Installing External Certificates for Internal and External Webservers.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Servers** tab and select a Cryptographic Security Platform Vault node.
   Note: You can use a different certificate on each Cryptographic Security Platform Vault node. In this case, however, Entrust recommends that all of the certificates be signed by the same Certificate Authority.
5. Select **Actions > Use Self-Signed Certificate**.
6. Select the web server on which the self-signed certificate is to be installed.
7. Click **Proceed** at the prompt.
   If you select the external web server, CSP Vault restarts the web server. This may interrupt the browser connection to the webGUI. When the restart is finished, you are returned to the webGUI login page.
   Tip: If you are using IE, you may receive an alert stating that revocation information for the certificate is not available. Click **Yes** to acknowledge the alert and restart the web service. If you are using Chrome and you

receive a series of connection errors when the web service restarts, open the webGUI login page in a new tab.
8. If you want to verify that the new certificate was properly installed, select the node and click the link next to **Internal/External web server**.

Downloading a CSP Vault CA Certificate

You may need to download the CA certificate that can verify Cryptographic Security Platform Vault's SSL certificate and upload it to a VM if that VM was inaccessible when the Cryptographic Security Platform Vault SSL certificate was updated.

Warning: Do not rename the downloaded certificate. The name of the certificate has additional information and a renamed certificate will fail.

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
2. Select **? > Download CA Certificate**.

The CSP Vault downloads a `pem` file to your browser's default download location.

Troubleshooting Certificate Issues

When you install a new, externally-signed SSL certificate on Cryptographic Security Platform Vault, Cryptographic Security Platform Vault automatically updates the CA certificate on all registered VMs at their next heartbeat.

If any of the VMs are unreachable for 4 consecutive heartbeats, Cryptographic Security Platform Vault considers the update request to have timed out for those VMs. It sends one alert for each inaccessible VM to the Cloud Admins associated with that VM and then continues with the SSL certificate installation process.

The next time one of the inaccessible VMs boots, it may be unable to retrieve the proper keys from Cryptographic Security Platform Vault because the old CA certificate the VM is using cannot verify the new Cryptographic Security Platform Vault SSL certificate. The VM will then reject any communication from Cryptographic Security Platform Vault until it has the correct CA certificate installed and can once again verify Cryptographic Security Platform Vault's identity.

If there are encrypted data drives on the VM, Cryptographic Security Platform Vault will not attach those drives when the VM reboots. If the boot partition is encrypted on the VM, the VM will fail to boot. At this point you need to manually update the CA certificate on the VM in order to restore the communication between the VM and Cryptographic Security Platform Vault.

For more information, see:

- Manually Updating the CA Certificate on a Data Encrypted VM. After you update the CA certificate, the VM can retrieve the keys from Cryptographic Security Platform Vault and the encrypted drives will be automatically reattached.
- Manually Updating the CA Certificate on a Windows Boot Drive Encrypted VM.
- Manually Updating the CA Certificate on a Linux Root Drive Encrypted VM.

Manually Updating the CA Certificate on a Linux Root Drive Encrypted VM

When you install a new SSL certificate on Cryptographic Security Platform Vault, Cryptographic Security Platform Vault automatically updates the associated CA certificate on all registered VMs. If a Linux root-drive-encrypted VM was inaccessible during this process, that VM may not be able to boot because the

CA certificate the VM is using can no longer verify the Cryptographic Security Platform Vault SSL certificate. This means that the VM cannot retrieve the proper keys from Cryptographic Security Platform Vault because it cannot verify the communication coming from Cryptographic Security Platform Vault.

To fix this issue you need to manually update the CA certificate on the VM so that it can verify the SSL certificate Cryptographic Security Platform Vault is currently using. This allows the VM to verify Cryptographic Security Platform Vault's identity and to retrieve the appropriate keys.

Important: Manually updating the certificate requires `ssh` access to the VM. If you did not enable the Entrust Debug Console when you ran the `htroot encrypt` command on the root drive, you need to contact Entrust Support at hytrust.support@entrust.com.

The following procedure is for Linux VMs with an encrypted root drive. For other types of VMs, see Manually Updating the CA Certificate on a Windows Boot Drive Encrypted VM or Manually Updating the CA Certificate on a Data Encrypted VM.

Procedure

1. If you need a copy of the CA certificate that can verify the SSL certificate that Cryptographic Security Platform Vault is currently using:
   a. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
   b. Select **? > Download CA Certificate**.
      The Cryptographic Security Platform Vault downloads a `pem` file to your browser's default download location.

   Note: If you are using an externally signed SSL certificate for Cryptographic Security Platform Vault, make sure that you use the CA certificate you download from Cryptographic Security Platform Vault Management webGUI on all registered VMs. Do *not* use the CA certificate that you received from the external certificate authority.
2. Download the Bootloader SSH key for the VM so that you can open an SSH session and copy the new certificate file to the Bootloader:
   a. Log into the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
   b. Navigate to the **Workloads > VMs** tab and select the VM whose CA certificate you want to update.
   c. Select **Actions > Download Bootloader SSH Key**. The Cryptographic Security Platform Vault for VM Encryption downloads the SSH key to file called `server-name.key` in your browser's default download location. For example, if the server name is rhelsvr74, the SSH key file would be called `rhelsvr74.key` .
3. Open an `ssh` session and access the Entrust Debug Console on the root drive encrypted VM by entering the command `ssh -i server-name.key root@vm_name` , where `server-name.key` is the name of the SSH key file and `vm_name` is the IP address or hostname. For example:

```
# ssh -i ~/Downloads/rhelsvr74.key root@192.168.140.133
Warning: Permanently added '192.168.140.133' (RSA) to the list of known hosts.
BusyBox v1.20.2 (Ubuntu 1:1.20.0-8.1ubuntu1) built-in shell (ash)
Enter 'help' for a list of built-in commands.

HyTrust Debug Console

1. Show HT encryption log file
2. Authenticate
3. Show Network info
4. Restart Network
5. Advanced access
```

6. logout

Action:

4. Select `Advanced access`. The Entrust Policy Agent displays a secure shell prompt (sh). For example:
   Action: 5
   sh-10.5.3#
5. Open a second `ssh` session and copy the CA certificate file to the VM by entering the command `scp -i server-name.key cacert.pem root@vm_name:cacert.pem`, where `server-name.key` is the name of the SSH key file, `cacert.pem` is the fully qualified path to the pem file, and `vm_name` is the IP address or hostname. For example:
   $ scp -i ~/Downloads/rhelsvr74.key ~/Downloads/180412071755_cacert.pem root@192.168.140.133:180412071755_cacert.pem
6. Return to the Entrust Debug Console on the encrypted VM and update the certificate by entering the command `hcl update_ca -f cacert.pem`, where `cacert.pem` is the fully qualified path to the pem file. For example:
   sh-10.5.3# hcl update_ca -f ./180412071755_cacert.pem

   Updating using cert file at: ./180412071755_cacert.pem
   Updated CA certificate
7. Enter the command `hcl heartbeat` to prompt the VM to contact Cryptographic Security Platform Vault. This updates the status information for the VM.
8. Enter the command `hcl status` to confirm that the last heartbeat between the VM and Cryptographic Security Platform Vault was successful. For example:
   sh-10.5.3# hcl heartbeat
   sh-10.5.3# hcl status

   Summary

   KeyControl: 10.238.65.65:443
   KeyControl list: 10.238.65.65:443 10.238.65.66:443
   KeyControl Mapping: kc41-nodes
   Status: Reauth needed (Virtual Machine not authenticated)
   Last heartbeat: Tue Oct 24 22:19:32 2017 (failed)
   AES_NI: enabled
   Certificate Expiration: Sep 11 22:16:13 2020 GMT
9. If the `hcl status` command says that the VM needs to be re-authenticated, enter the command `hcl auth -a [-u user [-s password]]`, where:
   - `-u` is a Cryptographic Security Platform Vault user account name with Cloud Admin privileges.
   - `-p` is the password for the Cloud Admin account.

   If you do not provide a user name and password, you will be prompted for one. For example:
   sh-10.5.3# hcl auth -a
   Please provide the KeyControl login details
   username: secroot
   password:
   Completing authentication on KeyControl node

   Authentication complete, machine ready to use

10. Enter the command `hcl heartbeat` to prompt the VM to contact Cryptographic Security Platform Vault. This updates the status information for the VM.
11. If the heartbeat is successful, enter the command `exit` to leave the secure shell and select `logout` from the Entrust Debug Console main menu. The VM should automatically continue booting from the encrypted root drive.

Manually Updating the CA Certificate on a Data Encrypted VM

When you install a new SSL certificate on Cryptographic Security Platform Vault, Cryptographic Security Platform Vault automatically updates the associated CA certificate on all registered VMs. If a data-drive encrypted VM was inaccessible during this process, the encrypted drives may become inaccessible because the CA certificate the VM is using can no longer verify the Cryptographic Security Platform Vault SSL certificate. This means that the VM cannot retrieve the proper keys from Cryptographic Security Platform Vault because it cannot verify the communication coming from Cryptographic Security Platform Vault.

To fix this issue you need to manually update the CA certificate on the VM so that it can verify the SSL certificate Cryptographic Security Platform Vault is currently using. This allows the VM to verify Cryptographic Security Platform Vault's identity and to retrieve the appropriate keys.

The following procedure is for VMs with encrypted data drives only. For other types of VMs, see Manually Updating the CA Certificate on a Windows Boot Drive Encrypted VM or Manually Updating the CA Certificate on a Linux Root Drive Encrypted VM.

Procedure

1. If you need a copy of the CA certificate that can verify the SSL certificate that Cryptographic Security Platform Vault is currently using:
   a. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
   b. Select **? > Download CA Certificate**.
      The Cryptographic Security Platform Vault downloads a `pem` file to your browser's default download location.

   Note: If you are using an externally signed SSL certificate for Cryptographic Security Platform Vault, make sure that you use the CA certificate you download from the Cryptographic Security Platform Vault Management webGUI on all registered VMs. Do *not* use the CA certificate that you received from the external certificate authority.
2. For Linux, log into the VM as `root`. For Windows, log in as a System Administrator and open a Command Prompt or start Windows PowerShell.
3. Copy the Cryptographic Security Platform Vault for VM Encryption CA certificate `pem` file to the VM.
4. Enter the command `hcl update_ca -f /path/to/cert.pem`, where `/path/to/cert.pem` is the path to the CA certificate file.
   ```
   # hcl update_ca -f /etc/ssl/certs/171012172410_cacert.pem

   Updating using cert file at: 171012172410_cacert.pem
   Updated CA certificate
   ```
5. Enter the command `hcl heartbeat` to prompt the VM to contact Cryptographic Security Platform Vault. This updates the status information for the VM.
6. Enter the command `hcl status` to confirm that the last heartbeat between the VM and Cryptographic Security Platform Vault was successful.

Manually Updating the CA Certificate on a Windows Boot Drive Encrypted VM

When you install a new SSL certificate on Cryptographic Security Platform Vault, Cryptographic Security Platform Vault automatically updates the associated CA certificate on all registered VMs. If a Windows boot-drive-encrypted VM was inaccessible during this process, that VM may not be able to boot because the CA certificate the VM is using can no longer verify the Cryptographic Security Platform Vault SSL certificate. This means that the VM cannot retrieve the proper keys from Cryptographic Security Platform Vault because it cannot verify the communication coming from Cryptographic Security Platform Vault.

To fix this issue you need to manually update the CA certificate on the VM so that it can verify the SSL certificate Cryptographic Security Platform Vault is currently using. This allows the VM to verify Cryptographic Security Platform Vault's identity and to retrieve the appropriate keys.

The following procedure is for Windows VMs with an encrypted boot drive. For other types of VMs, see Manually Updating the CA Certificate on a Linux Root Drive Encrypted VM or Manually Updating the CA Certificate on a Data Encrypted VM.

Procedure

1. If you need a copy of the CA certificate that can verify the SSL certificate that Cryptographic Security Platform Vault is currently using:
   a. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
   b. Select **? > Download CA Certificate**.
      The Cryptographic Security Platform Vault downloads a `pem` file to your browser's default download location.

   Note: If you are using an externally signed SSL certificate for Cryptographic Security Platform Vault, make sure that you use the CA certificate you download from the Cryptographic Security Platform Vault Management webGUI on all registered VMs. Do *not* use the CA certificate that you received from the external certificate authority.
2. If needed, reboot the VM and wait for the Console menu to appear.
   If you are unable to view the console directly, for example in environments such as Amazon Web Services (AWS), you can access the console using an SSH client. This requires the `id_rsa` key file generated during the Policy Agent installation. Copy the `id_rsa` file to the server an then reboot.

   Tip: If you need another copy of the `id_rsa` key file, you can download it from the Cryptographic Security Platform Vault webGUI by selecting the VM on the **Cloud > VMs** tab and then selecting **Actions > Download Bootloader SSH Key**.
3. From the Console menu, select **Drop to shell**.
4. Copy the Cryptographic Security Platform Vault for VM Encryption certificate `pem` file to the VM.
5. Enter the command `hcl update_ca -f /path/to/cert.pem`, where `/path/to/cert.pem` is the path to the certificate file.
   ```
   # hcl update_ca -f /etc/ssl/certs/171012172410_cacert.pem

   Updating using cert file at: 171012172410_cacert.pem
   Updated CA certificate
   ```
6. After the certificate is successfully updated, enter the command `touch /opt/hcs/etc/updatecert` to tell the hcl service that the certificate has changed. The hcl service then syncs the change from the Bootloader back to the client installation directory.
   ```
   # touch /opt/hcs/etc/updatecert
   ```
7. Enter the command `exit` to leave the secure shell.

8. Select `Boot Windows with encryption key`. Cryptographic Security Platform Vault reboots the VM using the updated Cryptographic Security Platform Vault certificate.
9. If the VM reboots but displays an error that it needs to be authenticated, select **Reauthenticate** from the Console menu.
10. To verify that the VM is connected to Cryptographic Security Platform Vault:
    a. Open a Command Prompt on the VM.
    b. Enter `hcl heartbeat` to force the VM to communicate with Cryptographic Security Platform Vault and update the connection status.
    c. Enter `hcl status` to verify the connection status.

```
C:\users\administrator> hcl heartbeat
C:\users\administrator> hcl status

Summary
--------------------------------------------------------------------------------
KeyControl: 10.238.65.65:443
KeyControl list: 10.238.65.65:443 10.238.65.66:443
KeyControl Mapping: kc41-nodes
Status: Connected
Last heartbeat: Tue Oct 24 22:30:32 2017 (successful)
AES_NI: enabled
Certificate Expiration: Sep 11 22:16:13 2020 GMT
```

Admin Keys

All Cryptographic Security Platform Vault data (policy information, encryption keys, user account information, and so on) are held in an encrypted object store that is shared across all Cryptographic Security Platform Vault nodes in the cluster.

The object store is ultimately protected (through multiple layers of key wrappings) by an Admin Key that Cryptographic Security Platform Vault generates and maintains. This key is required if you ever need to restore Cryptographic Security Platform Vault from a backup or you need to change the hardware configuration of a Cryptographic Security Platform Vault node. The Admin Key is a 4096 bit RSA asymmetric key pair.

When you install the first Cryptographic Security Platform Vault node in your system, Cryptographic Security Platform Vault generates an Admin Key as soon as you log into the Cryptographic Security Platform Vault Management webGUI for the first time. The initial key has a single part and is assigned to the default `secroot` user account. As you add additional Security Administrator accounts to the system, Cryptographic Security Platform Vault shifts to an "n of m" Admin Key backup model, where "m" is the number of user accounts with Security Admin privileges and "n" is a user-defined value that states how many key parts must be uploaded before Cryptographic Security Platform Vault considers the Admin Key to be valid.

For example, if you have five Security Admins and you set n to 3, then at least three of the Security Admins will need to upload their Admin Key parts in order to restore Cryptographic Security Platform Vault from a backup. If you set n to 1, then any one of the five Security Admins can restore Cryptographic Security Platform Vault without consulting with any of the other Security Admins.

While you can regenerate Admin Key parts at any time, in order to restore Cryptographic Security Platform Vault from a backup image you must have the required number of Admin Key parts that were valid when the backup was created. You cannot regenerate the Admin Key parts and then immediately use those new key parts to restore Cryptographic Security Platform Vault from a previously-created back up.

The Admin Key is assigned a generation count that is incremented each time a new Admin Key is generated. This generation count allows you to identify which Admin Key parts go together. The email that each Security Admin receives when a new Admin Key is generated contains the generation count. For example:

> This current Key Part supersedes any you may have previously received from this cluster. The Key Part is associated by a "generation count" with its relevant backups. The generation count for this key is:
>
> 8

The generation count is also included in the Admin Key Part filename, which is attached to the email. The attachment name is *username_kc-ip-addr*.key.gen# , where `username` is the Security Admin's Cryptographic Security Platform Vault account name, `kc-ip-addr` is the Cryptographic Security Platform Vault IP address from which the Admin Key was generated, and `#` is the generation count. For example, secroot_10.238.66.235.key.gen8 . This same naming convention is used if a Security Admin downloads their Admin Key Part from the Cryptographic Security Platform Vault Management webGUI.

If you want to restore Cryptographic Security Platform Vault from a backup created when the Admin Key shown above was valid, you must make sure that all the Admin Key Parts you upload have generation count = 8.

External Admin Key Storage

You can store the entire Admin Key on an external key server (EKS), such as a Hardware Security Module (HSM). If you configure an EKS, you can restore the Admin Key using the entire key from the EKS.

This has the advantage that Security Admins do not need to worry about which Admin Key parts are required for which backup image. Cryptographic Security Platform Vault automatically fetches the appropriate key from the EKS and no manual synchronization is needed.

If you configure one or more EKS, Cryptographic Security Platform Vault stores the Admin Key on each EKS automatically and you can restore the Admin Key from any configured EKS. If an EKS is configured, administrators do not define the storage location and Admin Key parts are no longer available for download.

For details about using an EKS, see Hardware Security Modules with CSP Vault.

- Downloading Your Admin Key Part
- Generating the Admin Key
- Verifying the Admin Key

Downloading Your Admin Key Part

Every user account with Security Admin privileges receives an encrypted Admin Key part.
Certain Cryptographic Security Platform Vault functions, such as restoring the system from a backup, require that a certain number of parts be uploaded to Cryptographic Security Platform Vault within a certain amount of time. Once Cryptographic Security Platform Vault receives the correct number of parts, it can validate the Admin Key and perform the requested procedure. Once you download your key part, make sure you store it securely and that you can find it when needed.

> Note: If an external key server (EKS) is used to store Admin Keys, administrators do not define the storage location and Admin Key parts are no longer available for download. For more information, see Admin Keys.

Important: You also need to keep previous Admin Key parts and know when each part was created. If you need to restore a system from a previous backup, you must have the key parts that were valid when that backup was created. If the Admin keys have been regenerated, you cannot download the current Admin Key parts and use those to restore a previous version of Cryptographic Security Platform Vault.

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **Account Settings** section, click **Download Key**. Cryptographic Security Platform Vault downloads a file to your browser's default download location called *username_kc-ip-addr*.key.gen# , where `username` is the currently logged in Cryptographic Security Platform Vault account name, `kc-ip-addr` is the Cryptographic Security Platform Vault IP address into which you are currently logged in, and `#` is the generation count. For example, secroot_10.238.66.235.key.gen8 .
5. If you want to remove the Admin Key part from the Cryptographic Security Platform Vault encrypted object store, click **Clear Key**. If you later attempt to download the key part after clearing it, you will get an error stating that the key part does not exist. You will need to regenerate the key as described in Generating the Admin Key.

Generating the Admin Key

When Cryptographic Security Platform Vault generates an Admin Key, it cryptographically divides the key into parts and sends one part to each Cryptographic Security Platform Vault user account with Security Admin privileges. In addition, if you have specified an EKS (external key server), Cryptographic Security Platform Vault stores a copy of the entire Admin Key on the EKS.

Cryptographic Security Platform Vault automatically generates new Admin Key:

- During installation of the first Cryptographic Security Platform Vault node. In this case, the **secroot** user account gets an Admin Key with a single part.
- When a Security Admin user account is added or deleted. In this case, a new Admin Key is divided into a new number of parts, "m", and sent to all current Security Admins.
  Note: The value of "n" is not changed. If you add three Security Admins immediately after the initial installation, the Admin Key will be divided into four parts, but only one part will be required when restoring the system. The way you set the required number of parts is described below.
- When you first configure Cryptographic Security Platform Vault to use an EKS.
- When you explicitly generate new a new Admin Key, as described below. In this case, the number of Admin Key parts is not changed.

Note: Whenever the admin key is regenerated, Cryptographic Security Platform Vault forces you to download the admin key.

Note: If an external key server (EKS) is used to store Admin Keys, administrators do not define the storage location and Admin Key parts are no longer available for download. For more information, see Admin Keys.

Before You Begin

If you have configured Cryptographic Security Platform Vault to store the Admin Key in an external KMIP server or HSM (hardware security module), make sure that KMIP server or HSM is available before you generate a new Admin Key. If Cryptographic Security Platform Vault cannot store the Admin Key on the external device, the generate request will fail.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges. In the top right, click the Switch to **Appliance Management** link.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Admin Key Parts**.
4. Verify the following options:

Option	Description
Minimum Key Parts	The minimum number of parts needed when you want to restore Cryptographic Security Platform Vault from a back up ("n") and you are not retrieving the key from an EKS.
Email Private Key on Generate	If Enabled, when you generate a new Admin Key, Cryptographic Security Platform Vault automatically sends each Security Admin their key part as an email attachment. The attachment name is *username_kc-ip-addr*.key.gen# , where `username` is the Security Admin's Cryptographic Security Platform Vault account name, `kc-ip-addr` is the Cryptographic Security Platform Vault IP address into which you are currently logged in, and `#` is the generation count. For example, secroot_10.238.66.235.key.gen8 . If Disabled, when you generate a new Admin Key, Cryptographic Security Platform Vault sends each Security Admin an alert stating that the admin key has been changed and prompting them to download their key part.

5. Click **Generate New Key**. Cryptographic Security Platform Vault increases the generation count by one and creates a new key part for each Security Admin in the system. If you have configured an EKS, Cryptographic Security Platform Vault also saves the Admin key to the EKS.
   Based on the setting of the **Email Private Key on Generate** option, Cryptographic Security Platform Vault also sends each Security Admin in the system an email with their key part or an alert stating that there is a new key part ready for download.
   Tip: If you intend to back up Cryptographic Security Platform Vault in the immediate future, we recommend that you notify your Security Admins that the new Admin Key part they just received is going to be tied to a backup image and they should download it to a secure location immediately. You cannot restore Cryptographic Security Platform Vault from a backup image unless you have the Admin Key parts that were valid when the back up was created, and you cannot download previous Admin Key parts from Cryptographic Security Platform Vault.
6. Click **Close**.

Verifying the Admin Key

Every 90 days, Cryptographic Security Platform Vault checks to ensure that the admin key you downloaded is still accessible. The Recovery Verification Required dialog box is displayed to prompt you to enter the admin key or regenerate it. If you close the window without verifying or regenerating the key, the dialog will be shown again the next time you log in.

Important: If the Admin Key is stored in EKS (HSM) then Cryptographic Security Platform Vault does not perform this check.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the General Settings section, click **Admin Key Parts**.
5. In the Admin Key Parts window, click **Verify Current Key**.

6. In the Recovery Verification Required page, click **Browse** to select your current Admin Key, and then click **Verify**.
   Note: If you do not have the Admin key, you can generate another one. See Generating the Admin Key.

If successful, the page will display the following message: Admin key is successfully verified. This dialog will then be repeated after another 90 days.

KMIP Server Configuration

KMIP (Key Management Interoperability Protocol) enables the secure creation and storage of keys and other security objects on a key management server.

> Note: You can also use an HSM (Hardware Security Module) to store the Admin Key. For details, see Hardware Security Modules with CSP Vault.

In addition, Cryptographic Security Platform Vault includes a fully functional KMIP server that you can use to serve requests from external KMIP clients. The Cryptographic Security Platform Vault KMIP server supports all KMIP versions up to 3.0. The KMIP server is required if you want to use Cryptographic Security Platform Vault with VMs and VSAN datastores encrypted by vSphere. For details, see CSP Vault with VSAN and VMware vSphere VM Encryption.

If you have linked Cryptographic Security Platform Vault with a Entrust CloudControl server version 5.1 or later, the Inventory feature in CloudControl provides an identifier that links each VM with its associated KMIP objects.

For details on KMIP, see the KMIP Technical Committee home page. For troubleshooting and error messages, see KMIP Errors and Troubleshooting.

- KEKs with KMIP
- Configuring a New KMIP Server (orig)
- Creating a Certificate Signing Request for KMIP Server
- Installing a Custom Certificate

KEKs with KMIP

A Key Encryption Key (KEK) provides an extra layer of security by encrypting all individual KMIP objects in a KMIP Vault. The KEK is created in your HSM for each KMIP vault and wraps all KMIP objects in the vault. Both the KEK and KMIP Vault must be available before a KMIP client can access the KMIP Vault.

To protect the KEK, the Cryptographic Security Platform Vault for KMIP requires that the KEK be stored in the hardware security module (HSM) associated with this Cryptographic Security Platform Vault for KMIP cluster. If the HSM is not available, then the KMIP objects in the KMIP Vault protected by the KEK cannot be accessed. If you decide to associate a KEK with KMIP, it is imperative that the HSM be available to the Cryptographic Security Platform Vault for KMIP at all times.

The Cryptographic Security Platform Vault for KMIP uses the AES-GCM algorithm for encrypting and decrypting KMIP Vaults. Each KMIP object will be encrypted with a unique key derived from the KEK. The KEK can be cached in Cryptographic Security Platform Vault kernel memory by specifying the KEK cache timeout.

The KEK also provides a way to control the accessibility of all KMIP objects with a single command. If the KEK is revoked on the HSM, then all KMIP objects become inaccessible after the specified KEK cache timeout.

For information on configuring an HSM, see Hardware Security Modules with CSP Vault.

Considerations

- The HSM must be available before you can enable KEK for KMIP objects.

- After you enable KEK for KMIP objects, the HSM must be available anytime a KMIP object is accessed by a KMIP client.
- KMIP KEK can be enabled or disabled at any time.
    - When KMIP KEK is disabled, all KMIP objects will be decrypted. Key material will continue to be accessible.
    - If KMIP KEK is enabled and the HSM is disabled or unavailable, key material will not be accessible, but the UUID entries continue to be visible in WebGUI and object state can be changed.
- KMIP objects will remain accessible when encryption or decryption is in progress.

Configuring a New KMIP Server (orig)

Any KMIP client can connect to the Cryptographic Security Platform Vault KMIP server and perform all standard KMIP operations with the following restrictions:

- The Cryptographic Security Platform Vault for KMIP KMIP server supports KMIP versions 1.0, 1.1,1.2,1.3,1.4, 2.0, 2.1, and 3.0. The KMIP server protocol version is configured automatically and set between 1.0 to 3.0, as requested by the client.
- The object count (for example, keys) has a limit of 1 million KMIP objects per KeyControl Vault cluster. This limit includes all of the Cryptographic Security Platform Vault for KMIP instances in that cluster. If you exceed this limit, the KMIP server will still create and maintain the objects but the Cryptographic Security Platform Vault for KMIP webGUI may not display those objects correctly.

Important: Cryptographic Security Platform Vault includes a component for creating a Root Certificate Authority (CA) that can generate digital certificates. When the first Cryptographic Security Platform Vault node is installed, it creates a Public CA that it also stores in the Cryptographic Security Platform Vault object store. For more information, see CSP Vault Certificates.
By default, the KMIP server uses a default certificate signed by the CA inside Cryptographic Security Platform Vault. This can be changed by installing a custom SSL certificate for the KMIP server. To generate a custom SSL certificate, you can use a CSR created from Cryptographic Security Platform Vault for the KMIP server (see Creating a Certificate Signing Request for KMIP Server) or you can use your own CSR. If you use your own CSR, you must upload a private key for that custom certificate.

For details about the standard KMIP operations and configuration settings, see the Oasis KMIP Technical Committee page or the KMIP wikipedia page.

When a KMIP client connects to the Cryptographic Security Platform Vault for KMIP KMIP server, the client must use the certificates associated with a KMIP server user account. The KMIP server does not support username/password login credentials. For details about downloading a user account certificate bundle, see Creating a KMIP Client Certificate.

Note:

- If you are configuring a KMIP server to use with VMware vSphere encryption or VSAN encryption, see the *Entrust KeyControl with VMware VSAN and vSphere VM Encryption* guide.
- If you are using a KMIP server with KEK enabled, please ensure that the KEK cache timeout is enabled. Set the value to anything other than 0.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI.
2. Select the Settings icon at the top right of the vault page.
3. On the KMIP Vault Settings page, complete the following:

Option	Description
State	If set to Enabled, clients can connect to this KMIP server.
Port	The server port number. The default port is 5696.
Verify	If set to Yes, the KMIP client identity is verified before the server handles its request. We recommend that you do not turn this option off.
Log Level	The lowest level of log messages that will be saved in the audit log. The options are: • **All**—Logs all requests to the KMIP server and responses from the KMIP server. • **Create-Modify**—Logs object creation, object modify requests, and object delete requests and responses. This is the default. • **Create-Get**—Logs object creation messages, object fetch requests, and object fetch responses. • **Create**—Logs object creation request and response messages. • **Get**—Logs object fetch and object locate requests and responses. • **Off**—No log messages are stored in the audit log.
TLS	Choose which version of TLS you want to support. If set to TLS 1.3, all clients must connect to this KMIP server using TLS 1.3. By default, both TLS 1.2 and TLS 1.3 are supported. Note: The TLS setting applies to the KMIP server only and affects the entire cluster.
Timeout	The length of time, in minutes, after which a client request will time out. If No is selected, client requests never time out. This is the default. To change this option, select Yesand select the number of minutes before the requests times out. This can be from 1 to 60 minutes.

Option	Description
KMIP Locate Operation: Maximum Items Default	Choose the maximum number of items to be returned from the KMIP server `Locate` operation. Note: The KMIP client allows you to set an offset items value (the record number the return starts with) and a maximum items value (how many items are returned) when you run the KMIP locate operation. The maximum number of items depends on both the choice that you set in the webGUI and the value that you set in the KMIP Client. For example: • If you choose the default value in the webGUI, and you DO set a max value in the KMIP Client, it returns up to 1000 UUIDs. • If you choose the default value in the webGUI, and you do NOT set a max value in the KMIP Client, it returns up to 100 UUIDs. • If you choose the value set to the maximum items value from the KMIP client in the webGUI, and you DO set a max value, it returns the maximum value of UUIDs that is set in the KMIP Client. • If you choose the value set to the maximum items value from the KMIP client in the webGUI, and you do NOT set max value, it returns all the UUIDs found in the locate operation. For more information on the KMIP `Locate` command, see https://docs.oasis-open.org/kmip/kmip-spec/.
SSL/TSL Ciphers	Enter the SSL ciphers in a comma-separated list that you want the KMIP server to use. Note: The following ciphers are not supported: DHE-DSS-AES128-256 and DHE-DSS-AES128-SHA256.

Option	Description
Certificate Types	This can be one of the following: If set to Default, the KMIP server uses a default certificate. If set to Custom, you must have a custom SSL certificate generated from Cryptographic Security Platform Vault or from your own CSR, and then provide the following: • SSL Certificate—Upload the SSL certificate file in Base64-encoded pem format. It should be able to function as a server certificate. • CA Certificate—Upload the certificate for the CA that signed the custom SSL certificate in Base64-encoded pem format. If you want to use the CA certificate to verify the KMIP client certificate select **Yes**. The default is **No**. **Important:** If you select Yes, you will need to upload a KMIP client certificate for every Cryptographic Security Platform Vault for KMIP. • Private Key—Optionally upload the private key file in Base64-encoded pem format. This is required if you used your own CSR and not the CSR generated on the KMIP page. • Password—Optionally enter the password for the custom certificate.

4. Click **Apply** and confirm your changes when prompted.

Creating a Certificate Signing Request for KMIP Server

A certificate signing request (CSR) tells an external Certificate Authority (CA) that you want an SSL certificate generated and signed by that CA. The SSL certificate can then be uploaded to Cryptographic Security Platform Vault and used in place of the default self-signed certificate.

When you use Cryptographic Security Platform Vault to create the CSR, Cryptographic Security Platform Vault creates a key pair and uses that key pair in conjunction with the information you specify to create the CSR. Cryptographic Security Platform Vault then encrypts the key pair and stores it for later use.

You can use the resulting CSR to generate an SSL certificate from the external CA you want to use. After you receive the SSL certificate from that external CA, you can upload it to Cryptographic Security Platform Vault. Because the key pair already exists on the system, you do not need to upload anything else.

If you create the CSR outside of Cryptographic Security Platform Vault, you need to upload both the SSL certificate and the matching private key file when you install the certificate on Cryptographic Security Platform Vault.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. Click the **Settings** icon.
3. On the KMIP Vault Settings page, select **Actions > Generate CSR**.
4. In the Generate Certificate Signing Request dialog box, specify the options you want to use.

Field	Description
Common Name	The name to associate with this request.
Locality	The locale to associate with this request.
State	The state to associate with this request.
Subject Alternative Names	The host names that will be protected by this certificate.
Key Size	Select the key size that you want to use. The default is 4096 bytes.
Country	The country to associate with this request. The default is US.
Organization	The organization to associate with this request.
Organization Unit	The organizational unit associate with this request.

5. Click **Generate**.
6. When you receive the message that Cryptographic Security Platform Vault has created the CSR, click **Download** to save a copy of the CSR to your browser's default download directory.
7. Use the CSR to request an SSL certificate from the external Certificate Authority you want to use. How you do this depends on the CA that you are using.

What to Do Next

After you receive the SSL certificate from the external CA, install it on Cryptographic Security Platform Vault. For more information, see Installing a Custom Certificate.

Installing a Custom Certificate

Before You Begin

Installing a custom certificate requires that you have at least your SSL certificate and CA certificate.

Note:

- When you use Cryptographic Security Platform Vault to create a CSR, and then use that CSR to generate an SSL certificate from the external CA you want to use, you will need to upload the CA certificate and the SSL certificate.
- If you create the CSR outside of Cryptographic Security Platform Vault, you will need to upload the CA certificate, the SSL certificate, and the matching private key file for the SSL certificate. If the private key file is encrypted, you will also need to enter the password used to decrypt the private key.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. Click **Settings**.
3. Under KMIP Vault Settings section, select **Enabled** to make changes.
4. In the Certificate Types field, select the **Custom** radio button.

5. In the SSL Certificate field, click **Browse**, select your SSL certificate, and then click **Open**.
6. In the CA Certificate field, click **Browse**, select your CA certificate, and then click **Open**.
7. Choose whether or not to use this CA certificate to verify your KMIP client certificate.
   Note: If you select **Yes**, then all existing KMIP client certificates in the individual KMIP vaults will no longer work. Vault Administrators will be required to upload a new KMIP client certificate, signed by this CA certificate, within their respective KMIP vaults. Until the Vault Administrators upload the new certificate, their vaults will not be able to communicate with the Cryptographic Security Platform Vault KMIP server.
   Important: If you change this value to **Yes**, the only way to set this back to **No** is to reset the KMIP server.
8. In the Private Key field, click **Browse**, select your private key, and then click **Open**.
   Note: This is only required if you created your SSL certificate outside of Cryptographic Security Platform Vault.
9. In the Password field, enter the password to decrypt your private key.
   Note: This is only required if you created your SSL certificate outside of Cryptographic Security Platform Vault, and the private key is encrypted.
10. Click **Apply** to overwrite the KMIP Server settings.

Hardware Security Modules with CSP Vault

A hardware security module (HSM) is a physical device that stores, protects, and manages cryptographic material. An HSM is often used to do cryptographic processing as well, including the generation of secure cryptographic keys. It is used in a client-server environment, which means that the server and the client each need to be prepared in advance. Using an HSM allows you to protect cryptographic keys and data, such as the Admin key and information you have stored in your vaults.

If you use multiple HSM servers and/or Cryptographic Security Platform Vault nodes to provide high availability of your services, you must ensure that all HSM servers are accessible from each Cryptographic Security Platform Vault instance.

When you configure an HSM, it does not automatically immediately start to protect data. You must regenerate the Admin key if you wish to store it in the HSM, and a Vault Admin must enable HSM protection in any vault where you want the HSM to protect keys or other material. See the documentation for the particular vault type:

- Cryptographic Security Platform Vault for Cloud Keys—Managing Key Sets.
- Cryptographic Security Platform Vault for KMIP—KEK with a KMIP Vault.
- Cryptographic Security Platform Vault for PKCS#11—CSP Vault for PKCS#11
- Cryptographic Security Platform Vault for Secrets—Hardware Security Modules with CSP Vault for Secrets.
- Cryptographic Security Platform Vault for Databases—Configuring a CSP Vault Database Connector, Configuring CSP Vault for Oracle TDE, Configuring CSP Vault for MariaDB TDE, Creating a Cloud VM Set for the CSP Vault for Databases
- Cryptographic Security Platform Vault for Cryptographic APIs—Signing in to the Vault for the first time.
- Cryptographic Security Platform Vault for VM Encryption—KEKs with Cloud VM Sets, Creating a Cloud VM Set for the CSP Vault for VM Encryption.

If using an Entrust nShield HSM you can also configure it as a root of trust for the system. For more information, see Adding HSM Root-of-Trust to nShield Server .

When an HSM is used with BYOK, keys are never stored as plaintext. In-memory keys are also encrypted (wrapped), except for software-protected keys in Azure. When a software-protected key has to be uploaded to Azure, Cryptographic Security Platform Vault unwraps it before upload. For other keys, including hardware-protected keys on Azure, when Cryptographic Security Platform Vault has to upload them to the cloud, it encrypts (wraps) them in the HSM using the master key and the cloud provider's wrapping key before uploading the wrapped keys to the cloud.

Cryptographic Security Platform Vault supports the following HSMs:

- nShield HSM
- nShield as a Service (nSaaS)
- Luna HSM
- Luna Cloud HSM

Requirements and Recommendations for nShield HSM Servers

The nShield HSM client version 13.9.0 is included in Cryptographic Security Platform Vault. Only nShield HSMs compatible with the 13.9.0 client are supported. The minimum HSM firmware version for BYOK, KEK generation, and TDE is 12.70. You can also use either the on-premise nShield HSM or nShield as a Service (nSaaS).

> Note: Elliptic Curve Cryptography (ECC) was an optional feature on nShield HSMs with firmware versions before 13.5. In order to use such HSMs with the Cryptographic Security Platform Vault for Cloud Keys or the Cryptographic Security Platform Vault for Cryptographic APIs containing Elliptic Curve Keys, you must have the feature enabled. You can check the feature status using the HSM's `fet` command.

The following details apply where nShield HSMs are configured in a FIPS 140-2 Level 3 compliant Security World environment:

Security World Files—For each nShield HSM, the following files must be present and up to date in Cryptographic Security Platform Vault. These files are supplied in the world.zip file uploaded when configuring the HSM:

- `world`
- A `module_<ESN>` file for each module that Cryptographic Security Platform Vault uses
- A `cards_<IDENT>` file for each card set that is to be used
- A `card_<IDENT>_<NUMBER>` file for each card in each card set that is to be used to provide FIPS authorization

These files are not updated automatically. You must ensure that they are synchronized whenever the Security World is updated on the module. For more information, see 'Creating a Security World' in your HSM User Guide. The updated files should be in included in a world.zip archive and updated using the 'Upload Security World' action on the nShield HSM Server Settings page.

Important: The Security World must be created for nShield client software version 13.6.3 or later.

Smart cards—When using an nShield HSM with a FIPS 140-2 Level 3 Security World, a FIPS authorization token is required to authorize most operations, including the creation of keys. This is provided by an ACS or OCS card must be loaded in the HSM or presented using a remote admin client. Cards are usually configured when setting up an HSM, so Entrust recommends leaving one of the configured OCS cards in the HSM slot to satisfy this requirement.

Smart card serial numbers—nShield HSMs include a security feature that checks the serial numbers of the cards as well as checking they are part of an OCS for this HSM. This allows the admin to disable a card that is mislaid for example. In Cryptographic Security Platform Vault, you can specify whether all cards are accepted, no cards are accepted, or cards in a specific list are accepted. Card serial numbers are 16 decimal digits and, if you enable the option, Cryptographic Security Platform Vault checks that the card in use matches one of the serial numbers listed.

For additional details, see your nShield documentation https://nshielddocs.entrust.com/ or the nShield support site https://nshieldsupport.entrust.com.

Requirements and Recommendations for Luna HSM Servers

You can configure the nodes in your Cryptographic Security Platform Vault cluster to either connect to the HSM using one certificate that they all share or with individual certificates for each node. The Cryptographic

Security Platform Vault nodes can also be connected to multiple HSM servers that have been configured as an HA Group to allow for High Availability. For more information, see Configuring Cryptographic Security Platform Vault as a Luna HSM Client with a Single Cluster Certificate, Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates, and Configuring a Luna HSM HA Group.

> Note: If you have a Luna HSM server with the `ipcheck` feature enabled, you must use unique node certificates.

- The Luna client version 10.9.0 is included in Cryptographic Security Platform Vault. This version of the Luna HSM client is compatible with Luna HSMs with firmware 6.2.1 or higher.
- Bandwidth recommendation:
  - Minimum: 10 Mbps half duplex
  - Recommended: 100 Mbps full duplex
- Latency recommendation:
  - Maximum: 500 ms
  - Recommended: 0.5 ms
- TCP port 1792 is required to establish a trusted connection between Cryptographic Security Platform Vault and Luna. The other ports used are:
  - TCP port 22 for SSH (Secure Shell).
  - TCP port 1503 for Remote PED. This is the only configurable port.
  - UDP port 514 for the Syslog service.
  - UDP port 123 for NTP service.
  - UDP ports 161/162 for SNMP service.

For additional details, see your Luna HSM documentation.

- Adding a CSP Vault Node to a Cluster using an nShield HSM client
- Configuring CSP Vault as an HSM Client using an nShield HSM
- Adding HSM Root-of-Trust to nShield Server
- Running nShield HSM Info Commands in the webGUI
- Configuring an nShield HSM for High Availability
- Replacing an nShield HSM on a CSP Vault Cluster
- Configuring Allowed Smart Cards for an nShield HSM
- KeySafe5 Agent Requirements
- Enabling the KeySafe5 Agent
- Configuring CSP Vault as a Luna Cloud HSM Client
- Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate
- Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates
- Configuring a Luna HSM HA Group
- Adding a CSP Vault Node to an Existing Luna HSM Configuration
- Adding a New Luna HSM to an Existing Luna HSM Configuration
- Adding a Luna Cloud HSM to an Existing Luna HSM Configuration
- Changing the Luna Client Certificate Mode
- Locating the HSM Server Admin Key
- Resetting the HSM Server Configuration

Adding a CSP Vault Node to a Cluster using an nShield HSM client

After you have configured a single node cluster for the nShield HSM, you can quickly add a new Cryptographic Security Platform Vault node. All members of the Cryptographic Security Platform Vault cluster must be added as clients of the nShield HSM server(s).

1. Use the webGUI to join the new node to your existing cluster that is configured with nShield HSM. For complete instructions, see Joining or Re-joining a Cryptographic Security Platform Vault Cluster.
2. After the process is finished, log in to the new cluster node using the webGUI.

3. In the **System Settings** section, click **HSM Server Settings**.
4. On the **HSM Server Settings** tab, select **nShield HSM**.
   You should see the nShield HSM Server Settings page with all of the settings imported from the original cluster node.
5. Click the **Client List** tab to view the cluster nodes.
6. Copy the Cryptographic Security Platform Vault IP address and the keyhash of the node that you just added, and paste them in a text window.
7. Use the IP address and keyhash to authenticate Cryptographic Security Platform Vault on nShield. Please see your nShield documentation.
   Important: For Cryptographic Security Platform Vault clusters, you will need to authenticate the IP address and keyhash for each cluster node, and authenticate each node to each HSM.
8. Return to the nShield HSM Server Settings page for the new cluster node.
9. Click the **Locate Admin Key** button to ensure that the new node is now fully connected to nShield HSM.

Configuring CSP Vault as an HSM Client using an nShield HSM

The following procedure describes how to configure Cryptographic Security Platform Vault as an nShield HSM client. You can either use a standalone Cryptographic Security Platform Vault node or a cluster.

Before You Begin

For the nShield HSM server that you want to connect to Cryptographic Security Platform Vault, make sure you have the following information available:

- The HSM Server Name, Server IP/FQDN, ESN, Port, and Keyhash.
- The Security World Bundle file that is provided by the HSM Administrator. This must contain the following:
  - The world file.
  - The module file for each HSM server you plan to use.
  - If it is a FIPS Level 3 security world, the card files for any smartcards that will be used to provide FIPS authorization.
- Information to create a softcard consisting of a label and password.

You will also need:

- A Cryptographic Security Platform Vault account with Security Admin privileges.
- If you are using an on-premise HSM server, you must have access.

If you plan to use a FIPS 140-2 Level 3 compliant Security World environment, see Hardware Security Modules with CSP Vault for more information.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
   Note: If you are using a cluster, you only need to use the Cryptographic Security Platform Vault Management webGUI for one node.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the **HSM Server Settings** tab, select **Entrust nShield HSM**.
   The nShield HSM Server Settings window displays the information you will need to continue.
6. Click the **Copy the IP address and keyhashes to the keyboard** link and paste them in a text window.
7. Copy the Security World Bundle from nShield and place it on your local machine. It should be in the format world.zip.
8. After reading the Get Started Screen, click **Continue**.
9. On the Enrollment screen, complete the following:

Note: All information is from the nShield HSM. The Server Name is used for display purposes and the Server IP/FQDN is used for communication.

Field	Description
Server Name	Enter the FQDN of the nShield HSM.
Server IP	Enter the IP address for the nShield HSM.
Server ESN	Enter the nShield Electronic Serial Number (ESN).
Port	Enter the port used for the nShield HSM.
Keyhash	Enter the keyhash of the nShield HSM.

10. Click **Enroll and Continue**.
11. On the Security World screen, click **Browse** and locate the security world bundle that you downloaded from the nShield HSM.
12. Click **Upload and Continue**.
13. If you are using a FIPS 140-2 Level 3 Security World, on the Card List screen, select one of the following:
    - Accept all cards—Accepts all nShield Remote Administration smart cards.
    - Add Specific cards—Accepts specific nShield Remote Administration smart cards. To add a card, click **+ Add Card**, enter the card serial number and optional description, check the Enable checkbox, and click **Add**. You can add multiple cards at one time.
14. If you are using a FIPS 140-2 Level 3 Security World, on the Softcard screen, enter the Softcard Label and Softcard Password that you want to use to link to the HSM server.
    You must have entered a valid smart card or selected Accept all cards in order to create a Softcard. The Softcard Label and Softcard Password must meet the following requirements:
    Softcard Label
    - At least 8 characters
    - No more than 31 characters
    - Can include uppercase, lowercase, numbers, and special characters
    - No space or tab character

    Softcard Password
    - At least 8 characters
    - No more than 127 characters
    - At least 1 uppercase
    - At least 1 lowercase
    - At least 1 number
    - No space or tab character
15. Click **Complete Setup**.
    After the setup is complete, you will be returned to the nShield HSM Server Settings page.
    Note: If the configuration failed, then you must select **Actions > Reset HSM Configuration** before you try again.
16. Select **Actions > Test Connection** from the Basic tab to ensure that the HSM is fully connected to Cryptographic Security Platform Vault.

What to Do Next

- If you want to use nShield HSM to store your Admin Key, you will need to generate a new one.
  See Generating the Admin Key.

The new Admin Key is automatically stored in the nShield HSM. Click **Locate Admin Key** in the nShield HSM Server Settings page to view.

- If you want to use HSM Root-of-Trust, see Adding HSM Root-of-Trust to nShield Server .
- If you want to form a Cryptographic Security Platform Vault cluster using the nShield HSM, see Adding a CSP Vault Node to a Cluster using an nShield HSM client.
- If you want to use an additional nShield HSM for a high availability cluster, see Configuring an nShield HSM for High Availability.
- If you want to use KeySafe5, see Enabling the KeySafe5 Agent.

Adding HSM Root-of-Trust to nShield Server

HSM Root-of-Trust provides enhanced protection for the contents of the object store. Root-of-Trust is gained when the HSM provides the cryptographic keys necessary to unlock the object store.

If the HSM cannot be contacted when Cryptographic Security Platform Vault boots, or if the correct keys cannot be located, trust cannot be established with the HSM and Cryptographic Security Platform Vault is not allowed to begin servicing key requests.

Important: Creating an HSM Root-of-Trust is not reversible. Once the HSM Root-of-Trust is enabled, you cannot remove the HSM. Contact Entrust Support to disable it.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the nShield HSM Server Settings page, select the HSM Root-of-Trust mode that you want to use:
    - Root-of-Trust mode using HWSIG—The hardware signature is used to wrap the HSM configuration file. Unless there is a change to Cryptographic Security Platform Vault's hardware configuration, booting Cryptographic Security Platform Vault will require no user intervention before it can begin servicing requests.
      Virtual machine configuration changes may result in a need to recover the HSM configuration changes. When this happens, the normal Cryptographic Security Platform Vault Masterkey Recovery procedure is used. This requires the softcard label and password if the admin key is stored in the HSM, or the downloaded admin key if it is not stored in the HSM.
    - Root-of-Trust mode using Password—The HSM's softcard password is used to wrap the HSM configuration file. When Cryptographic Security Platform Vault boots, the WebGUI will prompt for the HSM password. Only when the password is correctly entered is Cryptographic Security Platform Vault allowed to begin booting.
      The HSM password must be entered on each node of the cluster. For instance, if the entire cluster is restarted, read-only operations will start on each node as soon as it has finished booting, but the cluster will be degraded until the password has been entered on all of the nodes in the cluster, and the nodes are back up.
6. Select the HSM Root-of-Trust Timeout value in minutes and click **Save**. The default timeout value is 0, which means the nodes will never be locked down, but will be checked at boot time.
   You can select up to 1440 minutes (1 day).
   Note: If the node is unable to connect to any HSM server, and still cannot connect after the timeout period, that Cryptographic Security Platform Vault node will be locked down and will not respond to any requests via the webGUI or API. Diagnostic logs are available from the system console using the Cryptographic Security Platform Vault System Console. After resolving the connection issue, reboot the Cryptographic Security Platform Vault node to re-enable it.
   When using the System Console to download the diagnostic logs, you will see the message “Cryptographic Security Platform Vault not initialised yet. Proceeding may potentially leave the system unusable.” This is expected, and enabling the htrestricted account will not cause a problem.

7. Click **Apply**.

Running nShield HSM Info Commands in the webGUI

You can run several Info commands against your nShield HSM directly from the webGUI.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. Select **Actions > Run Info Commands**.
6. In the Run Info Commands window, select the command that you want to run and click **Apply**.
   The standard output and error output (if applicable) are displayed.

Configuring an nShield HSM for High Availability

After you have configured Cryptographic Security Platform Vault as an nShield HSM client, you can add an additional nShield HSM to create a high availability cluster. You can either use a standalone Cryptographic Security Platform Vault node or a Cryptographic Security Platform Vault cluster.

When the Cryptographic Security Platform Vault cluster is configured with multiple HSM servers, the Cryptographic Security Platform Vault cluster uses HSM servers for High Availability (HA) and load sharing purposes. The HSM servers are not affiliated with specific Cryptographic Security Platform Vault node(s), but are configured for and used by ALL members of the Cryptographic Security Platform Vault cluster.

Before You Begin

- Ensure that you have completed Configuring CSP Vault as an HSM Client using an nShield HSM.
- Obtain the Security World Bundle file for the new HSM that you want to add. It must have the same security world as the first HSM server inside of the Security World Bundle file, but the module file must be for the new HSM. Please contact your HSM Administrator to ensure that this is set up correctly.
  You cannot establish HA functionality if the servers do not share the same security world.
  Tip: For more information, see the 'Security Worlds' and 'Creating and Managing a Security World' chapters of your nShield Connect User Guide.

FIPS 140-2 Level 3 – smart card requirement

If your nShield HSMs are configured in a FIPS 140-2 Level 3 compliant Security World environment, an ACS or OCS card must be loaded in all HSMs. When using multiple HSMs for high availability, operations are load balanced between the HSM servers connected to Cryptographic Security Platform Vault. If one HSM fails, traffic is rerouted to another HSM. If a valid card is not located in the HSM, it will continue to receive traffic but operations requiring a FIPS authorization token will fail. A valid card (with a listed serial number, unless 'Accept all cards' is selected) must be loaded in the HSM to ensure operations do not fail. For more information regarding nShield HSMs and FIPS 140-2 Level 3, see Hardware Security Modules with CSP Vault

> Note: If you wish to use OCS cards that were not included in the security world bundle previously uploaded, ensure that the corresponding card files are included in the new bundle.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.

5. On the nShield HSM Server Settings page, click the **Client List** and copy the IP address and keyhash of the Cryptographic Security Platform Vaultnodes.
6. Use the IP address and keyhash to authenticate Cryptographic Security Platform Vault on nShield. Please see your nShield documentation.
   Important: For Cryptographic Security Platform Vault clusters, you will need to authenticate the IP address and keyhash for each cluster node.
7. Copy the Security World Bundle from nShield and place it on your local machine. It should be in the format world.zip.
8. On the Server List tab of the nShield HSM Server Settings page, select **Actions > Add New HSM Server**.
9. After reading the Get Started Screen, click **Continue**.
10. On the Enrollment screen, complete the following:
    Note: All information is from the nShield HSM. The Server Name is used for display purposes and the Server IP/FQDN is used for communication.

Field	Description
Server Name	Enter the FQDN of the nShield HSM.
Server IP/FQDN	Enter the IP address or FQDN for the nShield HSM.
Server ESN	Enter the nShield Electronic Serial Number (ESN).
Server Port	Enter the port used for the nShield HSM.
Server Keyhash	Enter the keyhash of the nShield HSM.

11. Click **Enroll and Continue**.
12. On the Security World screen, click **Browse** and locate the security world bundle that you downloaded from the nShield HSM.
13. Click **Upload and Continue**.
14. If you are using a FIPS 140-2 Level 3 Security World, on the Card List screen, select one of the following:
    - Accept all cards—Accepts all nShield Remote Administration smart cards.
    - Add Specific cards—Accepts specific nShield Remote Administration smart cards. To add a card, click **+ Add Card**, enter the card serial number and optional description, check the Enable checkbox, and click **Add**. You can add multiple cards at one time.
15. Click **Complete Setup**.
    After the setup is complete, you will be returned to the nShield HSM Server Settings page, which now displays the values for both HSMs on the Server List tab.
    Note: If the configuration failed, then you can simply remove the HSM by selecting it and then selecting **Actions > Remove Server** and add it again.

Replacing an nShield HSM on a CSP Vault Cluster

If you have a Cryptographic Security Platform Vault cluster on an nShield HSM, you can replace the HSM while maintaining the cluster. This procedure documents a 2-node cluster. If you have more than two nodes you will need to modify the instructions.

Before You Begin

To replace the nShield HSM, make sure you have the following information available:

- The HSM server name, server IP/FQDN, ESN, Port, and Keyhash for the replacement nShield HSM (HSM-2).

- The Security World Bundle file for the replacement HSM. Both HSM-1 and HSM-2 must have the same security world inside of the Security World Bundle file. Please contact your HSM Administrator to ensure that this is set up correctly.
  Tip: This information can be found in the sections on replacing, adding, or restoring an HSM to the Security World in chapters 2 and 9 of the nShield® Connect User Guide for Unix.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the nShield HSM Server Settings page, click the **Client List** tab.
6. Copy the Cryptographic Security Platform Vault IP addresses and keyhashes to notepad. You will need the IP address and keyhash of both the Cryptographic Security Platform Vault nodes (node-1 and node-2) to authenticate Cryptographic Security Platform Vault on the replacement nShield HSM (HSM-2).
7. Use the IP address and keyhash to authenticate Cryptographic Security Platform Vault on nShield. Please see your nShield documentation.
   Important: For Cryptographic Security Platform Vault clusters, you will need to authenticate the IP address and keyhash for each cluster node.
8. Copy the Security World Bundle from the replacement HSM-2 as world.zip and place it on your local machine.
9. On the nShield HSM Server Settings, click the **Server Settings** tab and then select HSM-1.
10. Replace the Server Name, Server IP/FQDN, Server ESN, Server Port and Server Keyhash of HSM-1 with the values for HSM-2.
11. Click **Apply**.
12. Select **Actions > Upload Security World** and upload the security world bundle for HSM-2.
13. Test your connection with HSM-2.

Configuring Allowed Smart Cards for an nShield HSM

When using an nShield HSM with a FIPS 140-2 Level 3 Security World a FIPS authorization token is required to authorize most operations, including the creation of keys. This is provided by an ACS or OCS card which must be loaded in the HSM or presented using a remote admin client. Cards are usually configured when setting up an HSM, so Entrust recommends leaving one of the configured OCS cards in the HSM slot to satisfy this requirement.

nShield HSMs include a security feature that checks the serial numbers of the cards as well as checking they are part of an OCS for this HSM. This allows the admin to disable a card if necessary.

The Card List tab of the nShield HSM Server Settings page In the Cryptographic Security Platform Vault Management webGUI allows you to control which card serial numbers are accepted. The tab is only available if the HSM is using a FIPS 140-2 Level 3 Security World and displays the current setting and details of any card serial numbers you have entered.

There are 3 basic modes:

- Accept All Cards—Does not check the card serial number. You can enter or leave this mode by selecting **Actions > Accept All Cards**. If the entry in the menu is preceded by a checkmark, it is enabled. Select **Actions > Accept All Cards** to disable.
- Reject All Cards—Does not allow any cards, so all operations requiring one will fail. You can enter or leave this mode by selecting **Actions > Reject All Cards**. If the entry in the menu is preceded by a checkmark, it is enabled. Select **Actions > Reject All Cards** to disable.

- Allow listed enabled cards—If neither of the modes is selected, any cards in the list that are Enabled will be allowed, and all other cards will be rejected.

Select a card from the list and then select a choice from the actions menu to delete, disable, or enable the selected card. You can add a card to the list by selecting Actions > Add Card. You can also add or edit a description for a card.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the **nShield HSM Server Settings** page, select the Card List tab.
6. Add or update your cards as necessary.

KeySafe5 Agent Requirements

Beginning with 10.5.3, you can use KeySafe5 for your nShield HSMs using the Cryptographic Security Platform Vault Management webGUI and Cryptographic Security Platform Compliance Manager webGUI. KeySafe5 contains an agent that runs on HSM clients and a GUI that allows remote management of setup and configuration tasks, provides visibility into the status of your nShield Security World, and allows real-time and historical monitoring.

To use KeySafe5 GUI, you must have the following:

- An nShield HSM must be enabled.
- Your Cryptographic Security Platform Vault Management webGUI must be connected as an Appliance Cluster in the Cryptographic Security Platform Compliance Manager webGUI.
- Anytime your Cryptographic Security Platform Compliance Manager is disconnected and reconnected, you will need to disable and re-enable the KeySafe5 agent in the Cryptographic Security Platform Vault Management webGUI.
- The KeySafe5 agent only runs on the primary node of the cluster.
- When you view the KeySafe5 GUI, the agent appears with the hostname of the cluster primary node. Even if you delete the primary node, the KeySafe5 agent name remains the same in the KeySafe5 GUI.
- After you enable the agent in the Cryptographic Security Platform Vault Management webGUI, it may take up to 15 minutes for the data to sync to the KeySafe5 GUI.
- After enabling the agent in the Cryptographic Security Platform Vault Management webGUI, you will need to log in to the Cryptographic Security Platform Compliance Manager webGUI, navigate to Data Sources, launch the KeySafe5 GUI, and perform the "reveal metadata" operation before your HSM keys will appear in the Cryptographic Security Platform Compliance Manager.

Enabling the KeySafe5 Agent

You need to enable the KeySafe5 agent in the Cryptographic Security Platform Vault Appliance before you can use it.

Before You Begin

- Ensure that an nShield HSM is properly configured in your Cryptographic Security Platform Vault Appliance. For more information, see Configuring CSP Vault as an HSM Client using an nShield HSM.
- Ensure that your Cryptographic Security Platform Vault Appliance webGUI is connected to the Cryptographic Security Platform Compliance Manager as an Appliance Cluster. For more information, see Connecting CSP Vault and CSP Compliance Manager.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the nShield HSM Server Settings page, set the KeySafe5 Agent to **Enable**.
6. Click **Apply**.
7. Navigate to the Compliance Manager page where you connected to the Cryptographic Security Platform Compliance Manager webGUI and click **Sync Now**.

Configuring CSP Vault as a Luna Cloud HSM Client

The following procedure describes how to configure Cryptographic Security Platform Vault as a Luna Cloud HSM Client.

Important: You can only configure both the Luna Cloud HSM and the Luna HSM if you are forming an HA Group to allow for High Availability. For more information, see Configuring a Luna HSM HA Group.

Before You Begin

For the HSM server that you want to connect to Cryptographic Security Platform Vault, make sure you have the following information available:

- The service client bundle for the HSM. When you create a service client, you will be prompted to download the service client bundle.
- The HSM partition name and password.
- A Cryptographic Security Platform Vault account with Security Admin privileges.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. On the **HSM Server Settings** page, select **Thales Luna HSM** from the Type drop-down list and click **Configure**.
6. On the **Luna HSM Server Settings** page, select the **Luna Cloud HSM** tab and then specify the options you want to use for the HSM server.

Field	Description
State	Make sure this field is set to Enabled.
Partition Label or HA Group Name	Enter the partition label for the partition on the HSM server that Cryptographic Security Platform Vault will be using. Note: Make sure you enter the partition label and not the partition name in this field.
Crypto Officer (CO) Password	Enter the password for the Crypto Officer (CO) password.

Field	Description
Service Client Bundle	Click Browse to specify the location of the service client bundle that you downloaded.
Session Timeout	The length of time Cryptographic Security Platform Vault keeps the communication session open with an HSM server. When the session expires, a new session is created with the same timeout value. The default is 30 minutes.

7. Click **Apply**, then click **Proceed** at the prompt.
8. Select **Actions > Test Connection** to test your connection. You should see a message that says the HSM connection is OK.

Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate

When you connect a Cryptographic Security Platform Vault cluster to a hardware security module (HSM), you can create one certificate for the Cryptographic Security Platform Vault cluster that you can use for all Cryptographic Security Platform Vault nodes or you can have an individual certificate for each node in the Cryptographic Security Platform Vault cluster.

Important: If you have a Luna HSM server with the `ipcheck` feature enabled, you must use Individual Node Certificates for Client Certificate Mode.

The following procedure describes how to configure Cryptographic Security Platform Vault as an HSM client that uses a single certificate for the entire cluster. If you want to use individual certificates for each node, see Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates.

Important: You can only configure both the Luna Cloud HSM and the Luna HSM if you are forming an HA Group to allow for High Availability. For more information, see Configuring a Luna HSM HA Group.

Before You Begin

For the HSM server that you want to connect to Cryptographic Security Platform Vault, make sure you have the following information available:

- The HSM server name.
- The user name and password for an HSM account with Admin privileges.
- The HSM partition name and password.
- The client name you want to assign to the Cryptographic Security Platform Vault cluster.

You will also need:

- A Cryptographic Security Platform Vault account with Security Admin privileges.
- Access to the HSM server via a shell account. The following procedure uses `scp` and `ssh` to connect to the server.

Note: The following instructions are specific to the Luna HSM.

Procedure

1. Download the HSM server certificate file `server.pem` from the HSM server to which you want to connect. We recommend that you rename the `server.pem` certificate file so that you can find the certificate file easily when you need to upload it to Cryptographic Security Platform Vault later in this procedure.
   For example, if your HSM server is `hsm1.my-company.com`, you could enter:

```
# scp admin@hsm1.my-company.com:server.pem ./hsm1cert.pem
admin@hsm1.my-company.com's password:

server.pem          100% 1155     1.1KB/s   00:00
```

2. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
3. In the top right, click the Switch to **Appliance Management** link.
4. In the top menu bar, click **Settings**.
5. In the **System Settings** section, click **HSM Server Settings**.
6. On the **HSM Server Settings** page, select **Thales Luna HSM** from the Type drop-down list and click **Configure**.
7. On the **Luna HSM Server Settings** page, select the **Luna HSM** tab and then specify the options you want to use for the HSM server.

Field	Description
State	Make sure this field is set to Enabled.
Hostname	Enter the hostname for the HSM server.
Partition Label or HA Group Name	Enter the partition label for the partition on the HSM server that Cryptographic Security Platform Vault will be using. Note: Make sure you enter the partition label and not the partition name in this field.
Partition or Crypto Officer (CO) Password	Enter the password for the Cryptographic Security Platform Vault partition or the Crypto Officer (CO) password for Luna HSM modules version 7 and above.
Server Certificate	Click Browse to specify the location of the HSM server certificate file.
Session Timeout	The length of time Cryptographic Security Platform Vault keeps the communication session open with an HSM server. When the session expires, a new session is created with the same timeout value. The default is 30 minutes.
Client Certificate Mode	Select the Single Cluster Certificate radio button so that Cryptographic Security Platform Vault will use the same certificate for all nodes in the cluster.
Client Name	Specify a name for the Cryptographic Security Platform Vault client on the HSM server. This name must be unique on the HSM server.
Admin Key ID	Indicates whether an Admin Key already exists on the HSM.

8. Click **Apply**, then click **Proceed** at the prompt. Do not test the connection yet.

9. Select **Actions > Generate Client Certificate** to download the cluster certificate that all Cryptographic Security Platform Vault nodes can use. Cryptographic Security Platform Vault automatically saves *client-name*.pem file to your browser's default download location.
   For example, if you use the default client name KC_Cluster, the cluster certificate name would be KC_Cluster.pem.
10. Upload the cluster certificate to the root directory on the HSM server. For example:
    ```
    # scp KC_Cluster.pem admin@hsm1.my-company.com:
    admin@hsm1.my-company.com's password:

    KC_Cluster.pem          100% 1164     1.1KB/s   00:00
    ```
11. Using a shell account, log into the HSM server and:
    a. Register the new Cryptographic Security Platform Vault client using the same client name you specified in the webGUI for both the client name and hostname.
       Tip: If the registration fails because a client of that name already exists, you either need to delete the existing client or go back to the webGUI, enter an new client name, click **Apply**, and then download a new cluster certificate that you can upload to the HSM server.
    b. Assign any partitions that you intend to use to the Cryptographic Security Platform Vault client.
       Note: This should include the partition specified above and any others that you intend to use from CSP Vaults.

    For example, if you want the Cryptographic Security Platform Vault client KC_Cluster to be assigned to KC_partition1 on hsm1.my-company.com, you could enter:
    ```
    # ssh admin@hsm1.my-company.com
    admin@hsm1.my-company.com's password:

    [hsm1] lunash:>client register -client KC_Cluster -hostname KC_Cluster
    'client register' successful
    Command Result : 0 (Success)
    [hsm1] lunash:>client assignPartition -client KC_Cluster -partition KC_partition1
    'client assignPartition' successful
    Command Result : 0 (Success)
    [hsm1] lunash:>exit
    ```
12. Return to the **Luna HSM Server Settings** page and click **Test**. You should see a message that says the HSM connection is OK and that the Admin Key needs to be regenerated.
    To regenerate the Admin key, go to **Settings > General Settings > Admin Key Parts**, then click **Generate New Key**. You should get a message that the Admin Key was successfully generated and distributed. To verify this, go back to **Settings > System Settings > HSM Server Settings**. The **Admin Key ID** field should display a GUID for the new Admin Key.

Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates

Important: You can only configure both the Luna Cloud HSM and the Luna HSM if you are forming an HA Group to allow for High Availability. For more information, see Configuring a Luna HSM HA Group.

When you connect a Cryptographic Security Platform Vault cluster to a hardware security module (HSM), you can create one certificate for the Cryptographic Security Platform Vault cluster that you can use for all Cryptographic Security Platform Vault nodes or you can have an individual certificate for each node in the Cryptographic Security Platform Vault cluster. If you have a Luna HSM server with the ipcheck feature enabled, you must use unique node certificates.

The following procedure describes how to configure Cryptographic Security Platform Vault as an HSM client that uses unique certificates for each node in the cluster. If you want to use a single certificate that will be shared by all nodes in the cluster, see Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate.

Before You Begin

For the HSM server that you want to connect to Cryptographic Security Platform Vault, make sure you have the following information available:

- The HSM server name.
- The user name and password for an HSM account with Admin privileges.
- The HSM partition name and password.

You will also need:

- A Cryptographic Security Platform Vault account with Security Admin privileges.
- Access to the HSM server via a shell account. The following procedure uses `scp` and `ssh` to connect to the server.

The following instructions are specific to the Luna HSM.

Procedure

1. Download the HSM server certificate file `server.pem` from the HSM server to which you want to connect. We recommend that you rename the `server.pem` certificate file so that you can find the certificate file easily when you need to upload it to Cryptographic Security Platform Vault later in this procedure.
   For example, if your HSM server is `hsm1.my-company.com`, you could enter:
   ```
   # scp admin@hsm1.my-company.com:server.pem ./hsm1cert.pem
   admin@hsm1.my-company.com's password:

   server.pem          100% 1155     1.1KB/s   00:00
   ```
2. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
3. In the top right, click the Switch to **Appliance Management** link.
4. In the top menu bar, click **Settings**.
5. In the **System Settings** section, click **HSM Server Settings**.
6. On the **HSM Server Settings** page, select **Thales Luna HSM** from the Type drop-down list and click **Configure**.
7. On the**Luna HSM Server Settings** page, select the **Luna HSM** tab and then specify the options you want to use for the HSM server.

Field	Description
State	Make sure this field is set to Enabled.
Hostname	Enter the hostname for the HSM server.
Partition Label or HA Group Name	Enter the partition label for the partition on the HSM server that Cryptographic Security Platform Vault will be using. Note: Make sure you enter the partition label and not the partition name in this field.

Field	Description
Partition or Crypto Officer (CO) Password	Enter the password for the Cryptographic Security Platform Vault partition or the Crypto Officer (CO) password for Luna HSM modules version 7 and above.
Server Certificate	Click Browse and open the appropriate HSM server certificate file.
Client Certificate Mode	Select the Individual Node Certificates radio button so that Cryptographic Security Platform Vault will use a unique certificate for each node in the cluster.
Admin Key ID	Indicates whether an Admin Key already exists on the HSM.

8. Click **Apply**, then click **Proceed** at the prompt. Do not test the connection yet.
9. Navigate to the **Client List** tab. You should see one entry for each Cryptographic Security Platform Vault node in the cluster.
10. Select the first node in the list, then select **Actions > Generate Client Certificate for *node-name.domain-name***. Cryptographic Security Platform Vault automatically generates a unique certificate for that node called `node-name.domain-name.pem` and downloads it to your browser's default download location.
    For example, if the name of the node is `KC-1` and it is running on the domain `my-company.com`, the certificate file would be called `KC-1.my-company.com.pem`.
11. Repeat the previous step for each Cryptographic Security Platform Vault node in the cluster.
12. Upload all certificates to the root directory on the HSM server. For example, if you have two Cryptographic Security Platform Vault nodes, you would copy both Cryptographic Security Platform Vault node certificates to HSM server:
    ```
    # scp KC-1.my-company.com.pem admin@hsm1.my-company.com:
    admin@hsm1.my-company.com's password:

    KC-1.my-company.com.pem          100% 1164     1.1KB/s   00:00

    # scp KC-2.my-company.com.pem admin@hsm1.my-company.com:
    admin@hsm1.my-company.com's password:

    KC-2.my-company.com.pem          100% 1164     1.1KB/s   00:00
    ```
13. Using a shell account, log into the HSM server and:
    a. Register the new Cryptographic Security Platform Vault client using `"node-name.domain-name"` for both the client name and hostname. The double quotes are required because of the period in the client name.
       Tip: If the registration fails because a client of that name already exists, you need to delete the existing client. You cannot change the name of the client pem file that CSP Vault generates.
    b. Assign any partitions that you intent to use to the Cryptographic Security Platform Vault client.
       Note: This should include the partition that you specified above as well as any other partitions that you intent to use from CSP Vaults.

    For example, if you want the Cryptographic Security Platform Vault client to be assigned to `KC_partition1` on `hsm1.my-company.com`, you could enter:

```
# ssh admin@hsm1.my-company.com
admin@hsm1.my-company.com's password:

[hsm1] lunash:>client register -client "KC-1.my-company.com" -hostname "KC-1.my-company.com"

'client register' successful
Command Result : 0 (Success)
[hsm1] lunash:>client register -client "KC-2.my-company.com" -hostname "KC-2.my-company.com"

'client register' successful
Command Result : 0 (Success)
[hsm1] lunash:>client assignPartition -client "KC-1.my-company.com" -partition KC_partition1
'client assignPartition' successful
Command Result : 0 (Success)
[hsm1] lunash:>client assignPartition -client "KC-2.my-company.com" -partition KC_partition1
'client assignPartition' successful
Command Result : 0 (Success)
[hsm1] lunash:>exit
```

14. Return to the **LunaHSM Server Settings** page and click **Test**. You should see a message that says the HSM connection is OK and that the Admin Key needs to be regenerated.
    To regenerate the Admin key, go to **Settings > General Settings > Admin Key Parts**, then click **Generate New Key**. You should get a message that the Admin Key was successfully generated and distributed. To verify this, go back to **Settings > System Settings > HSM Server Settings**. The **Admin Key ID** field should display a GUID for the new Admin Key.

Configuring a Luna HSM HA Group

If you want to connect a Cryptographic Security Platform Vault cluster to multiple HSM servers, you must create an HA group for those servers on *each*Cryptographic Security Platform Vault node in the cluster. That way any Admin Keys or KEKs that Cryptographic Security Platform Vault creates will be stored on all HSM servers in the group and can be accessed from any of the HSM servers by any of the Cryptographic Security Platform Vault nodes.

You can create a group with two or more Luna HSMs, or a single Luna Cloud HSM and one or more Luna HSMs.

Before You Begin

- Make sure you have configured the HSM servers in the Cryptographic Security Platform Vault webGUI and registered the Cryptographic Security Platform Vault clients with the HSM servers as described in Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate, Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates, or Adding a New Luna HSM to an Existing Luna HSM Configuration.
- Make sure the Luna HSM servers meet the Luna HSM requirements for membership in an HA group. The partitions you select for the HA Group must have the same CO password and be configured in Cloning Mode. For details about these requirements, see your Luna HSM documentation.

Procedure

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).

2. From the Entrust Cryptographic Security Platform Vault System Console, select **Manage HSM Client Account**.
3. From the Manage HSM Client Account page, select **Enable and Set Password for HSM Client Account**.
4. Acknowledge the password requirements at the prompt.
5. On the Change hsmadmin Password page, specify the password you want to use and select **OK**.
6. Select **Return to Main Menu**.
7. From the main Entrust Cryptographic Security Platform Vault System Console, select **Log Out**.
8. Log into the server as `hsmadmin` with the password you just specified. Wait until the Cryptographic Security Platform Vault node has retrieved the information about the registered HSM servers and has displayed the `lunacm:>` prompt. Depending on your network, it may take some time to retrieve this information.
9. Make sure that all HSM servers on which you registered the Cryptographic Security Platform Vault node, and the Luna Cloud HSM if you are using one, are displayed in the list with assigned Slot IDs and the correct partition labels.
   Important: If you do not see all of the HSM servers that you expect to see, do not continue with this step. Instead, use `exit` to return to the login prompt and then make sure that you have registered the Cryptographic Security Platform Vault node with all of the HSM servers you want to use.
10. Create an HA group according to your Luna HSM documentation. The following steps are shown for your convenience and may need to be changed based on the version of your Luna HSM server. The password you specify must be the password for the Luna HSM partitions you entered in the Cryptographic Security Platform Vault webGUI.

    ```
    lunacm:>haGroup createGroup -slot 0 -label hagroup -password HSMPartPswd
    Warning: There are objects currently on the new member.
    Do you wish to propagate these objects within the HA
    group, or remove them?

    Type 'copy' to keep and propagate the existing
    objects, 'remove' to remove them before continuing,
    or 'quit' to stop adding this new group member.
    >copy
    ```

    At this point, you should see messages stating that the HA group was created without error. If this succeeds, you can add all other HSMs to the HA group.

    ```
    lunacm:>haGroup addMember -slot 1 -group hagroup -password HSMPartPswd
    Warning: There are objects currently on the new member.
    Do you wish to propagate these objects within the HA
    group, or remove them?

    Type 'copy' to keep and propagate the existing
    objects, 'remove' to remove them before continuing,
    or 'quit' to stop adding this new group member.
    >copy

    Disable hagroup logging with
    lunacm:> hagroup halog -disable
    ```

    Repeat the `haGroup addMember` command for each additional HSM server until all HSM servers with which you registered this Cryptographic Security Platform Vault node are members of the HA group.
11. After all members have been added, use the `exit` command to log out of `hsmadmin`.
12. Repeat this procedure on all Cryptographic Security Platform Vault nodes in the cluster.
13. After you have created the HA group on *all* nodes in the cluster, go back to the Cryptographic Security Platform Vault webGUI HSM Server Settings page and do the following:
    a. Change the **Partition Label or HA Group Name** to be the name of the HA group you created.

Note: If your HA group contains both the Luna HSM and Luna Cloud HSM, you will need to update this field on both tabs on the Thales HSM Server Settings page. Do not generate a new admin key until both tabs have been updated and you have applied the changes.

b. Click **Apply**, then click **Proceed** at the prompt. You should see a message that the HSM hostname or partition label has changed and that you need to regenerate the Admin key. If this message appears then the connection to all of the HSM servers in the HA group succeeded.

c. To regenerate the Admin key, go to **Settings > General Settings > Admin Key Parts**, then click **Generate New Key**. You should get a message that the Admin Key was successfully generated and distributed. To verify this, go back to **Settings > System Settings > Luna HSM Server Settings**. The **Admin Key ID** field should display a GUID for the new Admin Key.
Important: If your HA group contains both the Luna HSM and Luna Cloud HSM, do not generate a new admin key until both tabs have been updated and you have applied all of the changes.

Adding a CSP Vault Node to an Existing Luna HSM Configuration

How you add a new Cryptographic Security Platform Vault node to an existing HSM configuration depends on whether you are using a single cluster certificate or individual node certificates.

In both cases, though, you should deploy the node as usual and then join it to the existing cluster. For details on adding an already-deployed node, see Joining or Re-joining a CSP Vault Cluster. For details on deploying a new node,

Single Cluster Certificate

If you are using a single cluster certificate, you do not need to do anything special to connect the new node to your existing HSM configuration. Cryptographic Security Platform Vault automatically adds to the new node to your existing HSM configuration when you add it to the cluster.

This is true for both single HSM and multiple HSM configurations.

Individual Node Certificates

Before You Begin

For *each* hardware security module (HSM) that is currently connected to Cryptographic Security Platform Vault, make sure you have the following information available:

- The HSM server name.
- The user name and password for an HSM account with Admin privileges.
- The HSM partition name and password for the partition to which the existing Cryptographic Security Platform Vault clients have been assigned.

You will also need:

- A Cryptographic Security Platform Vault account with Security Admin privileges.
- Access to the HSM servers via a shell account. The following procedure uses `ssh` to connect to the servers.

Note: The following instructions are specific to the Luna HSM.

Procedure

If you are using individual node certificates, you need to do the following after you have added the new node to the cluster:

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.

5. Navigate to the **Client List** tab. You should see one entry for each Cryptographic Security Platform Vault node in the cluster.
6. Select the new node in the list, then select **Actions > Generate Client Certificate for *node-name.domain-name***. Cryptographic Security Platform Vault automatically generates a unique certificate for that node called `node-name.domain-name.pem` and downloads it to your browser's default download location.
   For example, if the name of the node is `KC-4` and it is running on the domain `my-company.com`, the certificate file would be called `KC-4.my-company.com.pem`.
7. Upload the node certificate to the root directory on each HSM server that you want to use. For example, if you have two HSM servers, you would copy the new node certificate to both HSM servers:
   ```
   # scp KC-4.my-company.com.pem admin@hsm1.my-company.com:
   admin@hsm1.my-company.com's password:

   KC-4.my-company.com.pem          100% 1164     1.1KB/s   00:00

   # scp KC-4.my-company.com.pem admin@hsm2.my-company.com:
   admin@hsm2.my-company.com's password:

   KC-4.my-company.com.pem          100% 1164     1.1KB/s   00:00
   ```
8. Using a shell account, log into each HSM server and:
   a. Register the new Cryptographic Security Platform Vault client using `"node-name.domain-name"` for both the client name and hostname. The double quotes are required because of the period in the client name.
      Tip: If the registration fails because a client of that name already exists, you need to delete the existing client. You cannot change the name of the client pem file that Cryptographic Security Platform Vault generates.
   b. Assign a partition to the Cryptographic Security Platform Vault client.

   For example, if you want the Cryptographic Security Platform Vault client `KC-4.my.company.com` to be assigned to `KC_partition1` on `hsm1.my-company.com` and to `KC_partition2` on `hsm2.my-company.com`, you could enter:
   ```
   # ssh admin@hsm1.my-company.com
   admin@hsm1.my-company.com's password:

   [hsm1] lunash:>client register -client "KC-4.my-company.com" -hostname "KC-4.my-company.com"

   'client register' successful
   Command Result : 0 (Success)
   [hsm1] lunash:>client assignPartition -client "KC-4.my-company.com" -partition KC_partition1
   'client assignPartition' successful
   Command Result : 0 (Success)
   [hsm1] lunash:>exit

   # ssh admin@hsm2.my-company.com
   admin@hsm2.my-company.com's password:

   [hsm2] lunash:>client register -client "KC-4.my-company.com" -hostname "KC-4.my-company.com"

   'client register' successful
   Command Result : 0 (Success)
   [hsm2] lunash:>client assignPartition -client "KC-4.my-company.com" -partition KC_partition1
   'client assignPartition' successful
   ```

```
Command Result : 0 (Success)
[hsm2] lunash:>exit
```

9. If you want to verify the connection, return to the Cryptographic Security Platform Vault webGUI and navigate to the **Server Settings** tab, then click **Test**. You should see a message that says the HSM connection is OK.

Adding a New Luna HSM to an Existing Luna HSM Configuration

If you have already configured your Cryptographic Security Platform Vault cluster to use a Luna hardware security module (HSM) server, you can add a new Luna HSM server to your configuration at any time. Adding additional HSM servers and configuring an HA Group provides High Availability (HA) if one HSM server should become unreachable.

The following procedure describes how to add an additional Luna HSM when you have already configured one or more Luna HSMs. If you only have a Luna Cloud HSM configured, see Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate or Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates. If this is the first time you are configuring an HSM server for your Cryptographic Security Platform Vault cluster, see Hardware Security Modules with CSP Vault.

Before You Begin

For the new HSM server that you want to connect to Cryptographic Security Platform Vault, make sure you have the following information available:

- The HSM server name.
- The user name and password for an HSM account with Admin privileges.
- The HSM partition name and partition password. We recommend that you use a different partition name on each HSM server so that you can tell the servers apart when you are working with the HA group.
  Note: Luna requires that the partition password be the same on all servers in an HA group, and that certain configuration options be the same on all HSM servers in the group. For details, see your Luna HSM documentation.

You will also need:

- A Cryptographic Security Platform Vault account with Security Admin privileges.
- Access to the new HSM server via a shell account. The following procedure uses `scp` and `ssh` to connect to the server.

Note: The following instructions are specific to the Luna HSM.

Procedure

1. Download the HSM server certificate file `server.pem` from the new HSM server. We recommend that you rename the `server.pem` certificate file so that you know which HSM server goes with which certificate file.
   For example, if the new HSM server is `hsm2.my-company.com`, you could enter:
   ```
   # scp admin@hsm2.my-company.com:server.pem ./hsm2cert.pem
   admin@hsm2.my-company.com's password:

   server.pem          100% 1155     1.1KB/s   00:00
   ```
2. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
3. In the top right, click the Switch to **Appliance Management** link.
4. In the top menu bar, click **Settings**.
5. In the **System Settings** section, click **HSM Server Settings**.

6. On the **HSM Server Settings** page, select **Thales Luna HSM** from the Type drop-down list and click **Configure**.
7. On the **Luna HSM Server Settings** tab, select the **Luna HSM** tab and then specify the options you want to use for the HSM server.
    a. Change the **Hostname** to the name of the new HSM server.
    b. Change the **Partition Label or HA Group Name** to the partition that Cryptographic Security Platform Vault should use on the new HSM server. We recommend that you use a different partition name on each server so that you can tell which server is which when you are creating the Luna HA group later in this procedure.
    c. In the **Server Certificate** field, click **Browse** and select the server certificate for this HSM server.
    d. Click **Apply**, then click **Proceed** at the prompt. Do not test the connection yet.

    Note: Because Luna requires that all HSM servers in a High Availability group have the same password, you do not need to enter the password for any additional HSM servers. Cryptographic Security Platform Vault automatically uses the most recent password entered for all servers in the group.
8. If you do not have the original Cryptographic Security Platform Vault client cluster certificate or node certificates, you need to regenerate them. How you do so depends on the selected **Client Mode**.

Client Mode Setting	Steps to Regenerate the Certificates
CLUSTER	Select Actions > Generate Client Certificate. Cryptographic Security Platform Vault automatically saves *client-name*.pem file to your browser's default download location.
NODE	a. Navigate to the **Client List** tab. b. Select the first node in the list, then select **Actions > Generate Client Certificate for *node-name.domain-name***. Cryptographic Security Platform Vault automatically generates a unique certificate for that node called *node-name.domain-name*.pem and downloads it to your browser's default download location. c. Repeat step 2 for each node in the cluster until you have a full set of node certificates.

    Note: If you regenerate the cluster certificate or node certificates you must upload the new certificate(s) to all the Luna HSM servers.
9. Upload the cluster certificate or the individual node certificates to the root directory on the new HSM server.
    Cluster Mode Example
    If your Cryptographic Security Platform Vault cluster name is KC_Cluster and the new HSM server is hsm2.my-company.com, you would enter:
    # scp KC_Cluster.pem admin@hsm2.my-company.com:
    admin@hsm2.my-company.com's password:

    KC_Cluster.pem 100% 1164 1.1KB/s 00:00

    Node Mode Example
    If you have two Cryptographic Security Platform Vault nodes named KC-1 and KC-2 and the new HSM server is hsm2.my-company.com, you would enter:
    # scp KC-1.my-company.com.pem admin@hsm2.my-company.com:
    admin@hsm2.my-company.com's password:

    KC-1.my-company.com.pem 100% 1164 1.1KB/s 00:00

```
# scp KC-2.my-company.com.pem admin@hsm2.my-company.com:
admin@hsm2.my-company.com's password:

KC-2.my-company.com.pem          100% 1164     1.1KB/s   00:00
```

10. Using a shell account, log into the new HSM server and:
    a. Register the new Cryptographic Security Platform Vault client using the client name for both the client name and hostname parameters. Use double quotes if the client name includes any periods or spaces.
    Tip: If the registration fails because a client of that name already exists, you need to delete the existing client. You cannot change the client name after the initial HSM configuration has been completed.
    b. Assign any partitions that you intend to use to the Cryptographic Security Platform Vault client.
    Note: This should include the partition specified above, and any others that you intend to use from Vaults.

    Cluster Mode Example

    For example, if you want the Cryptographic Security Platform Vault client `KC_Cluster` to be assigned to `KC_partition2` on `hsm2.my-company.com`, you could enter:

    ```
    # ssh admin@hsm2.my-company.com
    admin@hsm2.my-company.com's password:

    [hsm2] lunash:>client register -client KC_Cluster -hostname KC_Cluster
    'client register' successful
    Command Result : 0 (Success)
    [hsm2] lunash:>client assignPartition -client KC_Cluster -partition KC_partition1
    'client assignPartition' successful
    Command Result : 0 (Success)
    [hsm2] lunash:>exit
    ```

    Node Mode Example

    For example, if you want the Cryptographic Security Platform Vault clients `KC-1` and `KC-2` to be assigned to `KC_partition2` on `hsm2.my-company.com`, you could enter:

    ```
    # ssh admin@hsm2.my-company.com
    admin@hsm2.my-company.com's password:

    [hsm2] lunash:>client register -client "KC-1.my-company.com" -hostname "KC-1.my-
    company.com"
    'client register' successful
    Command Result : 0 (Success)
    [hsm2] lunash:>client register -client "KC-2.my-company.com" -hostname "KC-2.my-company.com"

    'client register' successful
    Command Result : 0 (Success)
    [hsm2] lunash:>client assignPartition -client "KC-1.my-company.com" -partition KC_partition3
    'client assignPartition' successful
    Command Result : 0 (Success)
    [hsm2] lunash:>client assignPartition -client "KC-2.my-company.com" -partition KC_partition3
    'client assignPartition' successful
    Command Result : 0 (Success)
    ```

11. Repeat this procedure for any more Luna HSMs that you wish to add. If you wish to add a Luna Cloud HSM, see Adding a Luna Cloud HSM to an Existing Luna HSM Configuration.

After you have configured all the Luna HSM servers and optionally a Luna Cloud HSM, create a Luna HSM HA group that links the HSM servers together so that all keys will be saved to all servers in the group. For details, see Configuring a Luna HSM HA Group.

Adding a Luna Cloud HSM to an Existing Luna HSM Configuration

If you have already configured your Cryptographic Security Platform Vault cluster to use one or more Luna hardware security module (HSM) serverx, you can add a Luna Cloud HSM server to your configuration. You can then configure an HA Group or add it to the existing HA Group. This provides High Availability (HA) if one HSM server should become unreachable. For more information, see Configuring a Luna HSM HA Group.

You can only have a single Luna Cloud HSM configured. If you also have any Luna HSMs, you must configure an HA Group and specify the same HA Group in both the Luna HSM and Luna Cloud HSM tabs of the Luna HSM Server Settings page.

Follow the instructions at Configuring CSP Vault as a Luna Cloud HSM Client to add the Luna Cloud HSM, and then use the instructions at Configuring a Luna HSM HA Group to create and select the HA Group.

Note: The partition that you use on the Luna Cloud HSM must use the same password as those on the Luna HSMs and meet the other requirements for membership in an HA group. For details about these requirements, see your Luna HSM documentation.

Changing the Luna Client Certificate Mode

If you have an existing Luna HSM configuration and you want to change from using a single cluster certificate to individual node certificates, or if you want to change from individual node certificates to a single cluster certificate, you need to reset your HSM configuration and recreate it from the beginning.

Warning:

- When you reset your HSM configuration, Cryptographic Security Platform Vault permanently deletes all Admin keys stored on any HSM servers in the current configuration. It then generates a new Admin Key. Make sure you download this Admin Key and keep it securely in case you need to restore your CSP Vault system to its current state. After reconfiguring the HSM settings you can generate a new Admin Key stored in the HSM(s).
- If any of your Cloud VM Sets use a KEK (Key Encryption Key) , the KEKs will *not* be deleted. However, Cryptographic Security Platform Vault will not be able to access those KEKs until you reconfigure the connection to the same partition on at least one of the HSM servers that you originally used. If a VM protected by a KEK is rebooted before the HSM server connection had been reestablished, the reboot will fail and VM will not be accessible to any users. For more information, see KEKs with Cloud VM Sets.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. Click **Reset Server Settings** and confirm the reset at the prompt.
6. Reconfigure your HSM settings as described in Configuring CSP Vault as a Luna HSM Client with a Single Cluster Certificate or Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates.

Locating the HSM Server Admin Key

If your Admin key is stored in the HSM, you can use Cryptographic Security Platform Vault to locate it.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. In the Admin Key ID field, click **Locate Admin Key**.
   The location of the Admin key ID is displayed at the bottom of the page.

Resetting the HSM Server Configuration

When you reset your HSM configuration, keep the following in mind:

- Cryptographic Security Platform Vault permanently deletes all Admin keys stored on any HSM servers in the current configuration. It then generates a new Admin key. Make sure you download this Admin Key and keep it securely in case you need to restore your Cryptographic Security Platform Vaultsystem to its current state.
- If you are using Luna HSMs or Luna Cloud HSMs:
  - If any of your Cloud VM Sets use a KEK (Key Encryption Key) , the KEKs will *not* be deleted. However, Cryptographic Security Platform Vault will not be able to access those KEKs until you reconfigure the connection to the same partition on at least one of the HSM servers that you originally used. If a VM protected by a KEK is rebooted before the HSM server connection had been reestablished, the reboot will fail and VM will not be accessible to any users. For more information, see KEKs with Cloud VM Sets.
    Important: You must disable the KEK setting in every Cryptographic Security Platform Vault for KMIP before you reset the HSM.
  - The Cryptographic Security Platform Vault client on the Luna HSM servers will not be deleted. If you want to remove the Cryptographic Security Platform Vault client from the Luna HSM server, you must do this manually on each Luna HSM server in your configuration.
- If you are using *both* Luna HSMs and Luna Cloud HSMs you must reset both HSMs.
- If you are using nShield HSMs:
  - All keys will be deleted. You should disconnect all CSP Vaults from the HSM before resetting the HSM configuration.
  - If you have enabled HSM Root-of-Trust, you cannot reset the HSM server configuration.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **HSM Server Settings**.
5. Reset the server as follows:
   - For nShield, select **Actions > Reset HSM Configuration**.
   - For Luna HSM, select **Actions > Reset Luna HSM Configuration**.
   - For Luna Cloud HSM, select **Actions > Reset Luna Cloud HSM Configuration**.
6. Confirm the reset at the prompt.

SNMP Traps in Cryptographic Security Platform Vault

You can configure Cryptographic Security Platform Vault to send an SNMP (Simple Network Management Protocol) trap whenever an alert is generated. These alerts can be divided into two categories:

- System-level alerts apply to events that are handled by Security Admins, such as numerous failed login attempts for a Cryptographic Security Platform Vault user account or if the Cryptographic Security Platform Vault license is about to expire.

- Group-level alerts apply to events that are handled by Cloud Admins or Domain Admins, such as if a VM needs to be re-authorized or if the Cryptographic Security Platform Vault cluster status changes.

You can specify one system-level SNMP trap configuration and one group-level SNMP trap configuration for each Cloud Admin or Domain Admin user group in the system.

If a group-level alert is raised and there is no matching group-level SNMP trap configuration, Cryptographic Security Platform Vault defaults to the system-level SNMP trap configuration.

This section includes:

- Configuring Group-Level SNMP Traps
- Configuring SNMP Agent Users for Polling
- Configuring System-Level SNMP Traps
- Downloading the SNMP MIB File
- SNMP MIB File

Configuring Group-Level SNMP Traps

The group-level trap configurations are used for alerts that affect Cloud Admins or Domain Admins. If no group-level configuration is specified for a particular group-level alert, Cryptographic Security Platform Vault defaults to the System-level SNMP configuration settings.

1. Log into the Cryptographic Security Platform Vault webGUI on any node in the cluster using an account with the security privilege that matches the type of group configuration you want to create. For example, if you want to create a Cloud Admin group-level SNMP configuration, you need to log in with Cloud Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **Group Settings** section, click **Group SNMP Settings**.
4. On the SNMP Settings page, select the Cloud Admin Group to which you want the configuration to apply in the **Group** field.
5. Specify the SNMP configuration options you want to use.

Field	SNMP Version	Description
Enabled	All	Select True if you want Cryptographic Security Platform Vault to use this SNMP configuration.
Server	All	The hostname or IP address of the SNMP server.
Port	All	The SNMP port number. The default SNMP port is 162.

Field	SNMP Version	Description
Version	All	The SNMP version. Cryptographic Security Platform Vault supports version 3. Note: The rest of the fields displayed in page depend upon the selected version. Note: Starting with release 10.6.1, SNMP version 2c is no longer supported. Only SNMP version 3 is supported. During an upgrade from an earlier release to 10.6.1: • If SNMP is configured using version 2c, the version 2c configuration is removed and SNMP is disabled during the upgrade. • Any configured SNMP version 2c agent users are also deleted. • After the upgrade, you must configure SNMP version 3 and re-enable SNMP to continue using SNMP functionality. If SNMP version 3 is already configured, the existing configuration continues to function without changes. However, any associated agent users configured using version 2c are removed during the upgrade and must be recreated using SNMP version 3.
Community	2c	Specify the community string for your SNMP server.
User	3	The user ID that should be associated with the trap.
Notification Type	3	This can be: • Inform—Cryptographic Security Platform Vault sends the SNMP trap and expects an acknowledgment that the trap was received in return. • Trap—Cryptographic Security Platform Vault sends the SNMP trap but does not expect an acknowledgment.

Field	SNMP Version	Description
Engine ID Type	3	Choose the engine ID type from the following options: • Custom Engine ID—Choose this option if an SNMP engine ID is already configured in the SNMP Manager. This allows users to configure the same engine ID in the engine ID field. Cryptographic Security Platform Vault will send the traps with the supplied engine. • System Generated Engine ID—Choose this option if the SNMP Manager expects to receive the engine ID from the Cryptographic Security Platform Vault. The Engine ID field will be automatically filled with a system generated engine ID that cannot be edited. Updating the system generated engine ID may take a few minutes. Note: This field is only visible if the Notification Type is Trap.
Engine ID	3	If the Notification Type is Trap, enter the SNMP engine ID assigned to the SNMP manager. You can enter between 10 and 64 hexadecimal characters.
Security Level	3	This can be: • **No Authentication, No Privacy** — Cryptographic Security Platform Vault sends the messages in plain text and no authentication is done by the SNMP server. • **With Authentication, No Privacy** — Cryptographic Security Platform Vault sends the message in plain text but the SNMP server authenticates the message before logging it. • **With Authentication, With Privacy** — Cryptographic Security Platform Vault encrypts the message before sending it and the SNMP server authenticates the message before logging it. For encryption, Cryptographic Security Platform Vault supports AES (Advanced Encryption Standard) or DES (Data Encryption Standard).
Authentication Protocol	3	The type of authentication to use with the SNMP server if one of the authentication options is selected in the Security Level field. Cryptographic Security Platform Vault supports MD5 and SHA (Secure Hash Algorithm).

Field	SNMP Version	Description
Authentication Key	3	The authentication key that Cryptographic Security Platform Vault should send to the SNMP manager if one of the authentication options is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.
Privacy Protocol	3	The privacy protocol to use if With Authentication, With Privacy is selected in the Security Level field. This can be AES or DES.
Privacy Key	3	The privacy key to use if With Authentication, With Privacy is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.

6. When you are finished, click **Apply**.
7. If you want to test the configuration, click **Test SNMP Settings**.
   Note: The SNMP trap must be enabled and you must apply the settings before you can test the configuration.
8. If you want to download the MIB file, click **Download MIB File**.

Configuring SNMP Agent Users for Polling

After you enable SNMP traps, you can configure one or more SNMP agent users that allow the SNMP agent to poll Cryptographic Security Platform Vault for system information.

The following OIDS are available for querying:

- IF-MIB::ifTable (.1.3.6.1.2.1.2.2)
- HOST-RESOURCES-MIB::hrFSTable (.1.3.6.1.2.1.25.3.8)
- HOST-RESOURCES-MIB::hrSystem (.1.3.6.1.2.1.25.1)
- 'NET-SNMP-EXTEND-MIB::nsExtendOutputFull."svstat"' (.1.3.6.1.4.1.8072.1.3.2.3.1.2.6.115.118.115.116.97.116)
- SNMPv2-MIB::system (.1.3.6.1.2.1.1)
- UCD-SNMP-MIB::dskTable (.1.3.6.1.4.1.2021.10)
- UCD-SNMP-MIB::laTable (.1.3.6.1.4.1.2021.9)
- UCD-SNMP-MIB::memory (.1.3.6.1.4.1.2021.4)
- UCD-SNMP-MIB::systemStats (.1.3.6.1.4.1.2021.11)

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges. In the top right, click the Switch to **Appliance Management** link.
2. In the top menu bar, click **Settings**.
3. In the **System Settings** section click **SNMP Settings**.
4. Click the **Agent Users** tab.
5. To create a new agent, click **Actions > Add User** and specify the options you want to use. When you are done, click **Apply**.
   Note: SNMP agent settings cannot be changed after you save the agent.

Field	SNMP Version	Description
Version	All	The SNMP version. Cryptographic Security Platform Vault supports version 3. Note: The rest of the fields displayed in page depend upon the selected version. Note: Starting with release 10.6.1, SNMP version 2c is no longer supported. Only SNMP version 3 is supported. During an upgrade from an earlier release to 10.6.1: • If SNMP is configured using version 2c, the version 2c configuration is removed and SNMP is disabled during the upgrade. • Any configured SNMP version 2c agent users are also deleted. • After the upgrade, you must configure SNMP version 3 and re-enable SNMP to continue using SNMP functionality. If SNMP version 3 is already configured, the existing configuration continues to function without changes. However, any associated agent users configured using version 2c are removed during the upgrade and must be recreated using SNMP version 3.
Network	2c	An optional field that restricts access to the specified IP address of a host or network. For example: `192.168.100.0/24`.
Community	2c	The community string for your SNMP server.
User	3	The user ID that should be associated with the agent.

Field	SNMP Version	Description
Security Level	3	This can be: • **No Authentication, No Privacy**—Cryptographic Security Platform Vault sends the messages in plain text and no authentication is done by the SNMP server. • **With Authentication, No Privacy**—Cryptographic Security Platform Vault sends the message in plain text but the SNMP server authenticates the message before logging it. • **With Authentication, With Privacy**—Cryptographic Security Platform Vault encrypts the message before sending it and the SNMP server authenticates the message before logging it. For encryption, Cryptographic Security Platform Vault supports AES (Advanced Encryption Standard) or DES (Data Encryption Standard).
Authentication Protocol	3	The type of authentication to use with the SNMP server if one of the authentication options is selected in the Security Level field. Cryptographic Security Platform Vault supports MD5 and SHA (Secure Hash Algorithm).
Authentication Key	3	The authentication key that Cryptographic Security Platform Vault should send to the SNMP manager if one of the authentication options is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.
Privacy Protocol	3	The privacy protocol to use if With Authentication, With Privacy is selected in the Security Level field. This can be AES or DES.
Privacy Key	3	The privacy key to use if With Authentication, With Privacy is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.

6. To delete an existing agent, select that agent then select **Actions > Delete Selected User**. To delete multiple users, enable **Multi-Select**, click the agents you want to delete, then select **Actions > Delete Selected Users**.

Configuring System-Level SNMP Traps

The system-level trap configuration is always used for alerts that affect Security Admins. It is also used for group-level alerts if no specific group-level configuration exists in Cryptographic Security Platform Vault.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.

2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **SNMP Settings**.
5. On the SNMP Settings page, specify the options you want to use.

Field	SNMP Version	Description
Enabled	All	Select True if you want Cryptographic Security Platform Vault to use this SNMP configuration.
Server	All	The hostname or IP address of the SNMP server.
Port	All	The SNMP port number. The default SNMP port is 162.
Version	All	The SNMP version. Cryptographic Security Platform Vault supports and version 3. Note: The rest of the fields displayed in page depend upon the selected version. Note: Starting with release 10.6.1, SNMP version 2c is no longer supported. Only SNMP version 3 is supported. During an upgrade from an earlier release to 10.6.1: • If SNMP is configured using version 2c, the version 2c configuration is removed and SNMP is disabled during the upgrade. • Any configured SNMP version 2c agent users are also deleted. • After the upgrade, you must configure SNMP version 3 and re-enable SNMP to continue using SNMP functionality. If SNMP version 3 is already configured, the existing configuration continues to function without changes. However, any associated agent users configured using version 2c are removed during the upgrade and must be recreated using SNMP version 3.
Community	2c	Specify the community string for your SNMP server.
User	3	The user ID that should be associated with the trap.

Field	SNMP Version	Description
Notification Type	3	This can be: • Inform—Cryptographic Security Platform Vault sends the SNMP trap and expects an acknowledgment that the trap was received in return. • Trap—Cryptographic Security Platform Vault sends the SNMP trap but does not expect an acknowledgment.
Engine ID Type	3	Choose the engine ID type from the following options: • Custom Engine ID—Choose this option if an SNMP engine ID is already configured in the SNMP Manager. This allows users to configure the same engine ID in the engine ID field. Cryptographic Security Platform Vault will send the traps with the supplied engine. • System Generated Engine ID—Choose this option if the SNMP Manager expects to receive the engine ID from the Cryptographic Security Platform Vault. The Engine ID field will be automatically filled with a system generated engine ID that cannot be edited. Updating the system generated engine ID may take a few minutes. Note: This field is only visible if the Notification Type is Trap.
Engine ID	3	If the Notification Type is Trap, enter the SNMP engine ID assigned to the SNMP manager. You can enter between 10 and 64 hexadecimal characters.

Field	SNMP Version	Description
Security Level	3	This can be: • **No Authentication, No Privacy** — Cryptographic Security Platform Vault sends the messages in plain text and no authentication is done by the SNMP server. • **With Authentication, No Privacy** — Cryptographic Security Platform Vault sends the message in plain text but the SNMP server authenticates the message before logging it. • **With Authentication, With Privacy** — Cryptographic Security Platform Vault encrypts the message before sending it and the SNMP server authenticates the message before logging it. For encryption, Cryptographic Security Platform Vault supports AES (Advanced Encryption Standard) or DES (Data Encryption Standard).
Authentication Protocol	3	The type of authentication to use with the SNMP server if one of the authentication options is selected in the Security Level field. Cryptographic Security Platform Vault supports MD5 and SHA (Secure Hash Algorithm).
Authentication Key	3	The authentication key that Cryptographic Security Platform Vault should send to the SNMP manager if one of the authentication options is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.
Privacy Protocol	3	The privacy protocol to use if With Authentication, With Privacy is selected in the Security Level field. This can be AES or DES.
Privacy Key	3	The privacy key to use if With Authentication, With Privacy is selected in the Security Level field. If you want to view the key in plain text, click the eye icon.
Agent Port	All	The port to use for all SNMP Agent Users. The default is port 161.

6. When you are finished, click **Apply**.
7. If you want to test the configuration, click **Test SNMP Settings**.
   Note: The SNMP trap must be enabled and you must apply the settings before you can test the configuration.
8. If you want to download the MIB file, click **Download MIB File**.

Downloading the SNMP MIB File

1. Log into the Cryptographic Security Platform Vault webGUI on any node in the cluster using an account with Security Admin, Cloud Admin, or Domain Admin privileges.
2. In the top menu bar, click **Settings**.
3. If your user account has:
   - Security Admin privileges, click **SNMP Settings** in the **System Settings** section and select **Actions > Download MIB File**.
   - Domain Admin or Cloud Admin privileges, click **Group SNMP Settings** in the **Group Settings** section and click **Download MIB File** at the bottom of the SNMP Settings page.

   Cryptographic Security Platform Vault downloads `HTKC-MIB.txt` to your browser's default download location.
4. Import the MIB file into your SNMP trap receiver so that the Cryptographic Security Platform Vault traps are readable in your SNMP tool. For details, see your SNMP documentation.

SNMP MIB File

The SNMP MIB (Management Information Base) file defines the properties for the managed objects in Cryptographic Security Platform Vault. The MIB file is written in an independent format and the object information it contains is organized hierarchically. OIDs (Object Identifiers) in the MIB file uniquely identify each managed object. Each OID has an address that follows the levels of the OID hierarchy.

The Enterprise OID for HyTrust is 1.3.6.1.4.1.33095. Cryptographic Security Platform Vault's relative OID is 4.

Object Model

The model for a Cryptographic Security Platform Vault MIB trap object is:

```
-- 1.3.6.1.4.1.33095.4.1.0.1
htkcKeyServerAlert NOTIFICATION-TYPE
    OBJECTS     { htkcKeyServerAlertID, htkcKeyServerAlertSeverity, htkcKeyServerAlertText,
htkcKeyServerHostname, htkcKeyServerIP, htkcDeviceHostname, htkcDeviceIP, htkcObjectName,
htkcObjectID, htkcObjectType, htkcObjectDetail }
    STATUS      current
    DESCRIPTION "An HTKC alert."
    ::= { htkcKeyServerAlerts 1 }
```

Message Fields

Message Field	Description
htkcKeyServerAlertID	The Alert ID number.
htkcKeyServerAlertSeverity	The alert severity. This can be 0 (high), 5 (medium), or 10 (low).
htkcKeyServerAlertText	The alert text.

Host Identification Fields

Field	Description
htkcKeyServerHostname	Hostname of the Cryptographic Security Platform Vault server generating the alert.
htkcKeyServerIP	IP address of the Cryptographic Security Platform Vault server generating the alert.
htkcDeviceHostname	Hostname of device for which alert is being generated. If the alert is about the Cryptographic Security Platform Vault cluster, this will be the same as `htkcKeyServerHostname`. If it is about a client object such as a VM, disk, or filesystem, this will be the hostname of the VM on which the Policy Agent is running.
htkcDeviceIP	The IP address of the device for which alert is being generated. This will either be the IP address of the Cryptographic Security Platform Vault server or the address of the client VM on which the Policy Agent is running.

Object Identification Fields

The following fields only apply if the object identity is available.

Field	Description
htkcObjectName	Name of object for which alert is being generated.
htkcObjectID	UUID of object for which alert is being generated.
htkcObjectType	Type of object for which alert is being generated.
htkcObjectDetail	JSON string containing hierarchical list of objects starting from leaf node. This is necessary for identifying the object based on name.

Example

For example, here is a sample trap for the alert stating that Virtual Machine dkw2012 has been authenticated. The alert ID is 85 and the priority is 10 (low).

```
2018-07-26 14:57:44 dkkc2 [UDP: [172.16.14.22]:19357->[0.0.0.0]:0]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (0) 0:00:00.00 SNMPv2-MIB::snmpTrapOID.0 = OID:
HTKC-MIB::htkcKeyServerAlert
   HTKC-MIB::htkcKeyServerAlertID = Gauge32: 85
   HTKC-MIB::htkcKeyServerAlertSeverity = INTEGER: low(10)
   HTKC-MIB::htkcKeyServerAlertText = STRING: "Added Virtual Machine dkw2012 (Cloud VM Set: windows),
authentication complete"
   HTKC-MIB::htkcKeyServerHostname = STRING: "dkkc2.localdomain"
   HTKC-MIB::htkcKeyServerIP = STRING: "172.16.14.22"
   HTKC-MIB::htkcDeviceHostname = "dkw2012.localdomain"
```

HTKC-MIB::htkcDeviceIP = STRING: "172.16.14.169"
HTKC-MIB::htkcObjectName = STRING: "dkw2012"
HTKC-MIB::htkcObjectID = STRING: "24bc7e36-90b6-11e8-a0fc-000c29cd584d"
HTKC-MIB::htkcObjectType = STRING: "CVM"
HTKC-MIB::htkcObjectDetail = STRING: "[{\"type\": \"CVM\", \"name\": \"dkw2012\", \"id\": \"24bc7e36-90b6-11e8-a0fc-000c29cd584d\"}, {\"type\": \"CVMSET\", \"name\": \"windows\", \"id\": \"307e83d2-90b2-11e8-a0fc-000c29cd584d\"}, {\"type\": \"GROUP\", \"name\": \"Cloud Admin Group\", \"id\": \"d2e6a25b-9096-11e8-a0fc-000c29cd584d\"}]"

Setting CSP Vault Management webGUI Alert Settings

The CSP Vault Management webGUI receives alerts for your CSP Vault managed user objects which can impact cluster performance. You can disable these alerts to improve performance.

Note: Disabling webGUI alerts does not affect SNMP or email alerts.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **WebGUI Alert Settings**.
5. On the WebGUI Alert Settings page, select one of the following:
   - Select **Enable** if you want to receive webGUI alerts.
   - Select **Disable** if you do not want to receive webGUI alerts.
6. Click **Apply**.

Using the Entrust CSP Vault System Console

When you log into the Cryptographic Security Platform Vault VM console as `htadmin`, Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console. This menu lets you configure the local Cryptographic Security Platform Vault server. In general, the changes you make here do not apply to any other node in the cluster.

The menu is a TUI (Text-based User Interface). You navigate through the TUI using the Tab key to move between fields and pressing Enter when the correct choice is highlighted. If the TUI screen has numbers at the start of the line, you can also press the corresponding number key and then press Enter to navigate through the menus.

To return to the main Entrust Cryptographic Security Platform Vault System Console screen, press Esc (Escape). Based on where you are in the menus, you may need to press Esc several times.

The Entrust Cryptographic Security Platform Vault System Console contains the following options:

Option	Name	Description
1	Manage Network Settings	View or change the current network configuration. This menu also allows you to run network diagnostic tools. For details, see Troubleshooting Network Issues.

Option	Name	Description
2	Manage htadmin and SSH Access	Manage the `htadmin` account for this Cryptographic Security Platform Vault node and enable or disable access to the Entrust Cryptographic Security Platform Vault System Console via SSH.
3	Manage Accounts	Enable or disable the full support login account (`htsupport`), the restricted login account (`htrestricted`), or the Cryptographic Security Platform Vault webGUI default account (secroot).
4	Manage HSM Client Account	If you are connecting Cryptographic Security Platform Vault to multiple HSM servers, this option allows you to configure those servers as an HA group. For details, see Hardware Security Modules with CSP Vault.
5	Download Entrust Internal Certificate	Download the Entrust-generated CA certificate being used on this Cryptographic Security Platform Vaultnode so that you can add that certificate to your web browser as a trusted site. For details, see CSP Vault Certificates.
6	Gather Diagnostic Logs	Creates a support bundle with diagnostic information and log files that Entrust Support can use to diagnose issues with your Cryptographic Security Platform Vault cluster. To create a support bundle using the webGUI, see Creating a Support Bundle with the webGUI.
7	Manage CSP Vault Management Node	Allows you to delete internal snapshots created automatically during upgrade.
8	Reboot or Shut Down CSP Vault Management Node	Reboots or shuts down the current Cryptographic Security Platform Vault node. If you plan to remove the node from the cluster or decommission it, see Removing a CSP Vault Node from a Cluster or Decommissioning a CSP Vault Node.

Option	Name	Description
9	Manage Timeouts and Appearance	View or change the current timeout for the Entrust Cryptographic Security Platform Vault System Console. After this period of time elapses with no user input, Cryptographic Security Platform Vault closes the Entrust Cryptographic Security Platform Vault System Console and returns to the system login prompt. This option also lets you toggle the 3D appearance for the Entrust Cryptographic Security Platform Vault System Console.
10	Quit TUI Session	Close the Entrust Cryptographic Security Platform Vault System Console and return to the system login prompt.

CSP Vault Cluster Maintenance

- CSP Vault Nodes and Clusters
- Viewing the Cluster Status
- Setting Cluster Options
- Switching a Master Node
- Choosing the Node Failover Order
- Startup Authentication
- CSP Vault Backup and Restore

CSP Vault Nodes and Clusters

When you install Cryptographic Security Platform Vault, the process creates a Cryptographic Security Platform Vault node that can operate singly or be joined with other Cryptographic Security Platform Vault nodes to form an active-active cluster. These nodes can be installed in different geographic locations, but they *must* be able to communicate with each other, with the Policy Agent installed on the encrypted servers associated with the cluster, and other nodes, for example KMIP, HTSV, or BYOK.

All Cryptographic Security Platform Vault nodes in a cluster share configuration settings, keys, and policy information. Changes made on one node are automatically synced to all nodes in the cluster through an encrypted object store. This provides a failover mechanism in case a Cryptographic Security Platform Vault node becomes unreachable.

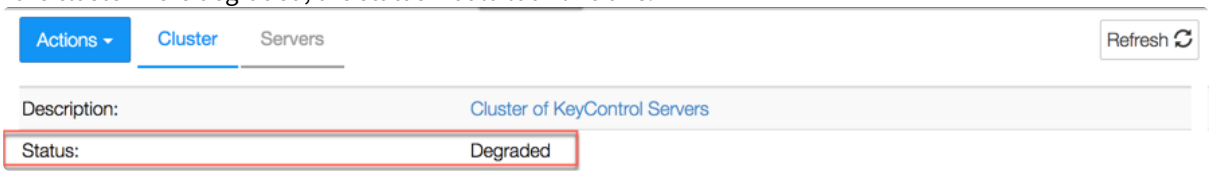
The Cryptographic Security Platform Vault nodes constantly exchange heartbeats to verify that every node in the cluster is reachable. If all nodes respond to the heartbeats, the cluster is considered "healthy". If one or more nodes stop responding for a given length of time, the cluster is considered "degraded". If a cluster is degraded, the active Cryptographic Security Platform Vault nodes can still serve requests for keys and policies from the associated Policy Agents, but you cannot make changes to the nodes in the cluster.

The heartbeat interval and status thresholds are user-configurable for the cluster. For details, see Setting Cluster Options.

Viewing the Cluster Status

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, look at the **Cluster** icon. If there is a green heart, the cluster is healthy. If there is a red X, the cluster is degraded. You can also look at the **Status** field on the **Cluster** tab.
   For example the following screenshot shows a healthy cluster containing two Cryptographic Security Platform Vault nodes.

   If the cluster were degraded, the status would look like this:



   Note: If the cluster is degraded, you cannot perform a backup.
4. To view the status of the individual servers in the cluster, click the **Servers** tab. The **Status** column shows the status for each server in the cluster:
   Maintenance—Same as cluster status, going through rolling upgrade.
   Offline—Unreachable and unavailable.
   Online—Reachable and available.
   Unavailable—Server to server connection (port 5432) works, but the KMIP Database is read-only.
   Unreachable—Unable to connect to the server (port 8443).
   Tip: To sort the unreachable servers to the top, click the Down Arrow (**v**) in the **Status** column and select **Sort Descending**.
5. A yellow star appears before the server name of the node that has been designated as the KMIP database master node. The other nodes in the cluster are replica nodes.
   All KMIP requests are forwarded to the master node for execution and when the master node's database is updated, all replica nodes receive the new updates synchronously.

Setting Cluster Options

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Specify the options that you want to use:

Option	Description
Description	A user-defined description for the cluster.

Option	Description
Status	The status of the cluster. If this is Healthy, all Cryptographic Security Platform Vault nodes are functioning normally. If this is Degraded, Cryptographic Security Platform Vault can still serve requests for keys and policies from the associated Policy Agents, but you cannot make changes to the nodes in the cluster.
Group Administrator	The Cryptographic Security Platform Vault administration group to which this cluster belongs. You cannot change this field.
Backup Hosts	The hostnames or IP addresses of systems that are allowed to access the Cryptographic Security Platform Vault backup directory through NFS. (`0.0.0.0` means any server can have access.) Any time you back up Cryptographic Security Platform Vault, it automatically stores the backup file in a folder called `/hcs/backup`. If you issue an NFS `mount` command to that directory from another server, you can access any of the backup files. Make sure these backup images are securely stored in case you ever need to restore Cryptographic Security Platform Vault. For details, see Network requirements and CSP Vault Backup and Restore.
Backup Over NFS	Whether backup over NFS is enabled. (Default: disabled.)
Cluster Operation Timeout	The amount of time that a Cryptographic Security Platform Vault node waits to receive a response from another Cryptographic Security Platform Vault node. If a response is not received by the specified timeout, the Cryptographic Security Platform Vault cluster goes into degraded mode, which indicates a network connectivity problem. Enter a value between 1 and 30 seconds. (Default: 5 seconds.) If a Cryptographic Security Platform Vault cluster frequently switches between degraded state and healthy state, you can increase this timeout. We recommend, however, that you keep the timeout as short as possible. Note: Typically, network latency is measured in milliseconds. Based on the clusters we have deployed at Amazon, the network latency from Northern California to Oregon was under ~100ms, North Virginia to Oregon was around ~200ms, and Northern California to Ireland was over ~280ms. The values varied based on time of day and the day of the week, but all values were considerably less than 5 seconds. If delays are consistently above 5 seconds, there is a network problem somewhere or a node is down.

Option	Description
Heartbeat Timeout	The number of seconds to wait for a Cryptographic Security Platform Vault heartbeat response between Cryptographic Security Platform Vault nodes in the cluster. If this time is exceeded, the heartbeat fails. Enter a value between 2 and 15 seconds. (Default: 3 seconds.)
Healthy Interval	The number of seconds between successful Cryptographic Security Platform Vault heartbeats for the cluster to be considered healthy. Enter a value between 1 and 10 seconds. (Default: 1 second.)
Degraded Interval	The number of seconds between failed Cryptographic Security Platform Vault heartbeats for the cluster to be considered degraded. Enter a value between 1 and 10 seconds. (Default: 1 second.)
Healthy Threshold	The number of successful consecutive heartbeats that must occur before Cryptographic Security Platform Vault determines that a degraded cluster is now healthy. Enter an integer between 2 and 10. (Default: 2.)
Degraded Threshold	The number of failed consecutive heartbeats that must occur before Cryptographic Security Platform Vault determines that a healthy cluster is now degraded. Enter a value between 2 and 10. (Default: 2.)

Any changes you make are communicated to all nodes in the cluster and take effect immediately.

Switching a Master Node

If you are using geographically distributed nodes in your cluster, and are having issues with performance, you can switch your master node to be the server closest to where the most data is being generated. When you switch your master node to a different node in the cluster, the cluster will automatically be placed in maintenance mode.

> Note: This is especially beneficial for the Cryptographic Security Platform Vault for Cryptographic APIs and the Cryptographic Security Platform Vault for KMIP. Other vaults will not see a noticeable improvement.

1. Log into the Cryptographic Security Platform Vault Management webGUI on any node using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Servers** tab.
5. Select one of the nodes in the cluster.
   - The current mode is displayed in the Node column with a padlock next to the text Current Node.
   - The master node is displayed in the Server Name column with a star next to the name.
6. Select **Actions > Switch Master Node**.

7. Choose the server node that you want to make the new master and click **Continue**.
   This process can take several minutes.
   Note: If the process fails, you will see an error message with a retry button. After retrying, if it fails again, there may be an underlying issue with the server, and we recommend that you contact Support.
8. When the node switch has completed, click **Close** to close the window.
   The Cryptographic Security Platform Vault switches the master node and refreshes the **Servers** tab. At this point, the cluster is no longer in maintenance mode.

Choosing the Node Failover Order

The node failover order allows you to choose which node will become the master node after the master node is removed from the cluster. If you do not select a failover order, by default the next oldest node becomes the master. For example, if you have a disaster recovery node you do not wish to become the master, you can make it the last node in the failover order.

1. Log into the Cryptographic Security Platform Vault Management webGUI on any node using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the System Settings section, click **Node Failover Order**.
5. Arrange the nodes in your preferred failover order, with the highest priority on top.
6. Click **Save**.

Startup Authentication

You can choose to enable passphrase-based startup authentication to provide further protection for the master key for all nodes in the same cluster. With passphrase-based startup authentication, the Cryptographic Security Platform Vault node will enter Recovery Mode every time it is rebooted. You will need to enter the passphrase in the Cryptographic Security Platform Vault webGUI. See the Recovery using Passphrase section in Recovering Access to CSP Vault

Startup Authentication allows Cryptographic Security Platform Vault to be used in tactical kits in hostile environments. Onsite staff can simply power off the Cryptographic Security Platform Vault nodes, which make them unusable until a passphrase or admin key is provided.

> Note: If Startup Authentication is enabled, you cannot add a new Cryptographic Security Platform Vault node. You must disable Startup Authentication first, add the new node, and then re-enable Startup Authentication.

- Enabling Startup Authentication
- Disabling Startup Authentication

Enabling Startup Authentication

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Go to the **Cluster** tab.
5. Select **Actions > Startup Authentication**.
6. In the Startup Authentication window, click **Edit**.
7. In the Passphrase Based Startup Authentication field, select **Enabled**.
8. Enter and confirm your passphrase.

The passphrase must be at least 12 characters long and include 1 digit, 1 uppercase character, 1 lowercase character, and 1 symbol.

9. Click **Apply**.

Disabling Startup Authentication

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Go to the **Cluster** tab.
5. Select **Actions > Startup Authentication**.
6. In the Startup Authentication window, click **Edit**.
7. In the Passphrase Based Startup Authentication field, select **Disabled**.
8. Click **Apply**.

CSP Vault Backup and Restore

Cryptographic Security Platform Vault stores the configuration information, keys, and objects for all Cryptographic Security Platform Vault nodes in an encrypted object store that is shared among all nodes. Any changes you make on any Cryptographic Security Platform Vault node in the cluster is automatically disseminated to the other nodes in the cluster in a secure manner. This also allows you to backup all required information from any node in the cluster.

Important: Because encryption keys are stored in the Cryptographic Security Platform Vault backup file, you should create a new backup file every time you encrypt a new disk or rekey existing disks. If you restore Cryptographic Security Platform Vault from a backup file made before the disks were encrypted or rekeyed, the new keys will be lost and you will not be able to access the encrypted data.

You can back up Cryptographic Security Platform Vault using:

- The Cryptographic Security Platform Vault webGUI. The encrypted backup files Cryptographic Security Platform Vault creates can be downloaded locally or accessed through NFS on authorized servers. For details, see Backing Up CSP Vault Through the webGUI.
- A third-party application that can take and restore system snapshots. You can restore Cryptographic Security Platform Vault at any time from a previous snapshot, but if any part of the VM changes you may be required to recover the Admin key as described in Recovering Access to CSP Vault.

Note: If the cluster is degraded, you cannot perform a backup.

You can restore Cryptographic Security Platform Vault from a backup file using the Cryptographic Security Platform Vault webGUI. For details, see Restoring CSP Vault Through the webGUI.

Automatic Backup Feature

Cryptographic Security Platform Vault automatically creates a backup file once every 12 hours as long as the cluster is healthy. If this is the first time the automatic backup has completed successfully since the node was first initialized or restarted, Cryptographic Security Platform Vault records this information in the audit log. It does *not* send an alert or email to any Cryptographic Security Platform Vault users. It also does not record any subsequent successful backups.

The automatic backup schedule may change based on the following rules:

- If the cluster is in a degraded state, no automatic backup is attempted. The cluster must be healthy in order for Cryptographic Security Platform Vault to create a backup file.
- If the cluster is healthy but the automatic backup fails for some reason, Cryptographic Security Platform Vault retries the backup operation every hour. The first time the automatic backup fails Cryptographic

Security Platform Vault records this information in the audit log and alerts all Cryptographic Security Platform Vault accounts with Domain Admin privileges. It does *not* record subsequent failed backup attempts.
- Changes to the Cryptographic Security Platform Vault configuration may trigger an automatic backup, but it is better to backup Cryptographic Security Platform Vault manually whenever you make changes to be certain that you have an up-to-date backup file available.

- Backing Up CSP Vault Through the webGUI
- Removing a CSP Vault Node from a Cluster
- Changing the IP Address for a Node
- Rebooting a CSP Vault Node
- Decommissioning a CSP Vault Node
- Enabling or Disabling the Support Login
- Accessing CSP Vault Backup Files

Backing Up CSP Vault Through the webGUI

This procedure creates an encrypted backup file that can be downloaded through NFS on authorized servers or downloaded via the Cryptographic Security Platform Vault webGUI to the administrator's default download directory.

The backup file can later be used to restore Cryptographic Security Platform Vault to the state it was in when the backup was taken.

Before You Begin

If you have an enabled a Linux Access Control Policy on any of the VMs registered with Cryptographic Security Platform Vault, you must disable those Access Control Policies *before*you create the backup file. You can then re-enable the Access Control Policies after the backup is complete.

If you create the backup with any Linux Access Control Policies still active, you may be unable to access those VMs when you restore your Cryptographic Security Platform Vaultconfiguration from the backup file.

For details, see Removing Access Controls from a Disk.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Go to the **Cluster** tab.
5. If you want to make the backup file available through NFS:
    a. Make sure the **Backup Over NFS** option is set to **Enabled**.
    b. Verify the IP addresses in the **Backup Hosts** field. If you want any server to have access to the backup directory, enter `0.0.0.0` .
6. Select **Actions > KeyControl Backup**. Cryptographic Security Platform Vault displays the latest backup information if one exists.
7. Click **Perform Backup**. Cryptographic Security Platform Vault creates a new backup file in the backup directory on the server and updates the information in this dialog box.
8. If you want to download the backup file locally, click **Download**. Cryptographic Security Platform Vault saves the encrypted backup file to your browser's default download location. The filename is in the format `<server-name>-<product_version><-datetimestamp>-<admin_key_version>.bu` .

If you want to access the backup file through NFS, log into one of the servers listed in the **Backup Hosts** field and mount the directory using the `mount` command. For example, if your Cryptographic Security Platform Vault node IP address is `192.168.140.135`, you would enter:

```
# mount -t nfs 192.168.140.135:/hcs/backup /backup
# ls -l /backup
total 506
lrwxrwxrwx  1 root root     30 Dec 16 14:57 htkc.bu -> testkc01-5.1-20191216092703-4.bu
-rw-r--r--  1 root root 191776 Dec 16 14:57 testkc01-5.1-20191216092703-4.bu
```

9. When you are done, click **Close**.

What to Do Next

If you disabled any Linux Access Control Policies for the backup, you can now re-enable those policies on the Linux VMs.

Backup and Restore Using the API

- Backup Image Status
- Create Object Store Backup Image
- Creating a Backup User
- Download Object Store Backup Image
- Restore Backup Image
- Restoring CSP Vault Through the webGUI
- Joining or Re-joining a Cryptographic Security Platform Vault Cluster
- Upload Backup Image

Backup Image Status

Returns information about backup image created using Create Object Store Backup Image.

Request

Method	URI
GET	v5/system_backup_status/

Privileges Required

DOMAIN_ADMIN or BACKUP_USER

Parameters

None.

Response

Name	Type	Example
backup_time	string	Thu Aug 3 21:19:21 2017
backup_exists	boolean	true

Name	Type	Example
backup_size	integer	1955390
backup_sha256	string	6286ea999404c730bfc6d9ba2629b216cd6debd8dd38cb4d1318de1025c66b76
result	string	success

Errors

Reason	Example
Unable to fetch backup information	Failed to retrieve backup details.

Create Object Store Backup Image

Creates a Cryptographic Security Platform Vault object store backup image on the Cryptographic Security Platform Vault node.

If you have an enabled a Linux Access Control Policy on any of the VMs registered with Cryptographic Security Platform Vault, you must disable those Access Control Policies *before*you create the backup file. You can then re-enable the Access Control Policies after the backup is complete.

If you create the backup with any Linux Access Control Policies still active, you may be unable to access those VMs when you restore your Cryptographic Security Platform Vaultconfiguration from the backup file.

Request

Method	URI
POST	v5/system_backup/

Privileges Required

DOMAIN_ADMIN or BACKUP_USER

Parameters

None.

Response

Name	Type	Example
result	string	success

Errors

Reason	Example
Backup image creation failed	Failed to create backup. No space available.

Creating a Backup User

Security Admin users can generate and download backup files. If you would prefer these actions to be performed by a more restricted account, for example if you are calling the APIs from a scheduled task, you can create a dedicated backup user. Backup users are users with the BACKUP_USER privilege, who can create, download, and view backups in both the webGUI and the API. Users who only have this role do not have any other admin access, and cannot access any other restricted APIs.

To create a user with the BACKUP_USER privilege, use a curl command similar to the following:

Copy

```
v=$(curl -s -k -d 'username=secroot&password=<password>' https://<IP-address>/v5/kc/login/ | jq .access_token| sed -e 's/"//g'); echo $v
curl -s -k https://<IP-address/v5/users/?access_token=$v -H 'Content-type: application/json' -d '{"email":"<backup@example.com>", "full_name":"<backup>", "login_name":"<backup@example.com>", "privileges": ["BACKUP_USER"], "account_enable":"Active"}' | tee qqq | jq .
```

Where:

- <password> is the password for the secroot user.
- <IP-address> is the IP address for your Cryptographic Security Platform Vault.
- <backup@example.com> is the email address to be used by the backup user.
- <backup> is the full name of the backup user.

Download Object Store Backup Image

Downloads the latest Cryptographic Security Platform Vault object store backup image available. The backup image can be created through the Cryptographic Security Platform Vault Management webGUI or the Create Object Store Backup Image method.

Request

Method	URI
GET	v5/system_backup/

Privileges Required

DOMAIN_ADMIN.

Parameters

None.

Response

Cryptographic Security Platform Vault backup file.

Errors

Reason	Example
Object store backup image not found	No backup available.

Restore Backup Image

This request restores Cryptographic Security Platform Vault using the backup file uploaded with the Cryptographic Security Platform Vault webGUI or the Upload Backup Imagemethod.

Warning: This is a destructive operation and should be used with care. If there has been is a hardware change since the backup file was created, you will be prompted to perform master key recovery after the restore operation has completed.

Request

Method	URI
POST	v5/restore_image/

Privileges Required

DOMAIN_ADMIN.

Parameters

None.

Response

Name	Type	Example
result	string	success

Errors

Reason	Example
Failed to restore object store image.	Multiple KeyControl nodes in the cluster. Excess KeyControl nodes must be removed before restore.

Restoring CSP Vault Through the webGUI

Restoring from a KeyControl backup should only be needed if there is a catastrophic failure in the Cryptographic Security Platform Vault cluster. If one Cryptographic Security Platform Vault node becomes unusable, for example due to hardware failures, simply remove the node from the cluster and add a new node.

Warning: Restore is a destructive process. Any changes made to objects created since the backup image was taken will be lost. This includes keys, policies, and Cryptographic Security Platform Vault user accounts. If the Cryptographic Security Platform Vault SSL certificate was changed since the backup was taken, the

older SSL certificate will be restored along with the rest of the system and the current SSL certificate will be discarded.

Custom SSL certificates for internal and external webservers will be restored only if the IP address specified in the certificate matches the Cryptographic Security Platform Vault IP address.

Note: If you are restoring a backup on Cryptographic Security Platform Vault with nShield HSM configured, you must do the following first:

- Initialize the Cryptographic Security Platform Vault node that you plan to restore to and copy its keyhash to the clipboard. You will need this keyhash to configure the HSM.
- Configure the nShield HSM to the new node before you start the restore process.
- Restore using a backup from the original Cryptographic Security Platform Vault.
- After the restore process, Cryptographic Security Platform Vault will go through admin key recovery.
- Select to recover the admin key using HSM.
- Provide the softcard name and softcard password used on the Cryptographic Security Platform Vault where the backup was created.
- After recovery, log in to the newly deployed Cryptographic Security Platform Vault and check that the admin key is available in the HSM.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Cluster**.
3. If there are any other nodes in this cluster, you must remove them before you restore the node. To do so:
    a. Click on the **Servers** tab.
    b. Click on each of the other nodes in the cluster and select **Actions > Remove**.
    c. Click **Proceed** at the prompt to confirm the request.
4. Go to the **Cluster** tab.
5. Select **Actions > Restore**.
6. Click **Browse** and select the backup file from which you want to restore Cryptographic Security Platform Vault. The name of the selected file appears next to the **Browse**button.
7. Click **Verify Image**. Cryptographic Security Platform Vault uploads the file and verifies that it is a valid backup file. It also displays a hint stating which Admin Key generation count goes with this backup file in case you need to upload the matching Admin Key parts. For example:
   Hint: Keypart generation version for this backup image is 16.
   For details, see Admin Keys.
8. Click **Restore Image**.
9. Click **Proceed** at the prompt to confirm the request. Cryptographic Security Platform Vault restores the system information from the backup file and reboots the server.
10. Verify the restoration by logging back into the Cryptographic Security Platform Vault Management webGUI. **Important:** Remember that all user account information has been reverted back to whatever it was when the backup was taken. That means your account may not exist or that the password may have changed.
11. If the hardware has changed since the backup was taken, Cryptographic Security Platform Vault presents you with additional options.

Option	Description
Recovery using Keypart upload	Allows you to recover the Admin key by uploading the parts from local files. You must upload the required number of parts of the Admin key within 10 minutes to use this method. Important: All Admin key parts must have the key generation count that was valid when the back up was taken. For details, see Admin Keys.
Recovery from External key server	Allows you to recover the Admin key by connecting to a server or HSM (Hardware Security Module).
Decommission	Tells Cryptographic Security Platform Vault to decommission the server. For more information, see Decommissioning a Cryptographic Security Platform Vault Node.

12. If you removed any nodes from the cluster, re-join them as described in Joining or Re-joining a Cryptographic Security Platform Vault Cluster.

Joining or Re-joining a Cryptographic Security Platform Vault Cluster

When you install Cryptographic Security Platform Vault, you can specify whether you want to configure the node as the first node in the system (standalone) or add it to an existing cluster.

If you ever need to change the node's cluster assignment, or you need to re-join a node with its previous cluster, you can do so using the Cryptographic Security Platform Vault webGUI installed on the node. You do not need to re-install the Cryptographic Security Platform Vault software.

Warning: When a node is added to a cluster, any existing configuration data and encryption keys are permanently deleted and cannot be restored. If this node was previously part of a different cluster or was used in standalone mode, make sure you do not need the encryption keys stored on this node before you add it to the new cluster.

Related Topics

Joining a Cryptographic Security Platform Vault Cluster

Re-Joining a Cryptographic Security Platform Vault Cluster

Joining a CSP Vault Cluster

The following procedure describes how to configure a newly deployed node to join an existing Cryptographic Security Platform Vault cluster.

Before You Begin

- Make sure you know the IP address of any Cryptographic Security Platform Vault node that is already part of the cluster you want to join.
- If the node is currently part of a different cluster, you should remove the node from the original cluster so that the original cluster does not become degraded. For details, see Removing a CSP Vault Node from a Cluster.
- Make sure that you have tested the port connection between the joining node and the existing cluster node to ensure that they can communicate with each other. You can test the port connection through the console.

- If you are re-joining a node to an existing cluster and you are using an externally signed SSL certificate for Cryptographic Security Platform Vault, make sure that you use the same hostname for the Cryptographic Security Platform Vault node that it had originally. If you change the hostname, you will need to reinstall the externally signed SSL certificate on that node.
- A Cryptographic Security Platform Vault node cannot be joined to an existing Cryptographic Security Platform Vault cluster if the internal web server of the joining node is configured with a custom SSL certificate.
- Entrust recommends that you configure the Cryptographic Security Platform Vault node with a private IP address.

Procedure

1. Log into the webGUI on the Cryptographic Security Platform Vault node you want to join with the cluster.
2. Review the EULA (end user license agreement). When you are done, click **I Agree** to accept the license terms.
3. On the Welcome to Cryptographic Security Platform Vault screen, click **Join an Existing Cluster**.
   The Join Existing Cluster window displays.
4. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   - A passphrase to use during the joining process. Passphrase requirements are configured by a Cryptographic Security Platform Vault administrator in the System Settings. This phrase is a temporary string used to encrypt the initial communication between this node and the existing cluster.
   - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
5. Click **Continue**.
6. On the Download CSR page, click **Generate and Download CSR**.
7. Click **Continue**.
8. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
9. Select **Actions > Add a Node**.
10. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.
11. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
12. Click **OK** to close the Add a Node window.
13. Return to the new node and click **Continue**.
14. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the private IP address of any node in the existing cluster, and enter the passphrase that you selected.
    Note: Cryptographic Security Platform Vault uses the private IP address of its cluster members for cluster communication, such as heartbeat and object store synchronization.
15. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
16. When the node has successfully restarted, click **Login**.

What to Do Next

If necessary, update the list of Cryptographic Security Platform Vault IP addresses on the VMs associated with this cluster. If you are maintaining the list of IP addresses on the VMs, see Updating Cryptographic Security Platform Vault Node IP Addresses on an Individual VM. If you are using Cluster Node Mappings, see Changing a Cluster Node Mapping.

If you are using an HSM, see the appropriate link to rejoin the cluster:

- Adding a Cryptographic Security Platform Vault Node to a Cluster using an nShield HSM client
- Adding a Cryptographic Security Platform Vault Node to an Existing Luna HSM Configuration

Re-Joining a CSP Vault Cluster

The following procedure describes how to configure a node that has been in use as either a standalone node or part of a cluster to join another existing Cryptographic Security Platform Vault cluster.

Important: This process will destroy all data on the node.

Before You Begin

- Make sure you know the IP address of any Cryptographic Security Platform Vault node that is already part of the cluster you want to join.
- If the node is currently part of a different cluster, you should remove the node from the original cluster so that the original cluster does not become degraded. For details, see Removing a CSP Vault Node from a Cluster.
- If you are re-joining a node to an existing cluster and you are using an externally signed SSL certificate for Cryptographic Security Platform Vault, make sure that you use the same hostname for the Cryptographic Security Platform Vault node that it had originally. If you change the hostname, you will need to reinstall the externally signed SSL certificate on that node.

Procedure

1. Log into the webGUI on the Cryptographic Security Platform Vault node you want to join with the cluster.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Select **Actions > Join a Cluster**.
   The Join Existing Cluster window displays.
5. On the Get Started page, review the overview information to determine that you are ready to begin. This includes:
   - Access to the cluster you are joining the node to. We recommend that you open the webGUI for the cluster in a different tab or browser window.
   - Permissions on both this node and the cluster node so you can download and import the required certificates and files.
   - A passphrase to use during the joining process. The passphrase must contain 12 alphanumeric characters. It *cannot* contain spaces or special characters. This phrase is a temporary string used to encrypt the initial communication between this node and the existing Cryptographic Security Platform Vault cluster.
   - Verifying that both this node and the cluster node are running the same Cryptographic Security Platform Vault version and build. The version number for the cluster node is on the **Settings > System Upgrade** page.
6. Confirm that you understand that all existing data on this node will be deleted by typing "delete my data".
7. Click **Continue**.
8. On the Download CSR page, click **Generate and Download CSR**.
9. Click **Continue**.
10. Switch to one of the existing nodes in the cluster and navigate to the Cluster page.
11. Select **Actions > Add a Node**.
12. On the Add a Node window, upload the CSR that you downloaded from the new node (in .pem format) and enter a passphrase to use during the joining process.

13. Click **Save and Download Bundle** to download the certificate bundle from the cluster node.
    The certificate bundle is a .zip file you must unpack. It contains both an encrypted SSL certificate in .p12 format and a CA certificate in .pem format.
14. Click **OK** to close the Add a Node window.
15. Return to the new node and click **Continue**.
16. On the Node page, upload the encrypted SSL certificate and CA certificate that you downloaded from the cluster node, enter the IP address or hostname of any node in the existing cluster, and enter the passphrase that you selected.
17. Click **Join**.
    During the joining process, a status page is displayed on the new node. Do not refresh the browser while this is in process.
    The cluster will automatically be placed in maintenance mode.
    The node will restart after the join is complete.
18. When the node has successfully restarted, click **Login**.

What to Do Next

If necessary, update the list of Cryptographic Security Platform Vault IP addresses on the VMs associated with this cluster. If you are maintaining the list of IP addresses on the VMs, see Updating Cryptographic Security Platform Vault Node IP Addresses on an Individual VM. If you are using Cluster Node Mappings, see Changing a Cluster Node Mapping.

If you are using an HSM, see the appropriate link to rejoin the cluster:

- Adding a Cryptographic Security Platform Vault Node to a Cluster using an nShield HSM client
- Adding a Cryptographic Security Platform Vault Node to an Existing Luna HSM Configuration

Upload Backup Image

This is the first step of restoring Cryptographic Security Platform Vault. This request uploads and verifies the Cryptographic Security Platform Vault backup file that you want to use.

Request

Method	URI
POST	v5/verify_image/

Privileges Required

DOMAIN_ADMIN.

Parameters

Name	Type	Example
file	Object store backup image	KC2.localdomain-201708032119.bu

Response

Name	Type	Example
result	string	success

Name	Type	Example
keypart_generation	string	6

Errors

Reason	Example
Failed to verify backup image.	Image verification failed.

Removing a CSP Vault Node from a Cluster

You can remove and later re-join nodes that are unreachable for an extended time due to maintenance or other issues. Because there may be multiple administrators for this appliance, please ensure that all other administrators are aware of any changes that you make to the cluster.

1. Log into the Cryptographic Security Platform Vault Management webGUI on any node you are *not* removing using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Click the **Servers** tab.
5. Select the node or nodes that you want to remove.
   Important: All unreachable nodes need to be removed together. To remove multiple nodes, click the **Multi-Select** checkbox at the top-right of the page.
6. Select **Actions > Remove**.
7. Click **Proceed** at the prompt to confirm the request.
8. Cryptographic Security Platform Vault removes the node and refreshes the **Servers** tab.

What to Do Next

If you want to rejoin the node to an existing Cryptographic Security Platform Vault cluster, see Joining or Re-joining a CSP Vault Cluster.

If you want to remove the node permanently, see Decommissioning a CSP Vault Node.

Changing the IP Address for a Node

After you have deployed a Cryptographic Security Platform Vault node, you cannot change its IP address, hostname, or domain name. In order to work around this restriction, you can do the following:

1. Deploy a new Cryptographic Security Platform Vault node using the IP address and hostname you want to use and join it with the original node to form a cluster.
   For details, see Installation Overview.
2. Update any Cluster Node Mappings that you have defined in your environment to use the new node. If you are replacing a standalone node, you must then make sure the new Node Mapping information has been successfully disseminated to all registered VMs before you continue. For more information, see High Availability Between a VM and the CSP Vault Cluster.
3. If there are any VMs that are registered directly with the old Cryptographic Security Platform Vault node, you need to update the Cryptographic Security Platform Vault list on those VMs or create a Cluster Node Mapping and assign that Node Mapping to the VMs. For details see Updating CSP Vault Node IP Addresses on an Individual VM or Managing the Cluster Node Mapping on a VM.

Tip: We highly recommend that you use a Cluster Node Mapping instead of registering VMs directly with Cryptographic Security Platform Vault to provide more flexibility and high availability between the VM and Cryptographic Security Platform Vault.

4. When all VMs have been updated to use the new Cryptographic Security Platform Vault IP address, you can decommission the old Cryptographic Security Platform Vault node as described in Decommissioning a CSP Vault Node or you can simply remove it from the cluster and destroy the VM as described in Removing a CSP Vault Node from a Cluster.

Rebooting a CSP Vault Node

You can only reboot the node that you are currently using.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Go to the **Servers** tab.
5. Select **Actions > System Reboot**.
6. Click **Proceed** to acknowledge the warning message.

Decommissioning a CSP Vault Node

Before You Begin

- Make sure the node is not part of a cluster before you decommision it. For details, see Removing a CSP Vault Node from a Cluster.
- Make sure you have access to all of the key parts for the Admin key that was generated for this system. All of the parts need to be uploaded within 10 minutes of the first file upload in order for the decommission to work.
  If there are multiple system administrators, each administrator has one of the key parts. You can either collect the parts and have one administrator upload them all or you can have each administrator log in and upload their part simultaneously.
  For this procedure you *must* use the Admin Key parts that were sent to the Security Administrators. You cannot use the Admin Key stored on an external key server.

Warning: When you decommission a Cryptographic Security Platform Vault node, Cryptographic Security Platform Vault uses zeroization to completely erase the data on the disks where the Cryptographic Security Platform Vault software and the object store are located. This is a non-reversible procedure.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI on the node you want to decommision using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **System Settings** section, click **System Decommission**.
5. Click **Browse** to upload the first part of the admin key. Navigate to the key part and click **Choose**. The filename of the key part replaces the text of the **Browse** button.
6. Click **Upload File**.
7. If there is only one admin key part, Cryptographic Security Platform Vault immediately logs you out of the system and zeroes out the disks associated with the Cryptographic Security Platform Vault node. If there are multiple key parts, Cryptographic Security Platform Vault starts a 10 minute timer. All admin key parts must be uploaded within the 10 minutes before Cryptographic Security Platform Vault will decommission the node.

8. If you need to restart the process, click **Reset**. You will need to re-upload all key parts to complete the process.

Enabling or Disabling the Support Login

You must enable support accounts before support personnel from Entrust can access your system. When the account is enabled, support personnel have full access to the system to carry out diagnosis and repairs in exceptional situations.

You can disable the support account after using, for example, after a successful upgrade, or else the support login will automatically be disabled after 24 hours.

1. Log into the Cryptographic Security Platform Vault webGUI using an account with Security Administrator or Cloud Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Click the **Servers** tab.
4. Select the node or nodes that you want to modify.
5. Select **Actions** and under the Support Login Settings section, select **- Full Access**.
   Note: If restricted access is all that is required, you can select **- Restricted Access** instead.
6. On the Full Support Login Settings page, check the Enable Full Support Login checkbox.
7. Enter and confirm the password for the support login.
   The password must be at least 8 characters long, including 1 digit, 1 uppercase character, 1 lowercase character, and 1 symbol.
8. Click **Save**.
9. If the support login is enabled, you can disable it by checking the Disable Full Support Login checkbox and clicking **Save**.

Accessing CSP Vault Backup Files

If you want to access an existing Cryptographic Security Platform Vault backup file, you can use the Cryptographic Security Platform Vault Management webGUI, the Entrust Cryptographic Security Platform Vault API or, if you have configured an NFS server, you can use NFS.

The following sections describe how to access the backup file through the webGUI and NFS.

Cryptographic Security Platform Vault Management webGUI Access

1. Log into the Cryptographic Security Platform Vault Management webGUI with your standard account credentials.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Cluster**.
4. Go to the **Cluster** tab.
5. Select **Actions > KeyControl Backup**. Cryptographic Security Platform Vault displays the latest backup information if one exists.
6. Click **Download**. Cryptographic Security Platform Vault saves the encrypted backup file to your browser's default download location. The filename is in the format `<server-name>-<product_version>-<datetimestamp>-<admin_key_version>.bu`.
7. Click **Close**.

NFS Access

To access the backup file through NFS, log into one of the Backup Host servers configured for the cluster and mount the directory using the `mount` command. For example, if your Cryptographic Security Platform Vault node IP address is `192.168.140.135`, you would enter:

```
# mount -t nfs 192.168.140.135:/hcs/backup /backup
# ls -l /backup
total 506
lrwxrwxrwx  1 root root     30 Dec 16 14:57 htkc.bu -> testkc01-5.1-20191216092703-4.bu
-rw-r--r--  1 root root 191776 Dec 16 14:57 testkc01-5.1-20191216092703-4.bu
```

CSP Vault System Maintenance and Troubleshooting

- CSP Vault Activity Tracking
- Moving a CSP Vault Node to a New Server in a Multi-Node Environment
- Moving a CSP Vault Node to a New Server in a Single Node Environment
- Increasing CSP Vault Storage in a VM
- VM Handlers for Attach/Detach in Linux
- VM Handlers for Attach/Detach in Windows
- Upgrading to a New Hardware Signature Format
- Troubleshooting Network Issues
- Cleaning Up Stale Tasks
- Support Access and Log Files

CSP Vault Activity Tracking

Cryptographic Security Platform Vault tracks all activity on the system in the audit log. Users can export the audit log from the webGUI but they cannot change it in any way. For security reasons, Cryptographic Security Platform Vault tracks most of the events in the system.

For important events, Cryptographic Security Platform Vault makes an entry in the audit log and also raises an alert. Users can look at the Alert tab in the webGUI to get a quick overview of the major events that have taken place in the system. webGUI users can delete an alert from their local view, but the same alert will still be visible to other Cryptographic Security Platform Vault users who have the same Cryptographic Security Platform Vault permissions.

Cryptographic Security Platform Vault categorizes audit log messages and alerts based on both the user's administrative roles (Cloud Admin, Domain Admin, and Security Admin) and the groups to which the user belongs. When a user logs into the webGUI, they can see the audit log messages and alerts generated by their groups that correspond to the privileges associated with their account. For example:

- If a Security Administrator logs in, they will see an alert if a user account is locked because a user exceeded the maximum number of consecutive failed login attempts. Security Administrators are not assigned to a group, so all Security Administrators see all security alerts.
- If a Cloud Administrator logs in, they will see an alert if a new Cloud VM Set has been created in one of the Cloud VM Sets in their associated groups. They will not see an alert about Cloud VM Sets created in other groups.
- If a Domain Administrator logs in, they will see an alert if a new Cryptographic Security Platform Vault node has been added to the cluster.
- If someone with Security, Cloud, and Domain Admin privileges logs in, they will see all three of the alerts mentioned above.

In addition to viewing alerts in the webGUI, administrators can also receive alerts by email depending on how the system is configured. For details, see Setting Email Server Preferences.

For a list of audit log messages, see CSP Vault Audit Messages.

- Managing Alerts
- Viewing the Audit Log
- Configuring Audit Log Settings

- Exporting the Audit Log

Managing Alerts

Cryptographic Security Platform Vault categorizes alerts based on both the user's administrative roles (Cloud Admin, Domain Admin, and Security Admin) and the groups to which the user belongs. When a user logs into the webGUI, they can see the alerts generated by their groups that correspond to the privileges associated with their account. For details, see CSP Vault Activity Tracking.

> Note: Cryptographic Security Platform Vault keeps a maximum of 500 alerts per user. If this amount is exceeded, Cryptographic Security Platform Vault deletes the oldest alert when a new alert is generated.

Viewing Alerts

In the top menu bar, click Alerts.

Copying and Filtering Alerts

To copy an alert to the clipboard, click it and use Ctrl+C on Windows or Command+C on the Mac. If you want to copy multiple alerts, click the Multi-Select button and then left-click on the alerts you want to select.

To filter the alert list:

1. In the **Filter** drop-down list, select the field that you want to filter on.
2. Enter the filter text in the text box.
3. Click the Plus (**+**) sign at the end of the field to add the filter.
4. Repeat this process to add additional filters and further refine the display.

Search tips for the available field types:

- Message—Searches the text displayed in the **Message** column.
- Date—Filters the list based on the date the alert was created. You can only select one day per filter. Cryptographic Security Platform Vault does not support searching on a range of dates.

Deleting Alerts

To delete one or more alerts from your local view:

1. Select the alerts you want to delete.
2. Select **Actions > Delete Alerts**.

If you need to see an alert you previously deleted, you can find it in the Audit Log. For details, see Viewing the Audit Log.

Viewing the Audit Log

CSP Vault generates detailed records that document activities and events associated with the Key Management System. Among these records, audit logs capture auditable events and can be accessed through multiple interfaces of Cryptographic Security Platform Vault, including the REST API, CLI, or the GUI. These logs serve as a comprehensive, chronological archive, facilitating the tracking of changes, access, and various operations. They are frequently utilized for understanding system behavior, diagnosing issues, and conducting security audits.

Audit logs offer flexibility in how they are consumed, and they can be exported in user-friendly CSV or XML formats or forwarded to an external syslog server for centralized logging and analysis.

The following table describes the audit log parameters:

Parameters	Description
Time	Date and time when the event was created.
Type	The severity of the record. The severity types are: • INFORMATION • CRITICAL • WARNING • ERROR
User	The user who initiated the operation.
Message	The operation and details associated with the operation performed.

How you access the audit log in the webGUI depends on which vault you using.

- For the Cryptographic Security Platform Vault Management webGUI, the Cryptographic Security Platform Vault for Cloud Keys webGUI, the Cryptographic Security Platform Vault for Databases webGUI, or the Cryptographic Security Platform Vault for VM Encryption webGUI, click **Audit Log** in the top menu bar.
- For the Cryptographic Security Platform Vault for Cryptographic APIs webGUI, the Cryptographic Security Platform Vault for KMIP webGUI, or the Cryptographic Security Platform Vault for Secrets webGUI, click **Audit Log** on the main page.

To view the details for a given message, click the Expand button > at the end of the row.

To copy a message to the clipboard, click it and use Ctrl+C on Windows or Command+C on the Mac. If you want to copy multiple rows, click the Multi-Select button and then left-click on the rows you want to select. If you want to export the entire audit log in CSV or XML format, see Exporting the Audit Log.

You can filter the audit log messages displayed using one or more text searches forming an AND search string. The webGUI displays the selected filters below the field. To remove a particular filter, click the X following the filter name.

All searches are partial word and case-insensitive. So "cre" would match "Create" and "Secret".

You cannot use regular expressions and you cannot specify a NOT condition in the search string. Complex searches can only be done through the API.

To filter the message list:

1. In the **Filter** drop-down list, select the field you want to filter on.
2. Enter the filter text in the text box.
3. Click the Plus (**+**) sign at the end of the field to add the filter.
4. Repeat this process to add additional filters and further refine the display.

Search Tips by Field Type

- Category—Common categories are Security and Clusters.
- Message—Searches the text displayed in the **Message** column.
- Date—Filters the list based on the date the log entry was created. You can only select one day per filter. Cryptographic Security Platform Vault does not support searching on a range of dates.
- Group—The name of the associated group, such as KeyControl Admin Group and Cloud Admin Group.
- Host—The hostname of the server where the activity took place. In general this will be one of the Cryptographic Security Platform Vault nodes.

- ID—The message ID. For example, if you want to see all messages where a Cloud VM Set was created, you would enter "12" in the filter field.
- User—Searches the text shown in the **User** column. For a user-defined webGUI account, this will be the Full Name specified for the account. For security reasons, the user login ID is not saved in the Audit Log.

Configuring Audit Log Settings

You can choose to retain audit logs depending on size, retention period, or both.

- The audit log retention policy (by size or retention period) is enforced every 10 minutes starting from system startup.
- Audit log retention by size is approximate:
  - If an audit is added to the log while the system is in this enforcement period, the size of the audit log may increase temporarily.
  - If an audit is in process when the enforced size is reached, then that audit is retained in the log and the rest are deleted.

If you want to use an external syslog server, see Configuring Syslog Server Settings.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top menu bar, click **Settings**.
3. In the **General Settings** section, click **Audit Log** and specify the options you want to use. The Cryptographic Security Platform Vault Management webGUI automatically saves your changes as you make them.

Option	Description
Log Retention	The Cryptographic Security Platform Vault webGUI displays the number of days for which it will keep old audit log messages. The default is 90 days. Click this value to set a new retention time. The minimum retention time allowed is 30 days. If you check the Retain All checkbox, then Cryptographic Security Platform Vault will never delete old messages from the audit log.
Maximum Log Size	The default is Unlimited, which means Cryptographic Security Platform Vault never deletes old messages from the audit log based on the size of log. To change this value, click Unlimited then enter an integer and select MB, GB, or TB in the units list box. The log size must be *at least* 10 MB. If you have changed the size and want to restore the default Unlimited setting, specify 0 (zero) in this field.

Exporting the Audit Log

You can export the audit log in CSV (comma-separated value) or XML format. Cryptographic Security Platform Vault stores the audit log until you can download it.

CSV Format

To download the entire audit log or selected audit log rows in CSV (comma-separated value) format:

1. If you want to download a subset of audit log messages, select the appropriate rows. If you have filtered the list, you can export just the filtered items without selecting them first.
2. Select **Actions > Export**.
3. Select **CSV** in the **Format Type** drop-down list.
4. In the **Which Rows?** drop-down list, select:
   All Loaded—Downloads the audit log messages that match the selected filters, if any. If there are no filters, this option downloads all audit log messages.
   Selected—Downloads just those audit log messages selected in the webGUI using the **Multi-Select** option.
5. In the **Which Columns?** drop-down list, select **All**.
6. Click **Generate**.
   Cryptographic Security Platform Vault generates a file called `htdc-auditlog-datetimestamp.csv`.
   The `datetimestamp` is in the format month, day, year, hour, minute, seconds, AM/PM. For example, `htdc-auditlog-4-6-2017--11_41_49-AM.csv`.
7. After the audit log has finished generating, click **Download**.

XML Format

1. Select **Actions > Export**.
2. Select **XML** in the **Format Type** drop-down list.
3. Click **Generate**.
   Cryptographic Security Platform Vault generates a file called `htdc-auditlog-datetimestamp.xml`.
   The `datetimestamp` is in the format month, day, year, hour, minute, seconds, AM/PM. For example, `htdc-auditlog-4-6-2017--11_41_49-AM.xml`.
4. After the audit log has finished generating, click **Download**.

Moving a CSP Vault Node to a New Server in a Multi-Node Environment

If you want to move a CSP Vault node to a different server, you can simply remove the old server and then install the Cryptographic Security Platform Vault software on the new server and join the new server to the cluster so that the object store is copied to the new server and all your configuration settings are retained. As long as one node remains in the cluster, you can change the other servers out as needed.

> Note: If you want to move a Cryptographic Security Platform Vault node in a single-node system, see Moving a CSP Vault Node to a New Server in a Single Node Environment.

Procedure

1. Log into the Cryptographic Security Platform Vault Management webGUI on any node you are *not* moving using an account with Domain Admin privileges.
2. In the top menu bar, click **Cluster**.
3. Click the **Servers** tab.
4. Select the Cryptographic Security Platform Vault node that you want to move and select **Actions > Remove**.
5. Log into the existing server as `htadmin`.
   Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
6. Select **Shutdown System** from the Entrust Cryptographic Security Platform Vault System Console.
7. Optionally, uninstall Cryptographic Security Platform Vault as described in Decommissioning a CSP Vault Node.
8. Decommission or re-purpose the server as needed.
9. Set up the new hardware and install Cryptographic Security Platform Vault as an additional node in an existing cluster. For details, see CSP Vault ISO Installation for Hypervisors or CSP Vault OVA Installation. If possible, make sure the new system uses the same IP address as the old system so that all Policy Agents can find the new systems. If you need to change the system IP address, you need to update the

appropriate Cluster Node Mappings or update the list of authorized IP addresses with each Policy Agent as described in Changing a Cluster Node Mapping and Updating CSP Vault Node IP Addresses on an Individual VM.

Moving a CSP Vault Node to a New Server in a Single Node Environment

If you want to move a Cryptographic Security Platform Vault node to a different server, you can install the Cryptographic Security Platform Vault software on the new server and join the new server to the cluster so that the object store is copied to the new server and all your configuration settings are retained. Then you can remove the old server from the cluster and decommission it.

Note: If you want to move a Cryptographic Security Platform Vault node in a multi-node cluster, see Moving a CSP Vault Node to a New Server in a Multi-Node Environment.

Procedure

1. Set up the new server and install Cryptographic Security Platform Vault as an additional node in a cluster with the old Cryptographic Security Platform Vault node. For details, see CSP Vault ISO Installation for Hypervisors or CSP Vault OVA Installation.
   Make note of the IP address you assigned to the new server.
2. Make sure your new node is properly configured by logging into the Cryptographic Security Platform Vault Management webGUI on the new server using an account with Domain Admin privileges.
   Note: If you are using Cluster Node Mappings, you need to log in using an account with Cloud Admin privileges as well in order to update the Mappings later in this procedure.
3. In the top menu bar, click **Cluster**. The cluster **Status** should be **Healthy** and both nodes should appear on the **Servers** tab.
4. If you have registered the Cryptographic Security Platform Vault IP address directly on each Policy Agent (as opposed to using a Cluster Node Mapping), log into each server connected to Cryptographic Security Platform Vault and issue the command:
   ```
   # hcl updatekc kc_hostname[:port]
   ```
   Where `kc_hostname` is the IP address of the new server and `port` is an optional port number if the port is anything other than the default (443).
5. If you set up one or more Cluster Node Mappings, you need to update them:
   a. Log into the Cryptographic Security Platform Vault for VM Encryption webGUI.
   b. In the top menu bar, click **Workloads**.
   c. Click the **Mappings** tab.
   d. Select the Node Mapping in the list, then select **Actions > Edit Mapping**.
   e. Add the new Cryptographic Security Platform Vault node to the Node Mapping and then remove the old Cryptographic Security Platform Vault node.
   f. Click **Update**.
   g. The new Cluster Node Mapping will be communicated to the associated Policy Agents on the next heartbeat. You can either wait for that to happen to make sure the agents are using the new Cryptographic Security Platform Vault IP address or you can log into the VMs and run the command `hcl updatekc –a`.
6. After all VMs in the system are using the new Cryptographic Security Platform Vault IP address, you can remove the old node and decommission the server.
   Important: If you are using Cluster Node Mappings, make sure that the Node Mapping information has updated on all the VMs registered with Cryptographic Security Platform Vault before you remove the old node from the cluster. Just changing the Node Mapping in Cryptographic Security Platform Vault is not enough. Each VM *must* heartbeat with Cryptographic Security Platform Vault *before* the change in the Node Mapping file can be disseminated to the VM. If you remove the old node before this happens, the VM will be unable to connect to Cryptographic Security Platform Vault and access to the encrypted data on the VM could be lost.

a. Log into the Cryptographic Security Platform Vault Management webGUI.
b. In the top menu bar, click **Cluster**.
c. Click the **Servers** tab.
d. Click the old node in the list and select **Actions > Remove**.
e. Log into the existing server as `htadmin`.
   Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
f. Shut down the server by selecting **Shutdown System** from the Entrust Cryptographic Security Platform Vault System Console.
g. If desired, uninstall Cryptographic Security Platform Vault as described in Decommissioning a Cryptographic Security Platform Vault Node.
h. Decommission or re-purpose the old server as needed.

Increasing CSP Vault Storage in a VM

If you installed Cryptographic Security Platform Vault in a VM, you can increase the amount of storage available without reinstalling Cryptographic Security Platform Vault. You just need to increase the size of the underlying disk and reboot the Cryptographic Security Platform Vault node.

Important: If you upgraded to Version 10.5.3, you must delete the pre-upgrade snapshots before you start. See Delete CSP Vault Snapshots.

1. Increase the size of the virtual disk in which Cryptographic Security Platform Vault is installed using your hypervisor tools.
   Note: You may need to shut down the VM before you can resize the disk. For details, see your hypervisor documentation.
2. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Domain Admin privileges.
3. In the top right, click the Switch to **Appliance Management** link.
4. In the top menu bar, click **Cluster**.
5. Select the Cryptographic Security Platform Vault node whose disk you just resized in the list.
6. Select **Actions > System Reboot**.
7. If necessary, log back into the webGUI after the Cryptographic Security Platform Vault node has rebooted.
8. Review the Audit Log messages. The node should report the new size upon success or provide information if the resize failed.

VM Handlers for Attach/Detach in Linux

There are scripts that are invoked when a device is either attached or detached. These scripts can be found under the `/opt/hcs/handlers` directory. The attach handler (`default.attach`) is invoked when a new device is attached and the detach handler (`default.detach`) is invoked when a new device is detached.

The default attach handler is shown below:

```
#!/bin/sh

# Post-attach handlers are called with at least 2 and at most 4 arguments:
# 1. the absolute path of the cleartext device e.g. /dev/mapper/clear_sda
# 2. the absolute path of the encrypted_device e.g. /dev/sda
# 3. (optional) mountpoint
# 4. (optional) mount options
# If the mountpoint and mount options are supplied, then the default handler
# will fsck and mount the cleartext device on the given mount point.
```

```
if [ $# -lt 2 -o $# -gt 4 ]; then
   exit 1
fi
if [ $# -eq 2 ]; then
   exit 0
fi

cleardev=$1
if [ $# -ge 3 ]; then
   mntpt=$3
fi
if [ $# -eq 4 ]; then
   mntopts=$4
fi

fsck -a "$cleardev"
if [ $? -eq 0 ]; then
   mount $mntopts "$cleardev" "$mntpt"
else
   exit 2
fi
```

The mount point and mount options are collected along with the clear-text path to the device and a mount call is made.

The handlers can be changed freely. We recommend that you back up your handlers, using your preferred backup solution.

VM Handlers for Attach/Detach in Windows

The windows client also supports attach and detach handler scripts, located at `c:\Program Files\hcs\handlers`. These run at the same times as the Linux client scripts. The attach handlers will be called immediately after a successful attach. Detach handling scripts will be called immediately before detaching disks.

You can create a handler script for each disk that is encrypted. The format of the name will be:

`DRIVE_LETTER.attach.cmd` and `DRIVE_LETTER.detach.cmd`

Individual disk handler scripts are not required. If not specified, then the default script will be called instead. Those are named `default.attach.cmd` and `default.detach.cmd`.

Each script invocation will be passed the following parameters:

1. The drive letter of the disk being attached or detached. This parameter will be an empty string if the encrypted partition does not have a drive letter assigned.
2. The device name of the volume that is being attached or detached.
3. The index into the list of encrypted drives. The index values start at 0. For example, if there are 4 encrypted drives, the index values will go from 0 to 3 as each drive is attached or detached.
4. The total number of encrypted drives. If this value is 0, it indicates that only a single disk has been attached or detached from the command line (for example, by an administrator issuing the `hcl attach` or `hcl detach` command or by revoking or restoring a disk with the Cryptographic Security Platform Vault webGUI).

The script can determine if all disks are attached or detached by comparing parameters 3 and 4. If parameter 3 (plus 1 because it is offset from 0) is equal to parameter 4, then the script can assume that all of the disks

in the system have been handled. If the total number of disks passed in is 0, that indicates that only a single disk is being operated on at that time.

If you have a disk that already contains data that you want to be encrypted, you can run the `hcl encrypt` command. All encryption, whether encrypting a new disk or removing and decrypting an existing disk, makes use of dynamic rekey. In the case of encrypting a disk, we do the conversion in the background, thus allowing you access the disk while the encryption process is taking place. This allows you to have no downtime for your applications and data.

> Note: If Windows disks are sparse, we will only encrypt allocated blocks ensuring that only the allocated blocks are encrypted and the sparseness remains. This is not currently available for Windows `C:` drives.

To demonstrate how rekey works, let's first look at the contents of the unencrypted `G:` :

```
C:\>dir g:

 Volume in drive G is New Volume
 Volume Serial Number is 44A1-E6A7

 Directory of G:\

10/25/2022  01:48 PM           346,454 HCS_BreachWhitepaper_v1.5.pdf
10/25/2022  01:48 PM           303,179 HCS_CSP_Whitepaper.pdf
10/25/2022  01:48 PM         2,278,559 HCS_Encryption_Use_Cases.pdf
10/25/2022  01:48 PM           883,773 HCS_HIPAA_Compliance.pdf
10/25/2022  01:48 PM         1,006,858 HCS_PCI_Compliance.pdf
10/25/2022  01:48 PM           310,103 HCS_Shack-P1.pdf
10/25/2022  01:48 PM           495,492 HCS_Shack-P2.pdf
               7 File(s)      5,624,418 bytes
               0 Dir(s)   2,098,798,592 bytes free
```

Now let's start the encryption process:

```
C:\>hcl encrypt g:
All the data on G: will be encrypted. This operation may take a long time.
Do you want to proceed? (y/n) y

registering drive G:, guid FF2A17F2-D7DE-404B-B977-018ADC611BCC

Encrypted device G: has been added.
```

You can view the progress of the rekey operation by running `hcl rekey` as follows:

```
C:>\hcl rekey status g:

device: \Device\Harddisk3\Partition1
drive: G
state: in progress
begin: 65536
end: 2144403456
current: 725794816
sector offset (from 0): 1417568
total sectors: 4188160
total size: 2144337920
```

pct done: 33.85%
elapsed time (seconds): 27

Even though the drive is only partially encrypted, we can still view the contents:

C:\>dir g:

```
 Volume in drive G is New Volume
 Serial Number is 44A1-E6A7

 Directory of G:\

10/25/2022  01:48 PM           346,454 HCS_BreachWhitepaper_v1.5.pdf
10/25/2022  01:48 PM           303,179 HCS_CSP_Whitepaper.pdf
10/25/2022  01:48 PM         2,278,559 HCS_Encryption_Use_Cases.pdf
10/25/2022  01:48 PM           883,773 HCS_HIPAA_Compliance.pdf
10/25/2022  01:48 PM         1,006,858 HCS_PCI_Compliance.pdf
10/25/2022  01:48 PM           310,103 HCS_Shack-P1.pdf
10/25/2022  01:48 PM           495,492 HCS_Shack-P2.pdf
               7 File(s)      5,624,418 bytes
               0 Dir(s)   2,098,798,592 bytes free
```

Upgrading to a New Hardware Signature Format

To ensure security, Cryptographic Security Platform Vault periodically upgrades the hardware signature format. When you upgrade your Policy Agent, you may see an alert message similar to "VM is using an older Hardware Signature format. Please run “hcl auth” cmd on the VM for a more secure signature".

This means that the hardware signature format on the policy agent has been updated. In order to use the new hardware signature format, you will need to reauthorize your client by running the `hcl auth -a` command inside Windows or Linux after the system is fully booted.

> Note: If you run the `hcl auth` command without the `-a` option, the encrypted disks will be detached during the reauthorization process.

Important: Although upgrading the hardware signature is optional, we highly recommend that you run the command when you see this alert.

Troubleshooting Network Issues

To ensure security, Cryptographic Security Platform Vault periodically upgrades the hardware signature format. When you upgrade your Policy Agent, you may see an alert message similar to "VM is using an older Hardware Signature format. Please run “hcl auth” cmd on the VM for a more secure signature".

This means that the hardware signature format on the policy agent has been updated. In order to use the new hardware signature format, you will need to reauthorize your client by running the `hcl auth -a` command inside Windows or Linux after the system is fully booted.

> Note: If you run the `hcl auth` command without the `-a` option, the encrypted disks will be detached during the reauthorization process.

Important: Although upgrading the hardware signature is optional, we highly recommend that you run the command when you see this alert.

Cleaning Up Stale Tasks

In some rare scenarios, CSP Vault fails to track some tasks. The state of those tasks is 'In Progress' and it is never updated. Because Cryptographic Security Platform Vault automatically sends delayed task alerts for inactive tasks every 6 hours, you will continue to receive alerts from those stale tasks until they are marked abandoned.

You can abandon tasks for VMs or Cloud VM Sets. The abandoned tasks will be cleared in 24 hours.

Important: Do not use this option to stop a task.

Marking Tasks as Abandoned Using the webGUI

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Cloud Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Workloads**.
4. Navigate to either the **VM Sets** or **VMs** tab.
5. Select the Cloud VM Set or VM that has inactive tasks.
6. Select **Actions > Abandon Inactive Tasks**.
7. In the confirmation window, click **Proceed**.

Marking Tasks as Abandoned Using the hicli

Log in to the hicli and select one of the following options:

- Abandon a task by the task ID:
  ```
  hicli cvmset abandon_task <cvmset_name> --taskid=<taskid>
  ```
- Abandon all tasks that have been inactive for 6 days or more on a Cloud VM Set:
  ```
  hicli cvmset abandon_inactive_tasks <cvmset_name>
  ```
- Abandon all tasks that have been inactive for 6 days or more on a VM:
  ```
  hicli cvm abandon_inactive_tasks <cvm_name>
  ```

Support Access and Log Files

Entrust Cryptographic Security Platform Vault provides two methods of support access:

- Restricted support—Customers can access support logs and run simple diagnostic tools through a limited SSH-accessible shell that can be invoked from the Entrust Cryptographic Security Platform Vault System Console. For details, see Using the Restricted Shell.
- Full support—The Entrust support staff can access and troubleshoot the customer's system. Full support access requires multi-factor authentication between the Cryptographic Security Platform Vault Administrator at the customer site and Entrust Support. If such access is required, Entrust Support will guide you through the process.

- Using the Restricted Shell
- Creating a Support Bundle with the webGUI
- Creating a Support Bundle from the CSP Vault System Console
- Disabling CSP Vault Support Logins
- Policy Agent Support Logs
- Backing Up the Policy Agent
- Uninstalling the Policy Agent on Linux
- Uninstalling the Policy Agent on Windows
- KMIP Errors and Troubleshooting
- Revert to Previous CSP Vault Version
- Delete CSP Vault Snapshots
- Troubleshooting CSP Platform Vault from the Bootloader

- Recovering Access to CSP Vault

Using the Restricted Shell

The restricted support login provides a limited SFTP-accessible shell in which the Cryptographic Security Platform Vault administrator can gather diagnostic information. It is disabled by default.

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Manage Accounts** and press **Enter**.
3. On the Manage Accounts page, select **htrestricted (read only support access)** and press **Enter**.
   The TUI displays the Manage the htrestricted account page.
   Note: If the account is currently enabled, Cryptographic Security Platform Vault displays that information along with the date on which the current restricted support password will expire. If you want to set a new password, select **Yes** at this prompt and then return to step 2.
4. Select **Yes** and press **Enter** to confirm the request.
5. Enter the password for the `htrestricted` support account. When you are done, select **OK** and press **Enter**, then press **Enter** again to confirm the request.
6. Use SFTP to log into the `htrestricted` account on the Cryptographic Security Platform Vault node using the password you specified above.
   Tip: Windows users can use WinSCP to access the `htrestricted` account via SFTP.
   The following example shows how to log into the restricted shell and navigate to the directory containing the latest support bundles. The first bundle contains the logs for the current node only, while the second bundle contains the logs from all nodes in the cluster:

```
$ sftp htrestricted@10.238.66.250
htrestricted@54.193.4.110's password:
Connected to htrestricted@54.193.4.110.
sftp> cd support/logs/node_logs
sftp> ls
htkc_dbginfo_kc-250.domain.mycompany.com_2019-07-03-21-27-57.tar.gz
sftp> cd ../cluster_logs
sftp> ls
htkc_cluster_dbginfo_2019-07-03-21-29-11.tar.gz
sftp>
```

   For details about using the restricted shell, contact Entrust Support.

Creating a Support Bundle with the webGUI

In certain circumstances it may be necessary to gather diagnostic information and logs from Cryptographic Security Platform Vault that can be sent to Entrust support for further analysis. The following procedure describes how to create a log bundle using the webGUI. To create the bundle with the Entrust Cryptographic Security Platform Vault System Console on the Cryptographic Security Platform Vault node, see Creating a Support Bundle from the Entrust CSP Vault System Console.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. In the **Support** section, click **Download Logs**.
5. If a log has not yet been created for this cluster or if you want to generate a new log, click **Create Bundle**.

6. In the Logs dialog box, enter the following information:

Option	Description
Include Audit Log	If Yes, Cryptographic Security Platform Vault includes the full audit log in the bundle. The default is Yes.
Include All Cluster Logs	If Yes, Cryptographic Security Platform Vault includes the log bundle from every Cryptographic Security Platform Vault node in the cluster. If No, Cryptographic Security Platform Vault only includes the log bundle from the current node. The default is No.
Include Core Files	If Yes, Cryptographic Security Platform Vault includes core files in the bundle. The default is No.
Passphrase	If you specify a passphrase, Cryptographic Security Platform Vault encrypts the bundle with an AES 256-bit key using the provided passphrase.

7. When you are done, click **Create**. Cryptographic Security Platform Vault creates the log file and then refreshes the information about the log bundle it created.
8. To download the bundle, click **Download**.
   Tip: Some browsers may display a warning that the log bundle is not commonly downloaded and may be dangerous. It is safe to ignore this message and continue the download.

Note: If you want to decrypt the log bundle, navigate to the directory where the bundle is located and type the following command:

gpg -d -o <output-file-name> <input-file-name>

Where `<output-file-name>` is the name you want to use for the decrypted log bundle and `<input-file-name>` is the name of the encrypted log bundle that you want to decrypt.

Creating a Support Bundle from the CSP Vault System Console

In certain circumstances it may be necessary to gather diagnostic information and logs from Cryptographic Security Platform Vault that can be sent to Entrust support for further analysis. The following procedure describes how to create a log bundle using the Entrust Cryptographic Security Platform Vault System Console on one of the nodes in the cluster. To create the bundle using the webGUI, see Creating a Support Bundle with the webGUI.

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Gather Diagnostic Logs**.
3. In the Create Log Options page, use the arrow keys to move to an option you want to change and then use the spacebar to toggle whether that option is selected. When you are done, press **Enter**. The options are:

Option	Description
Include Audit Log?	If selected, Cryptographic Security Platform Vault includes the full audit log in the bundle. This option is selected by default.
Include Log Bundle from ALL KeyControl Nodes?	If selected, Cryptographic Security Platform Vault includes the log bundle from every node in the cluster. Otherwise Cryptographic Security Platform Vault only includes the log bundle from the current node.
Include Core Files?	If selected, Cryptographic Security Platform Vault includes core files in the bundle.
Use a Passphrase to Encrypt the Bundle?	If selected, Cryptographic Security Platform Vault encrypts the bundle with an AES 256-bit key using the provided passphrase. Cryptographic Security Platform Vault will prompt you for the passphrase as soon as you press Enter.

When you press Enter, Cryptographic Security Platform Vault creates the bundle using the options you selected.

4. When you see the prompt that says the log bundle was successfully created, press **Enter**.
   If the Cryptographic Security Platform Vault webGUI is not available, please use the restricted shell to download the support bundle. For more information, see Using the Restricted Shell.
   You can also download the log bundle from the Cryptographic Security Platform Vault webGUI by selecting **Settings > Support > Download Logs**.

Note: If you want to decrypt the log bundle, navigate to the directory where the bundle is located and type the following command:

gpg -d -o <output-file-name> <input-file-name>

Where `<output-file-name>` is the name you want to use for the decrypted log bundle and `<input-file-name>` is the name of the encrypted log bundle that you want to decrypt.

Disabling CSP Vault Support Logins

Cryptographic Security Platform Vault support logins are automatically disabled 24 hours after being created. This procedure describes how to manually disable a support log in before that time has expired.

1. Use your hypervisor to access one of the VMs in which Cryptographic Security Platform Vault is running, then log into the Cryptographic Security Platform Vault VM console as `htadmin`. The Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Manage Accounts** and press **Enter**.
3. On the Manage Accounts page, select the account you want to disable and press **Enter**.
4. The confirmation page shows the account name and when the password will automatically expire. To disable the account immediately, make sure **Yes** is selected and press **Enter**.
   Cryptographic Security Platform Vault disables the support account and returns to the main menu.

Policy Agent Support Logs

The Policy Agent logs information to the following files on Linux and Windows:

Linux— `/var/log/hcl.log`

Windows— `C:\Program Files\hcs\hcl.log`

To generate a log bundle containing pertinent system information, use the `hcsinfo` command. For details, contact Entrust Support.

Backing Up the Policy Agent

If you want to backup an the Policy Agent on an encrypted disk, you need to make sure the entire disk is backed up (for example, the entire VMDK file in a VMware vSphere environment). This ensures that the Entrust GUIDs representing the keys are also backed up so the data can be decrypted if it is restored from the backup. Once the backup is reauthorized with Cryptographic Security Platform Vault, Cryptographic Security Platform Vault can use the restored GUIDs to determine which keys apply to the restored data.

To create the backup, see your hypervisor documentation. Entrust does not provide any tools for backing up a VM.

Warning: Before you back up your VM, make sure you check the expiration date for the data encryption keys on the disk. If you restore a backup with expired keys and the expiration option is set to SHRED, Cryptographic Security Platform Vault will destroy the keys immediately and the data will be inaccessible. If you set the expiration option to NO USE, the keys can be reactivated after the back up is restored. For more information, see Encrypting a Disk Using the CLI.

Uninstalling the Policy Agent on Linux

Before You Begin

This procedure requires that you have a copy of the Policy Agent installer in your current directory. If this is not there, download the installer before you begin.

If you are using the htcrypt driver, you must uninstall it before you begin. For more information, see Uninstalling the HTCrypt Driver.

The Policy Agent can be uninstalled using the `/opt/hcs/bin/uninstall.sh` script. As part of uninstallation, all the binaries and configuration files will be removed. The encrypted block devices can no longer be decrypted after uninstalling the Policy Agent which will result in data loss. The Policy Agent can be uninstalled only after all root (system) devices are unencrypted, and the online encryption driver is removed. For more information, see Uninstalling the HTCrypt Driver.

Procedure

1. Decrypt all encrypted disks in the VM and remove the VM from the Cryptographic Security Platform Vault for VM Encryption as described in Decrypting a Disk Using the webGUI and Removing a VM from the Cryptographic Security Platform Vault for VM Encryption.
   Important: If you uninstall the Policy Agent without decrypting the disks, all access to the encrypted files will be lost because the encryption keys are deleted during the uninstall procedure.
2. Make sure that the Policy Agent can be uninstalled on the VM. To do so, expand the VM in the webGUI and look at the **Policy Agent Uninstallation Allowed** field on the **Details** tab. If this field is set to **No**, click **No**, select **Yes** from the drop-down list, then click **Save**.

Tip: If you want to uninstall the Policy Agent from multiple VMs in this Cloud VM Set, you can change this property at the Cloud VM Set level and propagate the change to all VMs in the Cloud VM Set. For more information, see Changing Cloud VM Set Properties.

3. Log into the VM as `root`.
4. Run the shell command `hcs-client-agent-10.5.3-build.number.run uninstall`. For example:

```
# sh hcs-client-agent-10.5.3-12345.run uninstall
Creating directory hcs-agent-agent
Verifying archive integrity... All good.
Uncompressing hcs-agent-agent.run.....
Data on all encrypted volumes will be lost. Proceed with uninstall? (yes/no) yes
Encrypted device /dev/sdb1 detached; decrypted contents no longer visible
Encrypted device /dev/sdc1 detached; decrypted contents no longer visible
Encrypted device /dev/sdd1 detached; decrypted contents no longer visible
Stopping hcld... done
Uninstall successful
```

Uninstalling the Policy Agent on Windows

Before You Begin

This procedure requires that you have a copy of the Policy Agent installer in your current directory. If this is not there, download the installer before you begin.

If you are using the htcrypt driver, you must uninstall it before you begin. For more information, see Uninstalling the HTCrypt Driver.

The Policy Agent can be uninstalled using the `/opt/hcs/bin/uninstall.sh` script. As part of uninstallation, all the binaries and configuration files will be removed. The encrypted block devices can no longer be decrypted after uninstalling the Policy Agent which will result in data loss. The Policy Agent can be uninstalled only after all root (system) devices are unencrypted, and the online encryption driver is removed. For more information, see Uninstalling the HTCrypt Driver.

Procedure

1. Decrypt all encrypted disks in the VM and remove the VM from the Cryptographic Security Platform Vault for VM Encryption as described in Decrypting a Disk Using the webGUI and Removing a VM from the Cryptographic Security Platform Vault for VM Encryption.
   Important: If you uninstall the Policy Agent without decrypting the disks, all access to the encrypted files will be lost because the encryption keys are deleted during the uninstall procedure.
2. Make sure that the Policy Agent can be uninstalled on the VM. To do so, expand the VM in the webGUI and look at the **Policy Agent Uninstallation Allowed** field on the **Details** tab. If this field is set to **No**, click **No**, select **Yes** from the drop-down list, then click **Save**.
   Tip: If you want to uninstall the Policy Agent from multiple VMs in this Cloud VM Set, you can change this property at the Cloud VM Set level and propagate the change to all VMs in the Cloud VM Set. For more information, see Changing Cloud VM Set Properties.
3. Log into the VM as `root`.
4. Run the shell command `hcs-client-agent-10.5.3-build.number.run uninstall`. For example:

```
# sh hcs-client-agent-10.5.3-12345.run uninstall
Creating directory hcs-agent-agent
Verifying archive integrity... All good.
Uncompressing hcs-agent-agent.run.....
Data on all encrypted volumes will be lost. Proceed with uninstall? (yes/no) yes
Encrypted device /dev/sdb1 detached; decrypted contents no longer visible
```

```
Encrypted device /dev/sdc1 detached; decrypted contents no longer visible
Encrypted device /dev/sdd1 detached; decrypted contents no longer visible
Stopping hcld... done
Uninstall successful
```

KMIP Errors and Troubleshooting

KMIP Server Logs

- `/host/var/log/hcs/kmipsrv.log` : Transactions for server stop and start. This is mostly for debugging.
- `/host/var/log/hcs/traffic.log` : Fully-formatted KMIP protocol output. Key values are redacted.
- **Audit log**: You can configure the KMIP server to record all KMIP requests and responses or just the create/get requests and responses in the Cryptographic Security Platform Vault Audit log. You can also configure the server so that it does not log any KMIP information in the Audit log.

Troubleshooting

The most common errors are:

- Error 10 KMIP_ERROR_IO—Generally, the client is not talking to the server at all. This could be because of firewall issues, incorrect “Host Name” in KMIP client settings, or some other network issue. You can check connectivity with netcat via the console menu under “Diagnostic Tools”.
- Error 29 KMIP_ERROR_SSL_PARAMS—Seen when incomplete parameters are entered on the KMIP **Basic** tab.
- Error 30 KMIP_ERROR_SSL_PEER_VALIDATION—Seen when the KMIP server required Server Cert and one was not provided.
- Error 31 KMIP_ERROR_BAD_PASSWORD—One of the passwords entered for a KMIP client is incorrect.
- Error 32 KMIP_ERROR_BAD_TRUSTED_FILE—The CA cert argument specified for the KMIP client is incorrect.

Revert to Previous CSP Vault Version

When you upgrade to a newer version, Cryptographic Security Platform Vault automatically creates a pre-upgrade snapshot. Cryptographic Security Platform Vault allows you to revert to this previous version.

Important: If you have deleted the pre-upgrade snapshots, you cannot revert your upgrade to the previous installed version.

1. Log into the Cryptographic Security Platform Vault Management webGUI using an account with Security Admin privileges.
2. In the top right, click the Switch to **Appliance Management** link.
3. In the top menu bar, click **Settings**.
4. On the Account Settings page, select System Upgrade.
   On the System Upgrade page, the previous upgrade version is displayed at the top in a yellow box.
   "A previous version <version number> is available to revert to."
5. Click the link on the text that says "revert to".
6. Click **Revert Upgrade**.
7. In the confirmation box, click **Proceed**.
8. Click **Reboot**.
9. In the confirmation box, click **Proceed**.

Cryptographic Security Platform Vault reverts to the previous upgrade.

Delete CSP Vault Snapshots

Cryptographic Security Platform Vault automatically creates a pre-upgrade snapshot whenever you upgrade to a newer version of Cryptographic Security Platform Vault. If you plan to increase your VM storage, you must delete any snapshots first.

Important: If you delete the pre-upgrade snapshots, you cannot revert your upgrade to the previous installed version. See Revert to Previous CSP Vault Version.

1. Log into the Cryptographic Security Platform Vault VM console as `htadmin`.
   Cryptographic Security Platform Vault displays the Entrust Cryptographic Security Platform Vault System Console TUI (Text-based User Interface).
2. Select **Manage Cryptographic Security Platform Vault Node**.
3. In the Manage the Cryptographic Security Platform Vault Node page, select **Delete** Cryptographic Security Platform Vault **pre-upgrade snapshot**.
4. In the confirmation screen, select **Yes**.

The snapshot is deleted, and there will be an audit message when it is complete.

Troubleshooting CSP Platform Vault from the Bootloader

If CSP Vault requires master key recovery or if the startup passphrase is set, then admin input is required during boot to unlock the root volume. When this happens, the Cryptographic Security Platform Vault webGUI displays the System Recovery dialog box, which is similar to the System Recovery Options dialog box. For more details, see Recovering Access to Cryptographic Security Platform Vault

If you cannot recover your system, then you need to use the Cryptographic Security Platform Vault Bootloader System Console to troubleshoot your issues. You can access the Bootloader System Console from either the Cryptographic Security Platform Vault VM console or by using an SSH connection to your Cryptographic Security Platform Vault IP address. You must log in as htadmin.

Note: If you log in using the VM console, you will see the following text. Enter y to start the System Console.

```
Please recover Cryptographic Security Platform Vault System Keys from WebGUI.
Cryptographic Security Platform Vault System Keys are not accessible.
Do you want to start KeyControl System Console? (y/n): y
```

Important: If you access the System Console using the VM console, and then successfully recover your system, you must quit the TUI before the VM boot will proceed. This does not apply if you access the System Console over SSH.

After you have logged in, you will see the following:

Option	Name	Description
1	Show HT encryption log file	Displays the log generated during boot for encryption or rekey. Run this command if requested by Support.
2	Set htsupport password	Enable the full support login account (`htsupport`). Enter the password and then confirm the password to enable.
3	Show Active network	Displays the active network addresses and routes for your Cryptographic Security Platform Vault node. If you set a temporary network, it displays the information for the new network.
4	Show persistent Cryptographic Security Platform Vault network	Displays the network configuration parameters currently configured for your Cryptographic Security Platform Vault node. This includes IP address, netmask, gateway, DNS address, and domain name.
5	Activate persistent Cryptographic Security Platform Vault network	Automatically restarts the Cryptographic Security Platform Vault networking service using the persistent network parameters.
6	Configure temporary network	Create a temporary network for your Cryptographic Security Platform Vault node. This command prompts for the network interface name, IP address, netmask, gateway, DNS address, and domain name. You can also enable DHCP.
7	Quit TUI Session	Close the System Console and return to the prompt.

Recovering Access to CSP Vault

There are times when you will need to recover your Cryptographic Security Platform Vault system, such as when you increase the number of CPUs allotted to a Cryptographic Security Platform Vault server, change the network hardware address, migrate Cryptographic Security Platform Vault to a different host, or restore from a backup to a newly-created VM. The system recovery process prevents rogue administrators from making unauthorized changes to, or copies of, Cryptographic Security Platform Vault disks.

- When you make a change that affects the hardware signature, the Cryptographic Security Platform Vault webGUI displays the **System Recovery** dialog box.

- For backup/restore, the Cryptographic Security Platform Vault webGUI displays the **System Recovery Options** dialog box.

Procedure

1. Select the method you want to use to recover your system. The options are:

Option	Description
Recovery using Keypart Upload	Allows you to upload the minimum number of required Admin Key parts that were sent to the Security Admins in the system. If you select this option, the webGUI displays the Recover Admin Key page. To upload a part, click Browse and select the appropriate `recovery_key` file. The Browse button should change to show the name of the selected file. When the correct file is displayed, click Upload file. Make sure that all Admin Key parts you upload have the same generation count. This information can be found in the email accompanying the Admin Key part. For details, see Admin Keys. When the required number of parts have been uploaded, Cryptographic Security Platform Vault recovers the system and displays the Recovery Success message. Click Proceed to return to the Cryptographic Security Platform Vault login page.
Recovery using Passphrase	Allows you to recover your system when you are using passphrase-based authentication. If you select this option, the webGUI displays the Recovery Passphrase page. Enter your passphrase and click Recover. For more information, see Startup Authentication.
Recovery from KMIP Server	Allows you to get an Admin Key stored on a KMIP server. The Admin Key must already be stored on this server for this option to work.
Recovery from HSM Server	Allows you to get the Admin Key from an HSM server. The Admin Key must already be stored on the HSM server for this option to work. If you select this option, the webGUI displays the HSM Recovery page where you can specify the following: • Partition Label, HA Group Name, or SoftCard Name • Partition, Crypto Officer (CO) password, or SoftCard password
Decommission	If you want to decommission your Cryptographic Security Platform Vault system, see Decommissioning a Cryptographic Security Platform Vault Node.

2. If there are multiple Cryptographic Security Platform Vault nodes in the cluster, re-join those nodes with the node you just recovered. For details, see Joining or Re-joining a Cryptographic Security Platform Vault Cluster.

CSP Vault Management webGUI Page Reference

- Alerts Page
- Audit Log Page

- Cluster Page
- HSM Server Settings Page
- Proxy Settings
- Users Page
- Settings Page
- SNMP Settings Page
- License Page
- Syslog Server Settings Page
- System Decommission Page
- System Upgrade Page

Alerts Page

The Alerts page gives you a quick overview of the major events that have taken place in the system. webGUI users can delete an alert from their local view, but the same alert will still be visible to other Cryptographic Security Platform Vault users. For more information, see CSP Vault Activity Tracking

To copy an alert to the clipboard, click it and use Ctrl+C on Windows or Command+C on the Mac. If you want to copy multiple alerts, click the Multi-Select button and then left-click on the alerts you want to select.

To filter the alert list:

1. In the **Filter** drop-down list, select the field you want to filter on.
2. Enter the filter text in the text box.
3. Click the Plus (**+**) sign at the end of the field to add the filter.
4. Repeat this process to add additional filters and further refine the display.

Search tips for the available field types:

- Message—Searches the text displayed in the **Message** column.
- Date—Filters the list based on the date the alert was created. You can only select one day per filter. Cryptographic Security Platform Vault does not support searching on a range of dates.

Deleting Alerts

To delete one or more alerts from your local view:

1. Select the alerts you want to delete.
2. Select **Actions > Delete Alerts**.

Audit Log Page

Cryptographic Security Platform Vault tracks all activity on the system in the audit log. Users can export the audit log from the Cryptographic Security Platform Vault Management webGUI but they cannot change it in any way. For security reasons, Cryptographic Security Platform Vault tracks most of the events in the system.

> Note: You can also view the audit logs for each individual vault. The individual vaults do not support syslog and SNMP for audit logs.

For details, see:

- Cryptographic Security Platform Vault Activity Tracking
- Viewing the Audit Log
- Configuring Audit Log Settings
- Exporting the Audit Log

Cluster Page

The Cluster page contains the Cluster and Servers tabs, which show the health and basic configuration settings for the Cryptographic Security Platform Vault cluster as well as the connection status of all Cryptographic Security Platform Vault nodes in the cluster.

Cluster Tab

This tab displays the general health of the cluster as well as the basic configuration settings. It also allows you to join an existing cluster, add a new node to this cluster, backup your Cryptographic Security Platform Vault settings, or restore your settings from a previously-saved backup file.

For details, see:

- Cryptographic Security Platform Vault Nodes and Clusters
- Viewing the Cluster Status
- Setting Cluster Options
- Cryptographic Security Platform Vault Backup and Restore

Servers Tab

This tab includes one entry for each Cryptographic Security Platform Vault node in the cluster. For each node you can view or change the SSL certificate, reboot the node, or remove the node from the cluster.

For details, see:

- Removing a Cryptographic Security Platform Vault Node from a Cluster
- Joining or Re-joining a Cryptographic Security Platform Vault Cluster
- Changing the IP Address for a Node
- Rebooting a Cryptographic Security Platform Vault Node
- Cryptographic Security Platform Vault Certificates

HSM Server Settings Page

This page lets you configure the connection settings between Cryptographic Security Platform Vault and an Entrust or third-party Hardware Security Module (HSM).

An HSM is a physical server or PCI card that stores, protects, and manages cryptographic material. An HSM is often used to do cryptographic processing as well, including the generation of secure cryptographic keys. It is used in a client-server environment, which means that the server and the client each need to be prepared in advance. As with KMIP, the advantage of an HSM is that it protects and stores critical data such as your Admin Key and any Key Encryption Keys (KEKs) you have created for your Cloud VM Sets.

For details, see:

- Hardware Security Modules with CSP Vault
- Configuring Cryptographic Security Platform Vault as an HSM Client using an nShield HSM
- Adding a Cryptographic Security Platform Vault Node to a Cluster using an nShield HSM client
- Adding HSM Root-of-Trust to nShield Server
- Configuring Allowed Smart Cards for an nShield HSM
- Configuring an nShield HSM for High Availability
- Replacing an nShield HSM on a Cryptographic Security Platform Vault Cluster
- Configuring Cryptographic Security Platform Vault as a Luna HSM Client with a Single Cluster Certificate
- Configuring CSP Vault as a Luna HSM Client with Individual Node Certificates
- Adding a Cryptographic Security Platform Vault Node to an Existing Luna HSM Configuration
- Resetting the HSM Server Configuration
- Admin Keys
- KEKs with Cloud VM Sets

Proxy Settings

The Users page contains the Users tab, which shows all Cryptographic Security Platform Vault users configured in the system.

Cryptographic Security Platform Vault Managed Users Tab

You can create user accounts for Cryptographic Security Platform Vault that have access to certain areas of the Cryptographic Security Platform Vault webGUI based on their assigned user role. These accounts can also be used in the Entrust CLI (Command Line Interface) and the Entrust API calls when Cryptographic Security Platform Vault authorization is required.

For details, see:

- Cryptographic Security Platform Vault Authentication and User Accounts
- Authentication for Cryptographic Security Platform Vault User Accounts
- Setting the Cryptographic Security Platform Vault Management webGUI Session Timeout
- Creating a New Cryptographic Security Platform Vault-Managed User Account
- Setting webGUI User Preferences
- Changing Your Cryptographic Security Platform Vault User Account Settings
- About Two-Factor Authentication
- Changing Cryptographic Security Platform Vault Account Details as a Security Administrator
- Re-enabling a Cryptographic Security Platform Vault-Managed User Account

Users Page

The Users page contains the Users tab, which shows all Cryptographic Security Platform Vault users configured in the system.

Cryptographic Security Platform Vault Managed Users Tab

You can create user accounts for Cryptographic Security Platform Vault that have access to certain areas of the Cryptographic Security Platform Vault webGUI based on their assigned user role. These accounts can also be used in the Entrust CLI (Command Line Interface) and the Entrust API calls when Cryptographic Security Platform Vault authorization is required.

For details, see:

- Cryptographic Security Platform Vault Authentication and User Accounts
- Authentication for Cryptographic Security Platform Vault User Accounts
- Setting the Cryptographic Security Platform Vault Management webGUI Session Timeout
- Creating a New Cryptographic Security Platform Vault-Managed User Account
- Setting webGUI User Preferences
- Changing Your Cryptographic Security Platform Vault User Account Settings
- About Two-Factor Authentication
- Changing Cryptographic Security Platform Vault Account Details as a Security Administrator
- Re-enabling a Cryptographic Security Platform Vault-Managed User Account

Settings Page

The Settings page contains various sections that let you configure Cryptographic Security Platform Vault user account information, general configuration options, system settings, Cloud VM Set default settings, group SNMP settings, and Support options.

> Note: The sections and options displayed on this page depend on the privileges associates with your Cryptographic Security Platform Vault user account. If you cannot see an option that you want to set, contact your Cryptographic Security Platform Vault System Administrator.

Account Settings Section

This section lets you change your Cryptographic Security Platform Vault user account information, and, if applicable, download your portion of the Cryptographic Security Platform Vault Admin Key.

For details, see:

- Changing Your CSP Vault User Account Settings
- Admin Keys
- Downloading Your Admin Key Part
- About Two-Factor Authentication

  Note: If you have Security Admin privileges and you want to change the Cryptographic Security Platform Vault account details for a different user account, see Changing CSP Vault Account Details as a Security Administrator.

General Section

This section lets you configure general server settings and set the defaults for new Cryptographic Security Platform Vault user accounts.

For details, see:

- Authentication for CSP Vault User Accounts
  - Configuring Local Authentication Settings
  - Specifying an LDAP/AD Authentication Server
  - Specifying an OpenLDAP Authentication Server
  - Configuring an OpenID Connect Provider
- Connecting a CSP Vault to CSP Compliance Manager
- Admin Keys
- Configuring Audit Log Settings
- Setting the Default Account Expiration
- Setting Email Server Preferences
- Setting the CSP Vault Management webGUI Session Timeout
- Configuring TLS
- Uploading an OIDC CA Certificate

System Settings Section

This section lets you specify external connection information as well as upgrade, roll back, or decommission the system.

For details, see:

- Hardware Security Modules with CSP Vault
- Enabling an HTTP Proxy Server in CSP Vault
- SNMP Traps in Cryptographic Security Platform Vault
- Decommissioning a CSP Vault Node
- Configuring Syslog Server Settings
- Managing Two-Factor Authentication
- Setting CSP Vault Console Settings
- Setting CSP Vault Management webGUI Alert Settings

Cloud Settings Section

This section lets you specify the defaults you want to Cryptographic Security Platform Vault to use when you create a Cloud VM Set.

For details, see Setting Default Cloud VM Set Properties.

Support Section

This section lets you create a log bundle and then download that bundle so you can send it to Entrust.

For details, see:

- Support Access and Log Files
- Creating a Support Bundle with the webGUI

Group Settings Section

This section lets you configure SNMP for group-level alerts.

For details, see:

- SNMP Traps in Cryptographic Security Platform Vault
- Configuring Group-Level SNMP Traps

SNMP Settings Page

This page lets you configure your SNMP server connection for system-level alerts. This connection information will also be used for group-level alerts if no specific group-level connection information has been configured for this Cryptographic Security Platform Vault cluster.

You can also download the Cryptographic Security Platform Vault MIB file from this page.

For details, see:

License Page

Your Cryptographic Security Platform Vault license determines the number of nodes you can have in a cluster, the number of VMs that you can manage, and the length of time for which you can use the Cryptographic Security Platform Vault. Detailed license information is available in the Cryptographic Security Platform Compliance Manager, but you can view the status and the last time you have synced your Vaults and CSP Compliance Manager on the License page.

Several audit messages also contain information about your licenses for the CSP Vault for VM Encryption, the CSP Vault for Databases, the CSP Vault for Cloud Keys, and the CSP Vault appliance. For example:

- When you first upgrade from CSP Vault 10.4.x to 10.5.x, there is a 30-day upgrade grace period to get used to the new licensing model. The audit message informs you that you are in the grace period after upgrade, and that your system will become unlicensed when the grace period ends.
- When your CSP Vault is no longer connected to the CSP Compliance Manager, you will see a message saying that it has not synced to CSP Compliance Manager in x days. These messages start at 7 days after the last sync until the 30 day license sync grace period ends.

Beginning with 10.5.3, when there are important issues with your license, you will now see pop-up warnings in the Cryptographic Security Platform Vault webGUI as well as audit messages.

Syslog Server Settings Page

The Syslog Server Settings page allows you to view the settings of your Syslog Server, or enable or disable the server. When enabled, you can set the protocol to TCP or UDP, set the type of TLS authentication, the log format (RFC 5424 or CEF), and enter a list of syslog servers and their corresponding ports. You can also generate a certificate signing request, and, if required by your authentication mode, upload a CA certificate or client certificate. You can also reset the Syslog Server settings to the default values.

For details, see:

- Configuring Syslog Server Settings

- Resetting Syslog Server Settings

System Decommission Page

This page lets you decommission a Cryptographic Security Platform Vault node. When you decommission the node, Cryptographic Security Platform Vault zeroizes its disks and shuts down the node. If you want to decommission all nodes in a cluster, please decommission each node individually.

Warning: This is an irreversible procedure that could result in data loss if this is the only Cryptographic Security Platform Vault node in your system. If it is, make sure you have decrypted all disks registered with Cryptographic Security Platform Vault before you decommission the node or you will be unable to access the encrypted data after Cryptographic Security Platform Vault destroys the encryption keys.

For details, see Decommissioning a CSP Vault Node.

If you want to decommission a VM, see Decommissioning and Destroying a VM.

System Upgrade Page

This page displays the version of Cryptographic Security Platform Vault that you are currently running and gives you the option of upgrading the software or rolling it back to the previous version.

13 CSP Vault Audit Messages 10.6.1

The Cryptographic Security Platform Vault audit messages are divided into four separate audit message files.

- The main audit file contains audit messages from the CSP Vault Management Appliance, the CSP Vault for Cloud Keys, the CSP Vault for Databases, and the CSP Vault for VM Encryption.
- The three smaller files contain audit messages from the CSP Vault for Cryptographic APIs, the CSP Vault for KMIP, and the CSP Vault for Secrets.

- CSP Vault Audit Messages
- CSP Vault for Cryptographic APIs Audit Messages
- CSP Vault for KMIP Audit Messages
- CSP Vault for PKCS#11 Audit Messages
- CSP Vault for Secrets Audit Messages
- Differences in CSP Vault Audit Messages

CSP Vault Audit Messages

The audit messages in this section are from the Cryptographic Security Platform Vault Management Appliance, the Cryptographic Security Platform Vault for Cloud Keys, the Cryptographic Security Platform Vault for Databases, and the Cryptographic Security Platform Vault for VM Encryption.

There are many audit messages produced by Cryptographic Security Platform Vault. Many of these are informative and require no action. In the table below, we list many of the audit messages and show:

- Whether an Alert is also generated.
- The severity (L=Low, M=Medium, H=High).
- What the resolution is if any action should be taken.
- In the **Message** column,
  - a **%s** represents a string value. For example, in the following message:

    ```
    Added user %s to group %s
    ```

    The actual message will be displayed with the name of the user and group, for example:

    ```
    Added user fred to group IT
    ```

  - a value in braces, such as `{user_name}`, represents a placeholder that is replaced with an actual value. For example, in the following message:

    ```
    '{user_name}' created the policy '{policy_name}'
    ```

    The actual message will be displayed with the name of the user and policy, for example:

    ```
    'Fred' created the policy 'Default_Policy'
    ```

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
1	System License installed.	L	false	A new license has been uploaded and installed.		Security	Licensing
2	Begin System Initialization	L	false			Security	
3	Created group %s	M	false	The specified admin group has just been created.		Security	Account
4	Created Domain %s	L	false	This message appears during initialization of the first KeyControl node.		Security	Cluster
5	Added user %s to group %s	M	false	The user shown has been added to the specified admin group.		Security	Account
6	Expired password for user %s	H	false	A password has expired for the specified user.	The specified user needs to log in to the WebGUI and change his/her password.	Security	Account

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
7	User %s logged out from ipaddr %s	L	false	The specified user has just logged out from the IP address shown.		Security	Account
8	Changed following attributes for user Security Administrator :- Password, Password Expiration Date, Password History List	M	false	One or more of the listed attributes has been changed for the user.		Security	Account
9	Changed SMTP Auth Settings	M	false	Email settings have been modified.		Security	Configuration
10	EKS has been removed, not destroying old admin keypair	M	false	Permission to use External Key Store has been removed. The old Admin Key was NOT removed on the EKS to allow restoration of older backups.	Informational only. Restore or add new access if so desired.	Security	EKS, KMIP
11	Regenerated Admin Key. The generation count of this key is %s. Reason: %s	H	true			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
12	Created Cloud Virtual Machine Set %s	L	false			Security	
13	Could not create Cloud Virtual Machine Set %s, HTCC server connection not configured	M	false			Security	HTCC, Boundary Control
14	Masterkey Recovered on node %s	H	true			Security	
15	User %s logged in from ipaddr %s	L	false	The specified user has just logged in from the IP address shown.		Security	Account
16	Repeated log in failures for %s from ipaddr %s	H	true	There have been a succession of log in failures for the specified user.	A security admin should check whether the correct user has been trying to log in or not.	Security	Account

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
17	Account disabled for %s due to repeated log in failures	H	true	The number of failed log in attempts has reached the maximum allowed value.	A security admin needs to reset the account to enable access.	Security	Account
18	Server registration failed -- No license Installed	H	true			Security	Licensing
19	Attempt to register a new %s server "%s" failed -- licensed limit reached.	H	true	The number of KeyControl servers is already at the limit imposed by the license. An attempt is being made to another node.	A new license will be required before the number of nodes in the cluster can be extended. Please contact hytrust.support@entrust.com	Security	Licensing
20	Storage Pool %s Filestore %s on server %s is low on space.	H	true			Clusters	
21	Changed following Settings :- %s	M	false			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
22	Changed following attributes for group %s :- %s	M	false	One or more of the listed attributes has been changed for the group shown.		Security	Account
23	Virtual Machine %s authenticated	L	false	A virtual machine has registered or re-authenticated.	This message is in response to direct admin actions. No action is required.	Security	Reauth
24	Virtual Machine %s created in group %s	L	false			Security	
25	Removed Server %s from Cloud %s	L	false			Security	
26	Created Cluster Info %s	L	false			Security	
27	Removed Cluster Info %s	L	false			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
28	Activated account for user %s	M	false	A user's account has been activated.		Security	Account
29	Disabled account for user %s	H	false	A user's account has been disabled.	A security admin should check to see if the account should be enabled again.	Security	Account
30	Created user %s	M	false	The specified user has been created.		Security	Account
31	Deleted user %s	M	false	The specified user has been deleted.		Security	Account
32	Renamed user %s to %s	L	false	A username has been modified.		Security	Account
33	Deleted group %s	L	false	The specified group has been deleted.		Security	Account

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
34	Renamed group %s to %s	L	false	An admin group has been renamed.		Security	Account
35	Removed user %s from group %s	M	false	The specified user has been removed from the group shown.		Security	Account
36	Using EKS for MasterKey protection	M	false	An External Key Store has been configured to protect the Admin Key.		Security	EKS, KMIP
37	Admin Key regeneration failed. Failed to use external KMIP Server for MasterKey protection	M	true	An External Key Store has been configured to protect the Admin Key but access was not allowed for keypair creation.	EKS denied access to create/ retrieve an RSA keypair. Please check KMIP settings and configuration.	Security	EKS, KMIP
38	Could not register to HTCC, htcc server, password and log in must be specified	H	false			Security	Boundary Control

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
39	Could not register to HTCC %s: HTCC log in failed	H	false			Security	Boundary Control
40	Could not register to HTCC %s. Please check user privileges and Boundary Control License on HTCC	H	false			Security	Boundary Control
41	Successfully registered with HTCC Server %s	M	false			Security	Boundary Control
42	Keyid %s has %s	H	true	Keyid has expired and/or rotated. Keys only expire if a Cloud Admin has explicitly set them to expire.		Security	Key ID
43	The Key for disk %s Virtual Machine %s has %s	H	true	A key for the specified virtual machine has either expired or been rotated. Keys only expire or rotate if a Cloud Admin has explicitly set them to expire or rotate.		Security	Key ID

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
44	Key in VMSet %s on VMV %s has %s	M	true			Security	Key ID
45	Changed following KeyControl cluster settings :- %s	M	false	The name of the cluster has been modified.		Clusters	Domain
46	Deleted Domain %s	M	true			Security	Domain
47	Changed following KPS Settings :- %s	M	false			Security	Configuration
48	Changed following VS Appliance Settings :- %s	M	false			Security	
49	Unknown pool %s appeared on VMV, destroying...	M	true			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
50	Changed following Storage Pool Settings :- %s	M	false			Security	
51	Changed following attributes of filestore %s :- %s	M	false			Security	
52	Changed following settings for Cluster Info %s :- %s	M	false			Security	
53	Coretrace Server %s, changed following attributes :- %s	M	false			Security	CoreTrace
54	Changed following settings for Cloud VM Set %s :- %s	M	false			Security	
55	Cloud VM Set %s changed group ownership from %s to %s.	H	false			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
56	Deleted Cloud VM Set %s	M	false			Security	
57	Cloud VM Set %s: added keyid %s using %s cipher	H	false	A virtual machine user has explicitly requested creation of a KeyID using the specified cipher.		Security	Key ID
58	Cloud VM Set %s: Virtual Machine %s removed keyid %s	M	false	A virtual machine user has explicitly requested deletion of the specified KeyID. It has been removed from the specified Cloud VM.		Security	Key ID
59	Cloud VM Set %s: updated keyid %s	L	false	The KeyID description was changed.		Security	Key ID
60	Cloud VM Set %s: Virtual Machine %s attempted to fetch inactive keyid %s	M	false	The KeyID shown has been revoked but an attempt was made to fetch it.	The cloud admin who owns the key should determine whether access should be reinstated or not.	Security	Key ID

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
61	Cloud VM Set %s: Virtual Machine %s attempted to fetch expired keyid %s	M	false	An attempt has been made to fetch an expired KeyID.	The cloud admin who owns the key should determine whether access should be reinstated or not. This is only possible if the KeyID was set to 'No use?' on expiration.	Security	Key ID
62	Cloud VM Set %s: Virtual Machine %s fetched keyid %s	M	false	A request has been made to access the specified KeyID.		Security	Key ID
63	Revoked permission for keyid %s	M	true	KeyID is currently revoked. It must be activated before use.	The cloud admin who owns the key should determine whether access should be reinstated or not.	Security	Key ID
64	Granted permission for keyid %s	H	true	KeyID has been activated after having been previously revoked.		Security	Key ID

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
65	Cloud VM Set %s keyid %s updated - description %s	L	false	The description field for the specified KeyID has been updated.		Security	Key ID
66	Cloud VM Set %s keyid %s updated - key expires on %s, onexpiry %s	M	false	The expiration date and effect on expiration for the specified KeyID have been updated.		Security	Key ID
67	Cloud VM Set %s Keyid %s has expired	M	true	The specified KeyID has reached its expiration date.	The owning cloud admin should verify that the KeyID should be no longer used.	Security	Key ID
68	Keyid %s has expired	M	true	A request to access an expired KeyID has been made.	The owning cloud administrator should verify that the KeyID should no longer be used.	Security	Key ID
69	The Key for keyid %s in Cloud VM Set %s expires in %d day(s). Please extend the key life.	M	true	A KeyID is about to expire.	The owning cloud administrator should verify whether the KeyID should expire and, if not, update the expiration date.	Security	Key ID

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
70	Unable to check keyid %s	M	false	An error occurred while attempting to check properties of KeyID.	An internal error occurred while checking expiration/ rotation properties for specific keyid. Informational only, keyid will be checked again.	Security	Key ID
71	Cloud VM Set %s: added fsid %s using %s cipher	M	false			Security	
72	Cloud VM Set %s: Virtual Machine %s removed fsid %s	M	false			Security	
73	Cloud VM Set %s: Virtual Machine %s updated fsid %s	M	false			Security	
74	Revoked permission for fsid %s	M	true			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
75	Granted permission for fsid %s	M	true			Security	
76	Cloud VM Set %s fsid %s updated - key expires on %s, onexpiry %s	M	false			Security	
77	Cloud VM Set %s Fsid %s has expired	M	true			Security	
78	Properties changed for VMSet %s on server %s (%s)	M	false			Security	
79	Virtual Machine %s, changed following attributes: %s	M	false			Security	
80	Deleted Virtual Machine %s	L	true			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
81	Deleted Certificate %s	L	false	An unused certificate was deleted		Security	
82	The Virtual Machine %s, could not be checked for geo-location boundary. HTCC log in failed	H	true			Security	Boundary Control
83	The Virtual Machine %s, is not in the geo-location boundary. Key access is denied	H	true			Security	Boundary Control
84	The Virtual Machine %s, is in the geo-location boundary. Key access is granted	M	true			Security	Boundary Control
85	Added Virtual Machine %s, authentication complete	L	true	A virtual machine has completed registration.	This message is in response to direct admin actions. No action is required.	Security	Reauth

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
86	Added Virtual Machine %s, authentication pending	M	true	A virtual machine has a registration request pending.	The cloud admin needs to complete authentication in the KeyControl WebGUI.	Security	Reauth
87	Removed Server %s from Cloud %s	L	false			Security	
88	Renamed Server %s to %s	L	false			Security	
89	Virtual Machine %s re-connected, authentication pending	H	true	A virtual machine has a re-authorization request pending.	The cloud admin needs to complete re-authorization in the KeyControl WebGUI.	Security	Reauth
90	Revoked permissions for Virtual Machine %s	M	false			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
91	Re-authenticated Virtual Machine %s from KPS	M	false	A virtual machine has been re-authorized.	This message is in response to direct admin actions. No action is required.	Security	Reauth
92	Virtual Machine %s added disk %s	L	false	A new disk has been added to the specified virtual machine.		Security	Key
93	Virtual Machine %s removed disk %s	L	true	A disk has been removed from the specified virtual machine.		Security	Key
94	Virtual Machine %s : disk %s renamed to %s	L	false			Security	Key
95	Virtual Machine %s attempted to fetch key for inactive disk %s. %s	L	false	If a disk is not active, no keys will be delivered.		Security	Key

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
96	Virtual Machine %s attempted to fetch expired key for disk %s. %s	H	false	If a key has expired an attempt by a virtual machine to fetch the key will fail.	The cloud admin should determine whether the expiration date should be extended. This does not apply to shredded keys.	Security	Key
97	Virtual Machine %s fetched key for disk %s. %s	L	false	A key for the specified disk has been requested by the virtual machine shown.		Security	Key
98	Virtual Machine %s created key for disk %s using %s cipher	L	false	A disk has been encrypted. The type of cipher is shown.		Security	Key
99	Virtual Machine %s revoked permission for disk %s	M	true			Security	Key
100	Virtual Machine %s granted permission for disk %s	M	true			Security	Key

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
101	Virtual Machine %s added mount point %s	L	false	An encrypted folder has been mounted.		Security	Key
102	Virtual Machine %s removed fs %s	L	true	An encrypted folder has been removed.		Security	Key
103	Virtual Machine %s attempted to fetch key for inactive fsid %s	M	false	A virtual machine attempted to access an inactive FSID.	The cloud admin should determine whether the FSID should be made accessible.	Security	Key
104	Virtual Machine %s attempted to fetch expired key for fsid %s	H	false	The FSID has expired and therefore the filesystem cannot be mounted.	The cloud admin should determine whether the FSID should be made accessible. This is only possible if the FSID has not been shredded.	Security	Key
105	Virtual Machine %s fetched key for fsid %s	L	false	A filesystem was mounted using the specified FSID.		Security	Key

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
106	The Key for disk %s Virtual Machine %s has expired	H	true	An attempt is being made to change properties for an already expired key.	The cloud admin should determine whether the key of the disk should be made accessible. This is only possible if the disk's key has not been shredded.	Security	Key
107	Virtual Machine %s set key expiry to %s, onexpiry to %s for disk %s	H	false	An expiration date has been set on a key for the specified disk. The effect taken on expiration is shown.	The cloud admin should determine whether the expiration date should be extended.	Security	Key
108	The Certificate for Virtual Machine %s expire%s %d days%s. Please renew the certificate.	M	true			Security	
109	The Key for disk %s Virtual Machine %s has expired	H	true	The key shown for the specified virtual machine has expired.	The cloud admin should determine whether the expiration date should be extended.	Security	Key

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
110	The Key for disk %s Virtual Machine %s expires in %d day(s). Please extend the key life.	H	true	The encryption key shown is about to expire.	The cloud admin should determine whether the expiration date should be extended.	Security	Key
111	Unable to check key for disk %s Virtual Machine %s	M	false	An error occurred while attempting to check properties of key for the given disk and virtual machine.	An internal error occurred while checking expiration/ rotation properties for specified key. Informational only, key will be checked again.	Security	Key
112	Virtual Machine %s rebooted, reauthentication required	H	true	A virtual machine has rebooted and the reboot setting requires that the virtual machine is re-authenticated.	The cloud admin needs to complete re-authorization in the KeyControl WebGUI.	Security	Reauth
113	Virtual Machine %s has new alerts, please check	M	true			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
114	Added Coretrace policy "%s" to Virtual Machine %s	L	true			Security	CoreTrace
115	Activated Coretrace policy "%s" for Virtual Machine %s	M	false			Security	CoreTrace
116	De-activated Coretrace policy "%s" for Virtual Machine %s	M	false			Security	CoreTrace
117	Modified Coretrace policy "%s" for Virtual Machine %s	M	false			Security	CoreTrace
118	Removed Coretrace policy "%s" for Virtual Machine %s	M	false			Security	CoreTrace
119	Deleted CAStore %s	M	false			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
120	Removed Server %s from Domain %s	L	false			Clusters	Domain
121	Storage pool %s created on server %s (%s)	L	false			Security	
122	Storage pool %s extended on server %s (%s)	L	false			Security	
123	Log added to Storage pool %s on server %s (%s)	L	false			Security	
124	Log removed from Storage pool %s on server %s (%s)	L	false			Security	
125	Storage pool %s deleted from server %s (%s)	L	false			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
126	Disk added to hot spare list on server %s (%s)	L	false			Security	
127	Disk removed from hot spare list on server %s (%s)	L	false			Security	
128	Filestore %s created on server %s (%s)	L	false			Security	
129	Filestore %s deleted from server %s (%s)	L	false			Security	
130	Removed server %s (%s) from domain %s	L	true			Clusters	
131	KMIP Server restarted on %s	M	false	The KMIP server has been restarted on the specified host.		Security	KMIPServer

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
132	KMIP Server started on %s	L	true	The KMIP server has been started on the specified host.		Security	KMIPServer
133	KMIP Server halted on %s	H	true	The KMIP server has been halted on the specified host.		Security	KMIPServer
134	KMIP Server: All client certificates removed	H	true	All client certificates have been removed from the KMIP server.		Security	KMIPServer
135	KMIP Server: Client certificate %s removed	H	true	The specified client certificate has been removed from the KMIP server.		Security	KMIPServer
136	KMIP Server: Client certificate %s updated	M	false	The specified client certificate has been updated on the KMIP server.		Security	KMIPServer
137	KMIP Server: Client certificate %s created	M	true	The specified client certificate has been created on the KMIP server.		Security	KMIPServer

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
138	Could not store oskey on %s/%s. Needs recovery	H	true	Could not store object store key on joining KeyControl node	KeyControl join did not succeed, node should be removed from cluster. If problem persists contact support.	Clusters	HCAuth
139	Reconnect not allowed for %s/%s. Please follow reauthentication steps	H	true	KC has attempted to reauthenticate with cluster that does not recognize it	KeyControl node likely was in the cluster and removed. Should be re-joined	Clusters	HCAuth
140	Cluster join failed for %s/%s.	H	true	KC has failed to join cluster	KeyControl node join can be attempted again. If problem persists contact support	Clusters	HCAuth
141	Reconnect info does NOT match. Follow reauthentication steps for node %s/%s	H	true	KC has attempted to reauthenticate with cluster but its info has changed	KeyControl node likely needs MasterKey recovery or kicked out of cluster and re-joined	Clusters	HCAuth

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
142	Could not store connection info for %s/%s	H	true	KC cannot store info to reconnect to cluster on restart	Condition could be transitory, node could be restarted. Also could indicate that KCKeyControl disk is full	Clusters	HCAuth
143	Problem with auth/secd communication	H	true	Communication stack on KC is not working		Clusters	HCAuth
144	System utilities NOT functioning. Authentication will not happen	H	true	Auth daemon unable to query system information		Clusters	HCAuth
145	Attempt to add node %s/%s which has valid data but no clusterid. Please reauthenticate if this is a valid action.	M	true	KC was formerly in a cluster that has no identifying cluster ID	If action is a valid one, proceed with join. Note that the KCKeyControl data on joining node will be destroyed	Clusters	HCAuth

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
146	Attempt to add node %s/%s which has a different clusterid. Please reauthenticate if this is a valid action.	M	true	KC was formerly in a different cluster than the one it is attempting to join	If action is a valid one, proceed with join. Note that the KeyControl data on joining node will be destroyed	Clusters	HCAuth
147	Could not restore cluster to normal operating mode after adding new node, error $rc	M	true	KC cluster state could not be restored to normal operating state	Can indicate cluster join issues	Clusters	HCAuth
148	CSP Vault Management Server system `hostname` ($myip) $act.	L	false			Clusters	
149	Restricted support log in enabled on `hostname`	M	true	Restricted support log in was enabled on KC		Security	
150	%s support log in enabled on `hostname`	M	true	Full or Restricted support log in was enabled on KC		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
151	%s support log in disabled on `hostname`	M	true	Full or Restricted support log in were disabled on KC		Security	
152	KeyControl node {$myip[0]}/{$myhost[0]} has failed upgrade to version {$curver}	H	true	KC upgrade to new version has failed	KeyControl will revert to prior install. Upgrade can be attempted again if valid or contact support	Clusters	Upgrade
153	KeyControl node {$myip[0]}/{$myhost[0]} reverted from {$str[1]} to {$str[2]}	M	true	User initiated revert to previous version has succeeded.		Clusters	Upgrade
154	KeyControl node {$myip[0]}/{$myhost[0]} has successfully upgraded to version {$curver}	M	true	KC upgrade to new version has succeeded.		Clusters	Upgrade
155	KeyControl node {$myip[0]}/{$myhost[0]} has failed upgrade finalization to version {$curver}	H	true	KC upgrade to new version has failed	KeyControl will revert to prior install. Upgrade can be attempted again if valid or contact support	Clusters	Upgrade

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
156	Hostname %s, Management IP %s, Current Version %s, New Version %s. Upgrade from version {$oldver} (b{$oldrevision}) to version {$curver} (b{$newrevision}) not allowed. Consult product documentation for upgrade procedure	H	true	KC upgrade to this version is not supported from current version	Upgrade to a supported version and/or contact support	Clusters	Upgrade
157	Upgrade from version {$oldver} to version {$curver} not officially supported but allowed for development	L	true	KC upgrade to this version is not officially supported but allowed for development build		Clusters	Upgrade
158	Internal error $ret checking upgrade from {$oldver} to {$curver}	H	true	An error has occurred attempting to valid upgrade	Contact support	Clusters	Upgrade
159	Multiple KeyControl nodes still in cluster. All excess KeyControl nodes must be removed before upgrade.	H	true	Upgrade should be attempted on only a single node cluster	Remove all nodes from cluster except the node to be upgraded	Clusters	Upgrade
160	Insufficient free space to perform upgrade. Consult product documentation for procedure to add another disk	H	true	Disk does not have enough space for upgrade	Consult support for freeing disk space or create/join a node with more space and upgrade that	Clusters	Upgrade

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
161	System has reverted to prior installation.	L	true	System has successfully reverted to prior version		Clusters	Upgrade
162	Failed revert to prior installation.	H	true	System failed to revert to prior version	Contact support. Current version is still in place	Clusters	Upgrade
163	System utilities NOT functioning.	H	true	Unable to query system info		Clusters	
164	Error resizing partition	H	true	An error occurred while resizing the KeyControl storage. Please contact support.		Clusters	
165	Error resizing storage pool	H	true	An error occurred while resizing the KeyControl storage. Please contact support.		Clusters	
166	Successfully resized KeyControl storage pool	M	false	The storage pool on the KeyControl node was successfully resized.		Clusters	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
167	KMIP Server operation failed - internal error	M	true	KMIP server operation failed with an internal error.	Consult support or retry operation	Security	KMIPServer
168	%s operation %s for %s on %s, TaskId: %s.	L	false	A task has changed state		Security	
169	Virtual Machine %s : disk %s resized to %s	L	false	Virtual Machine disk is resized		Security	
170	Virtual Machine %s : KC mapping %s attached	L	false	A KC Mapping is attached to a virtual machine		Security	
172	Passwd changed for htadmin	M	true	An admin reset console/ htadmin passwd		Security	
173	User %s failed to change %s passwd	M	true	An administrator attempted to reset the console/htadmin password, but the operation failed.		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
174	A support event has occurred on CSP Vault Management node %s. Please create a Support Bundle and include core files as described in the online help, then contact support.	H	true	A support event has occurred. Generate a support bundle and contact Entrust Support for assistance.		Security	
175	New certificate created with guid %s in group %s	L	false	A new certificate has been created for use with policy agent or KMIP server		Security	
176	Backup created successfully for %s (%s)	L	false	A new backup image has been created on the KeyControl appliance		Clusters	
177	Failed to create backup for %s (%s)	M	false	Creation of the backup image failed.	Backup will be retried automatically or can be triggered manually via the WebGUI	Clusters	
178	KeyControl Cluster is in normal mode	L	false	The KeyControl cluster state has returned to normal operating mode		Clusters	
179	KeyControl Cluster is in degraded mode	H	false	The KeyControl cluster has gone into degraded mode. This occurs when the KeyControl nodes in the cluster are not able to communicate successfully	Check the availability and connectivity of the KeyControl nodes in the cluster	Clusters	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
180	KeyControl Cluster is in standby mode	L	false	The KeyControl cluster is in a standby state. This is a temporary state which occurs when a node is joining the cluster		Clusters	
181	Freespace available on %s has fallen below 2G. Consider increasing the storage capacity of this system.	H	true	The amount of free disk space available to the KeyControl appliance has dropped below our recommended threshold. Please increase the size of the disk or contact support for more assistance	Increase the size of the disk and reboot the KeyControl appliance to resize	Security	
182	Login failure for %s from %s	L	false	User unsuccessfully attempted to log in to the KeyControl instance		Security	
183	Reboot of %s initiated by %s	M	true	Domain administrator initiated reboot of KeyControl node		Clusters	
184	KeyControl node reboot initiated from console	M	true	The KeyControl node was rebooted from the console		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
185	KeyControl node shutdown initiated from console	M	true	The KeyControl node was shut down from the console.		Security	
186	Azure agent: illegal attempt to install plugin	M	true	Azure "extensions" (a.k.a. "plugins") to a KeyControl virtual machine are not allowed		Security	
187	Azure agent: illegal attempt to disable or uninstall a plugin	M	true	Azure "extensions" (a.k.a. "plugins") to a KeyControl virtual machine are not allowed		Security	
188	%d inactive tasks found on Cloud VM Set %s. %s task for %s on %s not updated since %s, TaskId: %s.	L	true	List of tasks that have not been updated for a long time		Security	
189	Updated LDAP configuration: %s	M	false	The values for the given LDAP fields have been updated		Security	
190	Virtual Machine %s synchronized devices. Following devices were not found - %s	M	false	The Policy Agent synchronized the registered device list; some devices not found		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
191	Virtual Machine %s synchronized devices. Reason for sync: %s	M	true	The Policy Agent synchronized the registered device list		Security	
192	Virtual Machine %s state for disk %s changed to %s. %s	L	false	Disk state on policy agent changed		Security	
193	HyTrust bootloader ssh key updated for %s	L	false	Private key required for ssh log in to Hytrust bootloader updated on KC		Security	
194	Two-factor authentication enabled for %s	L	false	Two factor authentication has been enabled for the user		Security	
195	Two-factor authentication disabled for %s	M	true	Two factor authentication has been disabled for the user		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
196	KeyControl Cluster is in degraded mode during node-join	L	false	The KeyControl cluster has gone into degraded mode while a new node is joining the cluster. This occurs as KeyControl restarts communication protocols after a new node has joined the cluster.		Clusters	
197	KeyControl Cluster is in degraded mode during node-join	L	false	The KeyControl cluster has gone into normal mode while a new node is joining the cluster. This occurs as KeyControl restarts communication protocols after a new node has joined the cluster.		Clusters	
198	New AppLink created to %s	M	true	A new Application Link has been created. This link will allow secure communication between the Entrust products.		Clusters	
199	Application link removed for Product (%s) Version (%s) IP List (%s)	L	false	Application link has been removed for the external product.		Clusters	
200	admin user logged in successfully	M	false	htadmin account log in successful in one of the KeyControl nodes		Security	Support

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
201	%s account logged in from	M	false	Full support account log in successful in one of the KeyControl nodes		Security	Support
203	%s account log in failure from -	M	false	Failed attempt to log in to full support account		Security	Support
204	Full support account logged in from and executed	M	false	Full support account log in successful and executed a command		Security	Support
205	%s account log in failure from attempting	M	false	Failed attempt to log in to full support account and execute command		Security	Support
206	Created new log bundle - %s with options - %s	L	false	New log bundle creation has been initiated by some user		Security	
207	Downloaded log bundle - %s	L	false	Latest log bundle has been downloaded by some user		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
208	Exported Cloud VM Set %s	M	false	A Cloud VM Set has been exported		Security	
209	Imported Cloud VM Set %s	M	false	A Cloud VM Set has been imported		Security	
210	Following guests have unsupported policy agent installed in Cloud VM Set %s: %s(%s)	M	true	A Cloud VM Set has guests with unsupported agent version	Upgrade policy agent on reported guests	Security	
211	Unsupported Policy Agent (version %s) detected on guest %s.	M	false	A guest has an unsupported agent version installed	Upgrade policy agent on reported guest	Security	
212	Download of admin key generation %s initiated by %s	M	false	Download of admin key initiated via admin_key GET call		Security	
213	Reset of KMIP server initiated	M	false	Reset of KMIP server initiated		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
214	KMIP Response/Request:	M	false	Create, destroy or revoke of KMIP object initiated		Security	
215	KMIP Response/Request:	M	false	Operation on some KMIP object initiated		Security	
216	The Certificate for Virtual Machine %s will auto-renew in %d days%s.	L	true			Security	
217	The Certificate for Virtual Machine %s failed to auto-renew. Certificate expire%s %d days%s. Please renew the certificate.	H	true			Security	
218	Set Key Encryption Key expiry to %s onexpiry to %s, for Cloud VM Set %s. %s Cloud VMs affected.	H	false	An expiration date has been set for Key Encryption Key for the specified Cloud VM Set. The effect taken on expiration is shown.	The cloud admin should determine whether the expiration date should be extended.	Security	Key Encryption Key

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
219	The Key Encryption Key for Cloud VM Set %s expire%s in %d days%s.	H	true		The cloud admin should determine whether the expiration date should be extended.	Security	Key Encryption Key
220	The Key Encryption Key for Cloud VM Set %s has expired. %s Cloud VMs affected.	H	true	The Key Encryption Key for specified Cloud VM Set has expired.	The cloud admin should determine whether the expiration date should be extended.	Security	Key Encryption Key
221	Access to Key Encryption Key of Cloud VM Set %s has been revoked. %s Cloud VMs affected.	H	true	Access to specified Cloud VM Set has been revoked.		Security	Key Encryption Key
222	Access to Key Encryption Key of Cloud VM Set %s has been granted. %s Cloud VMs affected.	H	true	Access to specified Cloud VM Set has been granted.		Security	Key Encryption Key
223	The Key Encryption Key for Cloud VM Set %s has expired. %s Cloud VMs deleted. Deleted CVM Set %s.	H	true	The Key Encryption Key for specified Cloud VM Set has expired.		Security	Key Encryption Key

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
224	The Certificate for Virtual Machine %s failed to auto-renew as the Virtual Machine is unreachable.	H	true	The Certificate Auto Renewal of a virtual machine fails if the virtual machine is in auto renewal period and is unreachable.		Security	
225	Authentication of Server %s (%s) failed due to incorrect passphrase	H	false	Authentication of KeyControl node failed due to incorrect passphrase.		Security	
226	Cloud VM Set creation failed. Error: Failed to store key in HSM. %s	H	true	Cloud VM Set creation failed. Failed to store key in HSM.	A security admin should check whether the HSM connection is configured properly	Security	Key Encryption Key
227	Key Encryption Key import failed. Error: Failed to store key in HSM. %s	H	true	Key Encryption Key import failed. Failed to store key in HSM.	A security admin should check whether the HSM connection is configured properly	Security	Key Encryption Key
228	Failed to fetch Key Encryption Key from HSM. Error: %s	H	true	Failed to fetch Key Encryption Key from HSM.	A security admin should check whether the HSM connection is configured properly	Security	Key Encryption Key

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
229	Successfully imported Key Encryption Key for Cloud VM Set %s.	M	false	Successfully imported Key Encryption Key		Security	Key Encryption Key
230	Removed Domain %s from group %s	L	false	Removed Domain from group		Security	
231	Authenticated Server %s (%s)	L	false	New KeyControl node has been successfully authenticated and added to the cluster		Clusters	
232	Added Server %s (%s) to Domain %s	L	false	Server has been successfully added to a domain		Clusters	
233	Invalid Key Encryption Key size specified for Cloud VM Set %s.	H	true	Invalid Key Encryption Key size	Verify that the Key Encryption Key size is 128 bits or 256 bits	Security	Key Encryption Key
234	Retention period has expired for Cloud VM Set %s. %s Cloud VMs deleted. Deleted Cloud VM Set %s.	L	true	Retention period has expired for Cloud VM Set		Security	Key Encryption Key

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
235	Retention period for Cloud VM Set %s will expire in %d days.	H	true	Retention period expiration for Cloud VM Set	The cloud admin should determine whether the retention date should be extended.	Security	Key Encryption Key
236	Set Retention Date to %s for Cloud VM Set %s.	L	false	Changed Retention period for Cloud VM Set		Security	Key Encryption Key
237	Failed to delete Key Encryption Key from HSM for Cloud VM Set %s. Error: %s.	M	true	Failed to delete Key Encryption Key from HSM		Security	Key Encryption Key
238	New CA Certificate added to Certificate Store for verifying %s	L	false	New CA certificate has been added to verify some subsystem		Clusters	
239	CA Certificate for %s removed from Certificate Store	H	false	CA Certificate for some subsystem has been removed from Certificate Store		Clusters	
240	Authentication for LDAP user %s failed. Reason :- %s	H	false	Reason for LDAP log in failures		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
241	Cannot register Cloud VM until Key Encryption Key for Cloud VM Set %s is imported	L	true	Cannot register Cloud VM		Security	Key Encryption Key
242	Virtual Machine %s HTcrypt driver update -- %s	L	false	HTcrypt driver state on policy agent changed		Security	
243	New self-signed certificates generated for %s	L	false	New self-signed certificates generated for server		Clusters	Certificate
244	New SSL certificate installed for %s	L	false	New SSL certificate installed for server		Clusters	Certificate
245	CSR generated with common name - %s	L	false	New CSR generated		Clusters	Certificate
246	Web server for %s restarted	L	false	Webserver/Apache restarted for server		Clusters	Certificate

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
247	Certificate installation task got timed out. There are VMs that did not receive the new CA certificate. Please contact Cloud Administrators to log in to the Virtual Machine and execute hcl heartbeat before restarting the webserver	H	true	One (or more) policy agents did not receive the new CA certificate uploaded. Cloud administrator has to log in to the policy agent and execute hcl heartbeat		Clusters	Certificate
248	Cannot update CA as part of SSL certificate installation for %s. Please log in to the Virtual Machine and execute hcl heartbeat	H	true	Domain Administrator has attempted to install a new SSL certificate for the webserver. Unfortunately one of the policy agents did not receive a copy of the new CA certificate that can verify the SSL certificate of the webserver. Cloud administrator has to log in to the policy agent and execute hcl heartbeat		Clusters	Certificate
249	External web server certificate of %s has expired. A new certificate must be installed before the associated VMs can communicate with %s. After the new certificate has been installed, the certificate information on the associated VMs must be manually updated if the new certificate is from a different Certificate Authority. For more information, search for certificates in the WebGUI online help.	H	true	Certificate used by the external webserver of one of the nodes has expired. Domain administrator has to install a new certificate. If the newly installed certificate is generated by a new CA, cloud administrators will have to log in to policy agent and update the CA certificate file. The latest CA certificate file can be found in the cloud tab in WebGUI		Clusters	Certificate

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
250	External web server certificate of %s will expire in %s days, %s hours and %s minutes. If another certificate is not installed before the current one expires, the VMs will not be able to communicate with %s after %s and all VMs may need to be manually updated after the new certificate is installed. For more information, search for certificates in the WebGUI online help.	H	true	Certificate used by the external webserver of one of the nodes is about to expire. Domain administrator has to install a new certificate before it gets expired. Otherwise policy agents will not be able to communicate with the KC after expiry		Clusters	Certificate
251	CA certificate used for verifying %s:%s on %s has already expired. Please upload a new CA certificate to verify the %s server certificate. Otherwise %s users will not be able to log in to the WebGUI.	H	true	CA certificate used by the LDAP server has already expired. Security Administrator has to install a new certificate to verify the LDAP server certificate. Otherwise LDAP users will not be able to log in to the WebGUI.		Clusters	Certificate
252	CA certificate used for verifying %s:%s on %s will expire in %s days, %s hours and %s minute. If another CA certificate is not installed before the current one expires, %s users will not be able to log in to the WebGUI after %s.	M	true	CA certificate used for evaluating LDAP server certificate is about to expire. Security Administrator has to install a new certificate before the current one expires. Otherwise LDAP users will not be able to log in to the WebGUI after the CA certificate expiry date.		Clusters	Certificate

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
253	Certificate for %s:%s has already expired. Please re-configure %s after updating the certificate in %s.	H	true	Certificate for APPLINK has already expired. APPLINK should be reconfigured after uploading a new certificate.		Clusters	Certificate
254	Certificate for %s:%s will expire in %s days, %s hours and %s minutes. Once the certificate of %s is updated, please re-configure the %s:%s	M	true	Certificate for APPLINK is about to expire. Security Administrator has to install a new certificate and re-configure the APPLINK before the current one expires.		Clusters	Certificate
255	KeyControl Cluster is in maintenance mode	L	false	The KeyControl cluster is in maintenance state. This is a temporary state which occurs during upgrade process		Clusters	
256	Virtual Machine with IP %s is a possible clone of %s (%s) and hardware signature verification is turned off.	H	true	A possible clone of a virtual machine that is already registered has been detected. Verify that the virtual machine is valid and register it as a new virtual machine using 'hcl register -c' command.		Security	
257	CSP Vault node %s has been successfully upgraded from version %s to version KC %s	M	true	CSP Vault node upgrade to new version has succeeded.		Clusters	Upgrade
258	CSP Vault node %s has been successfully reverted from version %s to version KC %s	M	true	CSP Vault node revert to old version has succeeded		Clusters	Upgrade

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
259	Access Control Policy: %s, at version: %s applied to disk: %s on Virtual Machine: %s	H	true	Access Controls Policy version update to disk.		Security	Access Control
260	Access Control Policy removed from disk: %s on Virtual Machine: %s	H	true	Access Controls Policy removed.		Security	Access Control
261	New Access Control Policy: %s created.	L	false	New Access Control Policy Created.		Security	Access Control
262	Access Control Policy: %s updated. Policy now available as: %s.	H	false	Access Control Policy Updated.		Security	Access Control
263	Access Control Policy: %s deleted.	L	false	Access Control Policy Deleted.		Security	Access Control
264	Access Control Rule: %s added to Policy: %s.	H	false	New Access Control Rule added to Policy.		Security	Access Control

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
265	Access Control Rule: %s updated for Policy: %s.	H	false	Access Control Rule updated for Policy.		Security	Access Control
266	Access Control Rule: %s deleted from Policy: %s.	H	false	Access Control Rule deleted from Policy.		Security	Access Control
267	hytrust_accesscontrols rpm state changed to: %s on Virtual Machine: %s	M	false	HyTrust Access Controls rpm state changed		Security	Access Control
268	Initiated application of Access Control Policy: %s to disk: %s on Virtual Machine: %s.	H	false	Access Control Policy application initiated by Admin.		Security	Access Control
269	Initiated removal of Access Control Policy: %s from disk: %s on Virtual Machine: %s.	H	false	Access Control Policy removal initiated by Admin.		Security	Access Control
270	Created Cloud VM Set %s with Single Encryption Key	L	true	CVMSet created with Single Encryption Key for dedup		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
271	Failed to upgrade KeyControl nodes: %s. Reverting upgraded nodes: %s.	L	true	Failed to upgrade KeyControl nodes.		Clusters	Upgrade
272	Failed to revert KeyControl nodes: %s. Remove nodes from KeyControl after reboot.	L	true	Failed to revert KeyControl nodes.		Clusters	Upgrade
273	Upgrade Cancelled. Error: %s	L	true	Failed to finalize upgrade.		Clusters	Upgrade
274	%s got reverted during upgrade. Reverting other nodes in the cluster to revision %s	L	false	Failed to upgrade KeyControl node.		Clusters	Upgrade
275	Successfully cancelled KeyControl Upgrade.	M	false	Cancelled KeyControl Upgrade.		Clusters	Upgrade
276	IP conflict detected for %ipaddr with MAC %this_mac on %this_month %this_day %this_time	H	true	Another virtual machine is/was using this KeyControl IP address.		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
277	Access Controls removed successfully on Virtual Machine %s	H	true	Successful Access Controls removal on virtual machine		Security	Access Control
278	Applying Policy %s, version %s failed on Virtual Machine %s. %s	H	true	Policy application failure on virtual machine with reason.		Security	Access Control
279	Applying Policy %s, version %s failed on disk %s of Virtual Machine %s	H	true	Failure in Policy application on a specific disk of a virtual machine.		Security	Access Control
280	Error removing Access Control Policy on disk %s of Virtual Machine %s	H	true	Error removing Access Control Policy on a disk.		Security	Access Control
281	%s doesn't allow local user creation. Cannot support Access Controls	H	true	Virtual machine doesn't support Access Controls due to inability to create local users		Security	Access Control
282	%s doesn't allow ssh for localhost. Cannot support Access Controls	H	true	Cannot setup Access Controls on virtual machine since it doesn't allow ssh for localhost		Security	Access Control

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
283	%s doesn't allow password-based ssh log in. Cannot support Access Controls	H	true	Cannot setup Access Controls on virtual machine since it doesn't allow password-based ssh log in.		Security	Access Control
284	Access Control setup failed on Virtual Machine %s. Please check /var/log/htac.log on Virtual Machine for more details	H	true	Failure in initial Access Controls setup		Security	Access Control
285	Insufficient free space on %s to perform upgrade. Consult product documentation for procedure to add another disk	H	true	Disk does not have enough space for upgrade	Consult support for freeing disk space or create/join a node with more space and upgrade that	Clusters	Upgrade
286	Access Control tampering detected on Virtual Machine %s	H	true	Access Control Tampering		Security	Access Control
287	Error enforcing policy %s, version %s on Virtual Machine %s. %s	H	true	Access Control Policy application failure due to htadmin error		Security	Access Control

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
288	New AD Server: %s created.	L	false	Create AD Server		Security	Active Directory
289	Updated AD Server config: %s.	L	false	Updated AD Server config		Security	Active Directory
290	Deleted AD Server: %s.	L	false	Deleted AD server		Security	Active Directory
291	User account htadmin already exists on Virtual Machine %s. Please delete htadmin, before enforcing Access Control Policy	L	true	Local user account htadmin detected before Access Control pre-setup tests		Security	Access Control

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
292	Virtual Machine - %s cannot verify communications from KeyControl because the KeyControl SSL certificate has changed but the CA certificate on the Virtual Machine was not updated when the new SSL certificate was installed for KeyControl. To update the CA certificate on the Virtual Machine and restore connectivity, log into the WebGUI, download the latest CA certificate from Cloud tab > Actions > Download CA Certificate, copy the CA certificate to the Virtual Machine, and execute "hcl update_ca -f </path/to/cert>"	H	true	SSL certificate of KeyControl has changed and webserver has been restarted. One of the VMs did not receive the latest copy of the CA certificate to verify KeyControl. To restore communication, download the latest CA certificate from WebGUI cloud tab, copy it to the virtual machine and execute hcl update_ca command		Security	Certificate
295	Virtual Machine %s is using an older Hardware Signature format. Please run "hcl auth" cmd on the Virtual Machine for a more secure signature.	H	true	Virtual machine is using an older Hardware Signature format. Please run "hcl auth" cmd on the virtual machine for a more secure signature.		Security	Client
296	Alert email sent to Security Admins on upgrade.	L	true	Alert email sent to Security Admins on upgrade.		Security	
297	Abandoning %d inactive tasks on %s. Abandoning %s task %s on %s not updated since %s, TaskId: %s	L	true	List of tasks that have been abandoned due to inactivity		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
298	Error!!! Could not enable support log in. Please make sure there is enough space in the filesystem	H	true	Cannot enable support log in. Please make sure there is enough space in the file-system	Increase the size of the disk and reboot the KeyControl appliance to resize	Security	Support
299	Error!!! Could not disable support log in. Please make sure there is enough space in the filesystem	H	true	Cannot disable support log in. Please make sure there is enough space in the file-system	Increase the size of the disk and reboot the KeyControl appliance to resize	Security	Support
300	%s attempting %s account log in when object store is not readable	M	false	Attempt to log in to support log in in one of the KeyControl nodes when object store is down		Security	Support
301	Decryption is not allowed for device %s on Virtual Machine %s. To decrypt: Access Control Policy : %s Version: %d must be removed from device. Auto Encryption Policy should be changed so as to exclude the device.	L	true	Device decryption refused due to applied policies.	Change policies as suggested in error message.	Security	
302	Space on HyTrust Bootloader partition %s is running low (%lld bytes free). Often times USN journal is the culprit. You can check USN journal size using the command: "fsutil usn queryjournal %s". To delete USN journal, use the command: "fsutil usn deletejournal /N %s "	H	true	Device decryption refused due to applied policies.	Change policies as suggested in error message.	Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
303	Login failure for %s from %s because %s is in lock out period.	M	false	Attempt to log in to secroot in the lock out period after repeated unsuccessful log in attempts		Security	Account
304	Changed AD group members for group %s. %s	L	false	List of AD Group members has been changed for a KeyControl Group		Security	Group
305	The current number of KeyControl nodes (%d) exceeds the maximum number of nodes allowed by your license (%d). You cannot add any more KeyControl nodes to this cluster until you upgrade your license.	M	true	KeyControl nodes in use exceeds license limit of installed license		Security	Licensing
306	The current number of VMs registered with this KeyControl cluster (%d) exceeds the maximum number of VMs allowed by your license (%d). You cannot register any additional VMs until you upgrade your license.	M	true	Registered virtual machine count exceeds license limit of installed license		Security	Licensing
307	Service %s is up	L	false	KeyControl system service is up		Security	SystemService

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
308	Service %s is down	H	true	KeyControl system service is down		Security	SystemService
309	Using AD group membership for %s - %s	M	false	AD group membership of the AD user that was returned by the LDAP server during first time log in. The AD group membership will be used to determine the KeyControl Group membership of the AD user.		Security	Licensing
310	Updating AD group membership for %s - %s	M	false	AD group membership of the AD user that was returned by the LDAP server. The new AD group membership will be used to determine the KeyControl Group membership of the AD user who has already logged into KeyControl previously.		Security	Licensing
311	Added KMIP client configuration. Server: %s	L	false	Added KMIP client configuration		Security	KMIP Client

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
312	Updated KMIP client configuration. Server: %s	L	false	Updated KMIP client configuration		Security	KMIP Client
313	Deleted KMIP client configuration. Server: %s	H	true	Deleted KMIP client configuration		Security	KMIP Client
314	Deleted all KMIP client configurations.	H	true	Deleted KMIP client configuration		Security	KMIP Client
315	Failed to delete key:%s on external KMIP server	M	false	Failed to delete key on KMIP server		Security	KMIP Client
316	Added AD Domain: %s	L	false	Added a new AD Domain		Security	LDAP
317	Updated AD Domain %s. Changed Attributes - %s	L	false	Updated the AD Domain		Security	LDAP

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
318	Removed AD Domain %s	L	false	Removed AD Domain from KeyControl		Security	LDAP
319	Added new Domain Controller %s for AD Domain %s	L	false	Added a new AD Domain Controller		Security	LDAP
320	Updated Domain Controller %s for AD Domain %s. Changed Attributes - %s	L	false	Updated Domain Controller		Security	LDAP
321	Removed Domain Controller %s for AD Domain %s	L	false	Removed Domain Controller from KeyControl		Security	LDAP
322	encrypt failed for device %s on Virtual Machine %s, error %d	M	true	Encrypt operation failed on virtual machine		Security	Client
323	decrypt failed for device %s on Virtual Machine %s, error %d	M	true	Decrypt operation failed on virtual machine		Security	Client

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
324	rekey failed for device %s on Virtual Machine %s, error %d	M	true	Rekey operation failed on virtual machine		Security	Client
325	Successfully deleted admin key on EKS: %s	M	false	Successfully deleted admin key on KMIP server		Security	KMIP Client
326	Successfully generated admin key on EKS: %s	M	false	Successfully generated admin key on KMIP server		Security	KMIP Client
327	Failed to generate admin key on EKS: %s	H	true	Failed to generate admin key on KMIP server		Security	KMIP Client
328	Failed to store admin key on EKS: %s	H	true	Failed to store admin key on KMIP server		Security	KMIP Client
329	Successfully stored admin key on EKS: %s	M	false	Successfully stored admin key on KMIP server		Security	KMIP Client

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
330	Failed to fetch admin key from EKS: %s	M	true	Failed to fetch admin key from KMIP server		Security	KMIP Client
331	KeyControl Upgrade failed. Please contact Support	H	true	Post upgrade failed		Clusters	Rolling Upgrade
332	Domain Controllers re-ordered for %s	L	false	Order of Domain Controllers has been changed for an AD domain configured		Security	LDAP
333	Failed to set backup hosts to %s on %s	H	true	Failed to update backup hosts		Security	
334	Virtual Machine %s is in BoundaryControl grace period	M	true	Virtual machine in Boundary Control grace period		Security	Boundary Control
335	Virtual Machine %s, BoundaryControl grace period expired	M	true	Virtual machine Boundary Control grace period expired		Security	Boundary Control

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
336	Application Link created from Product (%s) Version (%s) IP List (%s)	L	false	A new Application Link has been created from an external product. This link will allow the external product to make API calls to KeyControl.		Clusters	AppLink
337	Application Link renewed for Product (%s) Version (%s) IP List (%s)	L	false	An Application Link has been renewed for the external product.		Clusters	AppLink
338	Failed to upgrade LDAP Settings. Please reconfigure LDAP settings manually	H	true	Failed to upgrade LDAP Settings.		Security	LDAP
339	Failed to store admin key on HSM	H	true	Failed to store admin key on HSM		Security	HSM
340	Removed Server(s) %s from Domain %s	L	true			Clusters	
341	Grace period will expire on %s for Virtual Machine %s, please check connectivity	H	true			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
342	Grace period expired for Virtual Machine %s, please authenticate again	H	true			Security	
343	Virtual Machine %s, failed to update following attributes: %s	H	false	Failed to update virtual machine settings		Security	
344	Finished propagating changed attributes: %s to all Virtual Machines in Cloud VMSet: %s	H	false	Propagation of changed attributes completed for CVMSet		Security	
345	Invalid software was discovered on KeyControl system %s. This is a possible trojan horse attack. Contact Support for assistance	H	true	Whitelisting violation detected on production build		Security	Whitelisting
346	Entrust Whitelist validation on KeyControl system %s has discovered modified files. These changes are allowed for development systems, but please review Whitelist logs for correctness.	L	true	Whitelisting violation detected on development build		Security	Whitelisting

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
347	Could not set password for %s: %s	H	true	Failed to set password		Security	
348	Password changed for %s	H	true	Password changed		Security	
349	Enabled %s user	H	true	Enabled user		Security	
350	Failed to enable %s user	H	true	Failure in enabling user		Security	
351	Disabled %s account	H	true	Disable account		Security	
352	%s user logged out successfully	L	false	User logout		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
353	Could not download the certificate: %s	M	true	Download certificate failure		Security	
354	Downloaded a new CA certificate	M	true	Downloaded CA certificate		Security	
355	ssh %sd for %s	M	false	SSH enabled/disabled for user		Security	
356	Failed to %s ssh for %s	M	false	Failure in enabling/ disabling SSH for user		Security	
357	KeyControl restored from version %s backup file	M	false	KeyControl restored from backup successfully		Security	
358	License auto-update: %s	M	true	License change during auto-update		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
359	Failed to %s syslog on %s	H	true	Failed to enable/disable syslog on KeyControl node(s)		Security	syslog
360	Generated Syslog Certificate Signing Request with common name %s	L	false	Generated Syslog Certificate Signing Request with common name		Security	syslog
361	Changed following Syslog settings attributes: %s	L	false	Changed some Syslog settings attributes.		Security	syslog
362	Exporting audit log succeeded for %s (%s). Audit log is available to download.	M	true	Finish exporting audit log		Security	
363	Exporting audit log failed for %s (%s).	M	true	Exporting audit log failed		Security	
364	CVM Certificate %s, associated with CVM %s, CVMSet %s, revoked successfully	H	true			Security	Certificate

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
365	Cloud VM Set creation failed. Error: Failed to create root key in HSM. %s.	H	true	Root key creation failure on HSM during Cloud VM Set creation.	Security Admin should determine whether HSM is properly configured.	Security	Key Encryption Key
366	Cloud VM Set creation failed. Error: Failed to generate wrapped Key Encryption Key in HSM. %s.	H	true	Wrapped Key Encryption Key generation failed on HSM during Cloud VM Set creation	Security Admin should determine whether HSM is properly configured.	Security	Key Encryption Key
367	Virtual Machine %s moved from Cloud VM Set - %s (in KeyControl Group - %s) to Cloud VM Set - %s in (KeyControl Group - %s)	M	true	The virtual machine has been moved from one Cloud VM Set to another (which may belong to a different KeyControl Group).		Security	
368	Successfully enabled passphrase based startup authentication	M	false	Set startup authentication type		Clusters	Startup Authentication
369	Successfully changed passphrase for startup authentication	M	false	Changed passphrase for startup authentication		Clusters	Startup Authentication

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
370	Recovered access to KeyControl node %s using passphrase	M	true	Recovered Masterkey using passphrase		Clusters	Startup Authentication
371	Successfully disabled passphrase based startup authentication	M	false	Set startup authentication type		Clusters	Startup Authentication
372	Successfully reset nShield HSM configuration	M	false	nShield HSM configuration reset		Security	HSM
373	Cloud VM Set %s: Asymmetric KeyID %s created.	M	false	Asymmetric KeyID created		Security	Asymmetric KeyID
374	Cloud VM Set %s: Asymmetric KeyID %s revoked/unrevoked.	M	false	Asymmetric KeyID revoked/unrevoked		Security	Asymmetric KeyID

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
375	Cloud VM Set %s: Asymmetric KeyID %s updated - expires %s, onexpiry %s.	M	false	Asymmetric KeyID expiration attributes updated		Security	Asymmetric Key ID
376	Cloud VM Set %s: Asymmetric KeyID %s description updated.	M	false	Asymmetric KeyID description updated		Security	Asymmetric Key ID
377	Cloud VM Set %s: Asymmetric KeyID %s deleted.	M	false	Asymmetric KeyID deleted		Security	Asymmetric Key ID
378	Successfully encrypted plaintext using KeyID: %s	M	false	Encrypted plaintext using keyid key		Security	Key ID
379	Successfully decrypted ciphertext using KeyID: %s	M	false	Decrypted ciphertext using keyid key		Security	Key ID
380	Cloud VM Set %s: Asymmetric KeyID %s has expired	M	true	Asymmetric KeyID expired		Security	Asymmetric Key ID

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
381	Fatal error on KeyControl nodes: %s. Please contact Support	H	true	KeyControl Upgrade Failure	Reinstall specified nodes to secure KeyControl Cluster	Security	Rolling Upgrade
382	CRL regenerated and applied successfully on %s	M	false	CRL regeneration		Security	Certificate
383	Attempt to register a new KeyControl node (%s) with revision %s failed. Error: %s	M	true	Attempt to register a new KeyControl node failed		Clusters	Cluster Node Join
384	Successfully reset %s	M	true	The KeyControl node has been reset.		Clusters	Cluster Node Join
385	%s. Please contact Entrust to purchase or renew the license. If you do not plan to use this feature, you should delete your existing vault(s) to stop this message. For more information, see the Administration Guide.	M	true	Vault license not enabled or expired		Security	Licensing

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
386	Created Secrets Vault %s	M	false	The specified vault has just been created.		Security	SecretsVault
387	Successfully removed pre-upgrade snapshots.	M	true	KC pre-upgrade snapshots were removed.		Clusters	Upgrade
388	KeyControl node {$myip[0]}/{$myhost[0]} removed pre-upgrade snapshots.	M	true	KC pre-upgrade snapshots were removed from a node.		Clusters	Upgrade
389	KeyControl configuration has been successfully updated. New node %s needs to be added to nShield HSM server configuration	M	true	Update nShield HSM server configuration		Security	HSM
390	Failed to configure newly joined node %s for nShield HSM server	H	true	Failed to configure node for nShield HSM		Security	HSM
391	Successfully completed decryption of KMIP objects	H	true	Decrypt operation completed for KMIP objects		Security	KMIP

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
392	Successfully completed rekey of KMIP objects	H	true	Rekey operation completed for KMIP objects		Security	KMIP
393	Successfully enabled encryption of KMIP objects	H	true	Enabled encryption of KMIP objects		Security	KMIP
394	Successfully disabled encryption of KMIP objects	H	true	Disabled encryption of KMIP objects		Security	KMIP
395	Failed to generate Key Encryption Key on HSM. Error: %s	H	true	Failed to generate Key Encryption Key on HSM		Security	KMIP
396	Successfully generated Key Encryption Key on HSM	M	false	Generated Key Encryption Key on HSM		Security	KMIP
397	Successfully cancelled node-join	M	false	Cancelled KeyControl Node-Join		Clusters	ClusterNodeJoin

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
398	Failed to join %s to KeyControl Cluster. Error: %s	M	true	Failed to join KeyControl node		Clusters	ClusterNodeJoin
399	Successfully joined %s to KeyControl Cluster	M	false	Added new node to KeyControl Cluster		Clusters	ClusterNodeJoin
400	CSR generated with common-name %s for node-join	M	false	Certificate Signing Request generated for node-join		Clusters	ClusterNodeJoin
401	Certificate bundle generated for node-join	M	false	Certificate bundle generated for node-join		Clusters	ClusterNodeJoin
402	Returning keys to Virtual Machine %s running on ESXi Host %s. Virtual Machine UUID is %s.	M	false	Returning keys to virtual machine on successful authorization with HTCC with additional virtual machine info		Security	GET-KEY Container

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
403	Returning keys to Virtual Machine %s	M	false	Returning keys to virtual machine on successful authorization with HTCC		Security	GET-KEY Container
404	NTP servers not found on KeyControl %s	H	true	NTP servers not found on KeyControl	Configure NTP servers using KeyControl TUI	Clusters	NTP
405	NTP synchronization failed on KeyControl %s	M	true	NTP synchronization failed on KeyControl	Check if NTP servers are reachable from KeyControl	Clusters	NTP
406	Freespace available on %s has fallen below %s%% for the /boot volume. Please contact support.	H	false	The amount of free disk space on the KeyControl appliance /boot filesystem has dropped below our recommended threshold. Please contact support for assistance.	Contact support.	Clusters	
407	Set Key Encryption Key expiry to %s, onexpiry to %s for Cloud VMSet %s. Initiated rekey process to encrypt all Data Encryption Keys.	M	false	Added Key Encryption Key to Cloud VMSet		Security	Key Encryption Key
408	Successfully encrypted Data Encryption Keys of all CVMs in CVMSet: %s with a Key Encryption Key: %s. %s VMs, %s KeyIDs %s Asymmetric KeyIDs affected	M	false	Successfully encrypted Data Encryption Keys with Key Encryption Key		Security	Key Encryption Key

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
409	Successfully reset Luna HSM configuration	M	false	Luna HSM configuration reset		Security	HSM
410	Successfully tested nShield HSM configuration	M	false	nShield HSM configuration was successfully tested		Security	HSM
411	Luna HSM configuration changed:-	M	false	Luna HSM configuration changed		Security	HSM
412	Successfully tested Luna HSM configuration	M	false	Luna HSM configuration was successfully tested		Security	HSM
413	Luna Cloud HSM configuration changed:-	M	false	Luna Cloud HSM configuration changed		Security	HSM
414	Successfully reset Luna Cloud HSM configuration	M	false	Luna Cloud HSM configuration was reset		Security	HSM

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
415	Successfully tested Luna Cloud HSM configuration	M	false	Luna Cloud HSM configuration was successfully tested		Security	HSM
416	Failed to create /bootext filesystem. Please contact support for more assistance	H	true	Failed to create /bootext filesystem. Please contact support for more assistance		Security	
417	Failed to join %s/%s to KeyControl Cluster. Please contact Support	H	true	Failed to join KeyControl node to cluster		Clusters	ClusterNodeJoin
418	CloudKey: {} in KeySet {} modified	M	true	CloudKey: {} in KeySet {} modified		Security	BYOK
419	CloudKey: {} in KeySet {} migrated to HSM	M	false	CloudKey: {} in KeySet {} migrated to HSM		Security	BYOK
420	Cloud Key {} deleted from KMS	H	true	Cloud Key {} deleted from KMS		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
421	Cloud Key {} restored to KMS	M	true	Cloud Key {} restored to KMS		Security	BYOK
422	Cloud Key {} state changed to {} on KMS	H	true	Cloud Key {} state changed to {} on KMS		Security	BYOK
423	Tag {} (value {}) set on Cloud Key {}	M	false	Tag {} (value {}) set on Cloud Key {}		Security	BYOK
424	Removed Tag {} on Cloud Key {}	M	false	Removed Tag {} on Cloud Key {}		Security	BYOK
425	Set users ({}) and administrators ({}) to Cloud Key {}	M	true	Set users ({}) and administrators ({}) to Cloud Key {}		Security	BYOK
426	Removed {} ({}) from Cloud Key {}	M	true	Removed {} ({}) from Cloud Key {}		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
427	New Cloud Key {} created in KeySet {}	M	true	New Cloud Key {} created in KeySet {}		Security	BYOK
428	New Cloud Key {} created in KeySet {} {} {}	M	true	New Cloud Key {} created in KeySet {} Region/Vault {}		Security	BYOK
429	Cloud Key {} in KeySet {} uploaded to {} {}	M	true	Cloud Key {} in KeySet {} uploaded to {} {}		Security	BYOK
430	Cloud Key {} in KeySet {} rotated	M	true	Cloud Key {} in KeySet {} rotated		Security	BYOK
431	Cloud Key {} in KeySet {} scheduled for deletion in {} days	H	true	Cloud Key {} in KeySet {} scheduled for deletion in {} days		Security	BYOK
432	Deletion schedule canceled on Cloud Key {} in KeySet {}	M	true	Deletion schedule canceled on Cloud Key {} in KeySet {}		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
433	Cloud Key {} in KeySet {} deletion complete	M	false	Cloud Key {} in KeySet {} deletion complete		Security	BYOK
434	Processed Expiry Action {} on Cloud Key {} in KeySet {}	H	true	Processed Expiry Action {} on Cloud Key {} in KeySet {}		Security	BYOK
435	Cloud Key {} region {} imported in KeySet {}	M	false	Cloud Key {} region {} imported in KeySet {}		Security	BYOK
436	Started Key Import from {} {} from KMS to KeySet {}	M	true	Started Key Import from region/keyvault/keyring {} from KMS to KeySet {}		Security	BYOK
437	Keys imported from {} {} from KMS to KeySet {}	M	true	Keys imported from region/keyvault/keyring {} from KMS to KeySet {}		Security	BYOK
438	Keys imported from AWS KMS to KeySet {}	M	true	Keys imported from AWS KMS to KeySet {}		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
439	Keys migrated to HSM from KEYCONTROL for KeySet {}	H	true	Keys migrated to HSM from KEYCONTROL for KeySet {}		Security	BYOK
440	KeySet: {} modified	M	true	KeySet: {} modified		Security	BYOK
441	Started key migration, from {} to {}, for KeySet {}	H	true	Started key migration for KeySet		Security	BYOK
442	New KeySet: {} created	M	true	New KeySet: {} created		Security	BYOK
443	Key Set {} deleted	H	true	Key Set {} deleted		Security	BYOK
444	CSP Account: {} modified	M	true	CSP Account: {} modified		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
445	CSP Account {} access keys rotated	H	true	CSP Account {} access keys rotated		Security	BYOK
446	New CSP Account: {} created	M	true	New CSP Account: {} created		Security	BYOK
447	CSP Account {} deleted	H	true	CSP Account {} deleted		Security	BYOK
448	Access key rotation failed	H	true	Access key rotation failed		Security	BYOK
449	CloudKey rotation failed	M	true	CloudKey rotation failed		Security	BYOK
450	CloudKey expiry processing failed	M	true	CloudKey expiry processing failed		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
451	CloudKey import failed	M	true	CloudKey import failed		Security	BYOK
452	CloudKey auto import failed	M	true	CloudKey auto import failed		Security	BYOK
453	Set Key Policy for Cloud Key {}	M	true	Set Key Policy for Cloud Key		Security	BYOK
455	Encryption finished on system volumes of KeyControl {}	M	false	Encryption finished on system volumes of KeyControl		Clusters	BYOK
456	Successfully installed managed Secret Vault Plugin: {} (version {})	M	false	Managed Secret Vault Plugin install success		Security	SecretsVault
457	Cloud Key {} in KeySet {} deleted as upload failed	L	false	Cloud Key object deleted as upload failed		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
458	Enabled Root-of-Trust in password mode	M	false	Enabled Root-of-Trust in password mode		Security	HSMROT
459	Failed to enable Root-of-Trust	M	false	Failed to enable Root-of-Trust		Security	HSMROT
460	Enabled Root-of-Trust in hwsig mode	M	false	Enabled Root-of-Trust in hwsig mode		Security	HSMROT
461	Failed to enable Root-of-Trust	M	false	Failed to enable Root-of-Trust		Security	HSMROT
462	Disabled Root-of-Trust	M	false	Disabled Root-of-Trust		Security	HSMROT
463	Failed to disable Root-of-Trust: %s	M	false	Failed to disable Root-of-Trust: %s		Security	HSMROT

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
464	A different Cloud Key with name {} for KeyVault {} is already present in KeySet {}.If you want to overwrite the key in KeyControl node, delete the existing key from KeyControl node and import again	M	true	Could not import cloudkey as a different key with the same keyname already present in KeyControl node		Security	BYOK
465	Created new KMIP tenant {} with Active Directory domain {} and Active Directory user/group {} as initial KMIP administrator	M	true	Created new KMIP tenant with its own Active Directory config and an Active Directory user/ group for initial access		Security	KMIP
466	Deleted KMIP tenant {}	M	true	Deleted KMIP tenant		Security	KMIP
467	Internal web server certificate of %s has expired. A new certificate must be installed for KeyControl Cluster to be healthy	H	true	Certificate used by the internal web server of one of the nodes has expired. Domain administrator has to install a new certificate for the KeyControl cluster to be healthy.		Clusters	Certificate
468	Internal web server certificate of %s will expire in %s days, %s hours and %s minutes. A new certificate must be installed before the current one expires for the KeyControl Cluster to be healthy.	H	true	Certificate used by the internal web server of one of the nodes is about to get expired. Domain administrator has to install a new certificate before it gets expired. Otherwise cluster will be degraded		Clusters	Certificate

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
469	Cloud Key {} KeyVault {} in KeySet {} synced from KMS	M	false	Cloud Key {} KeyVault {} in KeySet {} synced from KMS		Security	BYOK
470	Cloud Key {} operations changed to {} on Azure KMS	M	true	Cloud Key {} operations changed to {} on Azure KMS		Security	BYOK
471	Cloud Key {} KeyVault {} imported in KeySet {}	M	false	Cloud Key {} KeyVault {} imported in KeySet {}		Security	BYOK
472	CloudKey import failed in KeyVault {} KeySet {} Error {}	M	false	CloudKey import failed in KeyVault {} KeySet {} Error {}		Security	BYOK
473	Client Secret for Service application {} (CSP {}) will expire on {}. Please update it now to avoid BYOK management service disruption	H	true			Security	
474	Client Secret for Service application {} (CSP {}) has expired on {}. Please update it now to resume BYOK management service	H	true			Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
475	Successfully started migration of KMIP objects to multi-tenant KMIP server	M	false	Started migration of KMIP objects to multi-tenant KMIP server		Security	KMIP
476	Successfully completed migration of KMIP objects to multi-tenant KMIP server	M	false	Completed migration of KMIP objects to multi-tenant KMIP server		Security	KMIP
477	Successfully cancelled migration of KMIP objects to multi-tenant KMIP server	M	false	Cancelled migration of KMIP objects to multi-tenant KMIP server		Security	KMIP
478	Successfully sent KMIP tenant account verification email to %s	M	false	Sent KMIP tenant account verification email		Security	KMIP
479	Successfully reset administrator account password of KMIP vault %s	M	false	Reset KMIP vault administrator account password		Security	KMIP
480	Successfully reset administrator account password of Secrets vault %s	M	false	Reset Secrets vault administrator account password		Security	SecretsVault

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
481	Failed to initialize Authentication database	M	true			Security	oidc
482	Cloud Key {} KeyRing {} imported in KeySet {}	M	false	Cloud Key {} KeyRing {} imported in KeySet {}		Security	BYOK
483	Cloud Key {} KeyRing {} in KeySet {} synced from KMS	M	false	Cloud Key {} KeyRing {} in KeySet {} synced from KMS		Security	BYOK
484	CloudKey import failed in KeyRing {} KeySet {} Error {}	M	false	CloudKey import failed in KeyRing {} KeySet {} Error {}		Security	BYOK
485	Label {} (value {}) set on Cloud Key {}	M	false	Label {} (value {}) set on Cloud Key {}		Security	BYOK
486	Removed Label {} on Cloud Key {}	M	false	Removed Label {} on Cloud Key {}		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
487	Failed to delete old access keys for CSP Account '{}'. Error - '{}'	M	false	Failed to delete old access keys for CSP Account '{}'. Error - '{}'		Security	BYOK
488	EKM Key Access Justification policy violation while accessing Cloud Key {} in KeySet {} : error {}	M	false	EKM Key Access Justification policy violation		Security	BYOK
489	TDE Connector {} state changed to {} on Keyset {}	M	true	TDE Connector state changed		Security	BYOK
490	TDE Connector {} expiry date changed to {} on Keyset {}	M	true	TDE Connector expiry date changed		Security	BYOK
491	Added TDE Connector {} for CVM {} in KeySet {}	M	true	Add TDE connector		Security	BYOK
492	Removed TDE Connector {} from CVM {} in KeySet {}	M	true	Remove TDE connector		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
493	Successfully registered with CSP Compliance Manager (id: {}) from {}	M	true	CSP Compliance Manager register		Security	KCM
494	Successfully unregistered with CSP Compliance Manager (id: {}) from {}	M	true	CSP Compliance Manager unregister		Security	KCM
495	Successfully reset CSP Compliance Manager registration configuration from {}	M	true	CSP Compliance Manager configuration reset		Security	KCM
496	User %s reset syslog settings	M	false	Reset Syslog settings		Security	syslog
497	Attempt to register a new node, named server "%s" failed -- maximum node limit reached.	M	true	Maximum allowed cluster node count reached		Security	Licensing
498	Backup failed due to insufficient space on root device. Please contact support.	H	true	Backup failed due to insufficient space on the root device.		Security	Backup

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
499	Backup was not started due to heavy load on %s	M	true	Backup was not started due to heavy load on KeyControl		Security	Backup
500	Admin Key generation %s can be downloaded from the Settings page (https://%s/appliance/#!/account). Reason for regeneration: %s	H	true	Regenerated Admin Key		Security	Appliance
501	Rescued %s vault: %s	L	true	Rescued Vault		Security	Account
502	%s logged in from ipaddr %s using Personal Access Token %s	L	false	The specified user has just logged in from the IP address shown with Personal Access Token.		Security	Personal Access Token
503	AD authorization (Personal Access Token log in) for user %s failed. Reason :- %s	H	false	Reason for AD/LDAP log in failure for Personal Access Token log in		Security	Personal Access Token

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
504	%s %s Personal Access Token %s from ipaddr %s	M	false	Create/Update/Delete Actions on Personal Access Token		Security	Personal Access Token
505	Keys migrated from HSM to KEYCONTROL for KeySet {}	H	true	Keys migrated from HSM to KEYCONTROL for KeySet {}		Security	BYOK
506	CloudKey: {} in KeySet {} migrated to KEYCONTROL	M	false	CloudKey: {} in KeySet {} migrated to KEYCONTROL		Security	BYOK
507	Keys migrated from KEYCONTROL to HSM for KeySet {}	H	true	Keys migrated from KEYCONTROL to HSM for KeySet {}		Security	BYOK
508	Updated %s Vault %s with CSP Compliance Manager %s	M	false	The specified vault has just been updated with CSP Compliance Manager.		Security	KCM

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
509	Configured OIDC without AD with client id %s	M	false	Configured OIDC without AD		Security	AUTHENTICATION
510	OIDC without AD configuration removed	M	false	OIDC without AD configuration removed		Security	AUTHENTICATION
511	Changed Password Settings :- %s from %s to %s	M	false	One or more of the listed password settings has been changed.		Security	Configuration
512	Keys cached from HSM to KEYCONTROL for KeySet {}	H	true	Keys cached from HSM to KEYCONTROL for KeySet {}		Security	BYOK
513	Keys uncached from KEYCONTROL for KeySet {}	H	true	Keys uncached from KEYCONTROL for KeySet {}		Security	BYOK
514	CloudKey: {} in KeySet {} cached to KeyControl	M	false	CloudKey: {} in KeySet {} cached to KeyControl		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
515	CloudKey: {} in KeySet {} uncached from KeyControl	M	false	CloudKey: {} in KeySet {} uncached from KeyControl		Security	BYOK
516	OIDC authorization failed. Reason :- %s	M	false	Reason for OIDC log in failure		Security	AUTHENTICATION
517	Connection from node %s to HSM %s has failed	H	true	The node is unable to communicate with the HSM	Security Admin should check the HSM configuration.	Security	HSM
518	Connection from node %s to HSM %s is restored	L	true	The node is able to communicate with the HSM again		Security	HSM
519	Connection from node %s to HSM %s still failed after HSMROT timeout, locking down	H	true	The node is shutting down because it has lost contact with the HSM	Fix the issue preventing the node from contacting the HSM and restart the node.	Security	HSM

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
520	HSM issue on node %s: %s	M	true	Some HSM issues have been detected on the node that do not prevent communication with the HSM	Security Admin should check the HSM configuration.	Security	HSM
521	HSM issues resolved on node %s	L	true	The HSM issues previously reported on the node have been resolved		Security	HSM
522	Failed to install self-signed certificate cluster-wide	M	true	Install self signed certificate cluster-wide		Clusters	
523	Failed to clean cacert list.	M	false	Clean cacert list guid from system setting		Clusters	
524	Successfully moved the cluster to self-signed certificate.	M	false	Install self signed certificate cluster-wide		Clusters	
525	Successfully changed the EMS Enforcement crypto policy.	M	false	Change EMS Enforced Configuration		Clusters	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
526	The license for this system expired %s days ago. Please renew or upgrade the license. Start that process from the licensing page in the WebGUI at https://%s/appliance/#!/license	H	true	License expired		Security	Licensing
527	The license for this system expires in %s days. Please renew or upgrade the license. Start that process from the licensing page in the WebGUI at https://%s/appliance/#!/license	H	true	License will expire after some days.		Security	Licensing
528	The license for this system expires today. Please renew or upgrade the license. Start that process from the licensing page in the WebGUI at https://%s/appliance/#!/license	H	true	License is expiring today.		Security	Licensing
529	This system has exceeded the licensed limit of %s Virtual Machines. Further Virtual Machine creation is disabled. Please renew or upgrade the license. Start that process from the licensing page in the WebGUI at https://%s/appliance/#!/license	H	true	This system has exceeded the licensed limit of virtual machines count. Further virtual machine creation is disabled.		Security	Licensing
530	This system has exceeded the licensed limit of %s Virtual Machines. Please renew or upgrade the license. Start that process from the licensing page in the WebGUI at https://%s/appliance/#!/license	H	true	This system has exceeded the licensed limit of virtual machines count.		Security	Licensing

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
531	System Initialization Complete	L	false	System Initialization Complete		Security	
532	System Autoconfiguration Complete	L	false	System Autoconfiguration Complete		Security	
533	Cloud Key {} in KeySet {} replicated to {}	M	true	Cloud Key {} in KeySet {} replicated to {}		Security	BYOK
534	The Cloud Key {} from KeySet {} will be rotated on {}.	H	true	Send notification before cloudkey rotation.		Security	BYOK
535	The Cloud Key {} from KeySet {} is expiring on {} with the Action {}.	H	true	Send notification before cloudkey expiration.		Security	BYOK
536	System has completed automatic renewal of self-signed certificates.	L	false	Automatic renewal of self-signed certificates.		Clusters	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
537	System has completed automatic renewal of CA certificates.	L	false	Automatic renewal of CA certificates.		Clusters	
538	Probable LOW DISK SPACE: refreshing KMIP database is failing. Most probably the disk is low on space. Please consider increasing disk space.	H	true			Security	
539	Generated Access Token for TDE Connector {} in KeySet {}	M	true	Add TDE connector		Security	BYOK
540	Internal CA signed certificate with common name and SANs - '%s', '%s' is generated and installed for %s.	L	false	New internal CA signed certificate generated and installed.		Clusters	Certificate
541	KeyControl upgrade failed. Failed to revert nodes. Please contact Support	H	true	Post upgrade failed		Clusters	Rolling Upgrade
542	Failure to change the EMS Enforcement crypto policy. Reverting to %s	M	false	Change EMS Enforced Configuration		Clusters	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
543	NTP synchronization succeeded on KeyControl %s	M	true	NTP synchronization succeeded on KeyControl	Check if NTP servers are reachable from KeyControl	Clusters	NTP
544	Backup of Cloud Key {} failed: {}	M	true	Backup of Cloud Key {} failed: {}		Security	BYOK
545	Cloud Key {} backup {} is not available in remote storage	M	true	Cloud Key {} backup {} is not available in remote storage		Security	BYOK
546	Unsupported ciphers found in KMIP server configuration: %s	L	true	Unsupported ciphers found in KMIP server configuration		Security	
547	Updated default cipher list to %s in KMIP server configuration	L	true	Updated default cipher list to %s in KMIP server configuration		Security	
548	Cloud Key {} with key id {} is the active key version and cannot be deleted. The scheduled deletion has been cancelled	M	true	Cloud Key {} with key id {} is the active key version and cannot be deleted. The scheduled deletion has been cancelled		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
549	Cloud Key {} with key id {} is the active key version and cannot be deleted. The scheduled expiry has been cancelled	M	true	Cloud Key {} with key id {} is the active key version and cannot be deleted. The scheduled expiry has been cancelled		Security	BYOK
550	CSP Account: {} access credentials are due for rotation. Please rotate through the Salesforce UI.	M	true	CSP Account: {} access credentials are due for rotation.		Security	BYOK
551	Started HSM key caching for KeySet {}	M	true	Started HSM key caching for KeySet {}		Security	TDE
552	Keys cached to HSM for KeySet {}	M	true	Keys cached to HSM for KeySet {}		Security	TDE
553	CSP Account {} failed to access AWS global infra API with the default region. The key management capabilty is unaffected, but some region's full names may not be displayed.	L	true	Unable to access AWS global infra API		Security	BYOK
554	Certificate based authentication enabled on CSP Account {}	M	true	Certificate based authentication enabled on CSP Account {}		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
555	Certificate based authentication disabled on CSP Account {}	M	true	Certificate based authentication disabled on CSP Account {}		Security	BYOK
556	Failed to create new client secret for CSP Account {}. Error {}	M	true	Failed to create new client secret for CSP Account {}. Error {}		Security	BYOK
557	CloudKey {} status changed from {} to {} on synchronization with Cloud	M	true	CloudKey {} status changed from {} to {} on synchronization with Cloud	Check the cloud status of the cloudkey is expected	Security	BYOK
558	Cache only key replay attack detected on on csp {}	H	true	Cache only key replay attack detected		Security	BYOK
559	To comply with certificate validity of CSP Vault's CA signed server certificate, the certificate will be automatically renewed on %s for %s. If you have a VM Encryption-vault, please ensure the authentication of all VMs after that renewal. Or if you have a Database-vault, please ensure the database clients reconnect after that renewal.	H	true	To comply with certificate validity of CSP Vault's CA signed server certificate, we will auto renew it on %s for %s. If you use a VME vault, please ensure the re-authentication of all VMs after that renewal.		Clusters	Certificate

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
560	CloudKey {} KeySet {} cannot be migrated to FIPS level 3 HSM because it uses cipher {}.	M	false	CloudKey {} KeySet {} cannot be migrated to FIPS level 3 HSM because it uses cipher {}.		Security	BYOK
561	Unknown error in check_ncipher_data - %s	H	true	Unknown error in HSM files		Security	HSM
562	Failed to clear error in check_ncipher_data - %s	H	true	Failed to clear error in HSM files		Security	HSM
563	CSP Vault has renewed the CA certificate that is being used by CSP Vault's external web server.	M	false	CSP Vault has renewed the CA certificate that is being used by CSP Vault's external web server.		Security	Certificate
564	CSP Vault has renewed the CA certificate that is being used by CSP Vault's internal web server.	M	false	CSP Vault has renewed the CA certificate that is being used by CSP Vault's internal web server.		Security	Certificate

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
565	CSP Vault's internal CA certificate, used for external communication (external webserver) will expire on %s. CSP Vault will renew the CA certificate on %s before the expiry. The system will reboot at the time of renewal and will be in read only mode. We recommend to re-authenticate all Virtual Machines connected to the VME vault using the commands 'hcl updatecert -a' and 'hcl auth -a' after the renewal. If your vault uses client certificate, then please generate new client certificate and use it at client application after the renewal.	M	true	CSP Vault's internal CA certificate, used for external communication (external webserver) will expire on %s. CSP Vault will renew the CA certificate on %s before the expiry. The system will reboot at the time of renewal and will be in read only mode. We recommend to re-authenticate all virtual machines connected to VME vault using the commands 'hcl updatecert -a' and 'hcl auth -a' after the renewal. If your vault uses client certificate, then please generate new client certificate and use it at client application after the renewal.		Security	Certificate
566	CSP Vault's internal CA certificate, used for internal communication (internal webserver) will expire on %s. CSP Vault will renew the CA certificate on %s before the expiry. The system will reboot at the time of renewal and will be in read only mode. If your cluster is in a degraded state following the renewal, reboot each node individually, making sure to reboot the master node last.	M	true	CSP Vault's internal CA certificate, used for internal communication (internal webserver) will expire on %s. CSP Vault will renew the CA certificate on %s before the expiry. The system will reboot at the time of renewal and will be in read only mode. If your cluster is in a degraded state following the renewal, reboot each node individually, making sure to reboot the master node last.		Security	Certificate

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
567	OIDC CA Certificate Uploaded Successfully	M	false	OIDC CA Certificate Uploaded Successfully		Security	OIDC
568	{} purged KeyVault {}.	M	true	{} purged KeyVault {}.		Security	BYOK
569	KC self-signed certificate for {server.hostname} (use for external webserver) is renewed.	L	false	KC self-signed certificate for {server.hostname} (use for external webserver) is renewed.		Security	Certificate
570	KC self-signed certificate for {server.hostname} (use for internal webserver) is renewed.	L	false	KC self-signed certificate for {server.hostname} (use for internal webserver) is renewed.		Security	Certificate
571	Failed to migrate Azure Keyvaults to target keyset {}. Error: {}.	M	true	Failed to migrate Azure Keyvaults to target keyset {}. Error: {}.		Security	BYOK
572	{} started migration of Azure keyvaults from source KeySets {} to target KeySet {}	M	true	Azure Keyvault migration between KeySets started		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
573	Migration of Azure Keyvaults to {} did not complete successfully. Expected {} cloud keys and {} key versions but found {} cloud keys and {} key versions.	M	true	Azure Keyvault migration between KeySets partially completed		Security	BYOK
574	Migration of Azure Keyvaults to {} completed successfully	M	true	Azure Keyvault migration between KeySets completed		Security	BYOK
575	Warning: CSP Account {} manages keys in overlapping subscriptions with existing Azure CSP accounts: {}. Subscription IDs: {}	M	true	Azure CSP created with overlapping subscriptions with existing Azure CSP accounts		Security	BYOK
576	Could not process {} on AWS Cloud Key {}. {}. The key has been disabled instead.	M	true	AWS Cloudkey expiry action failed.		Security	BYOK
577	Changed AD group members for group Appliance. %s	L	false	List of AD Group members has been changed for a CSP Vault Appliance		Security	Group
578	CSR generated for CSP Account {}	M	true	CSR generated for CSP Account		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
579	Azure keyvault {} containing replica keys has purge protection enabled. Rotation operations will fail.	M	true	A vault containing replica keys has purge protection enabled.		Security	BYOK
580	Replication of the key rotation for key {} to vault {} failed. The key must be manually restored to {} and synced in KeyControl to restore redundancy. Review other replica vaults in case replication has not occurred in them either.	H	true	Replication of a key rotation in Azure failed.		Security	BYOK
581	Trial period for vault {} has expired. This vault is now operating in restricted mode. Please connect to CSP Compliance Manager to retrieve a valid license.	H	true	Vault trial period has expired.		Licensing	
582	{} {} has not been able to connect to CSP Compliance Manager for {} days. This is required for licensing checks. This vault is now operating in restricted mode. Please check the network connectivity and CSP Compliance Manager status.	H	true	Vault grace period has expired.		Licensing	
583	{} {} is unlicensed. No license information is available for {}. This vault is now operating in restricted mode. Check that the vault type is covered by your license.	H	true	No license available for vault.		Licensing	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
584	The number of {} {} has exceeded the licensed limit of {}. Current usage: {}. This {} is now operating in restricted mode. Please purchase additional licenses.	H	true	License limit exceeded.		Licensing	
585	The license for {} expired on {}. This vault is now operating in restricted mode. Please renew your license.	H	true	License Expired.		Licensing	
586	Trial period for {} {} is nearing expiration. To avoid loss of service, please connect to CSP Compliance Manager to retrieve a valid license.	M	true	Vault trial period is nearing expiration.		Licensing	
587	The license for {} will expire on {}. Please renew your license to avoid loss of service.	M	true	License Nearing Expiry.		Licensing	
588	{} {} is in the grace period after upgrade to {} or later and will become unlicensed when this grace period ends.	M	true	Upgrade Grace Period Nearing Expiry.		Licensing	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
589	The number of {} {} is over 90% of the licensed limit of {}. Current usage: {}. To avoid loss of service, please purchase additional licenses if needed.	M	true	Usage is nearing license limit.		Licensing	
590	Attempt to register a new node, named server "%s" failed -- license check failed. Reason: %s.	L	false	Appliance license check failed.		Licensing	
591	Attempt to register a new node, named "%s" failed -- cluster not connected to KeyControl Compliance Manager.	L	false	Appliance is not connected to CSP Compliance Manager.		Licensing	
592	Enabled Authentication Inheritance	M	true	Enabled Authentication Inheritance		Security	AUTHENTICATION
593	Disabled Authentication Inheritance	M	true	Disabled Authentication Inheritance		Security	AUTHENTICATION

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
594	Successfully fetched Key Encryption Key from HSM. %s	H	false	Successfully fetched Key Encryption Key from HSM.	Successfully fetched Key Encryption Key from HSM	Security	Key Encryption Key
595	OIDC authentication settings updated for Appliance and inheriting vaults	M	true	OIDC authentication settings updated for Appliance and inheriting vaults		Security	AUTHENTICATION
596	OIDC authentication settings for inheriting vault updated by System Admin	M	true	OIDC authentication settings for inheriting vault updated by System Admin		Security	AUTHENTICATION
597	XKS store for {} ({}) in region {} is unreachable	H	true	XKS service unreachable		Security	BYOK
598	XKS store {} ({}) in region {} is {}.	H	true	XKS store not connected		Security	BYOK
599	XKS store {} ({}) in region {} is now CONNECTED.	M	true	XKS store connected		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
600	%s for Virtual Machine %s. %s. Reauthentication required.	H	true			Security	
601	Could not authenticate user. Unknown username {}.	H	false	Could not authenticate user. Unknown username		Security	
602	Failed to promote %s as KeyControl Cluster Master Node. Error: %s	H	true	Failed to change the KeyControl master node		Clusters	ClusterNodeSwitchover
603	Successfully promoted the node %s as KeyControl Cluster Master	M	false	Changed the master node		Clusters	ClusterNodeSwitchover
604	Could not pass CSP vault's appliance info to CSP CM {}	L	false	Failed to send CSP vault's appliance info to CSP CM		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
605	Import of cloudkey {} in {} {} skipped beacause it is managed by KeySet: {} (GUID: {}) already.	L	false	Cloudkey import skipped beacause it is already managed by another keyset on this system.		Security	BYOK
606	Import of cloudkey {} in {} {} skipped beacause it is managed by a KeySet on another system already. Owning keyset GUID: {}.	L	false	Cloudkey import skipped beacause it is already managed by another keyset on another system.		Security	BYOK
607	Import of SFDC cloudkey {} skipped beacause it is managed by KeySet: {} (GUID: {}) already.	L	false	SFDC Cloudkey import skipped beacause it is already managed by another keyset on this system.		Security	BYOK
608	Import of SFDC cloudkey {} skipped beacause it is managed by a KeySet on another system already. Owning keyset GUID: {}.	L	false	SFDC Cloudkey import skipped beacause it is already managed by another keyset on another system.		Security	BYOK
609	CloudKey {} is managed by multiple keysets. {} and {}	M	true	CloudKey {} is managed by multiple keysets.		Security	BYOK
610	Created distribution list {} for {}.	M	true	Created distribution list.		Security	GROUP

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
611	Updated distribution list {} in {}. {}	M	true	Updated distribution list.		Security	GROUP
612	Deleted distribution list {} in {}.	M	true	Deleted distribution list.		Security	GROUP
613	Distribution list {} associated with group {}. It will receive all alerts sent to the group.	M	true	Associated distribution list.		Security	GROUP
614	Distribution list {} dissociated from group {}. It will no longer receive alerts sent to the group.	M	true	Dissociated distribution list.		Security	GROUP
615	Two-factor authentication enforced by %s	M	false	Two factor authentication has been enforced for the users		Security	
616	Two-factor authentication enforcement removed by %s	M	false	Two factor authentication enforced removed for the users		Security	

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
617	Failed to add owning keyset guid to CloudKey {} during upgrade. Error: {}	M	true	Failed to add owning keyset guid to CloudKey during upgrade.		Security	BYOK
618	Failed to update failover order, triggerred by %s. Error: %s	M	true	Failed to update failover order		Clusters	Cluster
619	Failed to set the new primary to %s, please contact support	M	true	Failed to set new Postgres primary		Clusters	Cluster
621	Import of cloudkey {} in Region {} skipped beacause it uses on demand rotations with AWS generated key material. Such keys cannot be managed by CSP.	L	false	Cloudkey import skipped beacause it cannot be managed by CSP.		Security	BYOK
622	Failed to set keyset ownership tag on key {} in {} {} after import: {}.	L	false	Failed to set keyset ownership tag on key after import.		Security	BYOK
623	Failed to set keyset ownership tag on SFDC key {} after import: {}	L	false	Failed to set keyset ownership tag on key after import.		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
624	Failed to write KeySafeAgent Configuration to Database. Error: %s	H	false	Failed to write KeySafeAgent Configuration to Database.		Clusters	Cluster
625	Whitelisting database verification test	H	false	Whitelisting database verification test		Security	Whitelisting
626	Whitelisting database verification was successfull	H	false	Whitelisting database verification was successfull		Security	Whitelisting
627	Whitelisting database verification failed, entering error mode!	H	false	Whitelisting database verification failed, entering error mode!		Security	Whitelisting
628	FIPS POST tests	H	false	FIPS POST tests		Security	Whitelisting
629	Access credentials for CSP {} are not valid: {}. Please update the credentials to avoid management service disruption.	H	true	Access credentials for CSP account are invalid.		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
630	HYOK Key {} ({}) in keyset {} used to perform {} operation from remote address {}. {}	L	false	HYOK key used to perform crypto operation.		Security	BYOK
631	Failed to sync root CA cert for MHSM {} in KeySet {}: {}.	H	true	Failed to sync root CA cert for EKM enabled MHSM		Security	BYOK
632	Root CA certificate for MHSM {} in KeySet {} is expiring on {}. Please update the root CA certificate to avoid disruption to EKM crypto operations.	H	true	EKM enabled MHSM Root CA certificate is nearing expiry		Security	BYOK
633	Upgrade failed: not enough space in %s on host %s, %ld%% free, need min %ld%%	H	true	Not enough space	Consult support for freeing disk space or create/join a node with more space and upgrade that	Clusters	Upgrade
634	Upgrade failed: not enough space in %s on host %s, need %lldMB more free space	H	true	Not enough space	Consult support for freeing disk space or create/join a node with more space and upgrade that	Clusters	Upgrade

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
635	Upgrade failed: initiator argument missing from do_chkspace	H	true	Initiator argument missing from do_chkspace		Clusters	Upgrade
636	Upgrade failed: could not find space usage on host %s	H	true	Could not determine space	contact support or replace the node	Clusters	Upgrade
637	Upgrade failed: could not find available space on host %s	H	true	could not determine space	contact support or replace the node	Clusters	Upgrade
638	Upgrade failed: not enough space on host %s	H	true	Not enough space on host	contact support or replace the node	Clusters	Upgrade
639	Cleaning upgrade on %s	H	true	Cleaning upgrade		Clusters	Upgrade
640	Upgrade failed: could not scrub prior upgrade %s	H	true	Could not scrub prior upgrade		Clusters	Upgrade

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
641	Upgrade failed: could not find existing cipher of the KeyControl nodes	H	true	Could not find existing cipher of the KeyControl nodes		Clusters	Upgrade
642	Upgrade failed: could not find kit staging area usage	H	true	Could not find kit staging area usage		Clusters	Upgrade
643	Upgrade failed: could not find KeyControl nodes	H	true	Could not find KeyControl nodes		Clusters	Upgrade
644	Upgrade failed: could not find encryption status of volumes of the KeyControl node	H	true	Could not find encryption status of volumes of the KeyControl node		Clusters	Upgrade
645	Upgrade failed: rekey in progress on KeyControl nodes	H	true	Rekey in progress on KeyControl nodes		Clusters	Upgrade
646	CloudKey {} in KeySet {} key material exported.	M	true	CloudKey key material exported.		Security	BYOK

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
647	Upgrade bundle upload rejected: %s	H	true	Upgrade precondition check failed	Resolve the reported precondition and retry the upgrade	Clusters	Upgrade
648	Started key caching {} operation for KeySet {}	H	true	Started key caching operation for KeySet		Security	BYOK
649	Failed to refresh key cache for KeySet {}. Error: {}.	H	true	Failed to refresh key cache for KeySet		Security	BYOK
650	Multi-tenant KMIP migration in progress. Retry after migration is complete	H	true	KMIP migration in progress blocks upgrade	Wait for KMIP migration to complete before attempting upgrade	Clusters	Upgrade
651	No upgrade image found in the upload request	H	true	No upgrade image found in the upload request	Ensure the upgrade bundle file is included in the upload request	Clusters	Upgrade
652	Failed to save upgrade bundle: %s	H	true	Failed to save the uploaded upgrade bundle to disk	Check available disk space and file permissions, then retry	Clusters	Upgrade

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
653	Issue with bundle version. Bundle not valid for upgrade	H	true	Upgrade bundle has invalid version information	Obtain a valid upgrade bundle and retry	Clusters	Upgrade
654	Failed to properly fetch and decode upgrade bundle	H	true	Failed to mount or decode the upgrade bundle	Verify the upgrade bundle is not corrupted and retry	Clusters	Upgrade
655	Support license expired. Upgrade not allowed	H	true	Support license has expired preventing upgrade	Renew the support license before attempting upgrade	Clusters	Upgrade
656	The upgrade can not be started: %s	H	true	Pre-upgrade script failed	Check the pre-upgrade script output and resolve the issue	Clusters	Upgrade
657	Upgrade initiation failed: %s	H	true	Upgrade initiation failed	Check if another upgrade is already in progress. Contact support if the issue persists	Clusters	Upgrade
658	Unexpected error upgrading: %s	H	true	An unexpected error occurred during upgrade bundle upload	Contact support	Clusters	Upgrade

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
659	TLS configuration changed from %s to %s on node %s	H	true	TLS/SSL protocol or cipher configuration changed		Security	Configuration
660	[SCIM] Added user %s to group %s	L	false	SCIM provisioning added a user to a group.		Security	Account, SCIM
661	[SCIM] Created user %s, name %s	L	false	SCIM provisioning created a user.		Security	Account, SCIM
662	[SCIM] Removed user %s from group %s	L	false	SCIM provisioning removed a user from a group.		Security	Account, SCIM
663	[SCIM] Deleted user %s	L	false	SCIM provisioning deleted a user.		Security	Account, SCIM
664	[SCIM] Updated user %s name from %s to %s	L	false	SCIM provisioning updated a user's name.		Security	Account, SCIM

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
665	KeyControl Upgrade not allowed on a multinode cluster in passphrase based startup authentication mode	H	true	Passphrase based auth mode blocks multinode upgrade	Disable Passphrase based startup authentication or reduce to single node for upgrade	Clusters	Upgrade
666	Cluster must be in normal mode for upgrade	H	true	Cluster not in normal mode for upgrade	Wait for cluster to return to normal mode before attempting upgrade	Clusters	Upgrade
667	Failed to update trusted client root certificates on cluster {}.	M	true	Failed to update trusted client root certificates on cluster.		Security	BYOK
668	KMIP server custom certificate has expired. KMIP clients will not be able to connect to the KMIP server. Please install a new certificate.	H	true	KMIP server custom certificate has expired. KMIP clients will not be able to connect to the KMIP server.	Install a new custom certificate for the KMIP server.	Security	KMIP
669	KMIP server custom certificate will expire in %s days, %s hours and %s minutes. If a new certificate is not installed before the current one expires, KMIP clients will not be able to connect to the KMIP server.	M	true	KMIP server custom certificate will expire soon. Upon expiry, KMIP clients will not be able to connect to the KMIP server.	Install a new custom certificate for the KMIP server before it expires.	Security	KMIP

MsgID	Message	Severity	Alert?	Description	Resolution	Category	Tags
670	Imported Key name {} version {} to KeySet {}	M	false	Cloud Key imported in KeySet		Security	TDE
671	Failed to import key {} version {} into KeySet {}	M	false	Failed to import Cloud Key to KeySet		Security	TDE
672	Upgrade failed: Unable to delete boot backup for extra space in /boot on {}.	L	true	Could not free extra disk space		Clusters	Upgrade
673	An updated Policy Agent version %s is available for guest %s (current version: %s). Please upgrade to ensure optimal security and features.	M	true	A newer version of the Policy Agent is available for installation	Upgrade the Policy Agent on the affected guest to the latest version	Cloud	Cloud, Policy Agent, Update
674	SNMP has been disabled during upgrade because the configured trap version is no longer supported. Only SNMPv3 is allowed.Please reconfigure SNMP after upgrade.	H	false			Security	

Msg ID	Message	Severity	Alert?	Description	Resolution	Category	Tags
675	SNMP has been disabled during upgrade because all configured agent users were non-v3 and have been removed. Please reconfigure SNMP after upgrade.	H	false			Security	
676	{} non-v3 SNMP agent user(s) were removed during upgrade because only SNMPv3 is supported.	H	false			Security	

CSP Vault for Cryptographic APIs Audit Messages

The audit messages in this section are from the Cryptographic Security Platform Vault for Cryptographic APIs.

In the table below, we list many of the audit messages and show:

- Whether an Alert is also generated.
- The severity (L=Low, M=Medium, H=High).
- What the resolution is if any action should be taken.
- In the **Message** column, a value in braces, such as `{user_name}`, represents a placeholder that is replaced with an actual value. For example, in the following message:

  `'{user_name}' created the policy '{policy_name}'`

  The actual message will be displayed with the name of the user and policy, for example:

  'Fred' created the policy 'Default_Policy'

Msg ID	Message	Severity	Alert?	Category
300	'{user_name}' created the policy '{policy_name}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
301	'{user_name}' updated the policy '{policy_name}'. New policy version is {policy_version}.	M	false	Tokenization
302	'{user_name}' deleted the policy '{policy_name}'	M	false	Tokenization
303	'{user_name}' changed the current version of the policy '{policy_name}'. Current policy version is {policy_version}.	M	false	Tokenization
400	Cryptographic APIs Client Certificate '{name}' created	M	false	Tokenization
401	Cryptographic APIs Client Certificate '{name}' created using Certificate Signing Request	M	false	Tokenization
402	Cryptographic APIs Client Certificate '{name}' deleted	M	false	Tokenization
500	User '{user_name}' logged in successfully.	H	false	Tokenization
501	Active Directory login for '{username}' succeeded but failed to get information about user. The user might not belong to the Active Directory Domain {domain_name} or user/group Base DN in Active Directory configuration might be wrong. Please contact Token Administrator to validate the Active Directory setup.	H	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
502	Login failure for Active Directory user '{username}' from {client_ip}. Reason: {reason}	H	false	Tokenization
503	User '{user_name}' logged in successfully using Personal Access Token {token_name}.	H	false	Tokenization
504	'{user_name}' enabled authentication inheritance	M	false	Tokenization
505	Authentication settings for inheriting vault '{vault_name}' were '{action}' by the System Administrator.	M	false	Tokenization
600	'{user_name}' updated AD Setting '{ad_setting_name}'	M	false	Tokenization
601	'{user_name}' changed AD Domain from '{old_ad_setting_name}' to '{ad_setting_name}'	M	false	Tokenization
602	'{user_name}' added AD Setting '{ad_setting_name}'	M	false	Tokenization
800	'{user_name}' updated token '{token_name}' settings. 'degraded mode availability' {degraded_mode}. 'OIDC authentication' {oidc}. 'mTLS state' {mTLS}. 'audit alert distribution list' {audit_alert_dl}. 'alert read count' {alert_read_count}. 'email notify alerts' {email_notify_alerts}.	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
801	'{user_name}' renamed token '{old_name}' to '{token_name}'.	M	false	Tokenization
802	'{user_name}' updated tokenization '{token_name}' settings of authentication method to AD based authentication	M	false	Tokenization
803	'{user_name}' updated the CSP Compliance Manager settings for the CSP Vault for Cryptographic APIs '{token_name}' with CSP Compliance Manager IP '{kcm_ip}'.	M	false	Tokenization
804	'{user_name}' updated tokenization '{vault_name}' settings of authentication method to OIDC based authentication	M	false	Tokenization
900	'{user_name}' created the user '{name}'	M	false	Tokenization
901	'{user_name}' deleted the user '{name}'	M	false	Tokenization
902	'{user_name}' updated the user '{name}'	M	false	Tokenization
903	Account '{user_name}' locked for 5 minutes due to repeated login failures	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
904	Account '{user_name}' was disabled due to repeated login failures	M	false	Tokenization
905	Login failure for Local user '{username}' from {client_ip}. Reason: {reason}	H	false	Tokenization
906	Password successfully updated for user: '{username}'	H	false	Tokenization
907	Account '{user_name}' enabled Two-Factor Authentication	M	false	Tokenization
908	Account '{user_name}' disabled Two-Factor Authentication	M	false	Tokenization
909	'{user_name}' updated the Local user password policy	M	false	Tokenization
910	'{user_name}' enforced Two-Factor Authentication	M	false	Tokenization
911	'{user_name}' removed enforcement of Two-Factor Authentication	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1000	'{user_name}' created keyset '{keyset}'	M	false	Tokenization
1001	'{user_name}' failed to create keyset: '{message}'	M	false	Tokenization
1002	'{user_name}' enabled HSM support for keyset '{keyset}'	M	false	Tokenization
1003	'{user_name}' failed to enable HSM support. Reason: '{message}'	M	false	Tokenization
1004	'{user_name}' disabled HSM support for keyset '{keyset}'	M	false	Tokenization
1005	'{user_name}' failed to disable HSM support. Reason: '{message}'	M	false	Tokenization
1100	'{user_name}' tokenized data using policy '{policy}'	M	false	Tokenization
1101	'{user_name}' detokenized data using policy '{policy}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1102	'{user_name}' masked data using policy '{policy}'	M	false	Tokenization
1103	'{user_name}' detokenized and masked data using policy '{policy}'	M	false	Tokenization
1104	'{user_name}' encrypted data using key '{key}'	M	false	Tokenization
1105	'{user_name}' decrypted data using key '{key}'	M	false	Tokenization
1106	'{user_name}' failed to tokenize data: '{message}'	M	false	Tokenization
1107	'{user_name}' failed to detokenize data: '{message}'	M	false	Tokenization
1108	'{user_name}' failed to mask data: '{message}'	M	false	Tokenization
1109	'{user_name}' failed to detokenize and mask data: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1110	'{user_name}' failed to encrypt data: '{message}'	M	false	Tokenization
1111	'{user_name}' failed to decrypt data: '{message}'	M	false	Tokenization
1112	'{user_name}' rekeyed data using policy '{policy}'	M	false	Tokenization
1113	'{user_name}' batch tokenized data using policy '{policy}'	M	false	Tokenization
1114	'{user_name}' batch detokenized data using policy '{policy}'	M	false	Tokenization
1115	'{user_name}' batch masked data using policy '{policy}'	M	false	Tokenization
1116	'{user_name}' batch rekeyed data using policy '{policy}'	M	false	Tokenization
1117	'{user_name}' failed to rekey data using policy '{policy}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1118	'{user_name}' failed to batch tokenize data using policy '{policy}'	M	false	Tokenization
1119	'{user_name}' failed to batch detokenize data using policy '{policy}'	M	false	Tokenization
1120	'{user_name}' failed to batch mask data using policy '{policy}'	M	false	Tokenization
1121	'{user_name}' failed to batch rekey data using policy '{policy}'	M	false	Tokenization
1122	'{user_name}' signed data using key '{key}'	M	false	Tokenization
1123	'{user_name}' verified signature using key '{key}'	M	false	Tokenization
1124	'{user_name}' failed to sign data: '{message}'	M	false	Tokenization
1125	'{user_name}' failed to verify signature: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1126	'{user_name}' wrapped key using key '{key}'	M	false	Tokenization
1127	'{user_name}' unwrapped key using key '{key}'	M	false	Tokenization
1128	'{user_name}' failed to wrap key: '{message}'	M	false	Tokenization
1129	'{user_name}' failed to unwrap key: '{message}'	M	false	Tokenization
1130	'{user_name}' generated MAC using key '{key}'	M	false	Tokenization
1131	'{user_name}' verified MAC using key '{key}'	M	false	Tokenization
1132	'{user_name}' failed to generate MAC: '{message}'	M	false	Tokenization
1133	'{user_name}' failed to verify MAC: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1134	'{user_name}' generated message digest	M	false	Tokenization
1135	'{user_name}' failed to generate message digest: '{message}'	M	false	Tokenization
1136	'{user_name}' batch encrypted data using keys '{keys}'	M	false	Tokenization
1137	'{user_name}' batch decrypted data using keys '{keys}'	M	false	Tokenization
1138	'{user_name}' failed to batch encrypt data using keys '{keys}' with error: '{message}'	M	false	Tokenization
1139	'{user_name}' failed to batch decrypt data using keys '{keys}' with error: '{message}'	M	false	Tokenization
1140	'{user_name}' batch encrypted-decrypted data using keys '{keys}'	M	false	Tokenization
1141	'{user_name}' failed to batch encrypt-decrypt data using keys '{keys}' with error: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1200	'{user_name}' created tokenization policy: '{policy}'	M	false	Tokenization
1201	'{user_name}' deleted tokenization policy: '{policy}'	M	false	Tokenization
1202	'{user_name}' updated tokenization policy: '{policy}'	M	false	Tokenization
1203	'{user_name}' created masking policy: '{policy}'	M	false	Tokenization
1204	'{user_name}' deleted masking policy: '{policy}'	M	false	Tokenization
1205	'{user_name}' updated masking policy: '{policy}'	M	false	Tokenization
1207	'{user_name}' deleted encryption policy: '{policy}'	M	false	Tokenization
1209	'{user_name}' failed to create tokenization policy. Reason: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1210	'{user_name}' failed to delete tokenization policy. Reason: '{message}'	M	false	Tokenization
1211	'{user_name}' failed to update tokenization policy. Reason: '{message}'	M	false	Tokenization
1212	'{user_name}' failed to create masking policy. Reason: '{message}'	M	false	Tokenization
1213	'{user_name}' failed to delete masking policy. Reason: '{message}'	M	false	Tokenization
1214	'{user_name}' failed to update masking policy. Reason: '{message}'	M	false	Tokenization
1216	'{user_name}' failed to delete encryption policy. Reason: '{message}'	M	false	Tokenization
1300	'{user_name}' created the key: '{key_name}'	M	false	Tokenization
1301	'{user_name}' failed to create key: '{key_name}'. Reason: '{message}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1302	'{user_name}' updated details of key: '{key_name}'	M	false	Tokenization
1303	'{user_name}' changed state of the key: '{key_name}' to '{state}'	M	false	Tokenization
1304	'{user_name}' scheduled deletion of key: '{key_name}'	M	false	Tokenization
1305	'{user_name}' cancelled scheduled deletion of key: '{key_name}'	M	false	Tokenization
1306	'{user_name}' failed to schedule or cancel scheduled deletion of key: '{key_name}'. Reason: '{message}'	M	false	Tokenization
1307	'{user_name}' purged key: '{key_name}'	M	false	Tokenization
1308	'{user_name}' failed to purge key: '{key_name}'. Reason: '{message}'	M	false	Tokenization
1309	'{user_name}' rotated key: '{key_name}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1310	'{user_name}' failed to rotate key: '{key_name}'. Reason: '{message}'	M	false	Tokenization
1311	'{user_name}' retrieved clear value of key: '{key_name}'	M	false	Tokenization
1312	'{user_name}' failed to retrieve the clear value of key: '{key_name}'. Reason: '{message}'	M	false	Tokenization
1313	'{user_name}' exported key: '{key_name}'	M	false	Tokenization
1314	'{user_name}' failed to export key: '{key_name}'. Reason: '{message}'	M	false	Tokenization
1315	'{user_name}' generated a key and CSR for '{key_name}'	M	false	Tokenization
1316	'{user_name}' failed to generate a key and CSR for '{key_name}'. Reason: '{message}'	M	false	Tokenization
1317	'{user_name}' exported public key: '{key_name}'	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1318	'{user_name}' failed to export public key: '{key_name}'. Reason: '{message}'	M	false	Tokenization
1319	'{user_name}' imported key: '{key_name}'	M	false	Tokenization
1320	'{user_name}' failed to import key: '{key_name}'. Reason: '{message}'	M	false	Tokenization
1321	'{user_name}' successfully rebuilt keys database	M	false	Tokenization
1322	'{user_name}' failed to rebuild keys database. Reason: '{message}'	M	false	Tokenization
1323	'{user_name}' imported clear key: '{key_name}'	M	false	Tokenization
1324	'{user_name}' failed to import clear key: '{key_name}'. Reason: '{message}'	M	false	Tokenization
1400	'{user_name}' created Personal Access Token {token_name}	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1401	'{user_name}' {update_info} Personal Access Token {token_name}	M	false	Tokenization
1402	'{user_name}' deleted Personal Access Token {token_name}	M	false	Tokenization
1500	'{user_name}' created OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization
1501	'{user_name}' failed to create OIDC user {oidc_user_email}	M	false	Tokenization
1502	'{user_name}' updated OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization
1503	'{user_name}' failed to update OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization
1504	'{user_name}' deleted OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization
1505	'{user_name}' failed to delete OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1506	'{user_name}' created registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization
1507	'{user_name}' failed to create registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Tokenization
1508	Login failure for OIDC user '{username}' from {client_ip}. Reason: {reason}	M	false	Tokenization
1600	'{user_name}' cleared cache	M	false	Tokenization
1601	'{user_name}' failed to clear cache. Reason: '{message}'	M	false	Tokenization
1602	'{user_name}' changed caching state	M	false	Tokenization
1603	'{user_name}' failed to change caching state. Reason: '{message}'	M	false	Tokenization
1604	'{user_name}' fetched caching status	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1605	'{user_name}' failed to get caching status. Reason: '{message}'	M	false	Tokenization
1606	'{user_name}' fetched caching settings	M	false	Tokenization
1607	'{user_name}' failed to get caching settings. Reason: '{message}'	M	false	Tokenization
1608	'{user_name}' set caching settings	M	false	Tokenization
1609	'{user_name}' failed to set caching settings. Reason: '{message}'	M	false	Tokenization
1700	'{user_name}' created SCIM Token {token_id} expiring on {expiry_date}	M	false	Tokenization
1701	User {oidc_user_name} ({oidc_user_email}: {oidc_user_guid}) deleted by SCIM	M	false	Tokenization
1702	User {oidc_user_name} ({oidc_user_email}: {oidc_user_guid}) created by SCIM and added to policy {policy_name}	M	false	Tokenization

Msg ID	Message	Severity	Alert?	Category
1703	User ({oidc_user_email}: {oidc_user_guid}) updated by SCIM from '{old_name}' to '{new_name}'	M	false	Tokenization
1704	'{user_name}' deleted SCIM Token	M	false	Tokenization
1800	'{user_name}' updated OIDC configuration on vault '{vault_name}'	H	true	Tokenization
1801	'{user_name}' updated OIDC CA certificate for vault '{vault_name}'	H	true	Tokenization
1900	Client certificate '{cert_name}' has expired. Clients using this certificate will no longer be able to access the vault. Please create a new certificate.	H	true	Tokenization
1901	Client certificate '{cert_name}' will expire in {days} days, {hours} hours and {minutes} minutes. Please create a new certificate before it expires.	H	true	Tokenization

CSP Vault for KMIP Audit Messages

The audit messages in this section are from the Cryptographic Security Platform Vault for KMIP.

In the table below, we list many of the audit messages and show:

- Whether an Alert is also generated.
- The severity (L=Low, M=Medium, H=High).
- What the resolution is if any action should be taken.
- In the **Message** column, a value in braces, such as `{user_name}`, represents a placeholder that is replaced with an actual value. For example, in the following message:

  `'{user_name}' created the policy '{policy_name}'`

  The actual message will be displayed with the name of the user and policy, for example:

Fred created the policy 'Default_Policy'

Msg ID	Message	Severity	Alert?	Category
300	{user_name} created the policy '{policy_name}'	M	false	KMIP
301	{user_name} updated the policy '{policy_name}'. New policy version is {policy_version}.	M	false	KMIP
302	{user_name} deleted the policy '{policy_name}'	M	false	KMIP
303	{user_name} changed the current version of the policy '{policy_name}'. Current policy version is {policy_version}.	M	false	KMIP
400	KMIP Client Certificate '{name}' created	H	false	KMIP
401	KMIP Client Certificate '{name}' created using Certificate Signing Request	H	false	KMIP
402	KMIP Client Certificate '{name}' deleted	H	false	KMIP
403	KMIP Client Certificate '{name}' created using uploaded Certificate	H	false	KMIP
500	User '{user_name}' logged in successfully.	H	false	KMIP
501	Active Directory login for {username} succeeded, but KMIP portal failed to retrieve information about the user. The user might not belong to the Active Directory Domain {domain_name} or user/group Base DN in Active Directory configuration might be wrong. Please contact KMIP Administrator to validate the Active Directory setup.	H	false	KMIP
502	Login failure for Active Directory user {username}	H	false	KMIP
503	User '{user_name}' logged in successfully using Personal Access Token {token_name}.	H	false	KMIP

Msg ID	Message	Severity	Alert?	Category
504	{user_name} enabled authentication inheritance	M	false	KMIP
505	Authentication settings for inheriting vault '{vault_name}' were '{action}' by System Administrator	M	false	KMIP
600	{user_name} updated AD Setting '{ad_setting_name}'	M	false	KMIP
601	{user_name} changed AD Domain from '{old_ad_setting_name}' to '{ad_setting_name}'	M	false	KMIP
602	{user_name} added AD Setting '{ad_setting_name}'	M	false	KMIP
700	KMIP Request - Operation: {op}, Object: {obj}, UUID: {uuid} from KMIP Client - {user} (IP: {client_ip})	H	false	KMIP
701	KMIP Response - Operation: {op}, Object: {obj}, UUID: {uuid}, Result: {result}, from KMIP Client - {user} (IP: {client_ip})	H	false	KMIP
702	KMIP Action Request from WebGUI. Action: Revoke, UUID: {uuid}. Revocation Code: {revcode}, Revocation message: {revmsg}, Result: {result} (IP: {client_ip})	H	false	KMIP
703	KMIP Action Response from WebGUI. Action: {op}, UUID: {uuid}, Result: {result} (IP: {client_ip})	H	false	KMIP
800	{user_name} updated KMIP '{kmip_name}' settings. 'degraded mode availability' {degraded_mode}. 'OIDC authentication' {oidc}. 'audit alert distribution list' {audit_alert_dl}. 'alert read count' {alert_read_count}. 'email notify alerts' {email_notify_alerts}.	M	false	KMIP
801	{user_name} updated KMIP '{kmip_name}' settings of authentication method to AD based authentication with Active Directory domain '{ad_domain}'	M	false	KMIP
802	{user_name} updated KCM settings for KMIP '{kmip_name}' with KCM IP '{kcm_ip}'.	M	false	KMIP
803	{user_name} updated KMIP '{kmip_name}' settings of authentication method to OIDC based authentication	M	false	KMIP

Msg ID	Message	Severity	Alert?	Category
900	{username} updated KEK Setting	M	false	KMIP
901	{username} enabled KMIP KEK wrapping	M	false	KMIP
902	{username} disabled KMIP KEK wrapping	M	false	KMIP
1000	Successfully completed rekey of KMIP objects	L	false	KMIP
1001	Successfully completed decryption of KMIP objects	L	false	KMIP
1002	Successfully started rekey of KMIP objects	L	false	KMIP
1100	Successfully reset KMIP vault {tenant}	L	false	KMIP
1200	{user_name} created the user '{name}'	M	false	KMIP
1201	{user_name} deleted the user '{name}'	M	false	KMIP
1202	{user_name} updated the user '{name}'	M	false	KMIP
1203	Account {user_name} was locked for 5 minutes due to repeated login failures	H	false	KMIP
1204	Account {user_name} was disabled due to repeated login failures	H	false	KMIP
1205	Login failure for Local user {username} from {client_ip}. Reason: {reason}	H	false	KMIP

Msg ID	Message	Severity	Alert?	Category
1206	Password successfully updated for user: {username}	H	false	KMIP
1207	Account {user_name} enabled Two-Factor Authentication	L	false	KMIP
1208	Account {user_name} disabled Two-Factor Authentication	L	false	KMIP
1209	{user_name} updated the local user password policy	M	false	KMIP
1210	{user_name} enforced Two-Factor Authentication	M	false	KMIP
1211	{user_name} removed enforcement of Two-Factor Authentication	M	false	KMIP
1300	{user_name} created Personal Access Token {token_name}	M	false	KMIP
1301	{user_name} {update_info} Personal Access Token {token_name}	M	false	KMIP
1302	{user_name} deleted Personal Access Token {token_name}	M	false	KMIP
1400	{user_name} created OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP
1401	{user_name} failed to create OIDC user {oidc_user_email}	M	false	KMIP
1402	{user_name} updated OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP
1403	{user_name} failed to update OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP

Msg ID	Message	Severity	Alert?	Category
1404	{user_name} deleted OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP
1405	{user_name} failed to delete OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP
1406	{user_name} created registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP
1407	{user_name} failed to create registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	KMIP
1408	Login failure for OIDC user {username} from {client_ip}. Reason: {reason}	M	false	KMIP
1500	{user_name} created SCIM Token {token_id} expiring on {expiry_date}	M	false	KMIP
1501	User {oidc_user_name} ({oidc_user_email}: {oidc_user_guid}) deleted by SCIM	M	false	KMIP
1502	User {oidc_user_name} ({oidc_user_email}: {oidc_user_guid}) created by SCIM and added to policy {policy_name}	M	false	KMIP
1503	User ({oidc_user_email}: {oidc_user_guid}) updated by SCIM from '{old_name}' to '{new_name}'	M	false	KMIP
1504	{user_name} deleted SCIM Token	M	false	KMIP
1600	KMIP client certificate '{cert_name}' has expired. KMIP clients using this certificate will no longer be able to access the KMIP server. Please create a new certificate and update the KMIP clients.	H	true	KMIP
1601	KMIP client certificate '{cert_name}' will expire in {days} days, {hours} hours and {minutes} minutes. Please create a new certificate and update the KMIP clients before it expires.	H	true	KMIP
1602	{user_name} updated OIDC configuration on vault '{vault_name}'	H	true	KMIP

Msg ID	Message	Severity	Alert?	Category
1603	{user_name} updated OIDC CA certificate for vault '{vault_name}'	H	true	KMIP

CSP Vault for PKCS#11 Audit Messages

The audit messages in this section are from the Cryptographic Security Platform Vault for PKCS#11.

In the table below, we list many of the audit messages and show:

- Whether an Alert is also generated.
- The severity (L=Low, M=Medium, H=High).
- What the resolution is if any action should be taken.
- In the **Message** column, a value in braces, such as `{user_name}`, represents a placeholder that is replaced with an actual value. For example, in the following message:

  `'{user_name}' created the policy '{policy_name}'`

  The actual message will be displayed with the name of the user and policy, for example:

  Fred created the policy **Default_Policy**

Msg ID	Message	Severity	Alert?	Category
100	'{user_name}' created the policy '{policy_name}'	M	false	PKCS 11
101	'{user_name}' updated the policy '{policy_name}'. New policy version is {policy_version}.	M	false	PKCS 11
102	'{user_name}' deleted the policy '{policy_name}'	M	false	PKCS 11
103	'{user_name}' changed the current version of the policy '{policy_name}'. Current policy version is {policy_version}.	M	false	PKCS 11
200	'{user_name}' created client certificate '{cert_name}'	M	false	PKCS 11

Msg ID	Message	Severity	Alert?	Category
201	'{user_name}' created client certificate '{cert_name}' with CSR	M	false	PKCS 11
202	'{user_name}' deleted client certificate '{cert_name}'	M	false	PKCS 11
300	User '{user_name}' logged in successfully.	H	false	PKCS 11
301	Active Directory login for '{username}' succeeded but failed to get information about user. The user might not belong to the Active Directory Domain {domain_name} or user/group Base DN in Active Directory configuration might be wrong. Please contact PKCS11 Administrator to validate the Active Directory setup.	H	false	PKCS 11
302	Login failure for Active Directory user '{username}' from {client_ip}. Reason: {reason}	H	false	PKCS 11
303	User '{user_name}' logged in successfully using Personal Access Token {token_name}.	H	false	PKCS 11
304	'{user_name}' enabled authentication inheritance	M	false	PKCS 11
305	'{user_name}' updated OIDC authentication with AD	M	false	PKCS 11
306	User '{user_name}' logged out successfully.	H	false	PKCS 11
400	'{user_name}' updated AD Setting '{ad_setting_name}'	M	false	PKCS 11

Msg ID	Message	Severity	Alert?	Category
401	'{user_name}' changed AD Domain from '{old_ad_setting_name}' to '{ad_setting_name}'	M	false	PKCS11
402	'{user_name}' added AD Setting '{ad_setting_name}'	M	false	PKCS11
500	'{user_name}' updated PKCS11 vault '{vault_name}' settings. 'degraded mode availability' {degraded_mode}. 'OIDC authentication' {oidc}. 'audit alert distribution list' {audit_alert_dl}. 'alert read count' {alert_read_count}. 'email notify alerts' {email_notify_alerts}.	M	false	PKCS11
501	'{user_name}' renamed PKCS11 vault '{old_name}' to '{vault_name}'.	M	false	PKCS11
502	'{user_name}' updated PKCS11 vault '{vault_name}' settings of authentication method to AD based authentication	M	false	PKCS11
503	'{user_name}' updated the CSP Compliance Manager settings for PKCS11 Vault '{vault_name}' with CSP Compliance Manager IP '{kcm_ip}'.	M	false	PKCS11
504	'{user_name}' updated PKCS11 vault '{vault_name}' settings of authentication method to OIDC based authentication	M	false	PKCS11
505	'{user_name}' updated vault owner to {vault_owner}	M	false	PKCS11
600	'{user_name}' created the user '{name}'	M	false	PKCS11
601	'{user_name}' deleted the user '{name}'	M	false	PKCS11

Msg ID	Message	Severity	Alert?	Category
602	'{user_name}' updated the user '{name}'	M	false	PKCS 11
603	Account '{user_name}' locked for 5 minutes due to repeated login failures	M	false	PKCS 11
604	Account '{user_name}' disabled due to repeated login failures	M	false	PKCS 11
605	Login failure for Local user '{username}' from {client_ip}. Reason: {reason}	H	false	PKCS 11
606	Successfully updated password for user: '{username}'	H	false	PKCS 11
607	Account '{user_name}' enabled Two-Factor Authentication	M	false	PKCS 11
608	Account '{user_name}' disabled Two-Factor Authentication	M	false	PKCS 11
609	'{user_name}' updated the local user password policy	M	false	PKCS 11
610	'{user_name}' enforced Two-Factor Authentication for all users	M	false	PKCS 11
611	'{user_name}' removed Two-Factor Authentication enforcement	M	false	PKCS 11

Msg ID	Message	Severity	Alert?	Category
700	'{user_name}' created Personal Access Token '{token_name}'	M	false	PKCS 11
701	'{user_name}' updated Personal Access Token '{token_name}'	M	false	PKCS 11
702	'{user_name}' deleted Personal Access Token '{token_name}'	M	false	PKCS 11
800	'{user_name}' created OIDC user '{name}'	M	false	PKCS 11
801	'{user_name}' failed to create OIDC user '{name}'. Reason: {reason}	M	false	PKCS 11
802	'{user_name}' updated OIDC user '{name}'	M	false	PKCS 11
803	'{user_name}' failed to update OIDC user '{name}'. Reason: {reason}	M	false	PKCS 11
804	'{user_name}' deleted OIDC user '{name}'	M	false	PKCS 11
805	'{user_name}' failed to delete OIDC user '{name}'. Reason: {reason}	M	false	PKCS 11
806	'{user_name}' created OIDC registration link for '{name}'	M	false	PKCS 11

Msg ID	Message	Severity	Alert?	Category
807	'{user_name}' failed to create OIDC registration link for '{name}'. Reason: {reason}	M	false	PKCS 11
808	OIDC login failure for user '{username}' from {client_ip}. Reason: {reason}	H	false	PKCS 11
900	'{user_name}' created SCIM token	M	false	PKCS 11
901	'{user_name}' deleted SCIM user '{name}'	M	false	PKCS 11
902	'{user_name}' created SCIM user '{name}'	M	false	PKCS 11
903	'{user_name}' updated SCIM user '{name}'	M	false	PKCS 11
904	'{user_name}' deleted SCIM token	M	false	PKCS 11
1000	'{user_name}' updated OIDC configuration on vault '{vault_name}'	H	true	PKCS 11
1001	'{user_name}' updated OIDC CA certificate for vault '{vault_name}'	H	true	PKCS 11
1100	Client certificate '{cert_name}' has expired. Clients using this certificate will no longer be able to access the vault. Please create a new certificate.	H	true	PKCS 11

Msg ID	Message	Severity	Alert?	Category
1101	Client certificate '{cert_name}' will expire in {days} days, {hours} hours and {minutes} minutes. Please create a new certificate before it expires.	H	true	PKCS 11
1200	'{user_name}' created softcard '{label}'	M	false	PKCS 11
1201	'{user_name}' failed to create softcard '{label}'. Reason: {reason}	M	false	PKCS 11
1202	'{user_name}' deleted softcard '{label}'	M	false	PKCS 11
1203	'{user_name}' failed to delete softcard '{label}'. Reason: {reason}	M	false	PKCS 11
1204	'{user_name}' updated the password of softcard '{label}'	H	false	PKCS 11
1205	'{user_name}' failed to update the password of softcard '{label}'. Reason: {reason}	H	false	PKCS 11
1300	'{user_name}' restarted the PKCS#11 server	M	false	PKCS 11
1301	'{user_name}' updated the PKCS#11 server configuration: port={port}, log_level={log_level}, debug_level={debug_level}, assurance_overrides={assurance_overrides}	M	false	PKCS 11

CSP Vault for Secrets Audit Messages

The audit messages in this section are from the Cryptographic Security Platform Vault for Secrets.

In the table below, we list many of the audit messages and show:

- Whether an Alert is also generated.
- The severity (L=Low, M=Medium, H=High).
- What the resolution is if any action should be taken.
- In the **Message** column, a value in braces, such as `{user_name}`, represents a placeholder that is replaced with an actual value. For example, in the following message:

  `{user_name} created the box '{box_name}'`

  The actual message will be displayed with the name of the user and policy, for example:

  Fred created the box 'Finance_Secrets'

Msg ID	Message	Severity	Alert?	Category
1	{user_name} created the box '{box_name}'	M	false	Vault
2	{user_name} updated the box '{box_name}'	M	false	Vault
3	{user_name} deleted the box '{box_name}'	M	false	Vault
4	{user_name} revoked the box '{box_name}'	M	false	Vault
100	{user_name} created the secret '{secret_name}' in the box '{box_name}'	M	false	Vault
101	{user_name} updated the secret '{secret_name}' in the box '{box_name}'	H	false	Vault
102	{user_name} deleted the secret '{secret_name}' from the box '{box_name}'	H	false	Vault
103	{user_name} revoked the secret '{secret_name}' from the box '{box_name}'	H	false	Vault
104	{user_name} checked out the secret '{secret_name}' from the box '{box_name}'. Secret version is {secret_version}. Lease expiration: {expiration}. Purpose: {purpose}.	H	false	Vault
105	{user_name} checked in version {secret_version} of secret '{secret_name}' in the box '{box_name}'	H	false	Vault

Msg ID	Message	Severity	Alert?	Category
106	Secret '{secret_name}' in the box '{box_name}' was rotated. New secret version is {secret_version}.	H	false	Vault
107	Rotating the secret '{secret_name}' in the box '{box_name}' failed. Current secret version is {secret_version}.	M	false	Vault
109	{user_name} accessed secret data from the secret '{secret_name}' in the box '{box_name}'. Secret version accessed is {secret_version}.	H	false	Vault
110	{user_name} updated the secret data of the secret '{secret_name}' in box '{box_name}'. New secret version is {secret_version}.	M	false	Vault
111	{user_name} changed the current version of the secret '{secret_name}' in the box '{box_name}'. Current secret version is {secret_version}	M	false	Vault
112	Setting secret '{secret_name}' version {secret_version} in the box '{box_name}' invalid.	M	false	Vault
113	{user_name} appended key certificate pair to the secret '{secret_name}' in the box '{box_name}'.	H	false	Vault
115	{user_name} removed key certificate pair from the secret '{secret_name}' in the box '{box_name}'.	H	false	Vault
200	Lease for the secret '{secret_name}' from the box '{box_name}' checked out by '{checkout_user}' expired	H	false	Vault
201	{user_name} deleted the lease for the secret '{secret_name}' from the box '{box_name}'	H	false	Vault
202	{user_name} renewed the lease for the secret '{secret_name}' from the box '{box_name}'. Secret version is {secret_version}. Lease expires at '{expiration}'.	M	false	Vault
300	{user_name} created the policy '{policy_name}'	M	false	Vault
301	{user_name} updated the policy '{policy_name}'. New policy version is {policy_version}.	M	false	Vault

Msg ID	Message	Severity	Alert?	Category
302	{user_name} deleted the policy '{policy_name}'	M	false	Vault
303	{user_name} changed the current version of the policy '{policy_name}'. Current policy version is {policy_version}.	M	false	Vault
400	Secret '{secret_name}' from the box '{box_name}' was not rotated due to outstanding lease(s). Current secret version is {secret_version}.	M	false	Vault
500	User '{user_name}' logged in successfully.	H	false	Vault
501	Active Directory login for {username} succeeded but PASM Vault failed to get information about user. The user might not belong to the Active Directory Domain {domain_name} or user/group Base DN in Active Directory configuration might be wrong. Please contact Vault Administrator to validate the Active Directory setup.	H	false	Vault
502	Login failure for Active Directory user {username} from {client_ip}. Reason: {reason}	H	false	Vault
503	User '{user_name}' logged in successfully using Personal Access Token '{token_name}'.	H	false	Vault
504	{user_name} enabled authentication inheritance	M	false	Vault
505	Authentication settings for inheriting vault '{vault_name}' were {action} by the System Administrator.	M	false	Vault
600	{user_name} updated AD Setting '{ad_setting_name}'	M	false	Vault
601	{user_name} changed AD Domain from '{old_ad_setting_name}' to '{ad_setting_name}'	M	false	Vault
602	{user_name} added AD Setting '{ad_setting_name}'	M	false	Vault

Msg ID	Message	Severity	Alert?	Category
700	{user_name} created the secret rotation job {job_id} for the box '{box_name}'	M	false	Vault
701	Secret rotation job {job_id} started for the box '{box_name}', requested by {user_name}	M	false	Vault
702	Secret rotation job {job_id} completed for the box '{box_name}', requested by {user_name}	M	false	Vault
703	Secret rotation job {job_id} completed for the box '{box_name}', requested by {user_name}. Rotation of {failed_count} Secret(s) failed.	M	false	Vault
704	{user_name} deleted the secret rotation job {job_id} for the box '{box_name}'	M	false	Vault
800	{user_name} updated vault '{vault_name}' settings. 'degraded mode availability' {degraded_mode}. 'OIDC authentication' {oidc}. 'mTLS state' {mTLS}. 'audit alert distribution list' {audit_alert_dl}. 'alert read count' {alert_read_count}. 'email notify alerts' {email_notify_alerts}.	M	false	Vault
801	{user_name} renamed vault '{old_name}' to '{vault_name}'.	M	false	Vault
802	{user_name} updated KMIP '{vault_name}' settings of authentication method to AD based authentication with Active Directory domain '{ad_domain}'	M	false	Vault
803	'{user_name}' initiated HSM {op} operation on PASM vault '{vault_name}'.	M	false	Vault
804	'{user_name}' updated HSM DEK cache timeout of PASM vault '{vault_name}' to {period}.	M	false	Vault
805	HSM {state} successfully on PASM vault '{vault_name}'.	M	false	Vault
806	{user_name} updated KCM settings for PASM vault '{pasm_name}' with KCM IP '{kcm_ip}'.	M	false	Vault
807	{user_name} updated vault '{vault_name}' settings of authentication method to OIDC based authentication	M	false	Vault

Msg ID	Message	Severity	Alert?	Category
900	{user_name} created the user '{name}'	H	false	Vault
901	{user_name} deleted the user '{name}'	H	false	Vault
902	{user_name} updated the user '{name}'	H	false	Vault
903	Account '{user_name}' was locked for 5 minutes due to repeated login failures.	H	false	Vault
904	Account '{user_name}' was disabled due to repeated login failures.	H	false	Vault
905	Login failure for Local user {username} from {client_ip}. Reason: {reason}	H	false	Vault
906	Password successfully updated for user '{username}'.	H	false	Vault
907	Account {user_name} enabled Two-Factor Authentication	M	false	Vault
908	Account {user_name} disabled Two-Factor Authentication	M	false	Vault
909	{user_name} updated the local user password policy	M	false	Vault
910	{user_name} enforced Two-Factor Authentication	M	false	Vault
911	{user_name} removed enforcement of Two-Factor Authentication	M	false	Vault
1000	{user_name} updated kubernetes configuration of '{vault_name}'. 'degraded mode availability' {state}	M	false	Vault

Msg ID	Message	Severity	Alert?	Category
1001	Login failure for Kubernetes user {username}. Reason: {reason}	H	false	Vault
1002	Kubernetes user '{user_name}' logged in successfully.	H	false	Vault
1100	{user_name} created Personal Access Token {token_name}	M	false	Vault
1101	{user_name} {update_info} Personal Access Token {token_name}	M	false	Vault
1102	{user_name} deleted Personal Access Token {token_name}	M	false	Vault
1200	{user_name} created OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault
1201	{user_name} failed to create OIDC user {oidc_user_email}	M	false	Vault
1202	{user_name} updated OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault
1203	{user_name} failed to update OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault
1204	{user_name} deleted OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault
1205	{user_name} failed to delete OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault
1206	{user_name} created registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault
1207	{user_name} failed to create registration link for OIDC user {oidc_user_email}: {oidc_user_guid}	M	false	Vault

Msg ID	Message	Severity	Alert?	Category
1208	Login failure for OIDC user {username} from {client_ip}. Reason: {reason}	M	false	Vault
1301	Approver {approver} {status} the checkout approval request. Request id {request_id}. Comment: {comment}	M	false	Vault
1302	User {user} submitted Checkout approval request for secret {secret_id} in box {box_id}. Approvers {approvers} and minimum approvals required {min_approval}	M	false	Vault
1303	User {user} submitted box secondary approval update request for box {box_id}. Approvers {approvers} and minimum approvals required {min_approval}	M	false	Vault
1304	{user_name} deleted the request '{request_id}'	M	false	Vault
1400	Secret Vault Client Certificate '{name}' created	M	false	Vault
1401	Secret Vault Client Certificate '{name}' created using Certificate Signing Request	M	false	Vault
1402	Secret Vault Client Certificate '{name}' deleted	M	false	Vault
1500	{user_name} created SCIM Token {token_id} expiring on {expiry_date}	M	false	Vault
1501	User {oidc_user_name} ({oidc_user_email}: {oidc_user_guid}) deleted by SCIM	M	false	Vault
1502	User {oidc_user_name} ({oidc_user_email}: {oidc_user_guid}) created by SCIM and added to policy {policy_name}	M	false	Vault
1503	User ({oidc_user_email}: {oidc_user_guid}) updated by SCIM from '{old_name}' to '{new_name}'	M	false	Vault
1504	{user_name} deleted SCIM Token	M	false	Vault

Msg ID	Message	Severity	Alert?	Category
1600	{user_name} updated OIDC configuration on vault '{vault_name}'	H	true	Vault
1601	{user_name} updated OIDC CA certificate for vault '{vault_name}'	H	true	Vault
1700	Client certificate '{cert_name}' has expired. Clients using this certificate will no longer be able to access the vault. Please create a new certificate.	H	true	Vault
1701	Client certificate '{cert_name}' will expire in {days} days, {hours} hours and {minutes} minutes. Please create a new certificate before it expires.	H	true	Vault

Differences in CSP Vault Audit Messages

The following lists display the differences between audit log messages in CSP Vault.

Differences between v. 10.5.1 and 10.6.1:

- New audit messages in main audit file: 601, 602, 603, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 617, 618, 619, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676
- Updated audit messages in main audit file: 12, 13, 16, 17, 19, 23, 33, 38, 39, 43, 57, 58, 67, 68, 69, 82, 85, 86, 89, 91, 92, 93, 96, 97, 109, 111, 112, 138, 139, 148, 149, 150, 151, 170, 173, 174, 175, 181, 182, 185, 186, 187, 193, 200, 201, 203, 204, 205, 211, 224, 225, 229, 230, 231, 232, 236, 238, 239, 240, 247, 248, 249, 250, 251, 252, 256, 257, 258, 259, 260, 267, 268, 269, 276, 277, 278, 279, 280, 281, 282, 283, 284, 286, 287, 291, 292, 295, 296, 298, 299, 300, 301, 303, 306, 309, 310, 318, 322, 323, 324, 334, 335, 339, 366, 367, 385, 396, 402, 403, 406, 441, 454, 464, 493, 494, 495, 498, 500, 503, 504, 508, 516, 518, 526, 527, 528, 529, 530, 550, 559, 563, 564, 565, 566, 573, 577, 581, 582, 583, 584, 585, 588, 591, 600
- Removed audit messages from main audit file: 293, 294
- New audit messages in CSP Vault for Cryptographic APIs: 1700, 1701, 1702, 1703, 1704, 1800, 1801, 1900, 1901
- Updated audit messages in CSP Vault for Cryptographic APIs: 300, 301, 302, 303, 501, 502, 504, 505, 600, 601, 602, 800, 801, 802, 803, 804, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 1000, 1001, 1002, 1003, 1004, 1005, 1100, 1101, 1102, 1103, 1104, 1105, 1106, 1107, 1108, 1109, 1110, 1111, 1112, 1113, 1114, 1115, 1116, 1117, 1118, 1119, 1120, 1121, 1122, 1123, 1124, 1125, 1126, 1127, 1128, 1129, 1130, 1131, 1132, 1133, 1134, 1135, 1200, 1201, 1202, 1203, 1204, 1205, 1207, 1209, 1210, 1211, 1212, 1213, 1214, 1216, 1300, 1301, 1302, 1303, 1304, 1305, 1306, 1307, 1308, 1309, 1310, 1311, 1312, 1313, 1314, 1315, 1316, 1317, 1318, 1319, 1320, 1321, 1322, 1323, 1324, 1400, 1401, 1402, 1500, 1501, 1502, 1503, 1504, 1505, 1506, 1507, 1508, 1600, 1601, 1602, 1603, 1604, 1605, 1606, 1607, 1608, 1609, 1136, 1137, 1138, 1139, 1140, 1141
- New audit messages in CSP Vault for KMIP: 1500, 1501, 1502, 1503, 1504, 1600, 1601, 1602, 1603
- Updated audit messages in CSP Vault for KMIP: 300, 501, 505, 800, 801, 802, 803, 1203, 1204, 1206, 1207, 1208, 1210, 1211
- New audit messages in CSP Vault for Secrets: 1500, 1501, 1502, 1503, 1504, 1600, 1601, 1700, 1701

- Updated audit messages in CSP Vault for Secrets: 101, 104, 501, 503, 505, 602, 800, 802, 806, 903, 904, 906, 907, 908, 910, 911, 1001, 1002, 1200, 1201, 1202
- New audit messages in CSP Vault for PKCS#11: 100, 101, 102, 103, 200, 201, 202, 300, 301, 302, 303, 304, 305, 306, 400, 401, 402, 500, 501, 502, 503, 504, 505, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 700, 701, 702, 800, 801, 802, 803, 804, 805, 806, 807, 808, 900, 901, 902, 903, 904, 1000, 1001, 1100, 1101, 1200, 1201, 1202, 1203, 1204, 1205, 1300, 1301

Differences between v. 10.4.7 and 10.5.1:

- New audit messages in main audit file: 563-567, 571-576, 579-600, 604, 615-616
- Updated audit messages in main audit file: 251-252, 418-419, 429-434, 457, 488, 497, 506, 514-515, 533, 577
- New audit messages in CSP Vault for Cryptographic APIs: 504-505, 910-911, 1323-1324, 1136-1141
- Updated audit messages in CSP Vault for Cryptographic APIs: 400-402, 1205, 1214,
- New audit messages in CSP Vault for KMIP: 504-505, 1210-1211
- New audit messages in CSP Vault for Secrets: 504-505, 910-911

Differences between v. 10.4.5 and 10.4.7:

- New audit messages in main audit file: 561-562, 568-570, 577-578
- New audit messages in CSP Vault for Cryptographic APIs: 1134-1135, 1321-1322
- New audit messages in CSP Vault for Secrets: 1400-1402

Differences between v. 10.4.3 and 10.4.5:

- New audit messages in main audit file: 548-560
- New audit messages in CSP Vault for Cryptographic APIs: 400-402, 1600-1609

Differences between v. 10.4.1.1 and 10.4.3:

- New audit messages in main audit file: 539-547
- Updated audit messages: 538

Differences between v. 10.3.3 and 10.4.1.1:

- Separate audit logs were created for the CSP Vault for Cryptographic APIs, the CSP Vault for KMIP, and the CSP Vault for Secrets. The main audit file contains audit logs for the KeyControl Vault Management Appliance, the CSP Vault for Cloud Keys, the CSP Vault for Databases, and the CSP Vault for VM Encryption.
- New audit messages: 479, 525-538
- Updated audit messages: 386, 456, 480

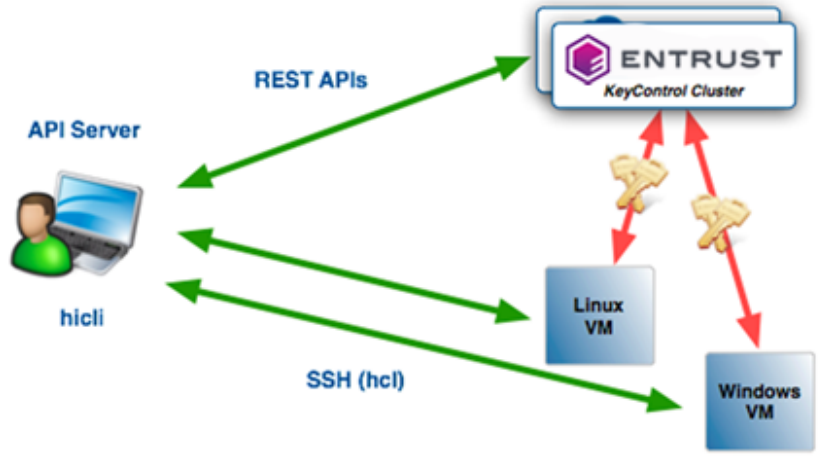
14 hicli scripting guide

This chapter describes the `hicli` tool for managing operations between the Cryptographic Security Platform Vault cluster and an Entrust Policy Agent present in Linux and Windows virtual machines. `hicli` uses a combination of the Cryptographic Security Platform Vault REST APIs to communicate with Cryptographic Security Platform Vault, and SSH to invoke `hcl` commands on Windows and Linux VMs.

The Policy Agent provides for encryption of devices within Linux and Windows virtual machines. The Cryptographic Security Platform Vault cluster manages keys and administers the Policy Agent. Administration can take place through the webGUI, through the RESTful APIs, or through using the `hicli` command.

`hicli` can only be accessed through the Cryptographic Security Platform Vault for Databases webGUI and the Cryptographic Security Platform Vault for VM Encryption webGUI.

We will be operating with one or more clustered Cryptographic Security Platform Vault nodes, a number of Linux or Windows VMs, and the API Server, a server from which `hicli` will be invoked. This can be almost any UNIX-like server, including Linux, BSD variants, OS/X and so on.



See below for installing and configuring the `hicli` command-line tool.

- Downloading hicli
- Extracting hicli
- Installing Python modules
- Setting the environment variable
- Enabling the python3 command
- Creating the configuration file
- Verifying
- Setting SSH communication

Downloading hicli

See below for downloading hicli.

To download hicli

1. Log in to the Cryptographic Security Platform Vault for VM Encryption using an account with Cloud Admin privileges.
2. In the top menu bar, click **Workloads**.
3. Select **Actions > Download Policy Agent**.
4. From the Available Downloads dialog box, download the `hcs-api-10.5.3-buildnum.tgz` file, where `buildnum` is the build number for the release you are installing.

Extracting hicli

Copy the `tgz` file to the VM on which you want to install the API and untar it as follows.

```
$ cd ~
$ tar xvfz hcs-api-10.5.3-buildnum.tgz

x hcs-api/
x hcs-api/hclcomm.py
x hcs-api/kpsapi.py
x hcs-api/docopt.py
x hcs-api/hicli
```

Installing Python modules

Install the `requests` and `winrm` Python modules.

```
$ pip install requests
$ pip install pywinrm
```

Setting the environment variable

Set the `PYTHONPATH` environment variable to point to the directory where you extracted `hicli`, and modify your `PATH` so that the shell can reference the `hicli` program. For example, if the install location is `/Users/spate`, the environment variables need to be set up as follows:

```
$ export PYTHONPATH=$PYTHONPATH:/Users/spate/hcs-api
$ export PATH=$PATH:/Users/spate/hcs-api
```

Enabling the python3 command

If your Python installation only includes a `python` command and not a `python3` command, then do one of the following:

- Edit the first line of `hicli` from `#!/usr/bin/env python3` to `#!/usr/bin/env python`.
- Define an alias like the following:

```
hicli='python /Users/<user_name>/hcs-api/hicli'
```

Creating the configuration file

Set up a configuration with the following path:

```
~/.hicli/hicli.cf
```

This file contains information about the virtual machines to be managed. Specifically:

- The number and location of curly brackets are important. Make sure your configuration file looks like the example below.
- If the platform is not specified, it defaults to `"linux"`.
- Windows platforms require a password to connect over WinRM.
- By default, the `hicli.cfg` file is used to resolve VM names. If no entries are found, DNS is used to resolve the VM names.
- On Linux, you can run `hicli` commands as `root` or as a `sudo` user. If you specify a `sudo` user, you also specify a password if the `sudo` user requires one. On Windows, you can run `hicli` with any Windows account that has Administrator privileges.

The following sample configuration file registers the following machines.

Virtual machine	OS	Authentication mode
ubuntu10.04	Linux	Standard root account
ubuntu12.10	Linux	Password
rhel73	Linux	Passwordless sudo user
Windows2012r2	Windows	Administrator account with password

```
{
  "cvmlist": {
    "ubuntu10.04": {
      "host":"192.168.140.129",
```

```
      "port":"22",
      "user":"root"
    },
    "ubuntu12.10": {
      "host":"192.168.140.130",
      "port":"22",
      "user":"spate",
      "sudo_password" : "<password>"
    },
    "rhel73": {
      "host":"192.168.140.131",
      "port":"22",
      "user":"jsmith"
    },
    "Windows2012r2": {
      "host":"192.168.140.132",
      "user":"Administrator",
      "password":"<password>",
      "platform": "windows"
    }
  }
}
```

To manage another virtual machine with `hicli`, add that entry to the configuration file.

```
{
  "cvmlist": {
    "ubuntu10.04": {
      "host":"192.168.140.129",
      "port":"22",
      "user":"root"
    },
    "ubuntu12.10": {
      "host":"192.168.140.130",
      "port":"22",
      "user":"spate",
      "sudo-password" : "<password>"
    },
    "rhel73": {
      "host":"192.168.140.131",
      "port":"22",
      "user":"jsmith"
    },
    "Windows2012r2": {
      "host":"192.168.140.132",
      "user":"Administrator",
      "password":"<password",
      "platform": "windows"
    },
    "ubuntu13.04": {
      "host":"192.168.140.133",
      "port":"22",
```

```
      "user":"root"
    }
  }
}
```

Verifying

To verify the installation, run the `hicli` command and you should see a comprehensive listing of the command and its options.

Setting SSH communication

To set up SSH communication on each Linux host, generate a key pair on the API server and copy the public key to each VM on which you want to run API commands.

In Linux, append the public key to `authorized_keys` file for either `root` or the sudo user you specified in the `hicli.cfg` file

In Windows, use WinRM.

The following example uses `ssh-keygen` on the API server to generate the key pair and then uses `ssh-copy-id` to send the public key to the Linux VMs we added to the `hicli.cfg` file above.

```
api# cd ~/.ssh
api# ssh-keygen -t dsa
api# ssh-copy-id id_dsa.pub root@192.168.140.129
api# ssh-copy-id id_dsa.pub spate@192.168.140.130
api# ssh-copy-id id_dsa.pub jsmith@192.168.140.131
api# ssh-copy-id id_dsa.pub root@192.168.140.133
```

After you copy the public key to the VM, make sure that, on each VM:

- You enable root or sudo user login over SSH to the VM. If you are using a passwordless sudo user, you need to set up passwordless SSH access for that user using the pub.
- You turn off SSH warnings.

To test that SSH access is working between your API server and your VM, issue a test command over SSH. For example, you can use SSH to query the hostname on the VM:

```
$ ssh root@192.168.140.129 hostname ubuntu10.04
```

15 Command reference

See below for a reference of `hicli` commands

- alert detail <alertnum>
- alert list
- alert rm <alertid>
- create_bucket
- delete_bucket
- global set
- hicli byok log <group>
- hicli cert detail
- hicli cert new
- hicli cert rm
- hicli cloudkey delete_from_cloud
- hicli cloudkey detail
- hicli cloudkey disable
- hicli cloudkey ekm_acls
- hicli cloudkey enable
- hicli cloudkey getpublickey
- hicli cloudkey has_ekm_acls disable
- hicli cloudkey has_ekm_acls enable
- hicli cloudkey import
- hicli cloudkey kaj_policy
- hicli cloudkey keyops
- hicli cloudkey list
- hicli cloudkey new
- hicli cloudkey policy_get
- hicli cloudkey policy_set
- hicli cloudkey purge
- hicli cloudkey rm
- hicli cloudkey roles_get
- hicli cloudkey roles_set
- hicli cloudkey rotate
- hicli cloudkey set
- hicli cloudkey set_primary
- hicli cloudkey tag clear
- hicli cloudkey tag list
- hicli cloudkey tag set
- hicli cloudkey upload_to_cloud
- hicli cloudkey users
- hicli cloudkey versions
- hicli csp cert_auth
- hicli csp detail
- hicli csp ekm_acls
- hicli csp ekmconnections
- hicli csp get_cert_details
- hicli csp kaj_policy
- hicli csp kaj_policy_state
- hicli csp key_algorithms
- hicli csp keyrings
- hicli csp keyvaults

- hicli csp list
- hicli csp managedhsms
- hicli csp new
- hicli csp regions
- hicli csp rm
- hicli csp roles
- hicli csp rotate
- hicli csp set
- hicli csp users
- hicli cvm add_disk
- hicli cvm decrypt_task
- hicli cvm detail
- hicli cvm detail_disk
- hicli cvm encrypt_task
- hicli cvm list
- hicli cvm list_tasks
- hicli cvm new
- hicli cvm reauth
- hicli cvm rekey_task
- hicli cvm renew clone
- hicli cvm revoke
- hicli cvm revoke_disk
- hicli cvm rm
- hicli cvm rm_disk
- hicli cvm s3 add_file
- hicli cvm s3 get_file
- hicli cvm s3 rm_file
- hicli cvm select
- hicli cvmset
- hicli cvm set
- hicli cvm set_disk expiration
- hicli cvm set_mapping
- hicli cvmset add_kek
- hicli cvmset detail
- hicli cvmset kek_edit
- hicli cvmset kek_state_change
- hicli cvmset list
- hicli cvmset list_tasks
- hicli cvmset new
- hicli cvm set rekey
- hicli cvmset select
- hicli cvmset set
- hicli cvmset set grace
- hicli cvmset set heartbeat
- hicli cvmset set name
- hicli cvmset set rekey
- hicli cvmset set rekeybucket
- hicli cvm status
- hicli cvm unrevoke_disk
- hicli domain detail
- hicli domain list
- hicli domain select
- hicli domain set

- hicli domain set allow_reconnect
- hicli domain set description
- hicli domain set hide_passphrase
- hicli generate_csr
- hicli group add_user
- hicli group detail
- hicli group list
- hicli group new
- hicli group rm
- hicli group rm_user
- hicli group set
- hicli group set description
- hicli group set name
- hicli kc
- hicli kc select <kchost>
- hicli keyid new
- hicli keyid revoke
- hicli keyid rm
- hicli keyid set expiration
- hicli keyid set onexpiry
- hicli keyid unrevoke
- hicli keyset add_tde_connector
- hicli keyset container_purge
- hicli keyset create_tde_connector_token
- hicli keyset detail
- hicli keyset keyrings
- hicli keyset list
- hicli keyset list_tde_connectors
- hicli keyset new
- hicli keyset rm
- hicli keyset select
- hicli keyset set
- hicli keyset set_sync_schedule
- hicli keyset tde_connector delete
- hicli keyset tde_connector disable
- hicli keyset tde_connector enable
- hicli keyset verify_hsm
- hicli keyset verify_tde_connector_token
- hicli mapping detail
- hicli mapping list
- hicli mapping new
- hicli mapping rm
- hicli mapping select
- hicli mapping set description
- hicli mapping set group
- hicli mapping set newname
- hicli mapping set servers
- hicli server auth
- hicli server auth
- hicli server default_csr_values
- hicli server detail
- hicli server install_cert
- hicli server install_cert_status

- hicli server show_cert
- hicli server use_default_certs
- hicli server webserver_restart
- hicli user defaults
- hicli user detail <username>
- hicli user list
- hicli user login <name>
- hicli user new <username>
- hicli user rm <username>
- hicli user set <username>
- kmipsrv_obj action uuid
- kmipsrv_obj fetch
- kmipsrv_user
- kmipsrv set
- list_bucket
- s3 add_file
- s3 get_file
- s3 rm_file
- set aws_access_key_id
- set aws_secret_access_key

alert detail <alertnum>

View the details for the alert with the `<alertnum>` number. For exmaple, to get the details of alert 1:

```
$ hicli alert rm b62c3bb3954611e3bfe6080027cbdf2a
```

alert list

List the alerts sent to the logged-in user account. For example:

```
$ hicli alert list
1 10/08/17 17:06:52 Account disabled for spate due to repeated failures
2 10/08/17 17:08:00 VM Set Admin Group group has been granted access to datastore
dedup on
```

alert rm <alertid>

Remove an alert with the <alertid> identifier sent to the logged-in user account. For example, to delete alert 1:

```
$ hicli alert rm b62c3bb3954611e3bfe6080027cbdf2a
```

create_bucket

Create a new S3 bucket.

delete_bucket

Delete an existing S3 bucket.

global set

Set the defaults for newly-created Cloud VM Sets. Changing these options does not affect any existing Cloud VM Sets.

Option	Value
--heartbeat	The default heartbeat interval in seconds (default is 5 minutes, or 300 seconds).
--grace	The value for the grace period in seconds (default is 1 day).

For example:

```
$ hicli global set --heartbeat=60 --grace=600
```

hicli byok log <group>

Display BYOK logs for the <group> group.

hicli cert detail

Displays information about the specified certificate.

hicli cert new

Creates a new certificate for the Cloud VM Set.

hicli cert rm

Removes an unused certificate.

hicli cloudkey delete_from_cloud

Delete a cloud key from the provider. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey detail

Display details for a cloud key.

hicli cloudkey disable

Disable a cloud key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey ekm_acls

Apply EKM ACLs to a keyring key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list

- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey enable

Enable a cloud key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge

- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey getpublickey

Get the public key for a cloud key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation

- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey has_ekm_acls disable

Disable EKM ACLs for a keyring key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions

- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey has_ekm_acls enable

Enable EKM ACLs for a keyring key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date

- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey import

Import a key into either:

- region
- key vault
- managed HSM
- keyring

See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher

- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey kaj_policy

Apply a KAJ policy to a keyring key. See below for the options supported by the cloudkey commands.

- <name>
- --name

- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey keyops

Set the operations allowed for a cloud key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey list

List keys in a region, key vault, managed HSM, or keyring. For example:

```
$ hicli cloudkey list

KeyRing                    | CloudKey Name | guid                                  |
Cloud Status  | handle
------------------------------------------------------------------------------------
-----------------------------------
ext_ekm_ring(europe-west2) | testkey1      | fd2c4f21-d390-4b05-bdce-9bd15b5bef75  |
AVAILABLE     | 21730251-2d6c-45e8-9852-74adf0308dae.europe-
west2~ext_ekm_ring.testkey1
ext_ekm_ring(europe-west2) | hsmkey1       | 13eaa6be-3c25-42a5-8cc1-235880e4c114  |
NOT AVAILABLE | 21730251-2d6c-45e8-9852-74adf0308dae.europe-
west2~ext_ekm_ring.hsmkey1
```

hicli cloudkey new

Create a cloud key and configure:

- location
- algorithm
- protection
- expiry
- provider-specific settings

See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval

- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey policy_get

Get a cloud key policy and optionally write it to a file. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring

- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey policy_set

Set a cloud key policy, optionally reading it from a file. See below for the options supported by the cloudkey commands.

- <name>

- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey purge

Purge a cloud key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey rm

Schedule removal of a cloud key or cancel scheduled removal. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey roles_get

Get roles for a keyring key and optionally write them to a file. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list

- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey roles_set

Set roles for a keyring key, optionally reading them from a file. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type

- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey rotate

Rotate a cloud key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date

- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey set

Update the settings of a cloud key:

- description
- rekey
- expiry
- activation
- provider-specific settings

See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description

- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey set_primary

Set a key version as primary. See below for the options supported by the cloudkey commands.

- <name>
- --name

- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey tag clear

Clear a tag from a cloud key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey tag list

List tags on a cloud key.

hicli cloudkey tag set

Set a tag on a cloud key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list

- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey upload_to_cloud

Upload a cloud key to the provider. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge

- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey users

Supply user and administrator lists for a cloud key. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire
- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type

- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli cloudkey versions

Schedule removal of a cloud key or cancel scheduled removal. See below for the options supported by the cloudkey commands.

- <name>
- --name
- --region
- --keyvault
- --managedhsm
- --keyring
- --handle
- --description
- --cipher
- --protection_level
- --purpose
- --algorithm
- --hardware_protected
- --rekey_interval
- --no-expire
- --expire_date
- --relative_expiry
- --no-key-wide-expire

- --key_wide_expire_date
- --expire_action
- --operations
- --activation_date
- --ekm_connection
- --dke_permissions
- --dke_cache
- --oci_compartment_id
- --sfdc_data_type
- --sfdc_use_derivation
- --sfdc_cache_only_key
- --after_days
- --cancel
- --force_purge
- --key
- --value
- --user_list
- --admin_list
- --in
- --out
- --guid

<name>

Name to assign to a new cloud key.

--name

Select a cloud key by name.

> The command may also require its provider resource.

--region

Region containing or used for the key.

--keyvault

Key vault containing or associated with the key.

--managedhsm

Managed HSM containing or associated with the key.

--keyring

Keyring containing or associated with the key.

--handle

Identify a key by its handle where supported.

--description

Optional human-readable description of the key.

--cipher

Cipher to use for the key.

--protection_level

GCP protection level or EKM connection type.

--purpose

Intended purpose of the key.

--algorithm

Key algorithm.

--hardware_protected

Request hardware protection for the key.

--rekey_interval

Rekey interval for the key.

--no-expire

Specify that the key should not expire.

--expire_date

Expiration date in mm/dd/yyyy format or a number of days.

--relative_expiry

Specify whether the expiry value is relative: True or False.

--no-key-wide-expire

Specify that the key should not use key-wide expiry.

--key_wide_expire_date

Key-wide expiration date in mm/dd/yyyy format.

--expire_action

Expiration action: DISABLE, DELETE_FROM_CLOUD, or DELETE.

--operations

Operations to allow for the key.

--activation_date

Date when the key should become active.

--ekm_connection

EKM connection to associate with the key.

--dke_permissions

DKE permissions to configure for the key.

--dke_cache

DKE cache setting.

--oci_compartment_id

OCI compartment ID for the key.

--sfdc_data_type

Salesforce data type associated with the key.

--sfdc_use_derivation

Salesforce key-derivation setting.

--sfdc_cache_only_key

Salesforce cache-only-key setting.

--after_days

Number of days before scheduled key removal.

--cancel

Cancel a scheduled key removal.

--force_purge

Force-purge option for the purge operation.

--key

Tag name to set or clear.

--value

Value to assign to a tag.

--user_list

User list supplied to the cloud key command.

--admin_list

Administrator list supplied to the cloud key command.

--in

Input file for policy, role, KAJ policy, or EKM ACL data.

--out

Output file for policy or role data.

--guid

GUID of the key version to set as primary.

hicli csp cert_auth

Configure certificate authentication for a CSP. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id

- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp detail

Check a CSP configuration. For example:

```
$ hicli csp detail --guid=67ebe878-79ea-43e0-9660-d255743ae86b
CSP Account Name                        : cloud_csp
Group Name                              : Cloud Admin Group
KeySet Name                             : cloudkeyset
Description                             :
CSP type                                : AZURE
CSP guid                                : 67ebe878-79ea-43e0-9660-d255743ae86b
Azure App Name                          : ank-test
Azure Tenant ID                         : a885294f-8307-4043-b78b-4a0e4c7f0213
Azure Subscription ID                   : e9f13067-10b4-4136-9fba-58950342182f
Azure Application (Client) ID           : a2da5dfa-78a4-44a9-91f1-bf6f3734ae77
Azure Application Object ID             : 93872964-657b-46da-976b-7bc8d1e02185
Use Certificate Auth                    : False
Access key rotation interval (in days): 0
Last key rotation (or set) date         : 09/28/2026 09:22:43 AM GMT
```

hicli csp ekm_acls

Apply EKM ACLs to a CSP, optionally using a file. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint

- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp ekmconnections

List EKM connections at the specified location. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth

- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp get_cert_details

Display certificate details for a CSP. See below for the options supported by CSP commands.

- <name>
- <group>

- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp kaj_policy

Apply a KAJ policy to a CSP, optionally using a file. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location

- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp kaj_policy_state

Enable or disable a CSP's KAJ policy. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content

- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp key_algorithms

List key algorithms supported by a CSP. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth

- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp keyrings

List keyrings for a CSP; can optionally request synchronization. See below for the options supported by CSP commands.

- <name>

- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp keyvaults

List key vaults available for a CSP. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location

- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp list

List configured CSPs. See below for the options supported by CSP commands. For example,

```
$ hicli csp list

CSP Account Name     | CSP type   | CSP guid                              | group
| KeySet
-------------------------------------------------------------------------------------
-------------------------------------------------------------
cloud_csp            | AZURE      | 67ebe878-79ea-43e0-9660-d255743ae86b | Cloud
Admin Group   | cloudkeyset
```

hicli csp managedhsms

List managed HSMs available for a CSP. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid

- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp new

Create a CSP configuration for one of the following providers

- AWS
- Azure
- GCP
- OCI
- Salesforce

See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp regions

List regions available for a CSP. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content

- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp rm

Remove a CSP configuration. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth

- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp roles

List roles associated with a CSP. See below for the options supported by CSP commands.

- <name>
- <group>

- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp rotate

Rotate a CSP certificate. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location

- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp set

Update a CSP's description, credentials, or provider-specific settings. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth
- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint

- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli csp users

List users associated with a CSP. See below for the options supported by CSP commands.

- <name>
- <group>
- --name
- --guid
- --csp_type
- --description
- --aws_access_key_id
- --aws_secret_access_key
- --default_region
- --azure_tenant_id
- --azure_subscription_id
- --azure_client_id
- --azure_application_objectid
- --azure_client_secret
- --use_cert_auth

- --generate_new_cert
- --self_sign_cert
- --cert_expiry
- --common_name
- --signed_cert_file
- --private_key_file
- --passphrase
- --gcp_key_file
- --ekm_uri
- --ekm_service_account
- --oci_user_ocid
- --oci_fingerprint
- --oci_key_content
- --oci_key_passphrase
- --oci_tenancy_ocid
- --oci_bucket
- --oci_storage_namespace
- --sfdc_client_id
- --sfdc_client_secret
- --sfdc_domain
- --sfdc_wrapping_cert
- --sfdc_named_credential
- --access_key_rotation_interval
- --sync
- --location
- --in

<name>

Name to assign to a new CSP.

<group>

Group associated with the new CSP.

--name

Select an existing CSP by name.

--guid

Select an existing CSP by GUID.

--csp_type

CSP provider type: AWS, AZURE, GCP, OCI, or SFDC.

--description

Optional human-readable description.

--aws_access_key_id

AWS access key ID.

--aws_secret_access_key

Secret access key corresponding to the AWS access key ID.

--default_region

Default AWS region used for CSP operations.

--azure_tenant_id

Azure tenant ID.

--azure_subscription_id

Azure subscription ID.

--azure_client_id

Client ID of the Azure application used for authentication.

--azure_application_objectid

Object ID of the Azure application.

--azure_client_secret

Client secret for the Azure application.

--use_cert_auth

Enable or disable certificate-based Azure authentication.

--generate_new_cert

Specify whether to generate a new certificate when updating the Azure CSP.

--self_sign_cert

Specify whether the certificate should be self-signed.

--cert_expiry

Certificate validity period in days.

--common_name

Common name to use for the certificate.

--signed_cert_file

Path to the signed certificate file.

--private_key_file

Path to the private key file.

--passphrase

Passphrase used to protect the private key.

--gcp_key_file

Path to the GCP key file.

--ekm_uri

URI for the GCP EKM configuration.

--ekm_service_account

Service account used for the GCP EKM configuration.

--oci_user_ocid

OCI user OCID.

--oci_fingerprint

Fingerprint associated with the OCI signing key.

--oci_key_content

OCI API signing key content.

--oci_key_passphrase

Passphrase for the OCI API signing key.

--oci_tenancy_ocid

OCI tenancy OCID.

--oci_bucket

OCI bucket used by the configuration.

--oci_storage_namespace

OCI object storage namespace.

--sfdc_client_id

Salesforce client ID.

--sfdc_client_secret

Salesforce client secret.

--sfdc_domain

Salesforce domain.

--sfdc_wrapping_cert

Certificate used for Salesforce key wrapping.

--sfdc_named_credential

Salesforce named credential.

--access_key_rotation_interval

Access-key rotation interval in days.

--sync

Specify whether keyring synchronization is requested: yes or no.

--location

Location used when listing EKM connections.

--in

Input filename for a KAJ policy or EKM ACL data.

hicli cvm add_disk

Add a disk to be encrypted.

hicli cvm decrypt_task

Perform decryption on specified disk

hicli cvm detail

Get the VM status (KeyControl perspective). For example:

```
$ hicli cvm detail ubuntu-12.10
KeyControl Status for ubuntu12.10
-----------------------------------------------------
Name                              ubuntu12.10
IP Address                        192.168.11.93
Status                            Online
Description
Cloud VM Set                      HCS
OS                                Linux ubuntu 2.7.32-38-generic #83-Ubuntu
                    SMP Wed Jan 4 11:12:07 UTC 2014 x86_64 GNU/Linux
Agent version                     10.5.3
Valid till                        02/01/2020
Heartbeat (sec)                   10
Grace period (sec)                3600
Reauth on H/W signature change    Yes
Reauth on IP address change       Yes
Reauth on reboot                  No

Disks:
sdb1                              ACTIVE
sdb2                              ACTIVE
```

hicli cvm detail_disk

Display details about a specified disk.

hicli cvm encrypt_task

Perform encryption on the specified disk.

hicli cvm list

List the VMs in the current Cloud VM Set. For example:

```
$ hicli cvm list
VM Name                Status
-----------------------------------------------------
ubuntu-10.04           Online
ubuntu-12.10           Online
```

hicli cvm list_tasks

Display list of tasks for the specified VM.

hicli cvm new

Add a new VM. For example:

```
$ hicli user login spate --password=********
$ hicli cvmset set 'Amazon EC2'
$ hicli cvm new ubuntu10.04
$ hicli cvm ubuntu10.04 add_disk sdb1
$ hicli cvm ubuntu10.04 add_disk sdb2
```

hicli cvm reauth

Re-authorize a VM

hicli cvm rekey_task

Perform rekey on the specified disk.

hicli cvm renew clone

Clone a VM certificate

hicli cvm revoke

Revoke access to the VM and its devices.

hicli cvm revoke_disk

Revoke access to the specified disk

hicli cvm rm

Remove a VM. For example:

```
$ hicli cvmset select "Amazon EC2"
$ hicli cvm ubuntu-10.04 rm_disk sdb1
$ hicli cvm ubuntu-10.04 rm_disk sdb2
$ hicli cvm revoke ubuntu-10.04
$ hicli cvm rm ubuntu-10.04
```

hicli cvm rm_disk

Remove a disk from HyTrust management

hicli cvm s3 add_file

Add a file to an S3 bucket

hicli cvm s3 get_file

Retrieve a file from an S3 bucket

hicli cvm s3 rm_file

Remove a file from an S3 bucket

hicli cvm select

Set the properties for the current Cloud VM Set as follows. For example:

```
$ hicli cvmset select "Amazon AWS"
$ hicli cvmset
Current Cloud VM Set: Amazon AWS
```

hicli cvmset

Displays the current Cloud VM Set.

hicli cvm set

Set properties of the VM.

hicli cvm set_disk expiration

Set the expiration date for a disk

hicli cvm set_mapping

Set KC mapping.

hicli cvmset add_kek

Add a KEK to an existing Cloud VM Set. For example:

```
$ hicli cvmset add_kek ”kek_cvmset" –kek_expire_days=12 –kek_expire_action="NO USE” –
expiration_options=extend
```

hicli cvmset detail

Displays details about the specified Cloud VM Set. For example:

```
$ hicli cvmset detail "Amazon-EC2"
Name                    Amazon-EC2
Admin Group             Cloud Admin Group
Guid                    d4a7093a-185e-11e8-a8fd-000c2997200a
Description             VMs running in Amazon Ubuntu-10.04,linux-12.10
Unused Certificate Ids  4c81a042a60b11e2b5cf000c29ed8423
KeyIDs                  aws_key,test_key
```

hicli cvmset kek_edit

Changes the settings for the KEK (Key Encryption Key) associated with the Cloud VM Set.

hicli cvmset kek_state_change

Revokes or unrevokes the KEK.

hicli cvmset list

Lists all Cloud VM Sets. For example:

```
$ hicli cvmset list
Cloud VM Set Name     Admin Group           Description
-------------------------------------------------
Amazon AWS            Cloud Admin Group     VMs sets sited on Amazon Servers
vCloud Air            Cloud Admin Group     VMs sets deployed on vCloud Air \
                                              servers
Sales Staff           Cloud Admin Group     Sales staff worldwide
```

hicli cvmset list_tasks

Displays a list of tasks for the specified Cloud VM Set.

hicli cvmset new

Creates a new Cloud VM Set. For example:

```
$ hicli cvmset new "Amazon-EC2" "Cloud Admin Group" --description="VMs running in
Amazon Ubuntu-10.04,linux-12.10"
$ hicli cvmset list | grep Amazon-EC2
```

```
$ hicli cvmset new "kek_cvmset" "Cloud Admin Group" --cvm_set_type='KEK_ASSOC' --
kek_expire_days=10 --kek_expire_action='NO USE'--expiration_options=change --
retention_period=2
```

hicli cvm set rekey

Set the value for the automatic rekey interval for disks in days/months/years (defaults to 0, which means not set)

hicli cvmset select

Selects a Cloud VM Set. For example:

```
$ hicli cvmset select "Amazon EC2"
```

hicli cvmset set

Changes properties. For example:

```
$ hicli cvmset set "Amazon-EC2" --description="Amazon Southwest"
```

hicli cvmset set grace

Sets the value for the grace period in seconds (default is 1 day).

hicli cvmset set heartbeat

Sets the value for the heartbeat in seconds (default is 5 minutes, or 300 seconds).

hicli cvmset set name

Changes the name of the Cloud VM Set.

hicli cvmset set rekey

Sets the value for the automatic rekey interval of disks in days/months/years (defaults to 0, which means not set).

hicli cvmset set rekeybucket

Sets the value for the rekeybucket for cvmset, which controls the max number of auto rekeys that can be processed in parallel. Auto rekey is triggered when the rekey interval expires. This value defaults to 1.

hicli cvm status

Get the status of the VM. For example:

```
$ hicli cvm status ubuntu-12.10
Host Status on ubuntu12.10
--------------------------------------------------
Summary
--------------------------------------------------
KeyControl: kc-1:443
KeyControl list: kc-1:443
Status: Connected

Registered Devices
--------------------------------------------------
Disk Name         Clear                           Cipher      Status
--------------------------------------------------
sdb2              /dev/mapper/clear_sdb2          AES-256     Attached
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT
sdb1              /dev/mapper/clear_sdb1          AES-256     Attached
 '--> auto_attach=ENABLED, attach_handler=DEFAULT, detach_handler=DEFAULT

Available Devices
--------------------------------------------------
Disk Name           Device Node                   Size (in MB)
--------------------------------------------------
sde                 /dev/sde                      2048
sdd                 /dev/sdd                      2048
sdc                 /dev/sdc                      2048

Other Devices
--------------------------------------------------
Disk Name           Device Node                   Status
--------------------------------------------------
sda5                /dev/sda5                     Mounted (swap)
sda1                /dev/sda1                     Mounted (/)
```

hicli cvm unrevoke_disk

Give permissions back to access the device

hicli domain detail

Display information about a domain. For example:

```
$ hicli domain detail "KeyControl Domain"
Name                    KeyControl Domain
Status                  Healthy
Group                   KeyControl Admin Group
Description             Domain of Clustered KeyControl Servers
Allow reconnect         Yes
Passphrase required     Yes
Passphrase hidden       No
Check hardware id       Yes
Server Count            2
Server Names            kc1.hytrust.com,kc2.hytrust.com
```

hicli domain list

Display all domains. For example:

```
$hicli domain list
Domain                  Admin Group                       Servers   Status
-------------------------------------------------------------------------
KeyControl Domain       KeyControl Admin Group            1         Healthy
```

hicli domain select

Select a domain on which to perform server operations.

```
$ hicli domain select "KeyControl Domain"
```

hicli domain set

Sets Cryptographic Security Platform Vault domain attributes. For example:

```
$ hicli domain set "KeyControl Domain" --description="New description" --
allow_reconnect=yes --require_passphrase=yes --hide_passphrase=no
```

hicli domain set allow_reconnect

Displays information about a domain.

hicli domain set description

Give the domain a new description.

hicli domain set hide_passphrase

Don't display the passphrase when adding a new node.

hicli generate_csr

Generates a CSR (Certificate Signing Request) that you can send to a CA (Certificate Authority) to generate a custom certificate.

hicli group add_user

Add a Cryptographic Security Platform Vault-managed user account to the selected Cloud Admin Group. This user account must already be defined in Cryptographic Security Platform Vault.

hicli group detail

View the details for the selected Cloud Admin Group. For example:

```
$ hicli group detail "Cloud Admin Group"
Name                      | Cloud Admin Group
Description               | Default Group for Administering Cloud VMs
Type                      | CLOUD_ADMIN
Number of objects         | 0
AC Policy Max Changes     | 50
User Members              | secroot
AD Group Members          | Azure Admins
```

hicli group list

List the Cloud Admin Groups defined in Cryptographic Security Platform Vault. For example:

```
$ hicli group list
Group Name              | AD Group Members                                    | User
Members
-------------------------------------------------------------------------------------
----------
Cloud Admin Group       | Azure Admins                                        |
secroot
```

hicli group new

Create a new Cloud Admin Group. For example:

```
$ hicli group new cld_group1 --privilege=CLOUD_ADMIN --
adgroup_members='[{"distinguishedName": "CN=AWS
```

```
Admins,CN=Users,DC=manualtest,DC=qa,DC=dc,DC=hytrust,DC=com", "objectGUID":
"29739b20-2fb2-4b99-b7a8-935560b5c8f4", "cn": "AWS Admins"}]'
$ hicli group list
Group Name              | AD Group Members                                    | User
Members
-------------------------------------------------------------------------------------
----------
Cloud Admin Group       | Azure Admins                                        | secroot
cld_group1              | AWS Admins                                          |
```

hicli group rm

Remove the selected Cloud Admin Group.

A common issue is that, even after you remove all users from a group, group removal fails because the group is still associated with one or more Cloud VM Sets. To avoid this, remove all associations between the group and any Cloud VM Sets before removing the users. Then you can remove the group.

hicli group rm_user

Remove a Cryptographic Security Platform Vault-managed user account from the selected Cloud Admin Group.

hicli group set

Changes the group set. For example, the following sample command line removes any existing AD group members from the Cloud Admin Group.

```
$ hicli group set cld_group1 --adgroup_members='[{"distinguishedName": "CN=VMware
Admins,CN=Users,DC=manualtest,DC=qa,DC=dc,DC=hytrust,DC=com", "objectGUID":
"b2e5d325-1d2c-455a-b2ee-9408fd9e4841", "cn": "VMware Admins"}]'
$
$ hicli group list
Group Name              | AD Group Members                                    | User
Members
-------------------------------------------------------------------------------------
----------
Cloud Admin Group       | Azure Admins                                        | secroot
cld_group1              | VMware Admins                                       |
```

hicli group set description

Change the description for the selected Cloud Admin Group.

hicli group set name

Changes the name of the selected Cloud Admin Group.

hicli kc

Display the CSP Vault client options.

hicli kc select <kchost>

Selects the `<kchost>` Vault node as the node to talk to.

> Before invoking `hicli` commands, you must first select a Cryptographic Security Platform Vault node to talk to. If you have a cluster of two or more nodes, it does not matter which Cryptographic Security Platform Vault node is chosen. Because the nodes operate in an active-active cluster, any change on one node is immediately reflected across the cluster.

For example:

```
$ hicli kc select kc-1
$ hicli kc
Current CSP Node: kc-1
$ hicli kc select 192.168.140.152
$ hicli kc
Current CSP Node: 192.168.140.152
```

hicli keyid new

Creates a KeyID. For example:

```
$ hicli keyid new aws_key --description "Key for Amazon"
```

```
$ hicli keyid new custom_key --description "This uses my Base64 key" --
crypto_algo='AES-XTS-512' --key="Q0NOdkJBQWZROUd6emhvRFU1a ... Bb0hJN2RYaQ==" --
iv="MTIzNDU2Nzg5MDEyMzQ1Ng==" --expiry=1000 --onexpiry='SHRED'
```

hicli keyid revoke

Revokes access to a KeyID.

```
$ hicli keyid revoke aws_key
```

hicli keyid rm

Removes a KeyID. For example:

```
$ hicli keyid rm aws_key
```

hicli keyid set expiration

Sets the expiration date for a KeyID.

hicli keyid set onexpiry

Sets the expiration policy of a KeyID.

hicli keyid unrevoke

Unrevokes access to a KeyID. For example;

```
$ hicli keyid unrevoke aws_key
```

hicli keyset add_tde_connector

Add a TDE connector to a keyset.

hicli keyset container_purge

Purge a container in a key vault or managed HSM. See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>

- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset create_tde_connector_token

Create a token for a TDE connector. See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset detail

Display details for a keyset.

hicli keyset keyrings

List keyrings associated with a keyset. See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset list

List keysets. For example:

```
$ hicli keyset list
```

```
KeySet Name          | CSP type | KeySet guid                          | group
| CSP Account name   | Number of keys
-------------------------------------------------------------------------------
-------------------------------------------------------------
cloudkeyset          | AZURE    | db61c7b0-543b-49dd-8983-6d8711b25c41 | Cloud Admin
Group  | cloud_csp          | 0
```

hicli keyset list_tde_connectors

List TDE connectors associated with a keyset. See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset new

Create a keyset and optionally configure the following settings.

- CSP
- HSM

- caching, rekey
- XKS
- TDE

See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset rm

Remove a keyset. See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label

- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset select

Select a keyset. See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault

- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset set

Update keyset settings. See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset set_sync_schedule

Set an automatic synchronization schedule for a resource. See below for the options supported by the keyset commands.

- <name>

- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset tde_connector delete

Delete the named TDE connector. See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key

- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset tde_connector disable

Disable the named TDE connector. See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset tde_connector enable

Enable the named TDE connector. See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset verify_hsm

Verify HSM configuration for a keyset. See below for the options supported by the keyset commands.

- <name>
- <group>

- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key
- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli keyset verify_tde_connector_token

Verify a token for a TDE connector. See below for the options supported by the keyset commands.

- <name>
- <group>
- --name
- --guid
- --csp_guid
- --description
- --rekey_interval
- --enable_hsm
- --key_caching_enabled
- --enable_hsm_key_caching
- --part_label
- --part_password
- --import_all_keys
- --xks_access_id
- --xks_access_key

- --tde_database_type
- --allow_mdb_key_creation
- <connectorname>
- <cvmid>
- --expiration
- <tde_access_token>
- --auto_sync_schedule
- --region
- --keyvault
- --managedhsm
- --keyringID

<name>

Name to assign to a new keyset.

<group>

Group associated with the new keyset.

--name

Select an existing keyset by name.

--guid

Select an existing keyset by GUID.

--csp_guid

GUID of the CSP to associate with the keyset.

--description

Optional human-readable description.

--rekey_interval

Rekey interval. The set command describes this value in days.

--enable_hsm

Enable or disable HSM use: yes or no.

--key_caching_enabled

Enable or disable key caching: yes or no.

--enable_hsm_key_caching

Enable HSM key caching.

--part_label

HSM partition label.

--part_password

Password for the HSM partition.

--import_all_keys

Request import of all keys.

--xks_access_id

XKS access ID.

--xks_access_key

XKS secret access key.

--tde_database_type

Database type for the TDE configuration.

--allow_mdb_key_creation

Controls whether MDB key creation is allowed.

<connectorname>

Name of the TDE connector.

<cvmid>

CVM ID associated with the TDE connector.

--expiration

Expiration date for the TDE connector.

<tde_access_token>

Token to verify for the TDE connector.

--auto_sync_schedule

Automatic synchronization schedule to configure.

--region

Region whose synchronization schedule is being configured.

--keyvault

Key vault whose synchronization schedule is being configured or whose container is being purged.

--managedhsm

Managed HSM whose synchronization schedule is being configured or whose container is being purged.

--keyringID

Keyring identifier used when setting a synchronization schedule.

hicli mapping detail

Display details about the specified Node Mapping.

hicli mapping list

Displays the Cluster Node Mappings configured in the domain.

hicli mapping new

Create a new Node Mapping.

hicli mapping rm

Removes the specified Node Mapping.

hicli mapping select

Sets the Node Mapping to which future commands will be applied.

hicli mapping set description

Set the Node Mapping description.

hicli mapping set group

Sets the Administration Group with which this mapping will be associated.

hicli mapping set newname

Change the Node Mapping name.

hicli mapping set servers

Sets the IP addresses of the Cryptographic Security Platform Vault nodes in this Node Mapping.

hicli server auth

Display information about a domain.

hicli server auth

Display information about a domain.

hicli server default_csr_values

Displays the default CSR values for the named server.

hicli server detail

Displays detailed information about a server.

hicli server install_cert

Installs a custom certificate on the server.

hicli server install_cert_status

Displays information about the status of the certificate installation process.

hicli server show_cert

Shows the current server certificate.

hicli server use_default_certs

Tells Cryptographic Security Platform Vault to ignore any custom certificates and to return to using the default, self-signed Cryptographic Security Platform Vault certificate.

hicli server webserver_restart

Restarts the web server on the Cryptographic Security Platform Vault node. This is required after you install a new custom certificate.

hicli user defaults

Set the default parameters for Cryptographic Security Platform Vault user accounts. You can specify:

- authentication
- password_expiry
- max_failed_logins
- min_passwd_length

For example, the following command line example sets the default authentication to local, sets password expiration to 60 days after the account is created or the password is changed, sets the maximum failed login attempts to 4, and sets the minimum password length to 12 characters.

```
$ hicli user defaults --authentication=local --password_expiry=60 --
max_failed_logins=4 --min_passwd_length=12
```

authentication

The default authentication method: local or ldap. This option affects only newly-created user accounts. It does not change the authentication method for existing accounts.

password_expiry

The number of days before the user's password expires. This option affects only newly-created accounts. It does not change the password expiration date for existing accounts.

max_failed_logins

The number of failed login attempts that can be made before Cryptographic Security Platform Vault disables the user account. This setting affects all user accounts, including existing accounts.

min_passwd_length

The minimum number of characters required in a Cryptographic Security Platform Vault account password. This setting affects all user accounts, including existing accounts.

hicli user detail <username>

Displays the details for the `<username>` user.

- SEC_ADMIN can view the details for any user.
- Others can view details only for their own user account.

hicli user list

Displays the list of Cryptographic Security Platform Vault users defined in the system.

- SEC_ADMIN sees all users
- Others see users in the user groups to which they belong.

hicli user login <name>

Logins to a selected Vault.

```
hicli user login <name> [--password=<pwd>] [--new_password=<npwd>] [--
vaultid=<vaultid>]
```

See below for the supported options.

- <name>
- --password=<pwd>
- --new_password=<npwd>
- --vaultid=<vaultid>

<name>

The name of the user logging in.

--password=<pwd>

The user's current password.

--new_password=<npwd>

The new password to set for the user.

--vaultid=<vaultid>

The ID of the vault associated with the login.

hicli user new <username>

Creates a new user account with the `<username>` username. See below for the supported options.

- email=<email>
- password=<passwd>
- full_name=<full_name>
- authentication=<authentication>
- account_state=<active|disabled>
- roles=<privlist>
- groups=<grouplist>
- password_expiration=<date>
- account_expiration=<date>
- email=<email>
- password=<passwd>
- full_name=<full_name>
- authentication=<authentication>
- account_state=<active|disabled>
- roles=<privlist>
- groups=<grouplist>
- password_expiration=<date>

- account_expiration=<date>

For example, the code selects one of the Cryptographic Security Platform Vault nodes, logs in as `secroot`, lists the users and groups, and creates two new users.

```
$ hicli kc select kc-1
$ hicli kc
Current KeyControl: kc-1
$ hicli user login secroot
Password for secroot: ********
$ hicli user list
Username    Full Name               Privileges
-------------------------------------------------
secroot     Security Administrator  SEC_ADMIN,DOMAIN_ADMIN,CLOUD_ADMIN
$ hicli group list
Group Name              Description                                 Members
-------------------------------------------------
Cloud Admin Group       Default Group for Administering Cloud VMs   secroot
West-Cloud-Group        Includes all West Coast Cloud VM Sets       secroot
$ hicli user new spate --email=spate@me.com --password=Mypasswd236! \
     --roles="SEC_ADMIN, DOMAIN_ADMIN, CLOUD_ADMIN" --full_name="Steve Pate" \
     --groups="Cloud Admin Group, SF-Datacenter"
$ hicli user new mrogers --email=martha@me.com --password=Passwd123! \
     --roles="CLOUD_ADMIN" --full_name="Martha Rogers" --groups="SF-Datacenter"
$ hicli user list
Username    Full Name               Privileges
-------------------------------------------------
mrogers     Martha Rogers           CLOUD_ADMIN
secroot     Security Administrator  SEC_ADMIN,DOMAIN_ADMIN,CLOUD_ADMIN
spate       Steve Pate              SEC_ADMIN,DOMAIN_ADMIN,CLOUD_ADMIN
$ hicli group list
Group Name              Description                                 Members
-------------------------------------------------
Cloud Admin Group       Default Group for Administering Cloud VMs   secroot,spate
West-Cloud-Group        Includes all West Coast Cloud VM Sets
secroot,spate,mrogers
```

email=<email>

The user email

password=<passwd>

The user password

full_name=<full_name>

The user password

authentication=<authentication>

The default authentication method: local or ldap. This option affects only newly-created user accounts. It does not change the authentication method for existing accounts.

account_state=<active|disabled>

The account state

roles=<privlist>

A comma-separated list of roles. Allowed roles are:

- CLOUD_ADMIN
- DOMAIN_ADMIN
- SEC_ADMIN

groups=<grouplist>

A comma-separated list of the groups to which this user should belong.

> ⚠ Each group name must be surrounded by double quotes.

password_expiration=<date>

The date on which the selected user's password expires.

> ℹ The next time that user logs in, they will be prompted to set a new password.

account_expiration=<date>

The date on which the user account will be automatically disabled.

email=<email>

The user email

password=<passwd>

The user password

full_name=<full_name>

The user password

authentication=<authentication>

The default authentication method: local or ldap.

This option affects only newly-created user accounts. It does not change the authentication method for existing accounts.

account_state=<active|disabled>

The account state

roles=<privlist>

A comma-separated list of roles. Allowed roles are:

- CLOUD_ADMIN
- DOMAIN_ADMIN
- SEC_ADMIN

groups=<grouplist>

A comma-separated list of the groups to which this user should belong.

Each group name must be surrounded by double quotes.

password_expiration=<date>

The date on which the selected user's password expires.

The next time that user logs in, they will be prompted to set a new password.

account_expiration=<date>

The date on which the user account will be automatically disabled.

hicli user rm <username>

Removes the `<username>` user.

Only Security Administrators can remove users.

The example below displays the current list of users and removes the user `spate`.

```
$ hicli user list
Username    Full Name               Privileges
-------------------------------------------------
secroot     Security Administrator  SEC_ADMIN
spate       Steve Pate              CLOUD_ADMIN
$ hicli user rm spate
$ hicli user list
```

```
Username    Full Name               Privileges
-------------------------------------------------
secroot     Security Administrator  SEC_ADMIN
```

All objects (Cloud VM Sets and VMs) are owned by administrative groups and not by the users themselves. So, if you remove a user, the object stays intact.

hicli user set <username>

Sets information for the `<username>` user.

- SEC_ADMIN can set all information for all accounts.
- Other users can only set the email address, full name, and password for their own account.

For example, consider the following user:

```
$ hicli user detail fred
Login name                | fred
Status                    | Active
Full name                 | Fred Flintstone
Email                     | fred@me.com
Last login                | 2018-04-13 10:21:03 PDT
Password Expiration       | Never
Account Expiration        | 06/09/2020
Failed logins             | 0
Privileges                | CLOUD_ADMIN
Groups                    | Cloud Admin Group
```

The following call adds Security Admin privileges and changes the email:

```
$ hicli user set fred --roles=SEC_ADMIN,CLOUD_ADMIN --email=fred@hytrust.com
$ hicli user detail spate
Login name                | fred
Status                    | Active
Full name                 | Fred Flintstone
Email                     | fred@hytrust.com
Last login                | 2018-04-13 10:21:03 PDT
Password Expiration       | Never
Account Expiration        | 06/09/2020
Failed logins             | 0
Privileges                | SEC_ADMIN,CLOUD_ADMIN
Groups                    | Cloud Admin Group
```

kmipsrv_obj action uuid

Performs one or more of the following actions on the KMIP server object whose UUID is specified in the command.

- --operation=<activate|archive|destroy|recover|revoke>

- --revcode=<revoke reason code>
- --revmsg=<revoke message>
- --desc=<description>

--operation=<activate|archive|destroy|recover|revoke>

The action to perform on the KMIP object.

- `activate` —By default, objects are created in PreActive state. Specify `activate` to enable more transitions for the object. **Note:** Many KMIP clients change objects to Active state as part of the creation process.
- `archive` —Objects will no longer return keys but they remain in the system. You can use the `recover` operation to return an archived object to active state and retrieve its keys.
- `destroy` —This operation permanently removes the object. Destroyed objects cannot be retrieved.
- `recover` —Restores an Archived object to the active state so that its keys can be retrieved.
- `revoke` —Revocation is permanent. Revoked objects cannot be moved back to Active, but the client can still retrieve any key material. You can also specify a revocation reason (any string) and a numeric Reason Code, which is one of the following KMIP standard codes. If you omit the reason code or use a non-standard code, it will be considered the same as "1—Unspecified."
    a. Unspecified
    b. Key Compromise
    c. CA Compromise
    d. Affiliation Changed
    e. Superseded
    f. Cessation of Operation
    g. Privilege Withdrawn

The following command activates a KMIP object:

```
$ hicli kmipsrv_obj action cd9e4370-e2cb-11e8-bdab-00505685b461 --operation=activate
success
```

The following commands archive and then restore a KMIP object, fetching details after each action to confirm the state changed correctly.

> After you restore an object, the ArchiveDate is retained, but the Archived flag is no longer set.

```
$ hicli kmipsrv_obj action cd9e4370-e2cb-11e8-bdab-00505685b461 --operation=archive
success
$ hicli kmipsrv_obj fetch uuid=cd9e4370-e2cb-11e8-bdab-00505685b461
Archived                 :   1
CryptographicUsageMask   :   Decrypt Sign
InitialDate              :   2018-11-07T20:29:19+00:00
State                    :   Active
ActivationDate           :   2018-11-09T20:22:18+00:00
ArchiveDate              :   2018-11-09T20:27:05+00:00
CryptographicAlgorithm   :   RSA
LastChangeDate           :   2018-11-09T20:27:05+00:00
CryptographicLength      :   4096
ObjectType               :   PrivateKey
```

```
$ hicli kmipsrv_obj action cd9e4370-e2cb-11e8-bdab-00505685b461 --operation=restore
success
$ hicli kmipsrv_obj fetch uuid=cd9e4370-e2cb-11e8-bdab-00505685b461
CryptographicUsageMask    :   Decrypt Sign
InitialDate               :   2018-11-07T20:29:19+00:00
State                     :   Active
ActivationDate            :   2018-11-09T20:22:18+00:00
ArchiveDate               :   2018-11-09T20:27:05+00:00
CryptographicAlgorithm    :   RSA
LastChangeDate            :   2018-11-09T20:27:05+00:00
CryptographicLength       :   4096
ObjectType                :   PrivateKey
```

The following command revokes a KMIP object for the revocation reason "This key has been replaced with a new key".

```
$ hicli kmipsrv_obj action cd9e4370-e2cb-11e8-bdab-00505685b461 --operation=revoke --
revcode=5
--revmsg='This key has been replaced with a new key'
success
$ hicli kmipsrv_obj fetch uuid=cd9e4370-e2cb-11e8-bdab-00505685b461
ActivationDate            :   2018-11-09T20:22:18+00:00
RevocationReasonCode      :   Superceded
CryptographicUsageMask    :   Decrypt Sign
InitialDate               :   2018-11-07T20:29:19+00:00
DeactivationDate          :   2018-11-09T20:31:24+00:00
RevocationMessage         :   This key has been replaced with a new key
State                     :   Deactivated
CryptographicAlgorithm    :   RSA
LastChangeDate            :   2018-11-09T20:31:24+00:00
CryptographicLength       :   4096
ObjectType                :   PrivateKey
```

--revcode=<revoke reason code>

If you are revoking the object, this is the standard KMIP reason code.

--revmsg=<revoke message>

If you are revoking the object, this is a user-defined string specifying the reason why you are revoking the object.

--desc=<description>

Sets the user-defined description for the object.

kmipsrv_obj fetch

Retrieves a list of objects stored on the KMIP server. You can specify the following properties:

- --uuid=<object uuid>
- --noattr
- --count=<list size>
- --offset=<offset>
- --total_count

--uuid=<object uuid>

The UUID of the KMIP server object. If this parameter is not specified, the command returns a list of the KMIP objects on the server. For example, the following command gets a specific KMIP object.

```
$ hicli kmipsrv_obj fetch --uuid=997dd60b-e2c9-11e8-9997-000c299ae5eb --noattr
CryptographicUsageMask    :   Encrypt Verify
InitialDate               :   2018-11-07T20:13:32+00:00
State                     :   PreActive
CryptographicAlgorithm    :   RSA
LastChangeDate            :   2018-11-07T20:13:32+00:00
CryptographicLength       :   4096
ObjectType                :   PublicKey
```

`hicli` ignores the `--noattr` option when using the `--uuid` one.

--noattr

Only include the object UUIDs in the returned list. For example, the following command gets only the UUIDs for the first four KMIP objects:

```
$ hicli kmipsrv_obj fetch --count=4 --offset=0 --noattr
bec40e89-e2c9-11e8-9997-000c299ae5eb
bec39ac3-e2c9-11e8-9997-000c299ae5eb
997dd60b-e2c9-11e8-9997-000c299ae5eb
996b5f4c-e2c9-11e8-9997-000c299ae5eb
```

`hicli` ignores the `--noattr` option when using the `--uuid` one.

--count=<list size>

The number of KMIP objects to retrieve. For example, the following command retrieves the details for the first 4 objects:

```
$ hicli kmipsrv_obj fetch --count=4 --offset=0
Object UUID                           Type          State       Initial Date
Last Change                  Identification   Description
```

```
-----------                          ----          -----       ------------
-----------                  --------------   -----------
bec40e89-e2c9-11e8-9997-000c299ae5eb  PublicKey     PreActive
2018-11-07T20:14:35+00:00     2018-11-07T20:14:35+00:00     []               None
bec39ac3-e2c9-11e8-9997-000c299ae5eb  PrivateKey    PreActive
2018-11-07T20:14:35+00:00     2018-11-07T20:14:35+00:00     []               None
997dd60b-e2c9-11e8-9997-000c299ae5eb  PublicKey     PreActive
2018-11-07T20:13:32+00:00     2018-11-07T20:13:32+00:00     []               None
996b5f4c-e2c9-11e8-9997-000c299ae5eb  PrivateKey    PreActive
2018-11-07T20:13:32+00:00     2018-11-07T20:13:32+00:00     []               None
```

--offset=<offset>

The index of the first object to retrieve in the list. If you specify 0 (zero) for this parameter, the command starts at the top of the list.

--total_count

Include the total number of objects stored on the KMIP server in the response. For example, the following command gets the total number of KMIP objects stored on the server:

```
$ hicli kmipsrv_obj fetch --total_count
Total number of KMIP objects: 10
```

kmipsrv_user

Creates, edits, or deletes a KMIP Client Certificate bundle. See below for the supported options.

- --username=<user name>
- --passwd=<password>
- --expire=<integer>
- --p12=<yes>
- --operation=<create|update|remove|removeall|list>
- --csr=<csrfile>
- --download

--username=<user name>

The user name for the KMIP client certificate bundle.

--passwd=<password>

An optional password for the client certificate bundle. Note that not all KMIP clients can accept a password-protected client certificate.

--expire=<integer>

The number of days before the KMIP certificate expires.

--p12=<yes>

Enables using PKCS #12

--operation=<create|update|remove|removeall|list>

The operation to perform on the client certificates.

--csr=<csrfile>

Optional. The name of the file containing the 3rd party certificate signing request (CSR) you want to use.

--download

If specified, the selected client certificate bundle is returned by this command.

kmipsrv set

Enables, disables, or changes the KMIP server settings. See below for the supported options.

- --state=<ENABLED|DISABLED>
- --host=<ip address>
- --port=<port number>
- --reconnect=<0|1>
- --protocol=<1.0|1.1|1.2|1.3|1.4|custom_hex>
- --nbio=<0|1>
- --timeout=<timeout>
- --verify=<yes|no>
- --reset
- --loglevel=<ALL|CREATE-GET|OFF>
- --cert_type=<DEFAULT|CUSTOM>
- --SSL_cert=<path>
- --CA_cert=<path>
- --private_key=<path>
- --custom_cacert_use_to_verify_kmip_client_cert=<0|1>
- --password=<password>

--state=<ENABLED|DISABLED>

Enables or disables the KMIP server.

--host=<ip address>

The IP address of the KMIP server.

--port=<port number>

The KMIP server port number.

--reconnect=<0|1>

Whether automatic reconnection is enabled (1) or disabled (0).

--protocol=<1.0|1.1|1.2|1.3|1.4|custom_hex>

The KMIP protocol to use for the server.

--nbio=<0|1>

Whether non-blocking I/O is required (1) or not required (0).

--timeout=<timeout>

The length of time, in seconds, after which a client request will time out. Specify 0 (zero) to indicate that the request should never time out.

--verify=<yes|no>

If set to yes, the KMIP client identity is verified before the server handles its request. We recommend setting this option to yes.

--reset

Resets the KMIP server.

--loglevel=<ALL|CREATE-GET|OFF>

The log level to use for the KMIP server.

--cert_type=<DEFAULT|CUSTOM>

The certificate type being used by the KMIP server.

--SSL_cert=<path>

The path of the SSL certificate (in base64 PEM format) to be used. Required if `--cert_type` is `CUSTOM`.

--CA_cert=<path>

The path of the CA certificate (in base64 PEM format) to be used. Required if `--cert_type` is `CUSTOM`.

--private_key=<path>

The path of the private key (in base64 PEM format) to be installed. Required if `--cert_type` is `CUSTOM` and you did not use a CSR generated by Cryptographic Security Platform Vault.

--custom_cacert_use_to_verify_kmip_client_cert=<0|1>

If enabled, the user must upload a custom certificate while creating the KMIP client certificate. Required if `--cert_type` is `CUSTOM`.

--password=<password>

The password of the private key. Required only if the private key is encrypted.

list_bucket

View the list of available buckets.

s3 add_file

Add a file to the S3 bucket.

s3 get_file

Retrieve a file from the S3 bucket.

s3 rm_file

Remove a file from the S3 bucket.

set aws_access_key_id

Set the AWS access key ID.

set aws_secret_access_key

Set the AWS shared secret.

16 Customer license

This section defines the licensing model and permitted uses of the Entrust Cryptographic Security Platform (CSP) software solution.

- Authorized Use
- License
    - Base Licensing Package: Entrust CSP on Premise Core
    - Add-on Licenses
- Deployment
- External Dependencies
- Trade Compliance
- Standard Compliance Packs Limitations
- Support and Record-Keeping

Authorized Use

In this Licensing Model section, the term "Customer" means an Entrust customer who has purchased one or more CSP software licenses, or an individual authorized by that customer to access components or capabilities of the CSP software ("Users").

CSP software is licensed for internal Customer use (i.e., use for the Customer's own business purposes). Customer may also grant access to Users who are employees of external contractors, but only to the extent that such Users are using CSP software on Customer's behalf in the operation or management of the Customer's business and Customer's own cryptographic assets. In addition, the Customer is permitted to provide digital certificates to Users outside the Customer's organization solely to enable communications and resource access between the Customer and that User.

Except as may be otherwise specified in an express license agreement signed by Entrust, neither Customer nor any User may use CSP software to set up or provide its own cryptographic management, analysis, or reporting service for other companies (e.g., provision of CSP software functionality as a "Managed Service Provider" or "Systems Integrator").

License

The Customer will receive one or more license keys ("licenses") to enable CSP software functionalities and volumes of Keys and Secrets, certificates, and Third-party Objects based on what the Customer has purchased.

The CSP software solution is offered with a base licensing package (Entrust CSP On -Premise Core) that can be extended with add-on licenses for specific capabilities and volumes.

Base Licensing Package: Entrust CSP on Premise Core

Inclusions	**Excluded/Separate License Required**
Compliance Manager: 2-node cluster	Additional Compliance Manager nodes require separate add-on licenses (*Entrust CSP ADD-ON Compliance Manager - 2 Nodes Virtual Appliance Cluster*)

Inclusions	Excluded/Separate License Required
Standard Compliance Pack: assessment, documentation, and risk scoring for Discovery scan results and one additional data source (e.g., Vault Cluster, Certificate Manager, KeySafe 5).	Additional data sources require a separate add-on license (*Entrust CSP ADD-ON Compliance Manager - Standard Assessment, Documentation, and Risk Scoring (per Vault Cluster)*). Discovery scan results do not count as a data source for licensing purposes.
Discovery (scanning)	
KeySafe 5 (HSM manager)	
File Encryption – 10 GB	The 10 GB protected data limit is calculated based on the original data size and excludes any overhead (added data size) resulting from the encryption. Licensing beyond 10 GB requires a separate license (per Terabyte per year) (*Entrust CSP ADD-ON File Encryption Subscription 1TB*). NOTE: Disc Encryption for Virtual Machines (Linux/Windows) requires a separate Vault Cluster (*Entrust CSP ADD-ON Compliance Manager - 2 Nodes Virtual Appliance Cluster for Vaults)* and Virtual Machines volume licenses (*Entrust CSP ADD-ON Virtual Machine Encryption Keys Subscription*)

Add-on Licenses

Capabilities	Add-on licenses	Notes/Consumption
Compliance Management	Third-party Objects (*Entrust CSP ADD-ON Integration with Third Party KMS Keys Subscription*)	Volume-based license, consumed when a Third Party Object is imported into Compliance Manager inventory, as follows: Active Object = 1 full license Inactive Object but still managed = 1/10 of a license (dormant object) Deleted Object, or unmanaged object = no license required
	Compliance Manager nodes (*Entrust CSP ADD-ON Compliance Manager - 2 Nodes Virtual Appliance Cluster*)	Additional 2 nodes for higher availability or multiple clusters – Compliance Manager supports up to a maximum of 8 nodes per cluster.

Capabilities	Add-on licenses	Notes/Consumption
	Standard Compliance Pack: assessment, documentation, and risk scoring (*Entrust CSP ADD-ON Compliance Manager - Standard Assessment, Documentation, and Risk Scoring (per Vault Cluster)*)	Every Vault Cluster, Certificate Manager, KeySafe 5, needs its own Standard compliance Pack.
HSM Management	KeySafe 5 Monitoring (*nShield - KeySafe 5 Monitoring Base*, *nShield - KeySafe 5 Monitoring Standard*, *nShield - KeySafe 5 Monitoring Mid*, or *nShield - KeySafe 5 Monitoring Enterprise*)	Tier-based license determined by the number of HSMs being monitored and subject to an annual (12-month) subscription.
Certificate Management	Certification Authority (*Entrust CSP ADD-ON Certification Authority*)	Certificates require separate licensing.
	Advanced PKI (*Entrust CSP ADD-ON Advanced PKI*)	Timestamping Authority software (included in Advanced PKI) may be deployed as a three-node cluster, limited to up to 600 timestamps per second (TPS).
	Advanced CLM (Entrust CSP ADD-ON Advanced CLM)	
	Timestamping Expansion (*Entrust CSP ADD-ON Timestamping Expansion*)	Expansion of Timestamping Authority (included in Advanced PKI) by two additional nodes or increase the limit on existing nodes by up to an additional 600 TPS. The maximum number of nodes per cluster is 5.
	Certificates (*Entrust CSP ADD-ON Production Certificates*)	Volume-based license. A certificate license is required for each active certificate.
Keys and Secrets Management	Vault Cluster: 2-node cluster (*Entrust CSP ADD-ON Compliance Manager - 2 Nodes Virtual Appliance Cluster for Vaults*)	Each license covers a single 2-node cluster. A Vault Cluster supports up to a maximum of 8 nodes.

Capabilities	Add-on licenses	Notes/Consumption
	KMIP Keys *(Entrust CSP ADD-ON KMIP Keys Subscription)*	Each of these is a volume-based license, consumed as follows: Active Key/Secret = 1 full license Inactive Key/Secret but still managed = 1/10 of a license (dormant Key/Secret) Deleted Key/Secret, or unmanaged Key/Secret = no license required
	Secrets *(Entrust CSP ADD-ON Managed Secrets Keys Subscription)*	
	Cloud Keys *(Entrust CSP ADD-ON Bring Your Own Key, Hold Your Own Key, and Native Key Mgmt Keys Subscription)*	
	TDE Databases *(Entrust CSP ADD-ON TDE Database Keys Subscription)*	
	Application Keys *(Entrust CSP ADD-ON Application Security inc. Tokenization and Cryptographic Rest API Keys Subscription)*	
	Virtual Machines Keys *(Entrust CSP ADD-ON Virtual Machine Encryption Keys Subscription)*	

These licenses are subject to the following terms:

- For items purchased on a volume basis, Customer may not exceed the total volume indicated in the applicable purchased license. If Customer's consumption exceeds the licensed volume entitlements that it has purchased, Entrust may invoice Customer an overage fee in arrears for its actual consumption.
- The Customer may not alter the license key or attempt to circumvent the licensing mechanism.
- The Customer may only use a valid license key provided by Entrust with the corresponding CSP software component.

Deployment

CSP software may be deployed on the Customer's own infrastructure and/or commercial cloud environments. Entrust strongly recommends keeping all deployments up to date with the latest product release.

External Dependencies

CSP software licenses do not include any Hardware Security Modules (HSM). These components are external dependencies that must be provided, installed, and configured separately by the Customer before the CSP software can operate.

Trade Compliance

CSP software contains cryptographic software components. The Customer's country of operation may have import and export requirements that apply.

Standard Compliance Packs Limitations

The Standard Compliance Packs included with CSP Compliance Manager (each a “Compliance Pack” and collectively the “Compliance Packs) are provided to assist organizations in reviewing their cryptographic keys, secrets, and certificates against industry standards and best practices. While these Compliance Packs will assist the Customer, Entrust does not represent, warrant, or guarantee that their use will ensure, guarantee, or confirm compliance with any particular industry standards and best practices or any specific policy, regulation, or other laws. The Customer is solely responsible for validating all requirements and managing compliance with all relevant industry standards and best practices or any specific policy, standard, or regulation, or other laws (and to determine which of these are applicable to its activities). Entrust disclaims any and all liability arising from Customer's reliance on the Compliance Packs.

Support and Record-Keeping

To ensure Entrust Customer Support is equipped to assist with reported issues, the Customer is expected to maintain reasonable records of CSP software deployment details, including the production instances in use and the environment(s) (on-premises or cloud) where those instances reside. In addition, upon Entrust's request, Customer will provide a report detailing its consumption of Keys and Secrets, certificates, and Third-party Objects.

17 CSP Vault with VSAN and VMware vSphere VM Encryption

The following topics explain how to set up a CSP Vault KMIP server as a vSphere KMS (Key Management Server), which allows CSP Vault to manage the encryption keys for virtual machines that have been encrypted with vCenter Server for vSphere Virtual Machine Encryption or VMware VSAN Encryption.

- CSP Vault with VSAN and VMware vSphere VM Encryption Overview
- Configuring a KMIP Server for vSphere KMS
- Adding a KMS Cluster in vSphere
- Establishing a Trusted Connection with a vSphere-Generated CSR
- Establishing a Trusted Connection with a CSP Vault-Generated CSR
- Troubleshooting

CSP Vault with VSAN and VMware vSphere VM Encryption Overview

Entrust Cryptographic Security Platform Vault supports a fully functional KMIP (Key Management Interoperability Protocol) server that can serve as a vSphere KMS (Key Management Server).

Once a trusted connection between Cryptographic Security Platform Vault and vSphere has been established, Cryptographic Security Platform Vault can manage the encryption keys for virtual machines in the cluster that have been encrypted with vCenter Server for vSphere Virtual Machine Encryption or VMware VSAN Encryption. The procedure is identical no matter which VMware encryption method you use.

> Note: If you are using KMIP with Key Encryption Key (KEK) enabled, please ensure that the KEK cache timeout is enabled. Set the value to anything other than 0. For details, see KEKs with KMIP.

To set up Cryptographic Security Platform Vault as a KMS for vSphere:

Step	Task	Notes
1	If you currently have a different KMS configured in vCenter that you want to replace with Cryptographic Security Platform Vault, make sure you decrypt all workloads associated with that KMS and that you remove the KMS from vCenter. You can then set up Cryptographic Security Platform Vault as your KMS.	For details on decrypting workloads or removing a KMS from vCenter, see your vCenter documentation.
2	Have access to a Cryptographic Security Platform Vault cluster that has been properly configured and is operational. Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.	For details, see Installation Overview.
3	Configure a KMIP server in the Cryptographic Security Platform Vault cluster.	See Configuring a KMIP Server for vSphere KMS.

Step	Task	Notes
4	Add a KMS Cluster in vSphere using the VMware vCenter Web Client. Important: Do *not* enter a user name or password for the KMS cluster.	See Adding a KMS Cluster in vSphere.
5	Establish a trusted connection to the Cryptographic Security Platform Vault KMIP server by creating a client certificate bundle on the KMIP server and uploading it to vSphere. You can create the KMIP client certificate bundle using a Certificate Signing Request (CSR) generated by vSphere or generated by Cryptographic Security Platform Vault. Important: Do *not* enter a password for the certificates. Due to a vSphere limitation, you cannot upload encrypted certificates.	See Establishing a Trusted Connection with a CSP Vault-Generated CSR.

Configuring a KMIP Server for vSphere KMS

After your Cryptographic Security Platform Vault cluster is configured, you need to enable the included KMIP server. This server becomes the vSphere KMS (Key Management Server) when you establish a trusted connection between vSphere and Cryptographic Security Platform Vault.

If you have already enabled the KMIP server in the cluster, make sure the configuration settings match the ones given below.

For details about the Entrust KMIP server implementation and how to manage KMIP server objects, or how to configure KMIP with a Hardware Security Module (HSM), see KMIP Server Configuration or Hardware Security Modules with CSP Vault.

Important: Make sure that all Cryptographic Security Platform Vault nodes reside on devices that are *not* encrypted. Cryptographic Security Platform Vault has its own internal encryption, and it must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.

1. Log into the Cryptographic Security Platform Vault Management webGUI.
2. Select the Settings icon at the top right of the vault page.
3. On the KMIP Vault Settings page, complete the following:

Option	Description
State	If set to Enabled, clients can connect to this KMIP server.
Port	The server port number. The default port is 5696.
Verify	If set to Yes, the KMIP client identity is verified before the server handles its request. We recommend that you do not turn this option off.

Option	Description
Log Level	The lowest level of log messages that will be saved in the audit log. The options are: • **All**—Logs all requests to the KMIP server and responses from the KMIP server. • **Create-Modify**—Logs object creation, object modify requests, and object delete requests and responses. This is the default. • **Create-Get**—Logs object creation messages, object fetch requests, and object fetch responses. • **Create**—Logs object creation request and response messages. • **Get**—Logs object fetch and object locate requests and responses. • **Off**—No log messages are stored in the audit log.
TLS	Choose which version of TLS you want to support. If set to TLS 1.3, all clients must connect to this KMIP server using TLS 1.3. By default, both TLS 1.2 and TLS 1.3 are supported. Note: The TLS setting applies to the KMIP server only and affects the entire cluster.
Timeout	The length of time, in minutes, after which a client request will time out. If No is selected, client requests never time out. This is the default. To change this option, select Yes and select the number of minutes before the requests times out. This can be from 1 to 60 minutes.

Option	Description
KMIP Locate Operation: Maximum Items Default	Choose the maximum number of items to be returned from the KMIP server `Locate` operation. Note: The KMIP client allows you to set an offset items value (the record number the return starts with) and a maximum items value (how many items are returned) when you run the KMIP locate operation. The maximum number of items depends on both the choice that you set in the webGUI and the value that you set in the KMIP Client. For example: • If you choose the default value in the webGUI, and you DO set a max value in the KMIP Client, it returns up to 1000 UUIDs. • If you choose the default value in the webGUI, and you do NOT set a max value in the KMIP Client, it returns up to 100 UUIDs. • If you choose the value set to the maximum items value from the KMIP client in the webGUI, and you DO set a max value, it returns the maximum value of UUIDs that is set in the KMIP Client. • If you choose the value set to the maximum items value from the KMIP client in the webGUI, and you do NOT set max value, it returns all the UUIDs found in the locate operation. For more information on the KMIP `Locate` command, see https://docs.oasis-open.org/kmip/kmip-spec/.
SSL/TLS Ciphers	Enter the SSL ciphers in a comma-separated list that you want the KMIP server to use. Note: The following ciphers are not supported: DHE-DSS-AES128-256 and DHE-DSS-AES128-SHA256.

Option	Description
Certificate Types	This can be one of the following: If set to Default, the KMIP server uses a default certificate. If set to Custom, you must have a custom SSL certificate generated from Cryptographic Security Platform Vault or from your own CSR, and then provide the following: • SSL Certificate—Upload the SSL certificate file in Base64-encoded pem format. It should be able to function as a server certificate. • CA Certificate—Upload the certificate for the CA that signed the custom SSL certificate in Base64-encoded pem format. If you want to use the CA certificate to verify the KMIP client certificate select **Yes**. The default is **No**. **Important:** If you select Yes, you will need to upload a KMIP client certificate for every Cryptographic Security Platform Vault for KMIP. • Private Key—Optionally upload the private key file in Base64-encoded pem format. This is required if you used your own CSR and not the CSR generated on the KMIP page. • Password—Optionally enter the password for the custom certificate.

4. Click **Apply** and confirm your changes when prompted.

What to Do Next

Create the KMS cluster in vSphere as described in Adding a KMS Cluster in vSphere.

Adding a KMS Cluster in vSphere

1. Launch the vSphere Client and log into the vCenter server that you want to add to Entrust Cryptographic Security Platform Vault.
2. Select the vCenter Server in the Global Inventory Lists.
3. Click **Configure**.
4. Select **Key Management Servers**.
5. Click **Add KMS** and set the following configuration options:

Option	Description
KMS cluster	Select <Create new cluster>.
Cluster name and Server alias	Enter a name and alias for the cluster. These names are local to vSphere and are not used by Cryptographic Security Platform Vault.

Option	Description
Server address	The IP address for the Entrust KMIP server. This IP address must match the Cryptographic Security Platform Vault KMIP server Host Name shown in the Cryptographic Security Platform Vault webGUI. Important: Make sure that the KMIP server resides on a device that is *not* encrypted. The KMIP server must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.
Server port	The port number for the Entrust KMIP server. The KMIP standard port is 5696.
Proxy address and Proxy port	Enter this information if required by your network administrator.
User name and Password.	Optional: The user name or password for the KMS cluster.

6. Click **OK**.
7. When prompted, click **Yes** to make this the default KMS cluster.
8. In the Trust Certificate dialog box, click **Trust**.
   Note: This adds the KMS cluster to vCenter but the connection status will be "Cannot establish trust connection".

What to Do Next

Establish a trusted connection between the KMS cluster and the Entrust KMIP server. How you do this depends on whether you want vSphere or CSP Vault to generate the Certificate Signing Request (CSR) used to establish the trusted connection. For more information, see Establishing a Trusted Connection with a CSP Vault-Generated CSR.

Establishing a Trusted Connection with a vSphere-Generated CSR

The following procedure describes how to generate a Certificate Signing Request (CSR) in vCenter and then use that CSR to create a certificate bundle on the Entrust KMIP server. The KMIP certificate can then be uploaded to vSphere to establish a trusted connection between vCenter and the Entrust KMIP server.

You can also establish a trusted connection using a Cryptographic Security Platform Vault-generated CSR. For details, see Establishing a Trusted Connection with a CSP Vault-Generated CSR.

1. Use the following VMware documentation to configure the KMS cluster:
   Add a Standard Key Provider Using the vSphere Client
2. Use the following VMware documentation to establish Trust:
   Establish a Standard Key Provider Trusted Connection by Exchanging Certificates
   Note: Ensure that you select the option "New Certificate Signing Request". Continue to follow the VMware procedures until you reach the point where it says "Follow the instructions from your KMS vendor to submit the CSR".
3. Log in to the Cryptographic Security Platform Vault for KMIP webGUI.
4. From the Cryptographic Security Platform Vault for KMIP webGUI, select **Security > Client Certificates**.
5. On the Client Certificates tab, click the **+** icon on right top corner to create new client certificate.

6. In the Create Client Certificate dialogue, specify the options you want to use and click **Create**.

Field	Description
Certificate Name	A user-defined name for this bundle. If you are going to create multiple KMIP certificate bundles, this name should be descriptive enough that you can tell the certificate bundles apart. The name can only contain letters, numbers, dashes, periods, underscores, and spaces, and cannot be changed after the bundle is created.
Certificate Expiration	The date on which the certificates in the bundle will expire. If the certificates expire, communication between the Cryptographic Security Platform Vault KMIP server and the client will be disrupted until a new certificate bundle is uploaded to the client.
Certificate Signing Request (CSR)	To use an external CSR, click Load File and upload the file that you just obtained from vSphere.
Certificate Password/ Confirm Password	If you have selected Encrypt Certificate Bundle, provide a passphrase to encrypt the certificates in the bundle. Whether the certificates need to be encrypted depends on the way your security is configured and the type of implementation you are using. Not all third-party KMIP clients can accept encrypted certificates. For example, if you are integrating Cryptographic Security Platform Vault with VMware vSphere Encryption, you *cannot* specify a certificate passphrase due to limitations with vSphere.

7. Select the certificate bundle you just created.
8. Click the Download button on right top corner to download the certificate bundle.
   The webGUI downloads `<certname_datetimestamp>.zip`, which contains a user certification/key file called `<certname>.pem` and a server certification file called `cacert.pem`.
9. Unzip the file so that you have the `<certname>.pem` file available to upload into vCenter. In the example above the certificate file would be named `KMIPvSphereCert.pem`.
10. Return to vCenter and follow the instructions in the following VMware documentation to upload the `<certname>.pem` file:
    Use the New Certificate Signing Request Option to Establish a Standard Key Provider Trusted Connection
    You do not need to do anything with the `cacert.pem` file.

After you have finished, please click the radio button (dot) to the left of the KMS cluster name and ensure that the Connection Status for each KMIP server in the cluster is Normal, and the Certificate Status for the overall KMS cluster is listed. The certificate status for the individual KMIP servers in the cluster can be ignored.

Establishing a Trusted Connection with a CSP Vault-Generated CSR

The following procedure describes how to create a certificate bundle on the Entrust KMIP server that uses a Certificate Signing Request (CSR) generated by Cryptographic Security Platform Vault. The KMIP certificate can then be uploaded to vSphere to establish a trusted connection between vSphere and the Entrust KMIP server.

You can also establish a trusted connection using a vSphere-generated CSR. For details, see Establishing a Trusted Connection with a vSphere-Generated CSR.

1. Log in to the Cryptographic Security Platform Vault for KMIP webGUI.
2. From the Cryptographic Security Platform Vault for KMIP webGUI, select **Security > Client Certificates**.
3. On the Client Certificates tab, click the **+** icon on right top corner to create new client certificate.
4. In the Create Client Certificate dialogue, specify the options you want to use and click **Create**.

Field	Description
Certificate Name	A user-defined name for this bundle. If you are going to create multiple KMIP certificate bundles, this name should be descriptive enough that you can tell the certificate bundles apart. The name can only contain letters, numbers, dashes, periods, underscores, and spaces, and cannot be changed after the bundle is created.
Certificate Expiration	The date on which the certificates in the bundle will expire. If the certificates expire, communication between the KMIP server and the client will be disrupted until a new certificate bundle is uploaded to the client.
Certificate Signing Request (CSR)	Not applicable. Do not upload any file.
Certificate Password/ Confirm Password	If you have selected Encrypt Certificate Bundle, provide a passphrase to encrypt the certificates in the bundle. Whether the certificates need to be encrypted depends on the way your security is configured and the type of implementation you are using. Not all third-party KMIP clients can accept encrypted certificates. For example, if you are integrating Cryptographic Security Platform Vault for KMIP with VMware vSphere Encryption, you *cannot* specify a certificate passphrase due to limitations with vSphere.

5. Select the certificate bundle you just created.
6. Click the Download button on right top corner to download the certificate bundle.
   The Cryptographic Security Platform Vault for KMIP webGUI downloads `<certname_datetimestamp>.zip`, which contains a user certification/key file called `<certname>.pem` and a server certification file called `cacert.pem`.

7. Unzip the file so that you have the `<certname>.pem` file available to upload into vCenter. In the example above the certificate file would be named `vSphereKMS.pem`.
8. Launch the vSphere Client and select the vCenter server to which you added the Cryptographic Security Platform Vault for KMIP KMS cluster.
9. Follow the instructions in the following VMware documentation to upload the `<certname>.pem` file:
   Use the Upload Certificate and Private Key Option to Establish a Standard Key Provider Trusted Connection
   You do not need to do anything with the `cacert.pem` file.

After you have finished, please click the radio button (dot) to the left of the KMS cluster name and ensure that the Connection Status for each KMIP server in the cluster is Normal, and the Certificate Status for the overall KMS cluster is listed. The certificate status for the individual KMIP servers in the cluster can be ignored.

Troubleshooting

Key Generation Error During Encryption

If vSphere Virtual Machine encryption or VMware VSAN encryption fails with the error "Cannot generate key", check the following:

- The Entrust Cryptographic Security Platform Vault appliance must be powered on and operational. To verify this, log into the appliance using the Cryptographic Security Platform Vault webGUI.
- The Entrust KMIP server must be enabled as described in Configuring a KMIP Server.
- The Cryptographic Security Platform Vault nodes must be able to communicate with one another. Make sure the server status is not shown as Degraded in the Cryptographic Security Platform Vault webGUI.
- The KMIP client certificate and private key must be valid and current. You can verify the certificate status in the Cryptographic Security Platform Vault webGUI on the KMIP Servers **Users** tab or in the vCenter Client on the **KMS** tab. For details about creating a new certificate and key, see Establishing a Trusted Connection with a CSP Vault-Generated CSR.
- If the vCenter Client reports that the KMIP connection status is Normal (green) but encryption fails, the KMS cluster could have been added with a user name and password. To verify this:
  a. Check the Entrust Cryptographic Security Platform Vault Audit log for the message "KMIP response rate OperationFailed DENIED".
  b. If you find that message, edit the properties of the Entrust KMS cluster in the vCenter Client and remove any user name or password.
- If the Cryptographic Security Platform Vault cluster is functioning properly and the certificates are valid but the vCenter Client reports that the EntrustKMS is not connected, log into the vCenter Client and navigate to the **KMS** tab. Select the Entrust KMS, then select **All Actions > Refresh KMS certificate**.
  If that does not work, you may need to remove the KMS instance and re-add it to vCenter in order to restore the Trusted connection. Select the EntrustKMS in vSphere Client and select **All Actions > Remove KMS**. Then add the KMS back as described in Adding a KMS Cluster in vSphere.
- If you are using VM encryption and everything shows as connected but encryption still fails, use the vCenter Client to verify that encryption is enabled for the ESXi host using ***ESXi-server-name* > Configure > Security Profile > Host Encryption Mode**.
- If KMIP key creation fails when KMIP KEK is enabled, check if the audit log shows "KMIP Response: Create OperationFailed DB_GENERAL". If so, retry the create operation after enabling KEK cache timeout.
- If you are attempting to encrypt VM or vSAN storage and see errors such as “Create OperationFailed DB_GENERAL” and "Admin Key Regeneration failed" in the Cryptographic Security Platform Vault webGUI and an operation failed message with “RuntimeFault.summary” status in ESXi, check your alerts to see if your KMIP license entitlement is disabled or the license has expired.

Certificate Update Errors

If you try to update the KMS certificate for a Cryptographic Security Platform Vault KMIP Server and vSphere responds with the error message:

The "Update KMS Certificate" operation failed for the entity with the following error message.

Database temporarily unavailable or has network problems.

There may be too many certificates for the KMS Cluster in the vCenter Certificate database. Please see the following knowledge base article https://knowledge.broadcom.com/external/article/383055/expired-kms-server-certificate-will-not.html, or contact Broadcom Support for assistance with this.