



ENTRUST

Cryptographic Security Platform 1.0.0

Installation and administration guide

Document issue: 1.1
Issue date: May 28, 2025

© 2025, 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 OF 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	10
	Revision information.....	10
	Documentation feedback	10
2	Overview	11
	CSP Compliance Manager.....	11
	CSP Public Key Infrastructure	11
	CSP Certificate Manager	11
	CSP Keys and Secrets Management.....	11
3	Release notes	13
	Platform release notes.....	13
	Management Console release notes	15
	Certificate Authority release notes	16
	CA Gateway release notes	17
	Certificate Enrollment Gateway release notes	21
	Certificate Manager release notes.....	23
	Validation Authority release notes	27
	Timestamping Authority release notes.....	28
4	Requirements.....	30
	Required number of nodes.....	30
	Machine requirements.....	30
	Network requirements.....	31
	Software requirements.....	37
	HSM requirements	40
5	Starting up CSP	41
	Downloading the installation files	41
	Verifying the downloaded files.....	42
	Installing the image	43
	Installing CSP	104
	Joining nodes.....	106

Replacing the default TLS certificate	106
Configuring the proxy	107
Changing the keyboard layout	107
Changing the operating system timezone	108
Configuring time synchronization	108
Manually starting the chrony service	108
Configuring an nShield HSM	109
6 Starting up the Management Console	111
Replacing the initial admin password	111
Setting or updating the license	112
Creating Management Console roles	112
Creating Management Console users	114
Integrating Identity providers	116
7 Managing Certificate Authority	125
Configuring and deploying Certificate Authority	125
Creating Certificate Authority tenants	130
Managing organizations	130
Managing Certificate Authority instances	136
Issuing certificates with Certificate Authority instances	150
Changing the HSM vendor	153
8 Managing Certificate Manager	155
Certificate Manager architecture	155
Configuring and deploying Certificate Manager	156
Using Certificate Manager	159
Certificate Manager API	343
Certificate Manager error reference	343
Migrating Certificate Manager database to an external host	362
9 Managing Certificate Enrollment Gateway	365
Certificate Enrollment Gateway overview	365
Preparing to deploy Certificate Enrollment Gateway	365

Issuing TLS certificates for Certificate Enrollment Gateway	387
Configuring and deploying Certificate Enrollment Gateway	394
Enrollment URLs for Certificate Enrollment Gateway	411
Integrating Certificate Enrollment Gateway	415
10 Managing Timestamping Authority	573
Timestamping Authority overview	573
Loading the HSM configuration on Timestamping Authority	573
Configuring Entrust Certificate Authority for Timestamping Authority	573
Generating a timestamping certificate and key pair	575
Configuring and deploying Timestamping Authority	578
Testing the timestamping service	585
11 Managing Validation Authority	587
CSP Validation Authority overview	587
Loading the HSM configuration on Validation Authority	588
Initializing the Validation Authority database	588
Configuring a certificate information source for Validation Authority	591
Generating a VA certificate and key pair	592
Configuring Entrust Certificate Authority for CSP Validation Authority	595
Configuring and deploying Entrust Validation Authority	597
Testing the OCSP Responder	614
12 Managing CA Gateway	616
CA Gateway architecture	616
Obtaining the Gateway server certificate	617
Integrating Certificate Authorities with CA Gateway	621
Configuring and deploying CA Gateway	653
Issuing public trust certificates with CA Gateway	696
Administrating CA Gateway	698
CSP CA Gateway endpoints	698
CA Capabilities reference	704
13 Managing Log Forwarder	714

Log Server	715
TLS	716
14 Upgrading.....	718
Upgrade requirements	718
Upgrading from Entrust Deployment Manager 2.0.2	719
Upgrading from PKI Hub 1.0.0.....	727
15 Administrating.....	728
Administrating nShield HSM integration	728
Checking the etcd database size	729
Checking the persistent volume disk usage	729
Defragmenting the etcd database	730
Managing the retention policies.....	730
Recovering from disaster.....	731
Restarting the nodes.....	732
Updating DNS resolution.....	732
16 Browsing logs with Grafana.....	733
Updating the Grafana initial administrator	734
Browsing and exporting logs with the Grafana Loki Dashboard	735
Browsing log file contents with Grafana.....	739
17 Backing up and restoring.....	743
Backing up.....	743
Restoring	745
18 Uninstalling	747
19 Command reference	748
clusterctl backup create	749
clusterctl backup restore.....	749
clusterctl certificate	750
clusterctl help.....	751
clusterctl install.....	752
clusterctl license import	753

clusterctl node add	753
clusterctl node info	754
clusterctl node join-token	755
clusterctl proxy clear	755
clusterctl proxy info	755
clusterctl proxy set.....	756
clusterctl retention config logs	758
clusterctl retention config metrics	759
clusterctl retention info	760
clusterctl solution config export	761
clusterctl solution config import.....	761
clusterctl solution deploy	762
clusterctl solution info	763
clusterctl solution secret set	764
clusterctl solution upload.....	766
clusterctl uninstall	767
clusterctl upgrade	767
clusterctl version	767
clusterctl volume capacity	768
clusterctl volume info	769
evactl check all	769
evactl check cert-source	772
evactl check db.....	773
evactl check hsm	773
evactl create-csr	775
evactl create-key	777
evactl delete-key	779
evactl enroll	781
evactl export-nshield	782
evactl import-nshield.....	782
evactl import-p12.....	783

evactl import-thales.....	784
evactl list-certs	786
evactl list-keys.....	787
evactl load-oracle-wallet.....	789
evactl reenroll	789
evactl stop	790
pki-hub-upgrade prepare	791
pki-hub-upgrade remove-node.....	792
pki-hub-upgrade upgrade	793
tsactl check clock.....	793
tsactl check hsm.....	794
tsactl create-csr.....	795
tsactl create-key.....	798
tsactl delete-key.....	800
tsactl export-nshield	802
tsactl import-nshield	802
tsactl import-thales	803
tsactl list-keys.....	805
tsactl stop	806
20 CIS benchmarks	808
Linux CIS benchmarks	808
Password policy CIS benchmarks	810
Kubernetes CIS benchmarks	811
21 Troubleshooting and technical assistance.....	821
Troubleshooting Certificate Enrollment Gateway	821
Troubleshooting Validation Authority	821
Troubleshooting Timestamping Authority	822
Generating technical assistance reports	822
22 Licensing.....	825
Customer license.....	825
Third-party license acknowledgments	828

23 Certificate profiles reference	829
Basic authority certificate profiles	829
External subordinate CA certificate profiles	831
Subscriber certificate profiles	839
24 Integration report	909
Base installation integration report.....	909
Certificate Authority integration report.....	910
CSP Certificate Manager integration report	912
CSP CA Gateway integration report	914
CSP Enrollment Services integration report.....	916
CSP Validation Authority integration report.....	924
CSP Timestamping Authority integration report	925

1 About this guide

This guide describes installing and managing the Entrust Cryptographic Security Platform (CSP) 1.0.0.

- [Revision information](#)
- [Documentation feedback](#)

Revision information

See the following table for the changes in each document issue.

Issue	Date	Section	Changes
1.1	May 2025	Configuring and deploying Entrust Validation Authority	Update parameter reference
		Integration report	New section
		Updating the Grafana initial administrator	New section
		Migrating Certificate Manager database to an external host	New section
1.0	May 2025	All	The first release of this document

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 Overview

The Cryptographic Security Platform (CSP) has the following features and functionalities.

- [CSP Compliance Manager](#)
- [CSP Public Key Infrastructure](#)
- [CSP Certificate Manager](#)
- [CSP Keys and Secrets Management](#)

CSP Compliance Manager

The CSP Compliance Manager assists with assessing and managing compliance of identified keys, secrets, and certificates with specified requirements. The CSP Compliance Manager uses:

- Multiple Compliance Manager appliances deployed in a clustered configuration,
- Pre-configured collections of requirements (**Compliance Packs**).

CSP Public Key Infrastructure

The CSP Public Key Infrastructure (PKI) provides an embedded internal **PKI** to create, manage, and distribute digital certificates across an organization's eco-systems. Optional add-on functionality includes:

- Out-of-the-box industrial protocols (**Certificate Enrollment Gateway**), **Validation Authority**, **Timestamping**,
- RESTful APIs to enable automated certificate management and issuance integrated with third-party PKIs (**CA Gateway**).

CSP Certificate Manager

The CSP Certificate Manager, included in the Pro and Enterprise licensing packages, facilitates certificate lifecycle management and automation. It includes:

- At the Pro level, **Discovery** capability to find and discover certificates across diverse platforms.
- At the Enterprise level, **Control** capability to automate the management of those certificates.

CSP Keys and Secrets Management

The CSP Keys and Secrets Management involves deploying multiple vault appliances in active-active clusters. It provides the capability to create and manage the following types of objects:

- **Certificates:** Electronic credentials used to authenticate the identities of entities and secure data transmissions.
- **Standard objects:**
- **KMIP Objects:** Cryptographic keys, secrets, and certificates managed using the Key Management Interoperability Protocol (KMIP), ensuring secure key lifecycle management across different environments.
- **Cloud Keys:** Encryption keys used in cloud environments (e.g., AWS KMS, Azure Key Vault, Google Cloud KMS) to secure cloud-native workloads and storage.
- **Secrets:** Confidential data such as passwords, API keys, access tokens, and other sensitive information that need secure storage and controlled access.
- **Enhanced objects:**

- **TDE Databases:** Transparent Data Encryption (TDE) protected databases, including Oracle, MS SQL, MariaDB, and Open-source PostgreSQL, ensuring data-at-rest encryption.
- **Application Security keys:** Cryptographic keys used by applications to perform cryptographic operations using the cryptographic API or CLI of the CSP, including encryption, digital signatures and hashing.
- **Virtual Machines:** Securely managed cryptographic assets used to protect and encrypt virtualized environments and workloads.
- **Third-Party Objects:** Keys, Secrets or Certificates not directly created or stored by the CSP, but whose metadata has been imported into the CSP to be included in the cryptographic inventory and/or used in compliance assessments.

3 Release notes

CSP 1.0.0 is the first commercial release of Cryptographic Security Platform. This release has the following known issues.

- [Platform release notes](#)
- [Management Console release notes](#)
- [Certificate Authority release notes](#)
- [CA Gateway release notes](#)
- [Certificate Enrollment Gateway release notes](#)
- [Certificate Manager release notes](#)
- [Validation Authority release notes](#)
- [Timestamping Authority release notes](#)

Platform release notes

The following Cryptographic Security Platform 1.0.0 issues and features are common to all types of installations.

- [Platform new features](#)
- [Platform fixed bugs](#)
- [Platform known issues](#)

Platform new features

Cryptographic Security Platform 1.0.0 adds the following features to PKI Hub 1.0.0.

- [Integration with Compliance Manager \(ATEAM-17848\)](#)
- [Log forwarding uses proxy configuration \(EDM-10449\)](#)
- [Docker Registry update to 2.8.3 \(EDM-14214\)](#)
- [Multi-node and single-node modes renamed \(EDM-14644, EDM-17327\)](#)
- [Upgrade from EDM 2.0.2 \(EDM-14996\)](#)
- [EntrustOS packages updated \(EDM-15602\)](#)
- [No proxy \(EDM-16084\)](#)
- [Minimal password length increased to 16 characters \(EDM-16086\)](#)
- [Hostname and IP address in the SAN of the default TLS certificate \(EDM-16358\)](#)

Integration with Compliance Manager (ATEAM-17848)

Cryptographic Security Platform 1.0.0 integrates with Compliance Manager to manage your key inventory. You need to:

1. Meet the [Compliance Manager requirements](#).
2. Start up CSP Certificate Manager as explained in [Managing Certificate Manager](#).
3. Integrate Compliance Manager with CSP Manager Certificate as explained in [Compliance Manager](#).

Log forwarding uses proxy configuration (EDM-10449)

The SIEM solution described in [Managing Log Forwarder](#) uses the proxy configuration set with the `clusterctl proxy set` command.

Docker Registry update to 2.8.3 (EDM-14214)

Cryptographic Security Platform 1.0.0 updates the Docker Registry component to 2.8.3.

Multi-node and single-node modes renamed (EDM-14644, EDM-17327)

The installation modes supported by the `clusterctl install` command have been renamed as follows.

Old name	New name
single-node	demo-mode
multi-node	prod-demo

Upgrade from EDM 2.0.2 (EDM-14996)

As explained in [Upgrading](#), Cryptographic Security Platform 1.0.0 supports upgrading from both:

- Entrust Deployment Manager 2.0.2
- PKI Hub 1.0.0

EntrustOS packages updated (EDM-15602)

Cryptographic Security Platform 1.0.0 includes updated versions of the EntrustOS packages.

No proxy (EDM-16084)

The `clusterctl proxy set` command for configuring the proxy includes a new `no-proxy` option to select the domain names and IP addresses for which to skip the proxy.

Minimal password length increased to 16 characters (EDM-16086)

As explained in [Password policy CIS benchmarks](#), the minimum supported length for the `sysadmin` user password is now 16 characters.

i After [Upgrading](#) from earlier versions, Cryptographic Security Platform 1.0.0 does not enforce this requirement for legacy passwords. However, when renewing them, you will be prompted to create passwords that meet this minimum length requirement.

Hostname and IP address in the SAN of the default TLS certificate (EDM-16358)

Node hostname and IP address added to the Subject Alternative Name (SAN) extension of the default TLS certificate generated on cluster installation.

Platform fixed bugs

Cryptographic Security Platform 1.0.0 fixes the following PKI Hub 1.0.0 bugs.

Identifier	Description
EDM-13524	The Helm component uses old credentials when renewing the K3s client and server TLS certificates.
EDM-15095	Under some circumstances, K3s and Calico components use network interface controllers.
EDM-15379	CVE-1999-0524 vulnerability in the firewalld service.
EDM-15388 EDM-15397	CVE-2008-5161 and CVE-2015-4000 vulnerabilities in the SSH server.
EDM-15800	Some solution deployments fail with a "DeploymentNotFoundError" message.
EDM-16127	When a solution update fails, the old version is sometimes deleted.
EDM-16154	When an HTTP proxy is configured, the online license registration fails with an HTTP 404 "Not Found" error.
EDM-16961	When a solution deployment fails, the deployment process is not always interrupted.

Platform known issues

The following known issues are common to all Cryptographic Security Platform 1.0.0 installations.

- [McAfee agent not supported \(EDM-4074\)](#)
- [Occasional restore failures of single-node installations \(EDM-16171\)](#)

McAfee agent not supported (EDM-4074)

You cannot install McAfee agent on Cryptographic Security Platform 1.0.0 nodes.

Occasional restore failures of single-node installations (EDM-16171)

The process described in [Restoring the state](#) fails 75% of the time on single node installations.

Workaround: Run the `clusterctl uninstall` command to uninstall the cluster and re-try [Restoring the state](#).


Management Console release notes

The Management Console of Cryptographic Security Platform 1.0.0 has the following known issues.

- [User names are case insensitive \(ATEAM-17300\)](#)
- [Session expiration does not redirect to the login page \(ATEAM-17362\)](#)

User names are case insensitive (ATEAM-17300)

When creating a user, the Management Console does not enforce the username to be lowercase.

 Management Console operations may raise an error after logging in with a username in uppercase.

Session expiration does not redirect to the login page (ATEAM-17362)

When a user session expires, the Management Console does not automatically redirect to the login page.

Certificate Authority release notes

Certificate Authority for Cryptographic Security Platform 1.0.0 has the following known and fixed issues.


- [Certificate Authorities fixed issues](#)
- [Certificate Authorities known issues](#)

Certificate Authorities fixed issues

This Certificate Authority release fixes the following known issue.

14-character limitation for organization names not enforced (ATEAM-17443)

When typing an organization name that exceeds 14 characters, the Management Console displays a warning tooltip but still allows creating the organization.

 Organizations with a name exceeding 14 characters are unusable.

Certificate Authorities known issues

This release of the Certificate Authority solution has the following known issues.

- [Datadog errors in logs \(ATEAM-17270\)](#)
- [CA identifier uniqueness not enforced \(ATEAM-17301\)](#)
- [Some failed deployments appear as successful \(ATEAM-17321\)](#)
- [Cannot remove issuing CAs after removing the root CA \(ATEAM-17445\)](#)
- [HSM configuration requires an RFS server \(ATEAM-17470\)](#)
- [No error message when losing the database connection \(ATEAM-17478\)](#)


Datadog errors in logs (ATEAM-17270)

The Certificate Authority logs include errors of the Datadog metrics tracker.

 See [Browsing logs with Grafana](#) for how to browse logs.

CA identifier uniqueness not enforced (ATEAM-17301)

The Certificate Authorities solution allows reusing CA identifiers in the CA-creation form.

 Removing a CA results in removing all CAs with the same identifier.

Some failed deployments appear as successful (ATEAM-17321)

Some Certificate Authorities deployments resulting in errors and non-running pods may appear as "successful" in the Management Console.

Cannot remove issuing CAs after removing the root CA (ATEAM-17445)

Certificate Authorities do not support removing issuing CAs that are subordinate to a root CA already removed.

HSM configuration requires an RFS server (ATEAM-17470)

Configuring an HSM (Hardware Security Module) for the Certificate Authorities solution requires access to a remote file system for nShield instead of simply uploading the `kmdata` TAR file.

No error message when losing the database connection (ATEAM-17478)

When losing the connection with the database, the Management Console displays no error message and allows clicking the **Create Organization** button.

CA Gateway release notes

The CA Gateway solution has the following known issues.

- [CA Gateway new features](#)
- [CA Gateway fixed bugs](#)
- [CA Gateway known issues](#)

CA Gateway new features

CA Gateway for Cryptographic Security Platform 1.0.0 adds the following new features.

- [Mandatory parameters are mutually exclusive \(ATEAM-16246\)](#)
- [subject.certificates field omitted \(ATEAM-16264\)](#)

Mandatory parameters are mutually exclusive (ATEAM-16246)

When configuring a CA Gateway client, the following mandatory parameters are mutually exclusive (that is, you must select one but not both).

- Tenant ID
- Integrator ID

However, the Management Console raises an error during validation if any of these values is unselected.

Detected in: CA Gateway 3.0.0 to 3.0.5.


Workaround:

1. Delete the client settings.
2. Recreate the client settings using either the **Tenant ID** or **Integrator ID** parameter.

subject.certificates field omitted (ATEAM-16264)

For performance reasons, the PKIaaS CA Plugin will not honor the `subject.certificates` field in the following endpoint.

```
api/v1/certificate-authorities/{caId}/subjects/dn
```

 Future releases may restore this functionality.

Detected in: CA Gateway 3.0.1 to 3.0.5.

CA Gateway fixed bugs

CA Gateway for Cryptographic Security Platform 1.0.0 fixes the following bugs.

- [Appliance deployment fails in multi-node \(ATEAM-14813\)](#)
- [LDAP entry creation not properly managed by Management Console \(ATEAM-15839\)](#)
- [Mandatory Subject Alternative Name not enforced \(ATEAM-16170\)](#)
- [Invalid date format for expiry date \(ATEAM-16797\)](#)
- [Certificate enrollment does not return the certificate chain \(ATEAM-16985\)](#)
- [Wrong spelling of UserPrincipalName \(ATEAM-17046\)](#)
- [Role selection not supported \(ATEAM-17182\)](#)
- [Certificate lifetime error \(ATEAM-17250 & ATEAM-17298\)](#)
- [Unowned files \(ATEAM-17355\)](#)
- [startDate format not specified by Swagger documentation \(ATEAM-17426\)](#)
- [Invalid bitwise OR example in documentation \(ATEAM-17501\)](#)
- [Missing filter-list setting \(ATEAM-17650\)](#)
- [Non-documented parameters \(ATEAM-17651\)](#)
- [CAA filter bypassed \(ATEAM-17708\)](#)
- [CA Gateway cannot handle non-printable characters in subject names from msca-proxy \(ATEAM-18063\)](#)
- [Mandatory subject variables not supported \(ATEAM-18126\)](#)

Appliance deployment fails in multi-node (ATEAM-14813)

On appliances with more than one node, the CA Gateway deployment intermittently fails.

LDAP entry creation not properly managed by Management Console (ATEAM-15839)

The Management Console of the appliance does properly manage the `create-ldap-entry` parameter configuration parameter.

Mandatory Subject Alternative Name not enforced (ATEAM-16170)

When configured in a profile, the SAN (Subject Alternative Name) requirement is not enforced. That is, certificate enrollments do not fail when the profile requires a SAN but the request does not specify one.

Invalid date format for expiry date (ATEAM-16797)

When enrolling certificates, the CA Gateway API may return a collapsed date format when the seconds are 00 for certificate expiry.

Certificate enrollment does not return the certificate chain (ATEAM-16985)

CA Gateway does not return the certificate chain of the enrolled certificates, even when explicitly requested in the CSR.

Wrong spelling of UserPrincipalName (ATEAM-17046)

The UserPrincipalName (UPN) certificate field was misspelled as "UserPrincipleName" in both the documentation and the configuration files.

Role selection not supported (ATEAM-17182)

When configuring an Entrust Deployment Manager installation of CA Gateway, the Management Console did not allow selecting the following roles:

- read-only-integrator
- read-only-tenant roles

Certificate lifetime error (ATEAM-17250 & ATEAM-17298)

When processing enrollments or renewals, the Entrust Certificate Authority plugin did not correctly verify validity dates if the certificate `notAfter` date was within an hour of the CA certificate `notAfter` date. This resulted in the `cagw-4027` error with the following message.

Extension of certificate lifetime beyond policy not permitted.

Unowned files (ATEAM-17355)

Some configuration files can remain "unowned" on the CA Gateway host machine.

Bug resolution details: document in the "CA Gateway Requirements" section of the deployment guide that "User and group identifiers 1339 are reserved for CA Gateway images, so the host server should not use them".

startDate format not specified by Swagger documentation (ATEAM-17426)

The Swagger documentation of the CA Gateway API does not properly specify the required format for the `startDate` parameter of the `certificate-events` endpoint,

Invalid bitwise OR example in documentation (ATEAM-17501)

The "Enabling of Subject Alternative Name attributes in the enrollment request" section of the deployment guide for Microsoft CA includes an incorrect output for an OR operation.

Missing filter-list setting (ATEAM-17650)

The profile configuration schema in the Management Console does not include the `filter-list` setting.

Non-documented parameters (ATEAM-17651)

The CA Gateway configuration reference does not include the following parameters.

- dns.cache-enabled
- dns.response-threshold (Prior to CAGW 3.1)
- dns.response-threshold (as of CAGW 3.1)

CAA filter bypassed (ATEAM-17708)

The CAA (Certification Authority Authorization) filter does not always block requests for non-authorized domains when CA Gateway is deployed in the appliance.

- **Bug cause.** Kubernetes sets ndots to 5 by default, expecting a fully qualified domain name as such:

```
<service-name>.<namespace-name>.svc.<cluster-domain>
```

- **Bug resolution.** Modify the Kubernetes settings to bypass this limitation.

CA Gateway cannot handle non-printable characters in subject names from msca-proxy (ATEAM-18063)

When issuing a certificate with a Microsoft CA, the following CA Gateway API endpoint stops processing events if the subject includes non-printable characters.

```
/v1/certificate-authorities/{caId}/certificate-events
```

Bug resolution: enhance the Entrust Proxy for Microsoft CA to support non-printable chars in the subject name.

Mandatory subject variables not supported (ATEAM-18126)

For each variable added to the `subject-variable-requirements` list, CA Gateway ignores the `required` setting value.

CA Gateway known issues

CA Gateway for Cryptographic Security Platform 1.0.0 has the following known issues.

- [Mandatory parameters are mutually exclusive \(ATEAM-16246\)](#)
- [subject.certificates field omitted \(ATEAM-16264\)](#)
- [Slashes not supported in passwords \(ATEAM-18325\)](#)

Mandatory parameters are mutually exclusive (ATEAM-16246)

When configuring a CA Gateway client, the following mandatory parameters are mutually exclusive (that is, you must select one but not both).

- Tenant ID
- Integrator ID

However, the Management Console raises an error during validation if any of these values is unselected.

Detected in: CA Gateway 3.0.0 to 3.0.5.


Workaround:

1. Delete the client settings.
2. Recreate the client settings using either the **Tenant ID** or **Integrator ID** parameter.

subject.certificates field omitted (ATEAM-16264)

For performance reasons, the PKIaaS CA Plugin will not honor the `subject.certificates` field in the following endpoint.

```
api/v1/certificate-authorities/{caId}/subjects/dn
```

 Future releases may restore this functionality.

Detected in: CA Gateway 3.0.1 to 3.0.5.

Slashes not supported in passwords (ATEAM-18325)

CA Gateway deployments on appliances do not support slashes ('/') in passwords (such as keystore passwords, truststore passwords, Entrust Profile File passwords, etc.).

Detected in: CA Gateway installations on EDM (Entrust Deployment Manager), PKI Hub, and CSP (Cryptographic Security Platform).

Certificate Enrollment Gateway release notes

See below for the release notes for the Certificate Enrollment Gateway solution running in Cryptographic Security Platform 1.0.0.

- [Enrollment Services new features](#)
- [Certificate Enrollment Gateway known issues](#)

Enrollment Services new features

This release of Entrust Certificate Enrollment Gateway includes the following new features.

- [Support for the EST protocol \(CEG-1003\)](#)
- [Support for the CMPv2 protocol \(CEG-1006\)](#)

 See [Enrollment protocols supported by CSP Enrollment Services](#) for a full list of the supported protocols.

Support for the EST protocol (CEG-1003)

This release adds support for the Enrollment over Secure Transport (EST) protocol. EST is a PKI communication protocol that allows administrators to automatically and securely issue certificates to client applications or devices that support EST. EST is considered secure because the device itself creates the private keys, and only the public keys are passed to the CA. The private keys never leave the device.

Support for the CMPv2 protocol (CEG-1006)

This release adds support for the Certificate Management Protocol version 2 (CMPv2) protocol. CMPv2 is a PKI communication protocol that allows network devices to enroll into a PKI and get a certificate for making secure authenticated connections to other network components. CMPv2 is an update of the CMP standard.

Certificate Enrollment Gateway known issues

This section describes known issues and limitations for Entrust Certificate Enrollment Gateway. For other known issues with Certificate Enrollment Gateway, see the [Knowledge](#) section of Entrust TrustedCare. Reference numbers are for internal purposes only.

Configuration backup is only supported in single-node deployments (CSF-704)

Certificate Enrollment Gateway is deployed as a solution into Entrust Deployment Manager. Only single-node deployments of Entrust Deployment Manager support the `clusterctl backup config` command for exporting the cluster configuration. For information about the limitations and workaround for a multi-node backup and restore process, see the Entrust Deployment Manager documentation.

Unsupported ACMEv2 features (PKI-30901)

The Certificate Enrollment Gateway implementation of the ACME Server does not support the following [RFC 8555](#) features:

- EdDSA signature algorithm
- Rate limits
- `termsOfService` optional string
- Changes of Terms of Service
- External Account Binding
- Pre-authorization

Unsupported Intune-SCEP operations (PKI-28149, PKI-31351)

The Certificate Enrollment Gateway integration with the Intune-SCEP protocol does not support the following [draft-nourse-scep-23](#) operations:

- GetCRL
- GetNextCACert

CSRs sent from ACMEv2 clients cannot have an empty Subject DN if they will be sent to Entrust Certificate Services for processing (ECS-39482)

If an ACMEv2 client sends a CSR (certificate signing request) with an empty Subject DN, Certificate Enrollment Gateway will use the first Subject Alternative Name value in the CSR as the Subject DN. Certificate Enrollment Gateway will not alter the CSR, but will send the Subject DN value as a separate parameter to CA Gateway for processing. Entrust Certificate Services requires that CSRs must have a Subject DN. Entrust Certificate Services will ignore the Subject DN parameter sent by Certificate Enrollment Gateway.

Workaround: You must generate the CSR externally from the ACMEv2 client using another tool, such as openssl. The ACMEv2 client can then use the externally-generated CSR.

CSRs sent from ACMEv2 clients cannot have an empty Subject DN if they will be sent to a Microsoft CA for processing (PKI-32853)

If an ACMEv2 client sends a CSR (certificate signing request) with an empty Subject DN, Certificate Enrollment Gateway will use the first Subject Alternative Name value in the CSR as the Subject DN. Certificate Enrollment Gateway will not alter the CSR, but will send the Subject DN value as a separate parameter to CA Gateway for

processing. A Microsoft Certification Authority (CA) requires that CSRs must have a Subject DN. A Microsoft CA will ignore the Subject DN parameter sent by Certificate Enrollment Gateway.

Note: This issue does not occur when using Certificate Enrollment Gateway with CA Gateway 2.5.0 or later. When using CA Gateway 2.5.0 or later, ACMEv2 clients can send a CSR with an empty Subject DN intended for a Microsoft CA without issue.

Workaround: You must generate the CSR externally from the ACMEv2 client using another tool, such as OpenSSL. The ACMEv2 client can then use the externally-generated CSR.

Authentication error message is always logged when enrolling for a certificate with a Cisco LibEST client using basic authentication (CEG-3287)

When enrolling for a certificate with a Cisco LibEST client and the client is using basic authentication, Certificate Enrollment Gateway will always log an authentication error, even when the `simpleenroll` and `serverkeygen` operations are successful. For example:

```
[2024-09-16 13:16:49.711] [ERROR] [10] [EST] [] [a06bef31] [https-jsse-nio-1443-exec-1]
[com.entrust.ceg.commons.audit.AuditLogger=>process] [Request to EST
operation:simpleenroll failed.Reason:Access to EST operation:simpleenroll must be
authenticated ]
```

This error is expected with the LibEST client. Even when using basic authentication, the LibEST client does not provide the parameters for basic authentication on the first request. When the EST server does not obtain the basic authentication parameters on the first request, it issues header "WWW-Authenticate" to the LibEST client. When LibEST client receives the "WWW-Authenticate" header, the client will repeat the request and include the basic authentication parameters.

Certificate Enrollment Gateway will log WARN messages during startup when attempting to create database tables that already existed (CEG-3392)

During startup, Certificate Enrollment Gateway will log WARN messages when attempting to create database tables that already exist. This issue will be fixed in a future release.

Certificate Manager release notes

Certificate Manager for Cryptographic Security Platform 1.0.0 has the following fixed and known issues.

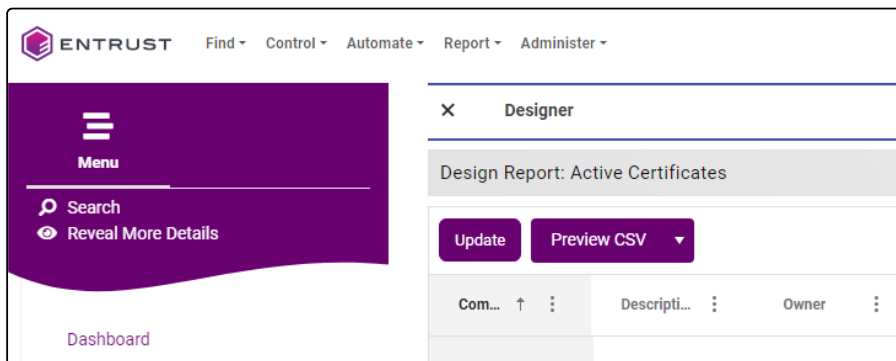
- [Certificate Manager fixed bugs](#)
- [Certificate Manager known issues](#)

Certificate Manager fixed bugs

Certificate Manager for Cryptographic Security Platform 1.0.0 fixes the following bugs.

CSV preview command fails on extensive reports (ATEAM-17431)

The **Preview CSV** command of the report designer throws an error when a report includes many records.



Bug fixing details: the report preview is now limited to a single page with up to 100 entries.

Certificate issuance fails on web server empty folders (ATEAM-18214)

Deploying a certificate to an Apache or Nginx web server destination fails with an error message if the target folder does not contain other certificates.

Certificate Manager known issues

Certificate Manager for Cryptographic Security Platform 1.0.0 has the following known issues.

- [Error when taking certificates off hold \(ATEAM-1445\)](#)
- [Issues when changing the display order of custom fields \(ATEAM-15463\)](#)
- [Some endpoint filters display invalid results on report files \(ATEAM-15933\)](#)
- [Certificates without names not synced from source \(ATEAM-16039\)](#)
- [Out-of-memory error when generating reports with many certificates \(ATEAM-16346\)](#)
- [Wildcard certificates not recorded \(ATEAM-16436\)](#)
- ['Manage Schedules' option disabled in non-scheduled reports \(ATEAM-16910\)](#)
- [Buttons language not affected when switching language \(ATEAM-16920\)](#)
- [Owner grid column not populated when accessing reports \(ATEAM-16923\)](#)
- [Authorities without authority certificate are not displayed \(ATEAM-16930\)](#)
- [Labels not affected when switching language \(ATEAM-16942\)](#)
- [The Verify button does not always trigger a verification \(ATEAM-16950\)](#)
- [The public key ID can refer to the private key ID \(ATEAM-16982\)](#)
- [Error when selecting the Domains widget \(ATEAM-16986\)](#)
- [Archive certificates option missing with FIND licenses \(ATEAM-16988\)](#)
- [Incomplete CA certificate chain \(ATEAM-16997\)](#)
- [Verification fails for IIS destinations \(ATEAM-17030\)](#)
- [Certificate creation fail \(ATEAM-17063\)](#)
- [Web server request fails \(ATEAM-17070\)](#)
- [Python requirement not documented \(ATEAM-17072\)](#)
- [Error message on Kubernetes with an external database \(ATEAM-17230\)](#)

Error when taking certificates off hold (ATEAM-1445)

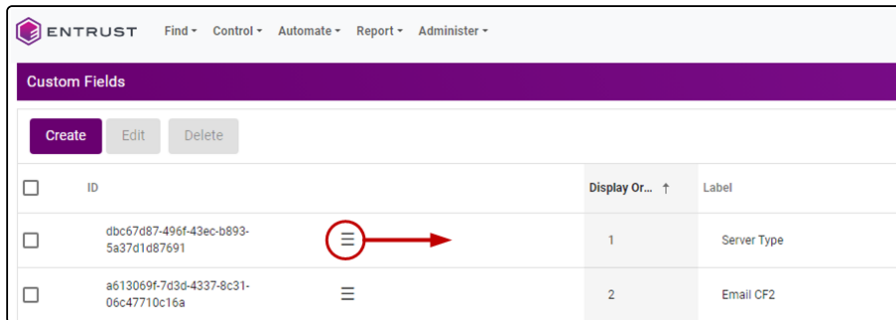
For certificates with **Revocation Reason: On Hold**, attempting to unhold the certificate may fail, or the **Unhold** option may be absent from the **Actions** dropdown.

Issues when changing the display order of custom fields (ATEAM-15463)

In the **Custom Fields** page of the web console, Certificate Manager administrators can change the display order of the custom fields. However:

- Reordering a custom field does not change the **Display Order** column value.
- Refreshing the **Custom Field** page reverts all changes.

Workaround: After dragging a custom field to a different position, move the ☰ drag icon within its row to make the changes persistent.



Some endpoint filters display invalid results on report files (ATEAM-15933)

The following endpoint filters do not display correct results on the downloaded report files.

- is empty
- is not empty

Certificates without names not synced from source (ATEAM-16039)

Certificates without a name are not successfully synced from Sources.

Out-of-memory error when generating reports with many certificates (ATEAM-16346)

When generating a report containing a large number of certificates, the report generation may fail with an out-of-memory error.

Workaround: Increasing the heap size of the `acm-api` pod (for report preview) and scheduler pod (for scheduled reports) may fix this issue. A Java Heap Size parameter has been added to the deployment script to allow for manual adjustment of the allocated heap size.

Wildcard certificates not recorded (ATEAM-16436)

Certificate Manager does not record wildcard certificates successfully scanned by the Discovery Scanner.



Wildcard certificates are certificates containing the wildcard asterisk in the issuer and subject.

'Manage Schedules' option disabled in non-scheduled reports (ATEAM-16910)

If a report does not have a **Schedule**, the **Manage Schedules** option is disabled from the **Actions** dropdown of the **Report Designer** page.

Buttons language not affected when switching language (ATEAM-16920)

Switching the language before logging in does not affect the language of the **Delete** and **Cancel** buttons in the **Confirm Delete** popup on the **Destinations** page.

Owner grid column not populated when accessing reports (ATEAM-16923)

The **Owner** grid column is not populated when accessing the **Report Schedules** from the **Report Designer** grid.

Workaround: Access the **Report Schedules** grid from the navigation bar.

Authorities without authority certificate are not displayed (ATEAM-16930)

The **Authorities** page does not display authorities missing an authority certificate.

Labels not affected when switching language (ATEAM-16942)

Switching language in the **Report Designer** page does not affect the labels of the grid columns.

The Verify button does not always trigger a verification (ATEAM-16950)

After the failed verification of a Destination, clicking **Verify** again does not trigger a new verification.

Workaround: Make any change in the create form – for example, change the **Description**.

The public key ID can refer to the private key ID (ATEAM-16982)

When issuing a certificate using the **Key Manager (KMIP)** destination, the **public key ID** is also referring to the **private key ID**

Error when selecting the Domains widget (ATEAM-16986)

When Certificate Manager is licensed with a FIND license, selecting the **Domains** widget on the **Dashboard** displays the following error.

Unable to show information: Forbidden. This request is not allowed.

Archive certificates option missing with FIND licenses (ATEAM-16988)

When Certificate Manager is licensed with a FIND license, the option to **Archive** certificates is missing in the **Actions** dropdown on the **Certificates** grid.

Incomplete CA certificate chain (ATEAM-16997)

When creating a new certificate, the downloaded chain only includes the certificate of the CA that issued the new certificate instead of including the entire chain.

Verification fails for IIS destinations (ATEAM-17030)

Verification fails for IIS destinations if the username includes a domain name – for example:

```
.\user
```

```
domain\user
```

Certificate creation fail (ATEAM-17063)

Certificate creation fails when adding an `otherName` field to the Subject Alternative Names.

Web server request fails (ATEAM-17070)

Administrator requests for certificate issuance with Apache, Nginx, or IIS destinations fail during the approval process if the administrator performing the approval has only the Approver role.

Workaround: Let a global administrator with the Authority role perform the approval.

Python requirement not documented (ATEAM-17072)

The user guide does not indicate that Python 3.9 or newer is a requirement for Apache and Nginx destinations.

Error message on Kubernetes with an external database (ATEAM-17230)

When installing Certificate Manager on Kubernetes with an external database, you can safely ignore the following error message:

```
Error from server (NotFound): configmaps "postgres-config" not found
```

Validation Authority release notes

Validation Authority for Cryptographic Security Platform 1.0.0 has the following known issues.


- [tsactl logs not forwarded to Splunk \(EDM-13275\)](#)
- [Temporary Kubernetes pods may run after command completion \(ATEAM-16336\)](#)
- [Running shims not moved after a node dies \(PKIPM-1090\)](#)
- [Newly deployed status after command execution \(ATEAM-16337\)](#)
- [Large kmdata files not supported \(ATEAM-16338\)](#)
- [Database validation error \(ATEAM-17466\)](#)



This Validation Authority release focuses on dependency updates, not adding features or fixing bugs.

tsactl logs not forwarded to Splunk (EDM-13275)

When integrated with a Splunk server, Cryptographic Security Platform does not forward logs recording `tsactl` commands. However, these logs can be browsed using the Grafana portal.

 See [Managing Log Forwarder](#) for integrating a Splunk server or [Browsing logs with Grafana](#) for browsing logs in the Grafana portal.

Temporary Kubernetes pods may run after command completion (ATEAM-16336)

Temporary Kubernetes pods may run after the completion of an `evactl` command. These pods will be deleted when deploying and do not compromise the Entrust Validation Authority operation or the execution of more `evactl` commands.

Running shims not moved after a node dies (PKIPM-1090)

When a node dies, Entrust Validation Authority does not move pod running shims to an alive node. Therefore, these shims stop updating the database.

Workaround: Wait until the dead node returns, or kill the pod as follows.

1. List the pods.

```
sudo kubectl get pods -n eva -o wide
```

2. Kill the dead pod. For example:

```
sudo kubectl -n eva delete pod --force eva-cagwshim-n-0
```

Newly deployed status after command execution (ATEAM-16337)

After running some `evactl` commands, the Management Console Entrust Validation Authority as newly deployed.

Large kmdata files not supported (ATEAM-16338)

The `tsactl import-nshield` command does not support `kmdata` files larger than ~100KB.

Database validation error (ATEAM-17466)

The Management Console displays a validation error when:


1. Importing a configuration file containing a non-empty database `sslValidationCert` value.
2. Setting the **SSL Mode** database configuration to **disable**.

Workaround: Delete the `sslValidationCert` value in the configuration file before importing it.

Timestamping Authority release notes


The Timestamping Authority solution has the following known issues.

- [tsactl logs not forwarded to Splunk \(EDM-13275\)](#)
- [The solution deployer does not properly check pod execution \(ATEAM-16344\)](#)
- [Large kmdata files not supported \(ATEAM-16338\)](#)

 This Timestamping Authority release focuses on dependency updates, not adding features or fixing bugs.

tsactl logs not forwarded to Splunk (EDM-13275)

When integrated with a Splunk server, Cryptographic Security Platform does not forward logs recording `tsactl c` commands. However, these logs can be browsed using the Grafana portal.

 See [Managing Log Forwarder](#) for integrating a Splunk server or [Browsing logs with Grafana](#) for browsing logs in the Grafana portal.

The solution deployer does not properly check pod execution (ATEAM-16344)

The CSP Timestamping deployer:

- Checks the execution of a single pod only.
- Uses a timeout too short for properly checking the successful pod execution.

As a consequence, successful deployments may appear as failed in the Management Console.

Large kmdata files not supported (ATEAM-16338)

The `tsactl import-nshield` command does not support `kmdata` files larger than ~100KB.

4 Requirements

You can run Cryptographic Security Platform on virtualization platforms and cloud providers. See below for the requirements shared by all types of installation.

- [Required number of nodes](#)
- [Machine requirements](#)
- [Network requirements](#)
- [Software requirements](#)
- [HSM requirements](#)

Required number of nodes

In case of disaster, an Cryptographic Security Platform installation with N nodes is available if at least $(N/2)+1$ nodes are available. This minimum number of working nodes is referred to as "quorum".

When deploying Cryptographic Security Platform in high availability, we recommend 3 or 5 nodes because:

- A 2-node installation fails when a single node fails.
- A 4-node installation fails when 2 nodes fail, just like a 3-node installation. Adding a node to an odd number of nodes does not increase the number of tolerated node failures.
- Cryptographic Security Platform does not support more than 5 nodes.

See the table below for the supported node failures.

Cluster nodes	Nodes alive	Nodes broken	Quorum
3	1	2	✗
3	2	1	✓
5	1	4	✗
5	2	3	✗
5	3	2	✓
5	4	1	✓

Machine requirements

The machines running the Cryptographic Security Platform must meet the following requirements.

- [Memory requirements](#)
- [CPU requirements](#)
- [Main disk requirements](#)
- [Additional disk requirements](#)

Memory requirements

Each node needs at least 16 GB of RAM

CPU requirements

Each node needs at least 8 CPU cores

Main disk requirements

You need a main disk with the following requirements.

Setting	Required value
Size	1 TiB or more
Storage type	SSD (Solid-state Drive)

Additional disk requirements

The `etcd` daemon requires a dedicated disk with the following requirements.

Setting	Required value
Size	15 GiB or more
Storage type	SSD (Solid-state Drive)
fsync latency	As explained in the etcd documentation , the p99 percentile of the <code>wal_fsync_duration_seconds</code> duration should be less than 10ms to confirm the disk is reasonably fast for production workloads.
IOPS (input/output operations per second)	50 or more sequential write operations per second.

Network requirements

Connect Cryptographic Security Platform to a network with the following requirements.

- [DNS requirements](#)
- [IP address requirements](#)
- [Load balancing requirements](#)
- [Required open ports](#)
- [Reserved subnets](#)

DNS requirements

The selected DNS servers must be accessible without a proxy, as Cryptographic Security Platform cannot access a DNS server through a proxy.

IP address requirements

Cryptographic Security Platform only supports IPv4 and disables IPv6 by default. In multi-node deployments, all nodes:

- Must have a fixed hostname and IP address.
- Must be in the same subnet, cloud region, or virtual network.

After the installation, run the following command in each node to check the IP address and subnet mask.

```
nmcli
```

Verify that all nodes are in the same subnet.

✗ After running the [clusterctl install](#) or [clusterctl node add](#) commands you cannot change the IP address or hostname of a node.

Load balancing requirements

In multi-node installations, you must set up an external load balancer to operate as a single point of contact for Entrust solutions users and distribute the incoming traffic across all the cluster nodes. This prevents any node from becoming a single point of failure.

⚠ It is recommended to use sticky web connections because sessions with Entrust solutions can experience issues when the load balancer switches nodes.

Required open ports

The Cryptographic Security Platform operation requires verifying the following ports are open for traffic.

- [Required ports for incoming traffic](#)
- [Required ports for internode communication](#)
- [Required ports for outgoing traffic](#)
- [Solution-specific port requirements](#)

Required ports for incoming traffic

In all the installation nodes, check that the following ports are accessible for incoming traffic to Cryptographic Security Platform.

Target Port	Protocol	Source	Target service
22	TCP/SSH	The IP of the sysadmin Cryptographic Security Platform administrator.	SSH
443	TCP/HTTPS	The IP of the Grafana and Management Console users.	Grafana and the Management Console.

Required ports for internode communication

In multi-node installations, check that the following ports are accessible for internal services – such as monitoring node status or synchronizing data between nodes.

Port	Protocol	Source	Destination
179	TCP	All nodes	All nodes
2379	TCP	All nodes	All nodes
2380	TCP	All nodes	All nodes
2381	TCP	All nodes	All nodes
4789	UDP	All nodes	All nodes
5473	TCP	All nodes	All nodes
6443	TCP	All nodes	All nodes
8000	TCP	All nodes	All nodes
9100	TCP	All nodes	All nodes
10250	TCP	localhost	localhost
15014	TCP	All nodes	All nodes
15021	TCP	All nodes	All nodes
30000	TCP	localhost	localhost

Port	Protocol	Source	Destination
51820	UDP	All nodes	All nodes

Required ports for outgoing traffic

Some start-up operations require opening ports for outgoing traffic – for example:

- Selecting the DNS server, as later explained in [Configuring the connection of an ISO installation](#).
- Configuring the NTP client, as later explained in [Configuring time synchronization](#).

Verify these ports are accessible for outgoing traffic in all the installation nodes.

Solution-specific port requirements

See the following table for the additional open ports each Entrust solution requires.

- [Port requirements for Certificate Authority](#)
- [Port requirements for Certificate Enrollment Gateway](#)
- [Port requirements for CA Gateway](#)
- [Port requirements for Timestamping Authority](#)
- [Port requirements for Validation Authority](#)

Port requirements for Certificate Authority

The Certificate Authority solution adds the following port requirements.

- [Incoming traffic to Certificate Authority](#)
- [Outgoing traffic from Certificate Authority](#)

Incoming traffic to Certificate Authority

In all the installation nodes, check that the following ports are accessible for incoming traffic to Cryptographic Security Platform.

Target Port	Protocol	Source	Target Service
4443	TCP/HTTPS	CAs	Green deployment testing
7443	TCP/HTTPS	CAs	Internal CA Gateway
8880	TCP/HTTP	CAs	Green deployment testing



The deployment of the Certificate Authority solution automatically opens these ports in the firewall of the machines hosting Cryptographic Security Platform.

Outgoing traffic from Certificate Authority

In all the installation nodes, check that the following ports are accessible for outgoing traffic from Cryptographic Security Platform.

Target Port	Protocol	Source	Target Service
1792	NTLS	CAs	Luna Network HSM (if any)
9000-9004	TCP/HTTPS	CAs	nShield HSM (if any)

Port requirements for Certificate Enrollment Gateway

Certificate Enrollment Gateway deployment automatically opens port 1443 in the firewall of the machines hosting Cryptographic Security Platform. Ensure no network restriction blocks incoming traffic to this port.

Port requirements for CA Gateway

CA Gateway deployment automatically opens port 8444 in the firewall of the machines hosting Cryptographic Security Platform. Ensure no network restriction blocks incoming traffic to this port.

Port requirements for Timestamping Authority

The Timestamping Authority solution adds the following port requirements.

- [Incoming traffic to Timestamping Authority](#)
- [Outgoing traffic from Timestamping Authority](#)

Incoming traffic to Timestamping Authority

In all the installation nodes, check that the following ports are accessible for incoming traffic to Cryptographic Security Platform.

Target Port	Protocol	Source	Target Service
80	TCP/HTTP	Timestamp client	Timestamp responder

Outgoing traffic from Timestamping Authority

In all the installation nodes, check that the following ports are accessible for outgoing traffic from Cryptographic Security Platform.

Target Port	Protocol	Source	Target Service
1792	NTLS	TSA	Luna Network HSM (if any)
9000-9004	TCP/HTTPS	TSA	nShield HSM (if any)

Port requirements for Validation Authority

The Validation Authority solution adds the following port requirements.

- [Incoming traffic to Validation Authority](#)
- [Outgoing traffic from Validation Authority](#)


Incoming traffic to Validation Authority

The Entrust Validation Authority deployment automatically opens the following ports for incoming traffic in the firewall of the host machines.

Target Port	Protocol	Source	Target Service
80	TCP/HTTP	OCSP client	OCSP Responder

Outgoing traffic from Validation Authority

The Validation Authority deployment automatically opens the following ports for outgoing traffic in the firewall of the host machines.

 You can later modify these ports in the solution configuration, as explained in [Configuring and deploying Entrust Validation Authority](#). However, remember to deploy or redeploy Validation Authority after the changes to make them effective and to automatically open the ports.

Target Port	Protocol	Source	Target Service
80	HTTP	CRL shim	HTTP Server
389	LDAP	CRL shim	LDAP Server
8444	TCP/HTTPS	CA Gateway shim	CA Gateway
1433	TCP/HTTPS	Status Feeder and OCSP Responder	SQL Server Database
1792	NTLS	OCSP Responder	Luna Network HSM
1521	TCP/HTTPS	Status Feeder and OCSP Responder	Oracle Database
5432	TCP/HTTPS	Status Feeder and OCSP Responder	PostgreSQL Database
9000-9004	TCP/HTTPS	OCSP Responder	nShield HSM

Reserved subnets

Reserve the following subnets for Cryptographic Security Platform use.

Subnet	Reserved use
10.42.0.0/16	Kubernetes Pods
10.43.0.0/16	Kubernetes ClusterIP Services

✗ Any LAN component utilizing an IP within these ranges will interfere with the operation of Cryptographic Security Platform.

Software requirements

Cryptographic Security Platform supports integration with the the following third-party software.

- [Compliance Manager requirements](#)
- [Database requirements](#)
- [SIEM requirements](#)
- [Web browser requirements](#)

Compliance Manager requirements

Cryptographic Security Platform 1.0.0 integrates with Entrust Cryptographic Security Platform Compliance Manager v 10.4.5.

i See [Compliance Manager](#) for the integration steps.

Database requirements

The Cryptographic Security Platform does not require a database. However, some Entrust solutions have the requirements described in the table below.

- [Database Management System](#)
- [Database storage](#)
- [Database platform](#)
- [Database user permissions](#)
- [Database allowed connections](#)
- [Database SSL certificate](#)
- [Database names](#)

Database Management System

The external databases of Entrust solutions support the following Database Management Systems (DBMSs).

Solution	Oracle	PostgreSQL	Microsoft SQL Server
Certificate Authority	✗	15+	✗

Solution	Oracle	PostgreSQL	Microsoft SQL Server
Certificate Manager	✗	15+	✗
Validation Authority	21.3.0	14.3 or 15.10	2019 CU15
			2022 CU13

Database storage

Calculate the required database storage based on the expected data.

For example, the Certificate Manager solution database requires nearly 1GB for 25,000 certificates and a few weeks of reports.

25,000 certificates x 20 KB/certificate = 500 MB

200 reports x 1 MB/report = 200 MB

Total: 700 MB

Database platform

Check DBMS requirements for the supported platforms. In the case of PostgreSQL, we recommend downloading the official Docker image:

https://hub.docker.com/_/postgres

Database user permissions

The database user must have permissions on the public schema.

For example, to create a Certificate Manager database user with sufficient permissions, connect to PSQL using the default PostgreSQL user and execute the following commands.

```
CREATE USER ${POSTGRES_USER} WITH NOSUPERUSER CREATEDB ENCRYPTED PASSWORD '${POSTGRES_PWD}';
\c postgres ${POSTGRES_USER}
CREATE DATABASE cm;
\c cm ${POSTGRES_USER}
CREATE EXTENSION IF NOT EXISTS pg_trgm;
```

Where:

- `${POSTGRES_USER}` is the database user name selected when [Configuring and deploying Certificate Manager](#).
- `${POSTGRES_PWD}` is the database user password selected when [Configuring and deploying Certificate Manager](#).

Database allowed connections

Restrict database incoming connections to those originating from the Cryptographic Security Platform host.

To restrict incoming connections on a PostgreSQL database

1. Edit the following PostgreSQL configuration file.

```
pg_hba.conf
```

2. Add the following line.

```
hostssl      cm      ${POSTGRES_USER}      <host>      scram-sha-256
```

Where `<host>` is the IP address of the Cryptographic Security Platform host.

Database SSL certificate

In SSL-protected connections with the database, the SSL certificate of the database must include the IP address or hostname Cryptographic Security Platform will use to connect with the database. You can alternatively:

- Set the hostname or IP address in the CN attribute of the certificate subject.
- Set the hostname in a SAN attribute of the `dNSName` type.
- Set the IP address in a SAN attribute of the `iPAddress` type.

✗ Entrust solutions in production mode should always be configured to enforce SSL-protected connections with the database.

Database names

In the Certificate Manager database, names should not use uppercase letters to avoid case sensitivity problems. Unquoted identifiers in SQL syntax are converted to lowercase, which can lead to problems when mapping to a name with uppercase letters.

SIEM requirements

Cryptographic Security Platform can forward logs to the following SIEM (Security Information and Event Management) systems.

- Splunk Enterprise
- Splunk Cloud

Cryptographic Security Platform allows the ingestion of system records via the HTTP Event Collector (HEC) interface.

ℹ See [Managing Log Forwarder](#) for how to enable log-forwarding.

Web browser requirements

Cryptographic Security Platform provides web portals such as the Management Console, Grafana, and the Certificate Manager administration console. These portals support the following web browsers.

Browser	Supported versions
Apple Safari	5 or higher
Google Chrome	8 or higher
Microsoft Edge	The stable versions listed by Microsoft in https://learn.microsoft.com/en-us/deployedge/microsoft-edge-support-lifecycle
Mozilla Firefox	9 or higher

Browser compatibility is quite high, so most versions operate without issue. If there is an issue, we will address it using the latest browser version available for the operating system.

HSM requirements

The following Entrust solutions support a Hardware Security Module (HSM) for cryptographic operations.

- Certificate Authority (CA)
- Timestamping Authority (TSA)
- Validation Authority (EVA)

When integrating a Hardware Security Module (HSM):

- You do not need to install the client drivers because the solution already includes this software. However, these client drivers cannot be updated.
- You cannot use HSMs from different providers simultaneously, meaning that nShield and Thales HSMs cannot coexist within the same deployment.
- You can only use 1/N card sets. A card set of, for example, 2/5 cards is not supported.
- Changing the settings of an Entrust nShield HSM requires the steps described in [Administering nShield HSM integration](#).

See the following table for supported versions.

Hardware	Client driver	Firmware	CA	TSA	VA
Entrust nShield Connect XC	13.6.3	12.60.15 & 12.60.2	✓	✓	✓
Entrust nShield 5c	13.6.3	13.2.4	✓	✓	✓
Thales Luna HSM 7	10.7.0	7.7.1-20	✗	✓	✓

5 Starting up CSP

To start up Cryptographic Security Platform, perform the following operations in a node meeting the [Requirements](#).

- [Downloading the installation files](#)
- [Verifying the downloaded files](#)
- [Installing the image](#)
- [Installing CSP](#)
- [Joining nodes](#)
- [Replacing the default TLS certificate](#)
- [Configuring the proxy](#)
- [Changing the keyboard layout](#)
- [Changing the operating system timezone](#)
- [Configuring time synchronization](#)
- [Manually starting the chrony service](#)
- [Configuring an nShield HSM](#)

Do not perform operating system modifications that are not covered in this guide. Specifically, do not:

- Change file permissions.
- Change partitions or mount points in a different way than documented.
- Change SELinux permissions or configuration.
- Change sysadmin privileges.
- Change the boot loader configuration.
- Change the kernel configuration.
- Change the system locale.
- Create new users.
- Create or modify a crontab. Any automation task must be performed from an external machine accessing the system via SSH.
- Install antivirus, agents, or any other additional software.
- Modify the privileges of the sysadmin administrator.
- Move or delete files.
- Update, modify, or remove operating system packages using mechanisms other than the one provided by Entrust.

Downloading the installation files

See below for instructions on downloading the Cryptographic Security Platform installation files.

To download the Cryptographic Security Platform installation files

1. Log in to the secure trustedcare.entrust.com portal with your customer credentials.
2. Select the **PRODUCTS** tab.
3. Click **Cryptographic Security Platform**.
4. Select the product version.
5. Download the following files.
 - [Cryptographic Security Platform PKI installation files](#)
 - [Cryptographic Security Platform Compliance Manager installation files](#)
 - [Cryptographic Security Platform utility files](#)

Cryptographic Security Platform PKI installation files

Download the Cryptographic Security Platform PKI image suited to your platform.

- PKI Hub 1.1.0 for Amazon Web Services

- PKI Hub 1.1.0 for Azure
- PKI Hub 1.1.0 for VMWare vSphere, Hyper-V and Nutanix

If your current platform is EDM 1.0.0 or Entrust Deployment Manager 2.0.2, download also the following file.

- EDM 2.0.x to PKI Hub upgrade tool

Cryptographic Security Platform Compliance Manager installation files

Download the Cryptographic Security Platform Compliance Manager image suited to your platform.

- Cryptographic Security Platform Compliance Manager 10.4.5 ISO Install
- Cryptographic Security Platform Compliance Manager 10.4.5 OVA Install
- Cryptographic Security Platform Vault 10.4.5 ISO Install
- Cryptographic Security Platform Vault 10.4.5 OVA Install

Download also the following files if you must upgrade from an older version.

- Cryptographic Security Platform Compliance Manager 10.4.5 Upgrade ISO
- Cryptographic Security Platform Vault 10.4.5 Upgrade ISO

Cryptographic Security Platform utility files

Download the utilities required by the different Cryptographic Security Platform products.

- CA Gateway Config Utility
- CEG Power Shell Scripts
- Entrust Proxy for Microsoft CA
- EVA Database Scripts
- Profile Creation Utility for CAGW - Linux
- Profile Creation Utility for CAGW - Windows x64

Verifying the downloaded files


Generate a digest to verify the integrity of each downloaded installation and documentation file. On a Windows machine, you can run the following command line to generate the digest of the `<file>` file.

```
certutil -hashfile <file> SHA256
```

For example:

```
>certutil -hashfile c:\Users\john\Downloads\pki-hub-1.1.0.iso SHA256
SHA256 hash of c:\Users\john\Downloads\pki-hub-1.1.0.iso:
d841d57c7e1433622d219a7dea405935ff593a6831c1c94ba1c9dbde763b5baa
CertUtil: -hashfile command completed successfully.
```

On the **SOFTWARE DOWNLOADS** and **DOCUMENTATION** tabs, click the **Digest** column for each downloaded file and verify the displayed SHA-256 digest matches the generated one.

 Although TrustedCare also displays the MD5 and SHA-1 digests, we recommend using only the SHA-256 algorithm, which is more secure. Further versions of TrustedCare will remove the MD5 and SHA-1 algorithms from the digest list.

Installing the image

See below for instructions on installing and configuring the Cryptographic Security Platform image on the supported platforms.

- [Installing the ISO image on an HCI](#)
- [Installing the RAW image on AWS](#)
- [Installing the VHD image on Azure](#)

Repeat the installation and configuration steps for each node you want to add to your Cryptographic Security Platform cluster.



Contact Entrust support for instructions on installing Cryptographic Security Platform on platforms not listed in this guide.

Installing the ISO image on an HCI

See below for installing and configuring the Cryptographic Security Platform ISO image on different HCI (hyper-converged infrastructure) providers.

- [Installing the ISO image on Microsoft Hyper-V](#)
- [Installing the Cryptographic Security Platform ISO image on Nutanix](#)
- [Installing the Cryptographic Security Platform ISO image on Proxmox](#)
- [Installing the Cryptographic Security Platform ISO image on VMware vSphere](#)
- [Configuring a Cryptographic Security Platform ISO image installation](#)

Installing the ISO image on Microsoft Hyper-V

See below for installing and configuring a Cryptographic Security Platform ISO image on a virtual machine hosted by a Microsoft Hyper-V hypervisor.

To install the Cryptographic Security Platform image in Hyper-V

1. Download the ISO image, as explained in [Downloading the installation files](#).
2. Follow the below steps.
 - [Creating a virtual machine on Hyper-V](#)
 - [Configuring an Cryptographic Security Platform virtual machine on Hyper-V](#)
 - [Configuring the boot mode on Microsoft Hyper-V](#)
 - [Starting an Cryptographic Security Platform machine on Hyper-V](#)
3. Configure the image installation as explained in [Configuring a Cryptographic Security Platform ISO image installation](#).

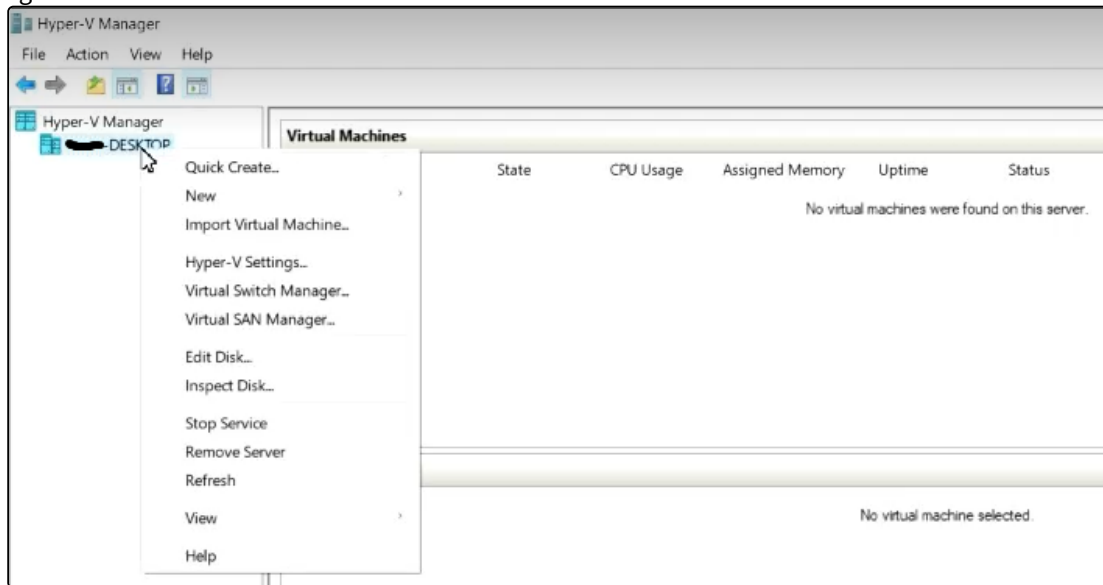
Creating a virtual machine on Hyper-V

Install the Cryptographic Security Platform ISO image as a new Hyper-V virtual machine.

To create a Cryptographic Security Platform virtual machine on Hyper-V

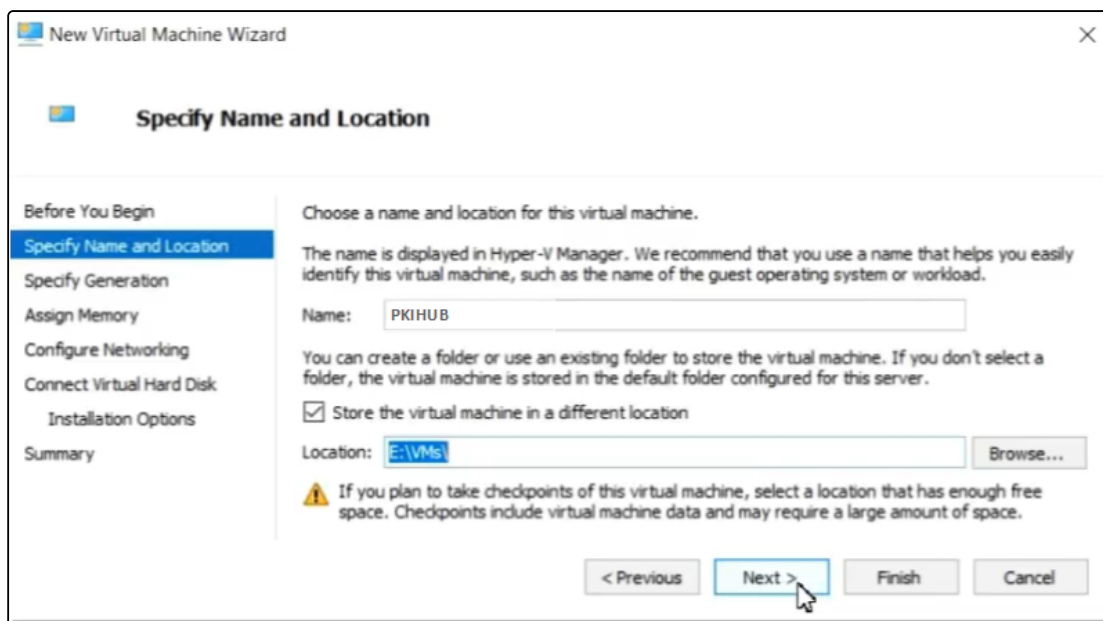
1. Open the **Hyper-V Manager** console.

2. Right-click on a server name and select **New**.



3. In each step of the **New Virtual Machine Wizard** wizard, select the values described below.

- [Specify Name and Location](#)
- [Specify Generation](#)
- [Assign Memory](#)
- [Configure Network](#)
- [Connect Virtual Hard Disk](#)
- [Installation Options](#)
- [Summary](#)



Specify Name and Location

Configure the following settings.

Field	Value
Name	Enter a name for the new virtual machine. For example, "CSP".
Store the virtual machine in a different location	Enable this checkbox.
Location	Select a folder for the virtual machine file.

Specify Generation

Configure the following settings.

Field	Value
Choose the generation of this virtual machine	Select Generation 1 .

Assign Memory

Configure the following settings.

Field	Value
Startup memory	Select the RAM size stated in Machine requirements .
Use Dynamic Memory for this virtual machine	Enable this checkbox.

Configure Network

Configure the following settings.

Field	Value
Connection	Select a connection with a network meeting the Network requirements .

Connect Virtual Hard Disk

Under **Create virtual hard disk**, configure the root and `etcd` disks described in [Machine requirements](#).

Field	Root disk	etcd disk
Name	The name of the virtual machine file	The name of the virtual machine file
Location	The folder for storing the virtual machine file	The folder for storing the virtual machine file
Size	At least 1 TiB	At least 15 GiB

Installation Options

Configure the following settings.

Field	Value
Install an operating system from a bootable CD/DVD-ROM	Enable this radio button.
Image file (.iso)	Select the location of the ISO file described in Downloading the installation files .

Summary

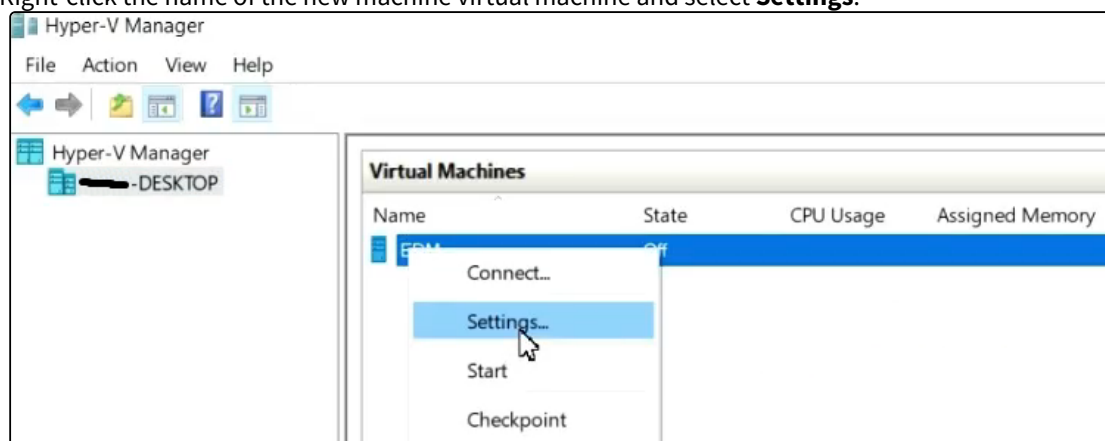
Review the selected settings and click **Finish** to complete the virtual machine creation.

Configuring an Cryptographic Security Platform virtual machine on Hyper-V

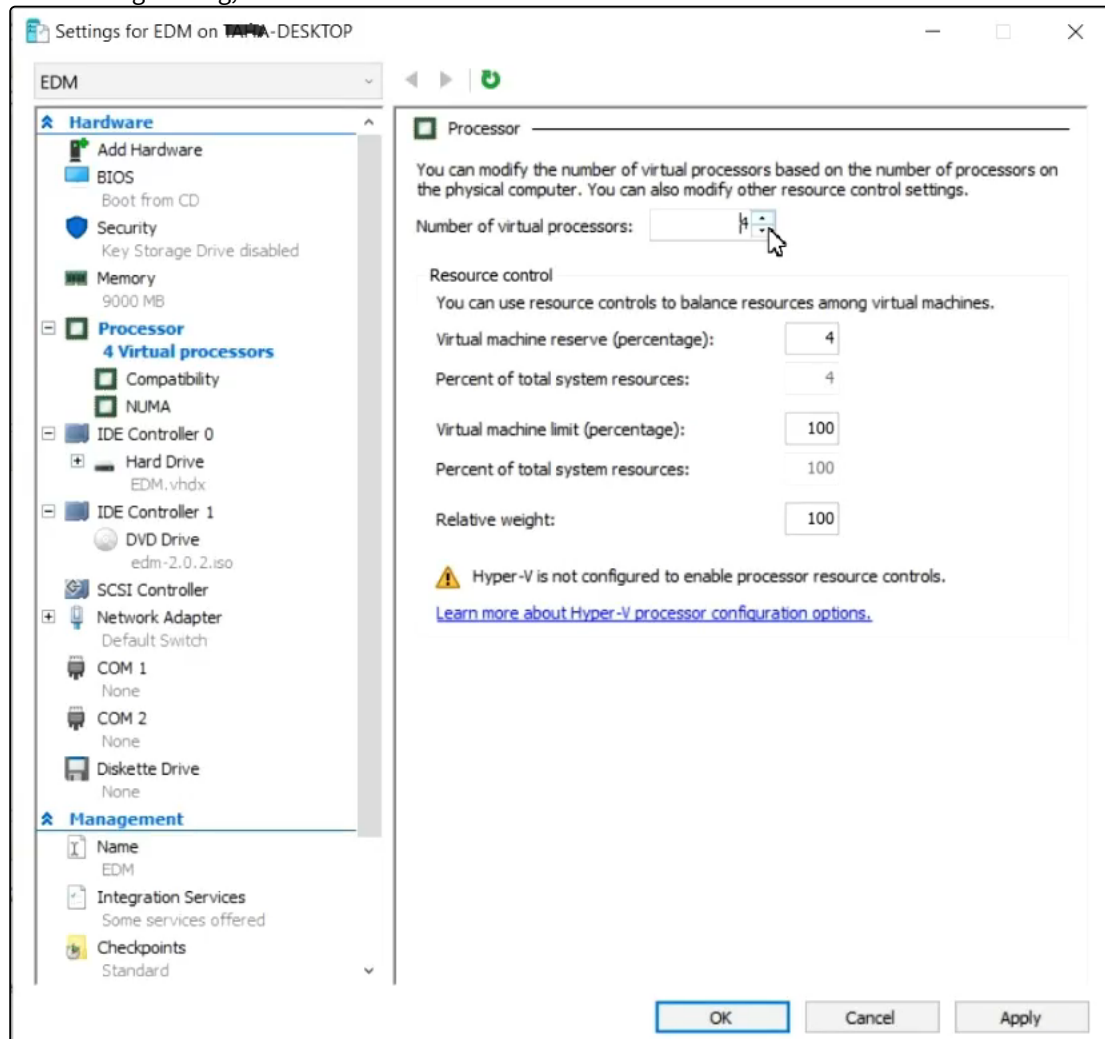
Once created, complete the new Cryptographic Security Platform virtual machine as follows.

To configure an Cryptographic Security Platform virtual machine on Hyper-V

1. Open the **Hyper-V Manager** console.
2. Right-click the name of the new machine virtual machine and select **Settings**.



3. In the settings dialog, select **Processors** under **Hardware**.



4. In the **Number of virtual processors** field, select the cores stated in [Machine requirements](#).
5. Click **Apply**.

Configuring the boot mode on Microsoft Hyper-V

Depending on the selected boot mode (BIOS or UEFI), perform the following steps before booting the machine.


- [Selecting the boot order in the BIOS settings](#)
- [Importing the ELRepo key for UEFI boot](#)

Selecting the boot order in the BIOS settings

As explained in [Machine requirements](#), Cryptographic Security Platform requires two disks. Therefore, if your machine uses BIOS boot firmware, ensure the biggest disk is placed first in the boot order. Otherwise, the system will not boot.

Importing the ELRepo key for UEFI boot

If your machine uses the UEFI boot firmware, you must import and enroll the ELRepo key.


 For more details on enrolling the ELRepo key, see <https://elrepo.org/wiki/doku.php?id=secureboot>

To enroll the ELRepo key

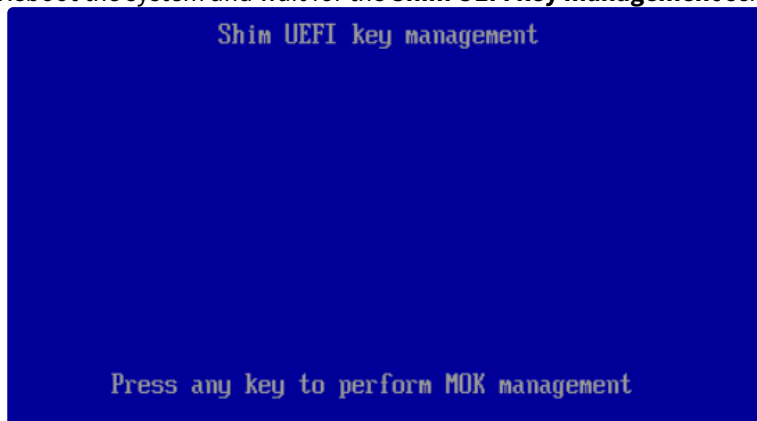
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

```
sudo mokutil --import /etc/pki/elrepo/SECURE-BOOT-KEY-elrepo.org.der
```

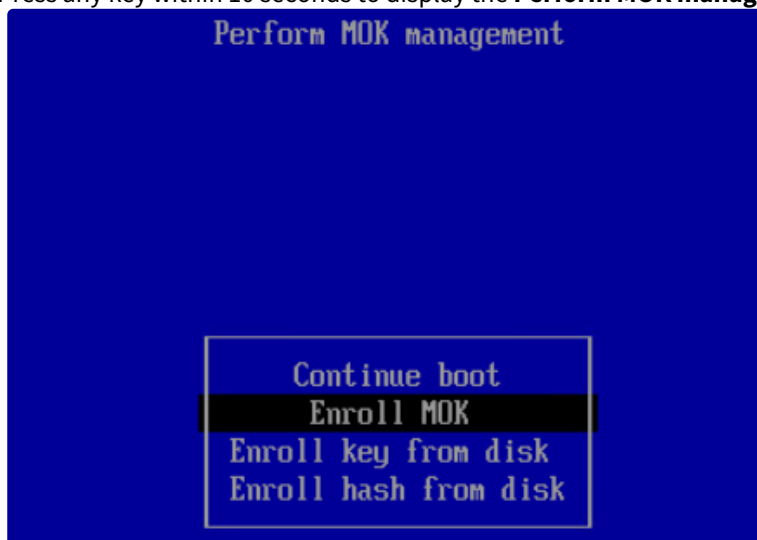
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

 The following operations do not support a remote console like an SSH client.

6. Reboot the system and wait for the **Shim UEFI key management** screen.



7. Press any key within 10 seconds to display the **Perform MOK management** dialog.



8. Select **Enroll MOK** and press **Enter** to display the **Enroll MOK** dialog.

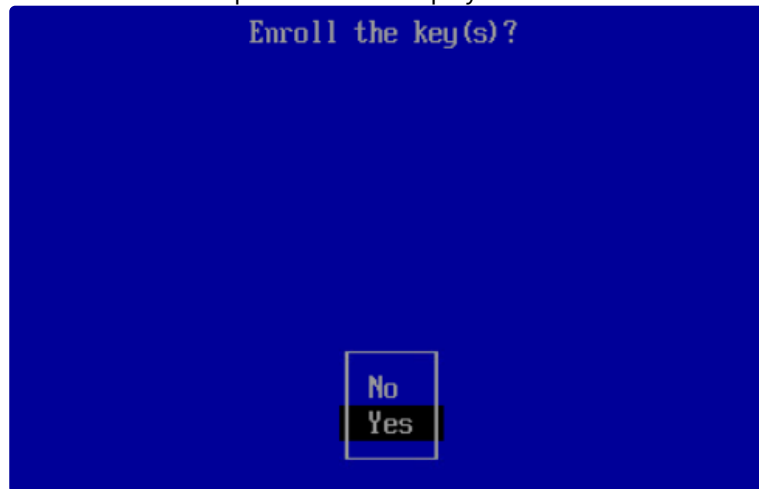


9. Select **View key 0** and press **Enter** to display the key information.

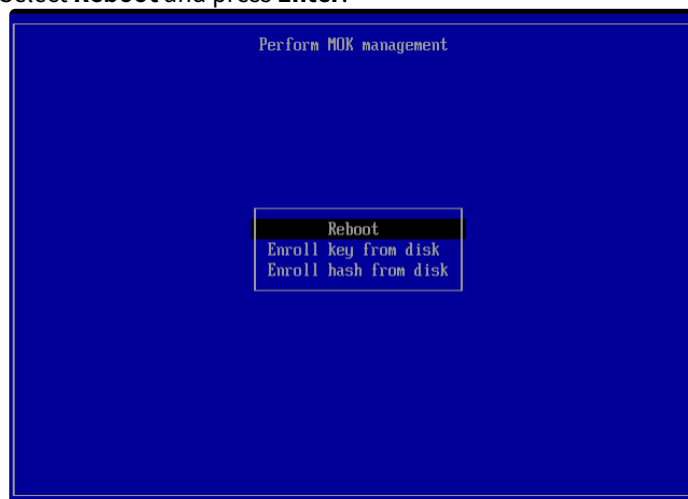


10. Check that the serial number is 0xe9d471cfb4fe136c .
11. Check that the SHA1 fingerprint is e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7 .
12. Press ESC to return to the **Enroll MOK** dialog.

13. Select **Continue** and press **Enter** to display the enrollment confirmation dialog.



14. Select **Yes** and press **Enter** to display the password form.
15. Type the key password you selected when importing the ELRepo key.
16. Press **Enter** to return to the **Perform MOK management** dialog.
17. Select **Reboot** and press **Enter**.



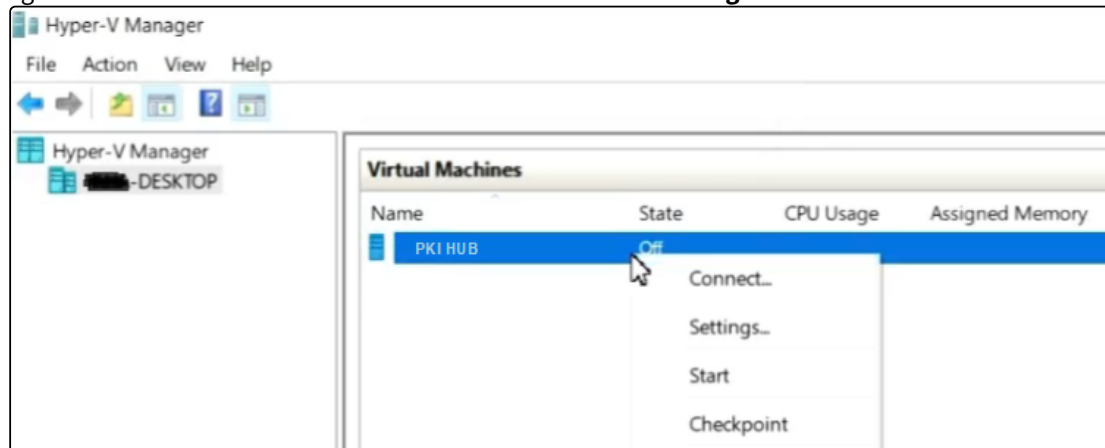
Starting an Cryptographic Security Platform machine on Hyper-V

Start the new virtual machine and open a session as Cryptographic Security Platform administrator.

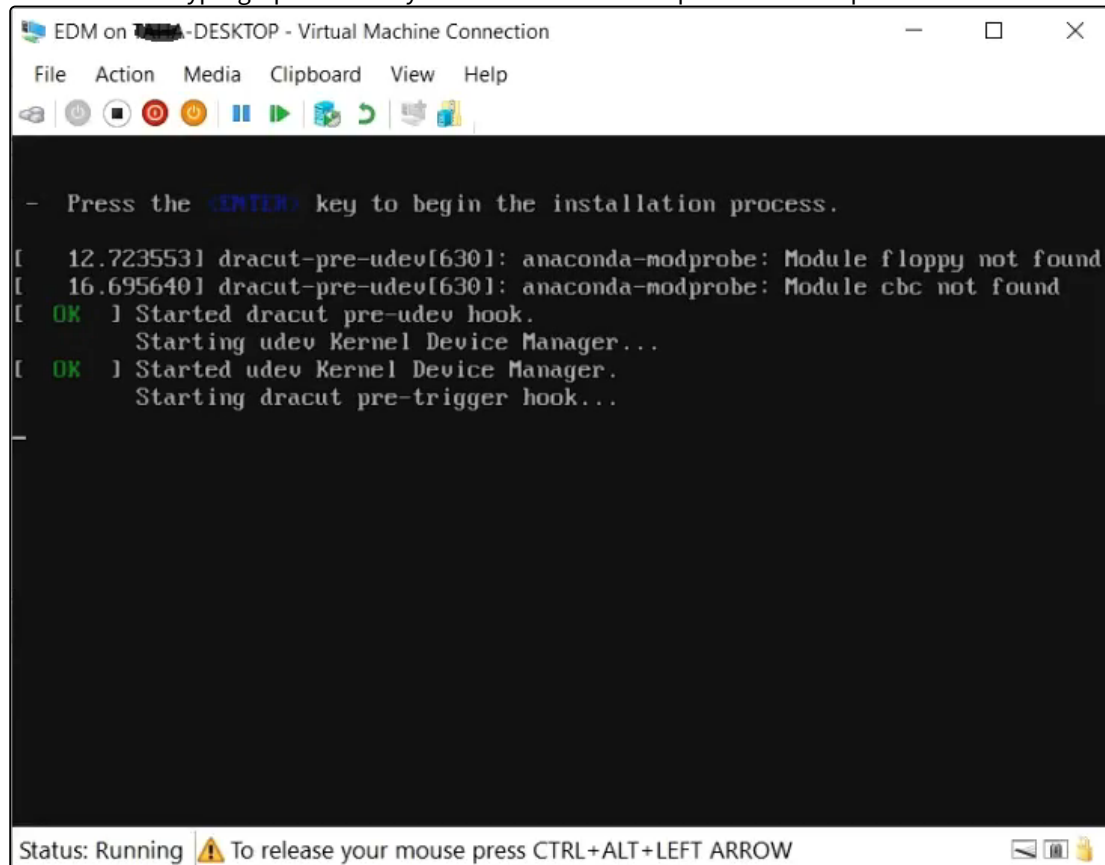
To start an Cryptographic Security Platform virtual machine on Hyper-V

1. Open the **Hyper-V Manager** console.

2. Right-click the name of the new virtual machine and select **Settings**.



3. Wait while the Cryptographic Security Platform machine completes the start process.



4. Login with the `sysadmin` username and the `changeme` password.
5. When prompted, change the initial password with a password meeting the requirements described in [Password policy CIS benchmarks](#).

Installing the Cryptographic Security Platform ISO image on Nutanix

See below for installing and configuring an Cryptographic Security Platform image on a virtual machine hosted by a Nutanix hypervisor.

i The installation and deployment steps in this guide have been tested with Nutanix version 6.5.5.7 LTS.

To install and configure the Cryptographic Security Platform image on Nutanix

1. Download the ISO image as explained in [Downloading the installation files](#).
2. Follow the below steps.
 - [Uploading the Cryptographic Security Platform image to Nutanix](#)
 - [Creating an Cryptographic Security Platform virtual machine on Nutanix](#)
 - [Configuring the boot mode on Nutanix](#)
3. Configure the image installation as explained in [Configuring a Cryptographic Security Platform ISO image installation](#).

Uploading the Cryptographic Security Platform image to Nutanix

Upload the Cryptographic Security Platform ISO image to Nutanix, as explained in one of the following sections.

- [Uploading the Cryptographic Security Platform ISO image with Nutanix Prism Element](#)
- [Uploading the Cryptographic Security Platform image file with Nutanix Prism Central](#)
- [Importing the Cryptographic Security Platform image to Nutanix Prism Central](#)

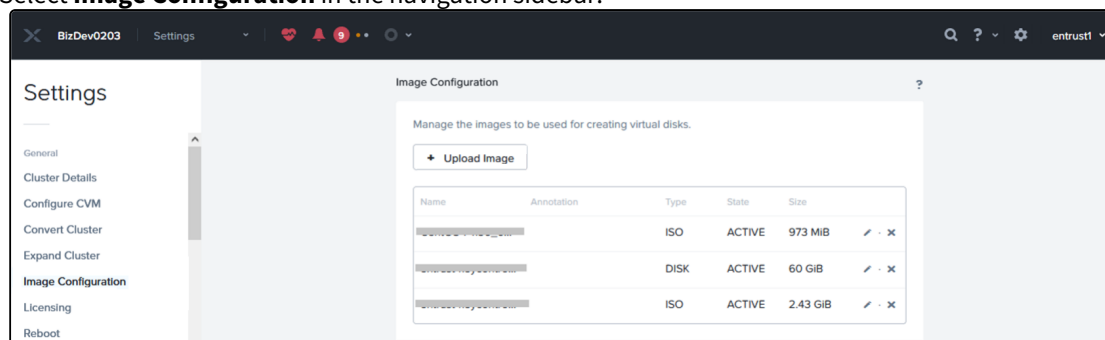
i As explained in [Creating a cluster of Cryptographic Security Platform virtual machines with Nutanix Prism Central](#), uploading the image to Nutanix Prism Central allows you to create a cluster of Cryptographic Security Platform machines.

Uploading the Cryptographic Security Platform ISO image with Nutanix Prism Element

Follow the steps below to upload the Cryptographic Security Platform ISO image using the Nutanix Prism Element portal.

To upload the Cryptographic Security Platform ISO image with Nutanix Prism Element

1. Log into the Prism Element web portal of your Nutanix infrastructure.
2. Select the **Settings** gear icon on the top toolbar.
3. Select **Image Configuration** in the navigation sidebar.



- Click **Upload Image** to display the **Create Image** dialog.



The 'Create Image' dialog box contains the following fields and options:

- Name:** PKI_HUB
- Annotation:** (empty)
- Image Type:** ISO
- Storage Container:** default-container-13584
- Image Source:**
 - ☐ From URL
 - ☒ Upload a file: Choose File edm-2.0.2.iso
- Buttons:** Back, Cancel, Save

- Enter a unique image name in the **Name** field. For example: **CSP**.
- Write an optional description in the **Annotation** field.
- Select **ISO** in the **Image Type** field.
- Select the required container in the **Storage Container** field.
- Click **Upload file** and select the file with ISO extension obtained when [Downloading the installation files](#).
- Click **Save** and wait while the file uploads.

❌ Do not refresh the page while the file uploads.

- Check the image **State** is **ACTIVE** on the image list.



Image Name	Created By	Image Type	State	Size	Actions
cryptosecure-1.0.0	Created By OpenShift	ISO	ACTIVE	340 KiB	✎ ✖
cryptosecure-1.0.0	Created By OpenShift	DISK	ACTIVE	16 GiB	✎ ✖
cryptosecure-1.0.0	Created By OpenShift	DISK	ACTIVE	16 GiB	✎ ✖
PKI_HUB		DISK	ACTIVE	60 GiB	✎ ✖
cryptosecure-1.0.0		DISK	ACTIVE	81 GiB	✎ ✖
cryptosecure-1.0.0		DISK	ACTIVE	81 GiB	✎ ✖
cryptosecure-1.0.0		DISK	INACTIVE	-	✎ ✖
PKI_HUB		ISO	ACTIVE	5.36 GiB	✎ ✖
cryptosecure-1.0.0			ACTIVE	100 GiB	✎ ✖
cryptosecure-1.0.0			ACTIVE	100 GiB	✎ ✖

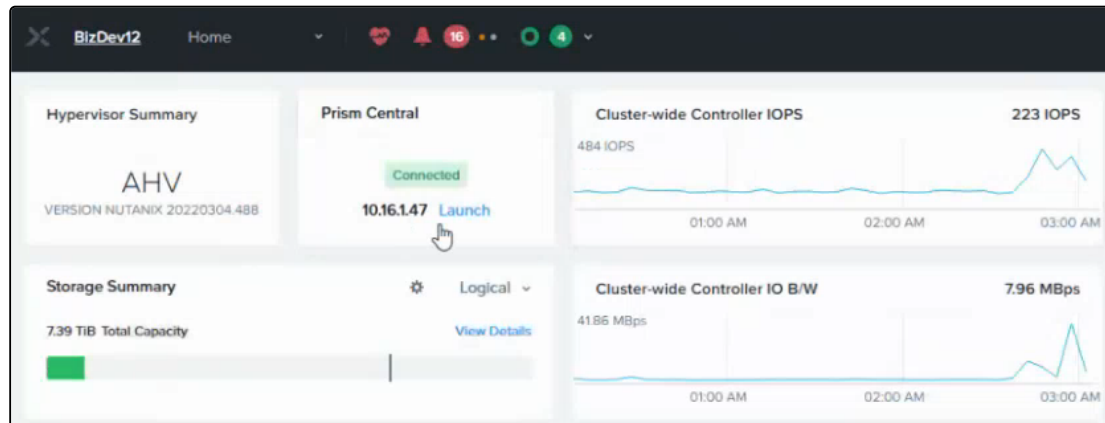
Uploading the Cryptographic Security Platform image file with Nutanix Prism Central

Follow the steps below for uploading the Cryptographic Security Platform image using the Nutanix Prism Central portal.

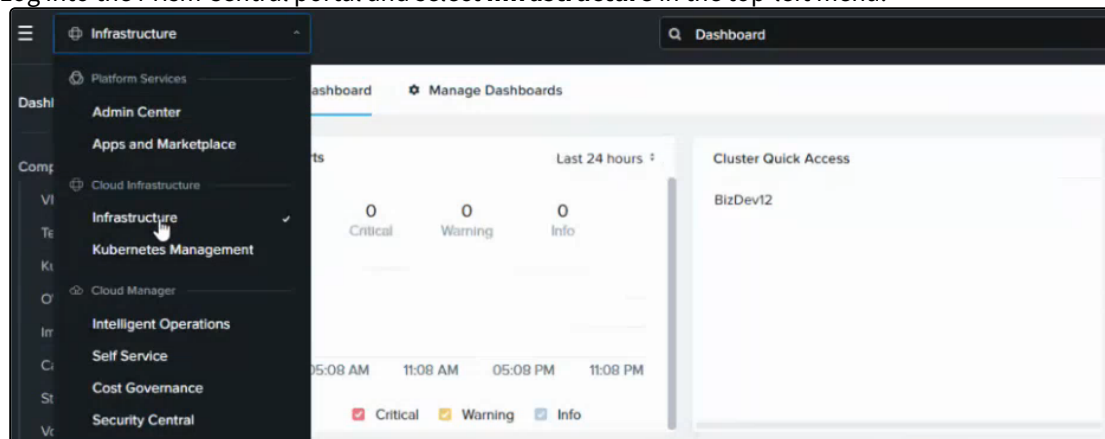
To upload the Entrust Cryptographic Security Platform image file with Nutanix Prism Central

- Log into your Nutanix Prism element web portal.

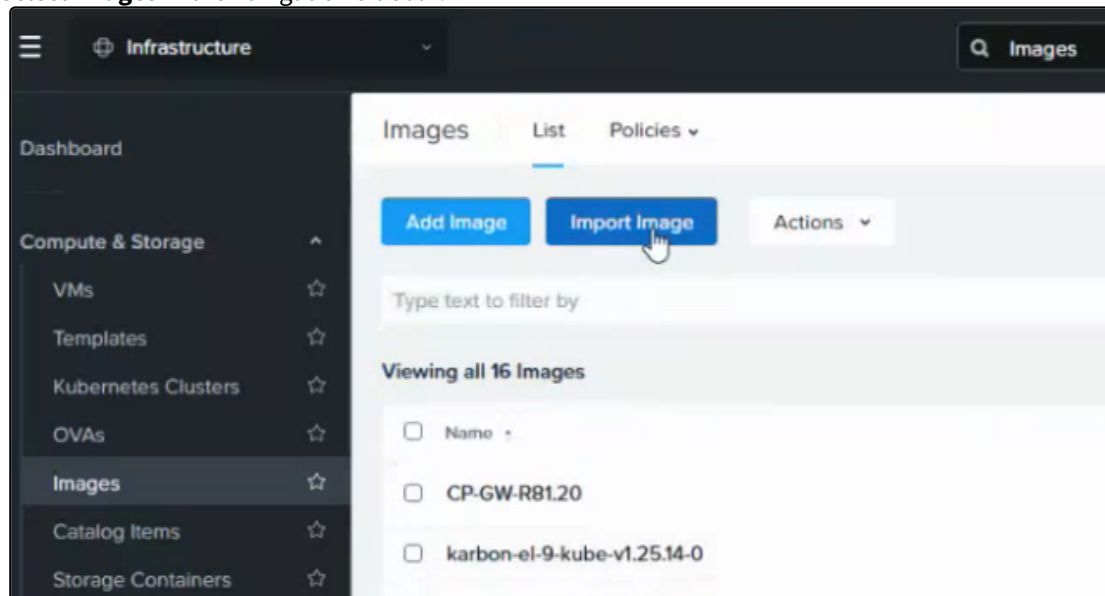
- Click **Launch** under **Prism Central**.



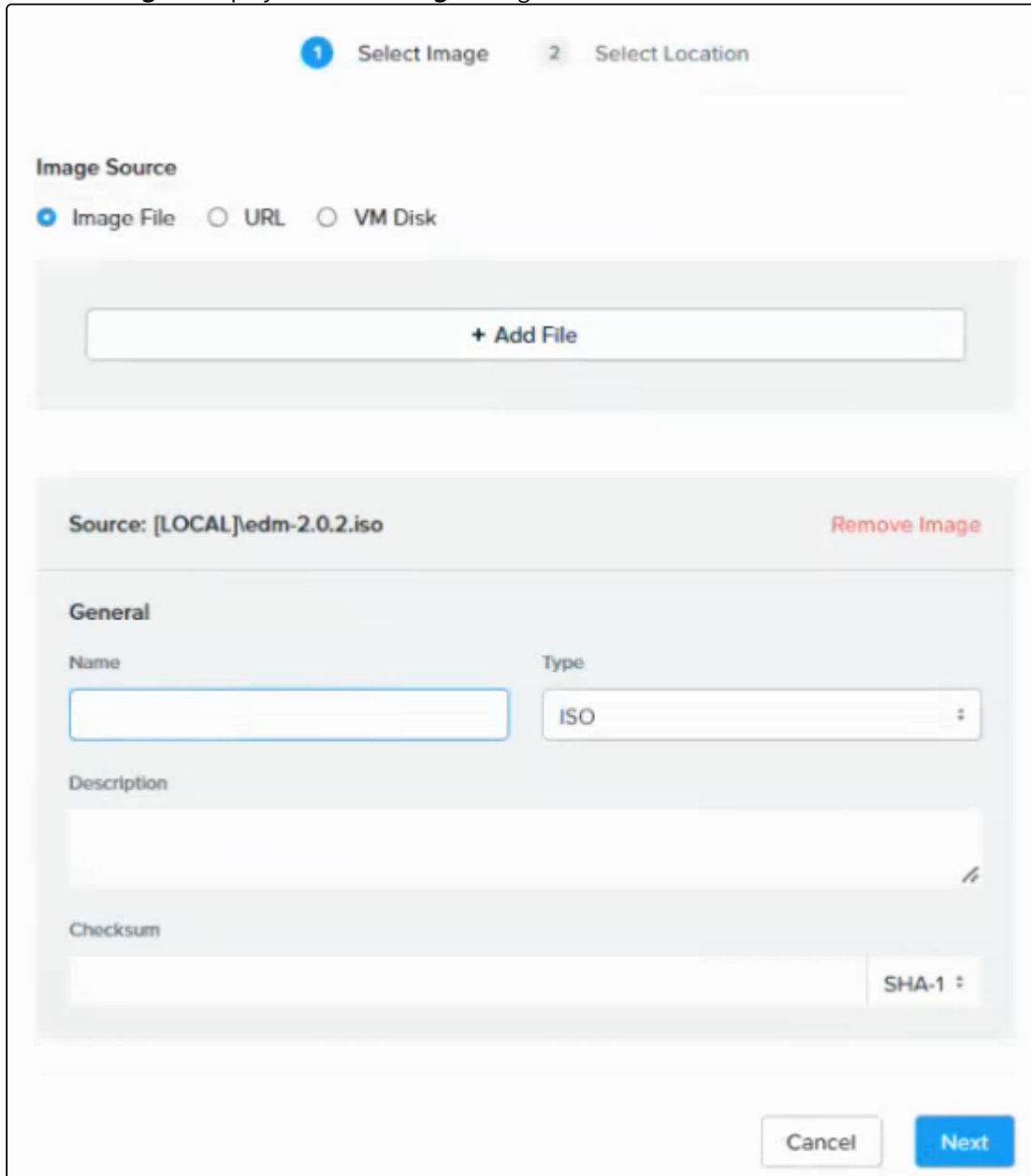
- Log into the Prism Central portal and select **Infrastructure** in the top-left menu.



- Select **Images** in the navigation sidebar.



5. Click **Add Image** to display the **Select image** dialog.



The dialog box is titled "Select Image" and has two tabs: "1 Select Image" (active) and "2 Select Location".

Image Source

☒ Image File ☐ URL ☐ VM Disk

+ Add File

Source: [LOCAL]edm-2.0.2.iso Remove Image

General

Name

Type

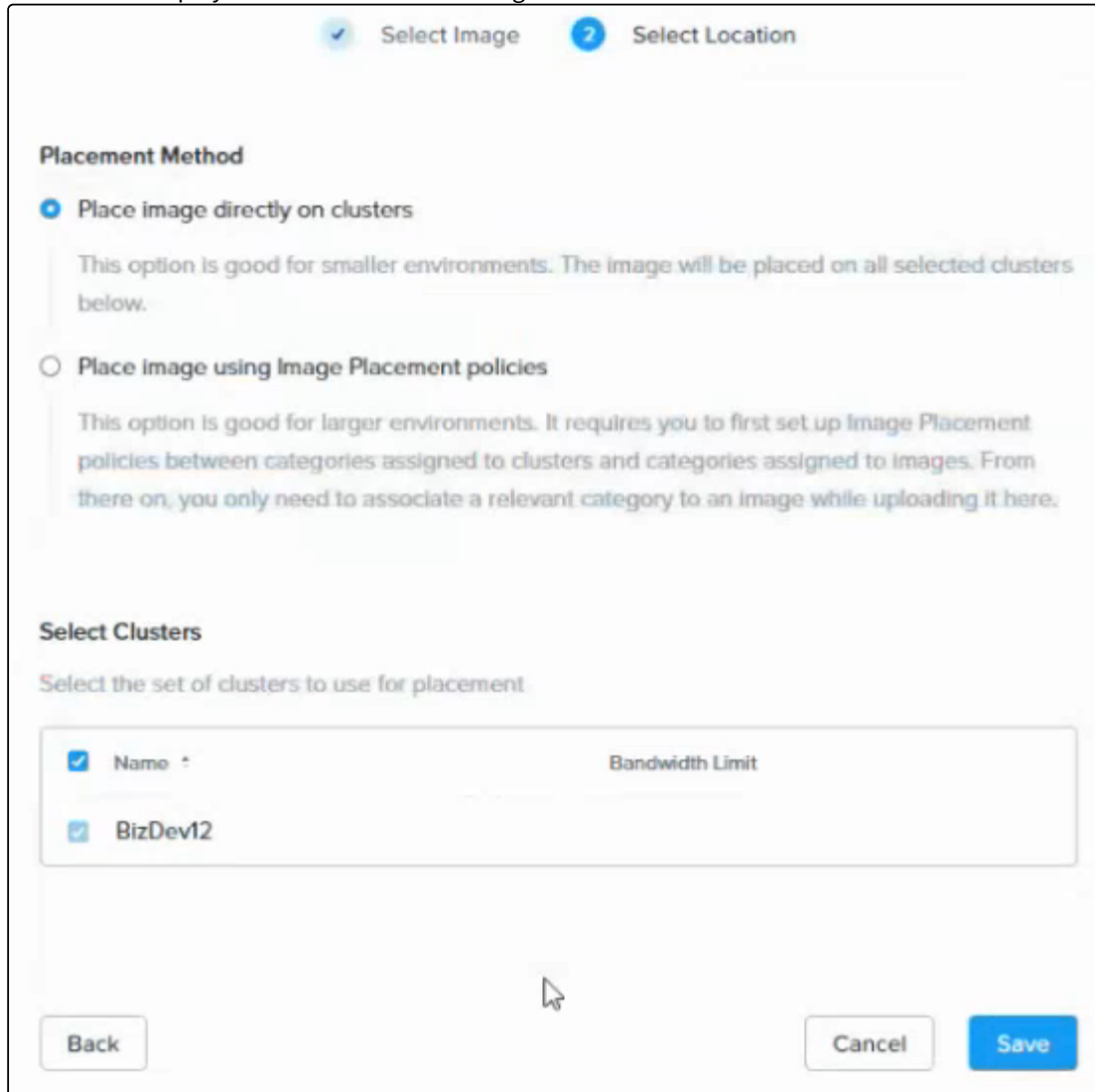
Description

Checksum SHA-1

Cancel Next

6. Select **Image File** under **Image source**.
7. Click **+ Add File**
8. Select the file obtained when [Downloading the installation files](#).
9. Enter a unique image name in the **Name** field. For example: **CSP**.
10. Select **ISO** in the **Type** drop-down list.
11. Write an optional description in the **Description** field.

12. Click **Next** to display the **Select Location** dialog.



Placement Method

☒ Place image directly on clusters

This option is good for smaller environments. The image will be placed on all selected clusters below.

☐ Place image using Image Placement policies

This option is good for larger environments. It requires you to first set up Image Placement policies between categories assigned to clusters and categories assigned to images. From there on, you only need to associate a relevant category to an image while uploading it here.

Select Clusters

Select the set of clusters to use for placement.

<input checked="" type="checkbox"/> Name	Bandwidth Limit
<input checked="" type="checkbox"/> BizDev12	

Back Cancel Save

13. Under **Select Clusters**, select the Nutanix cluster that will host the uploaded image.
14. Click **Save** and wait while the upload task completes.

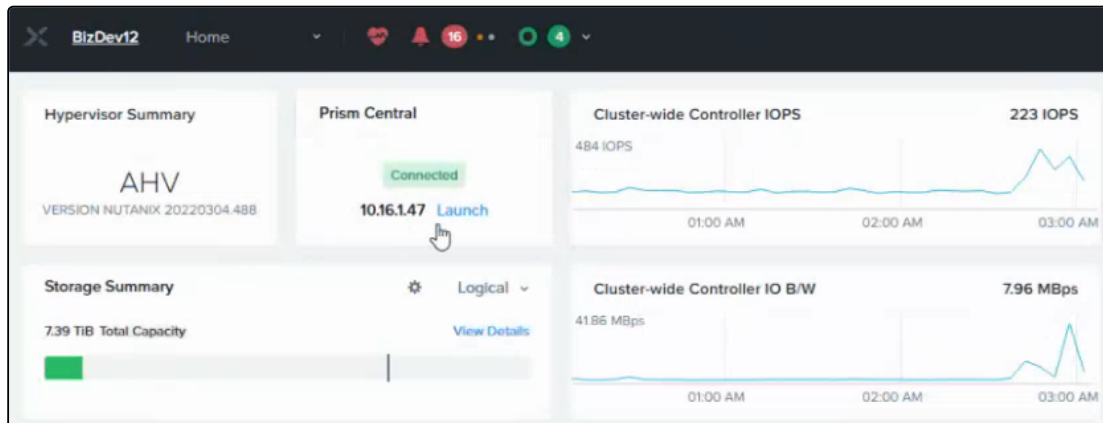
Importing the Cryptographic Security Platform image to Nutanix Prism Central

If already uploaded as explained in [Uploading the Cryptographic Security Platform ISO image with Nutanix Prism Element](#), you can import the Cryptographic Security Platform image on Nutanix Prism Central.

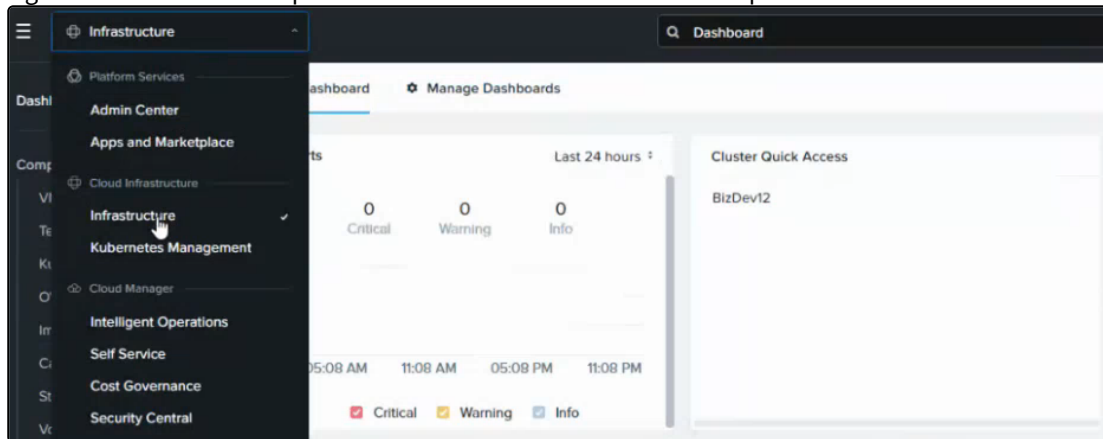
To import the Entrust Cryptographic Security Platform image from Nutanix Prism Element to Nutanix Prism Central

1. Log into your Nutanix Prism element web portal.

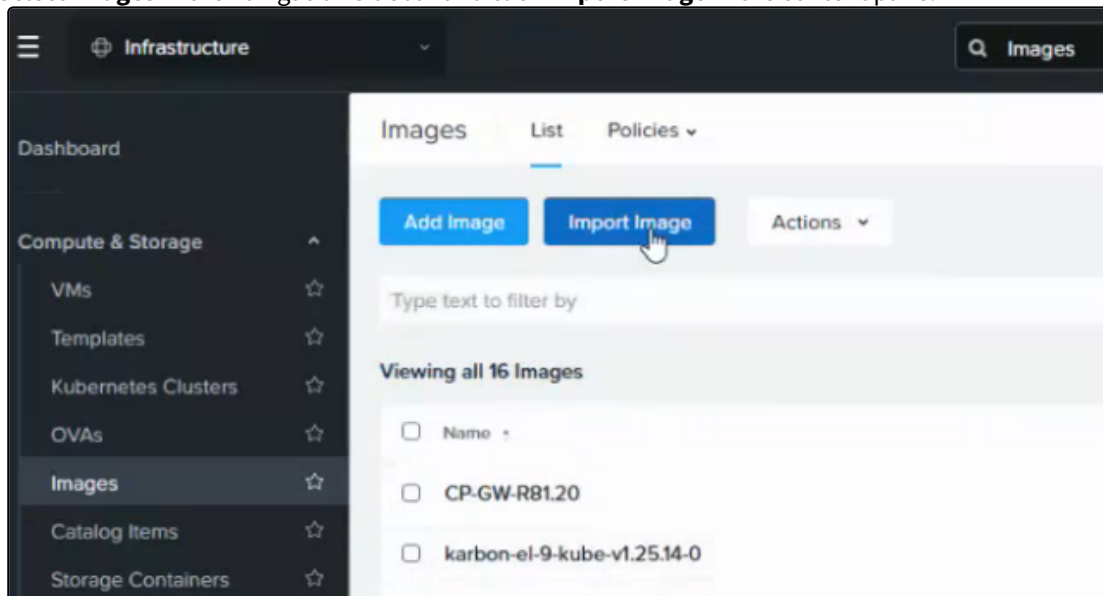
- Click **Launch** under **Prism Central**.



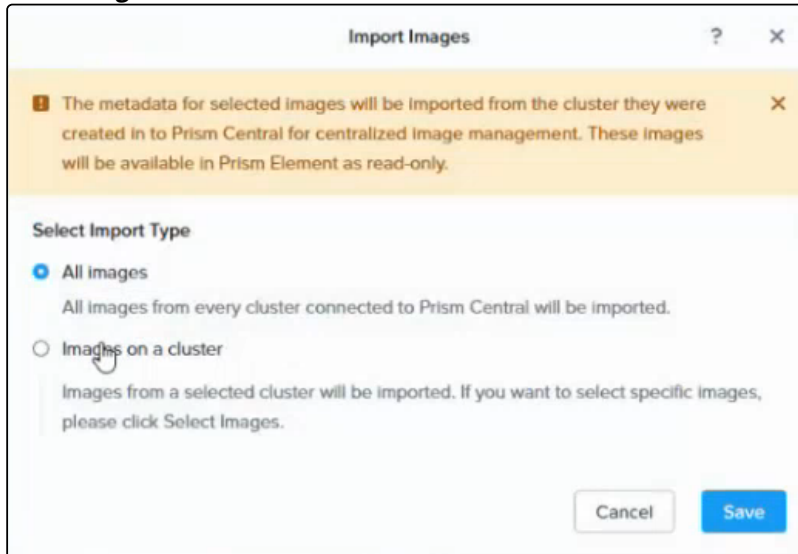
- Log into the Prism Central portal and select **Infrastructure** in the top-left menu.



- Select **Images** in the navigation sidebar and click **Import Image** in the content pane.



5. Select **Images on a cluster**.



Import Images ? X

! The metadata for selected images will be imported from the cluster they were created in to Prism Central for centralized image management. These images will be available in Prism Element as read-only. X

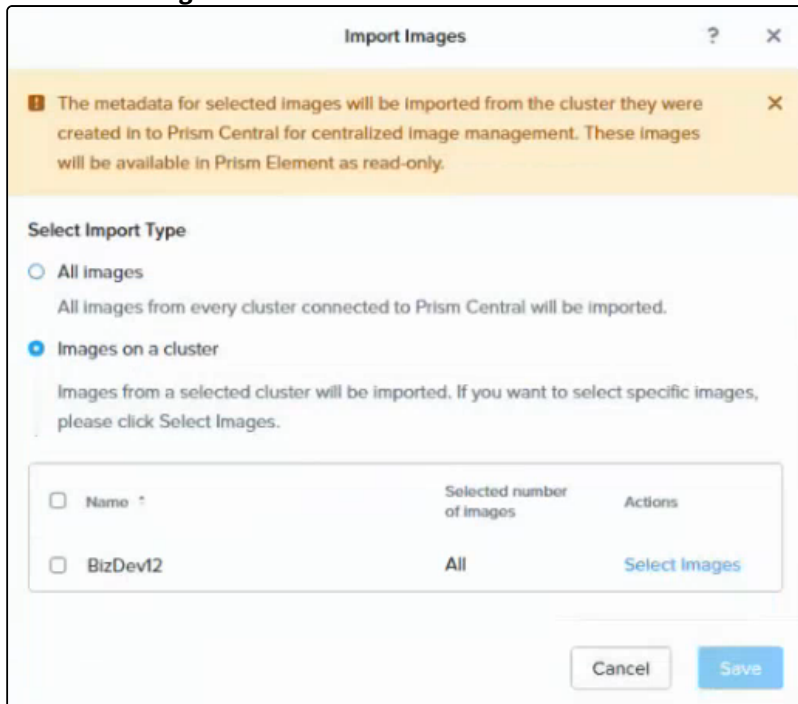
Select Import Type

☒ All images
All images from every cluster connected to Prism Central will be imported.

☐ Images on a cluster
Images from a selected cluster will be imported. If you want to select specific images, please click Select Images.

Cancel Save

6. Click **Select Images** for one of the listed clusters.



Import Images ? X

! The metadata for selected images will be imported from the cluster they were created in to Prism Central for centralized image management. These images will be available in Prism Element as read-only. X

Select Import Type

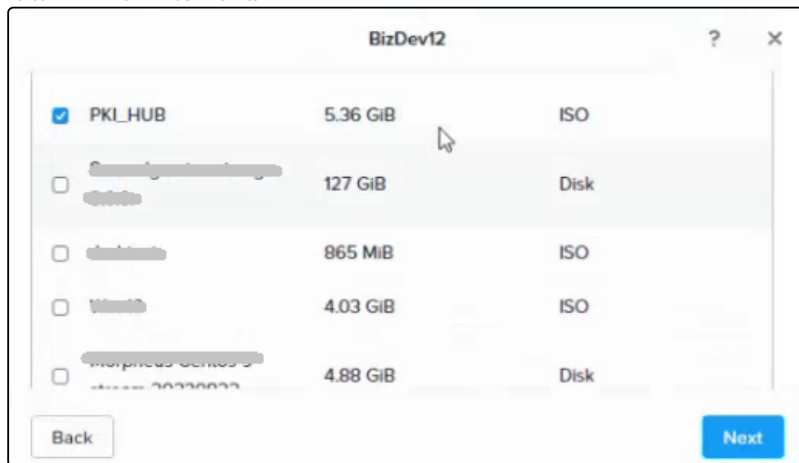
☐ All images
All images from every cluster connected to Prism Central will be imported.

☒ Images on a cluster
Images from a selected cluster will be imported. If you want to select specific images, please click Select Images.

<input type="checkbox"/> Name *	Selected number of images	Actions
<input type="checkbox"/> BizDev12	All	Select Images

Cancel Save

7. Select the image previously imported in [Uploading the Cryptographic Security Platform ISO image with Nutanix Prism Element](#).



8. Click **Next** and wait while the import task completes.

Creating an Cryptographic Security Platform virtual machine on Nutanix

You have the following options to create an Cryptographic Security Platform virtual image on Nutanix.

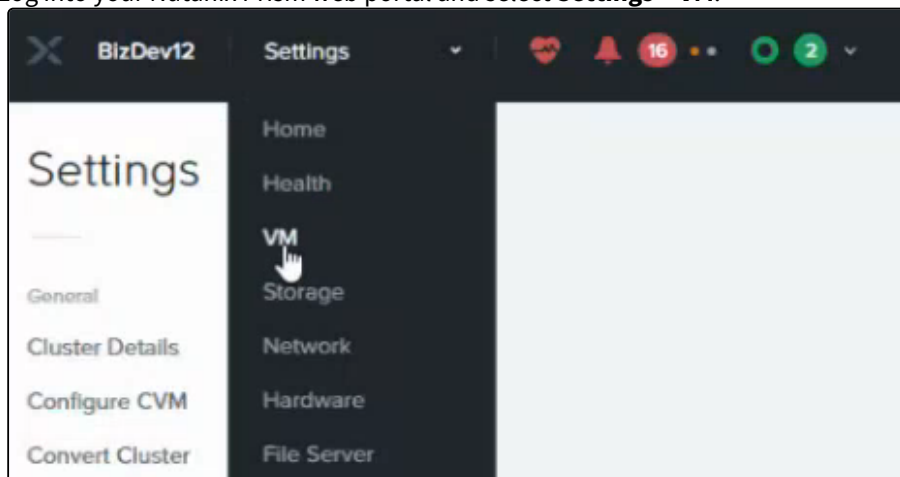
- [Creating a Cryptographic Security Platform virtual machine with Nutanix Prism Element](#)
- [Creating a cluster of Cryptographic Security Platform virtual machines with Nutanix Prism Central](#)

Creating a Cryptographic Security Platform virtual machine with Nutanix Prism Element

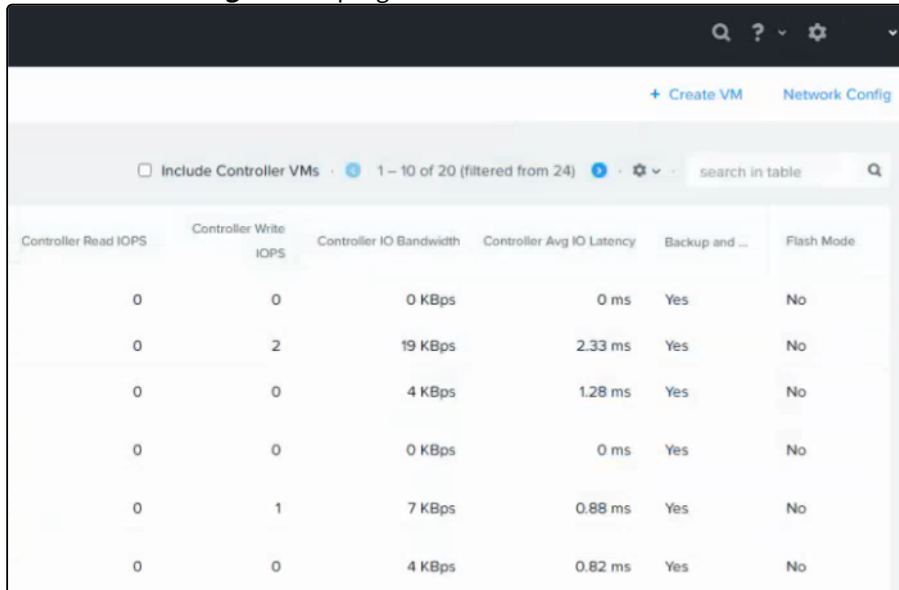
Follow the steps below to deploy the Cryptographic Security Platform image as a virtual image with the Nutanix Prism Element portal.

To create a Cryptographic Security Platform virtual machine with Nutanix Prism Element

1. Log into your Nutanix Prism web portal and select **Settings > VM**.




- Click **Network Config** in the top-right corner.



Controller Read IOPS	Controller Write IOPS	Controller IO Bandwidth	Controller Avg IO Latency	Backup and ...	Flash Mode
0	0	0 KBps	0 ms	Yes	No
0	2	19 KBps	2.33 ms	Yes	No
0	0	4 KBps	1.28 ms	Yes	No
0	0	0 KBps	0 ms	Yes	No
0	1	7 KBps	0.88 ms	Yes	No
0	0	4 KBps	0.82 ms	Yes	No

- Create a new network or configure an existing one to meet the [Network requirements](#).
- Click **+ Create VM** in the top-right corner.
- Configure the following settings in the **Create VM** dialog.
 - [General Configuration](#)
 - [Compute Details](#)
 - [Boot Configuration](#)
 - [Disks](#)
 - [Network Adapters \(NIC\)](#)



Create VM

General Configuration

Name:

Description:

Timezone:

Use UTC timezone for Linux VMs and local timezone for Windows VMs.

☐ Use this VM as an agent VM

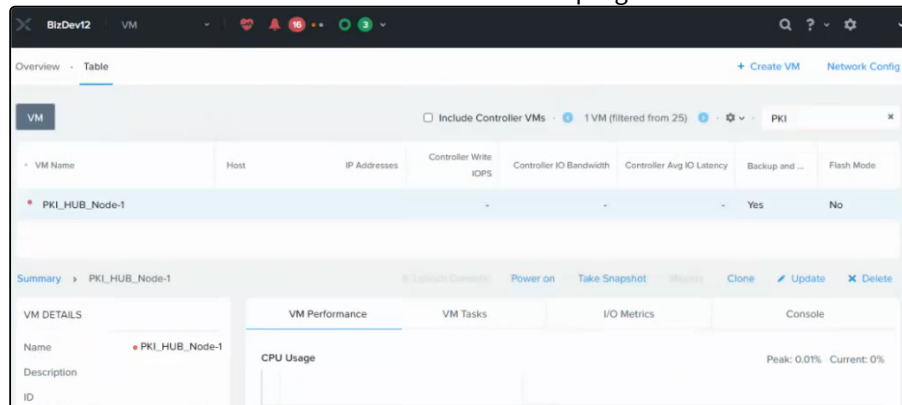
Compute Details

vCPU(s):

Number Of Cores Per vCPU:

- Click **Save** and wait while the virtual machine is created.

- Write the name of the new virtual machine on the top-right search box.



- Select the new virtual machine on the content pane and click **Power On** in the bottom menu.
- Click **Launch Console** in the bottom menu and wait while Cryptographic Security Platform starts.
- Log in with the `sysadmin` username and the `changeme` password.
- When prompted, change the initial password with a password meeting the requirements described in [Password policy CIS benchmarks](#).

General Configuration

Configure the following settings.

Setting	Value
Name	Enter a unique name for the new virtual machine. For example, CSP_NODE_1 .
Description	Enter an optional description for the new virtual machine.
Timezone	Select a timezone for the new virtual machine.
Use the VM as an agent VM	Do not enable this checkbox.

Compute Details

Configure the following settings.

Setting	Value
vCPU(s)	Enter the number of cores recommend in Machine requirements .
Number Of Cores Per vCPU	Select 1.

Setting	Value
Memory	Enter the RAM size recommended in Machine requirements .

Boot Configuration

Select either **Legacy Boot** or **UEFI**.

Disks

Click the pencil edit button for **CD-ROM** and configure the following settings in the **Update Disk** dialog,

Setting	Value
Operation	Select Clone from Image Service .
Bus Type	Select SATA .
Image	Select the name previously assigned to the Cryptographic Security Platform image when Uploading the Cryptographic Security Platform ISO image with Nutanix Prism Element .

Click **+ Add New Disk** to successively configure the root and `etcd` disks described in [Machine requirements](#).

Setting	Root disk	etcd disk
Type	Disk	Disk
Operation	Allocate on Storage Container	Allocate on Storage Container
Bus Type	SCSI	SCSI
Storage Container	The container for the new virtual machine	The container for the new virtual machine
Size	At least 1 TiB	At least 15 GiB
Index	Next Available	Next Available

Network Adapters (NIC)

Click **+ Add New NIC** and configure the following settings in **Create NIC**.

Setting	Value
Subnet Name	Select a subnet meeting the Network requirements .
Network Connection Status	Select Connected .

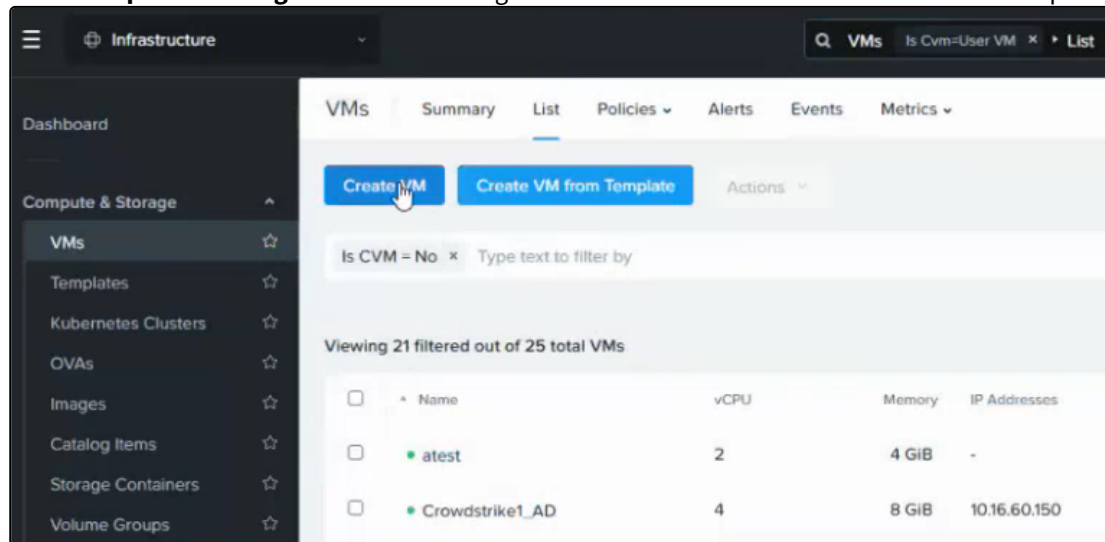
Click **+ Set Affinity** to select the host that will run the virtual machine.

Creating a cluster of Cryptographic Security Platform virtual machines with Nutanix Prism Central

Follow the steps below to deploy a cluster of multiple Cryptographic Security Platform virtual machines.

To a cluster of Cryptographic Security Platform virtual machines with Nutanix Prism Central

1. Log into the Nutanix Prism Central web portal.
2. Select **Compute & Storage > VMs** in the navigation sidebar and click **Create VM** in the content pane.



3. Fill in the forms on each page of the **Create VM** wizard.
 - [Configuration](#)
 - [Resources](#)
 - [Management](#)
 - [Review](#)
4. Click **Create VM**.

Configuration

Configure the following settings in the **Configuration** page of the **Create VM** wizard.

Setting	Value
Name	Enter a unique name for the new virtual machines.
Description	Enter an optional description for the new virtual machines.

Setting	Value
Cluster	Select the Nutanix cluster that will host the virtual machines.
Number of VMs	Select the number of virtual machines you want to create.
CPU	Enter the number of cores recommend in Machine requirements .
Cores Per CPU	Select 1
Memory	Enter the RAM size recommended in Machine requirements .

Resources

In the **Resources** page of the **Create VM** wizard, click **Attach Disk** and configure the following settings.

Setting	Value
Type	Select CD-ROM .
Operation	Select Clone from Image .
Image	Select the image imported or uploaded in Uploading the Cryptographic Security Platform image to Nutanix .
Bus Type	Select SATA .

Click again **Attach Disk** and configure the following settings in the **Attach Disk** dialog.

Setting	Value
Type	Select Disk .
Operation	Select Allocate on Storage Container .
Storage Container	Select a storage container for the disk of the Cryptographic Security Platform virtual machine.
Capacity	Select at least 1 TiB (1024 GiB) as explained in Machine requirements .
Bus Type	Select SCSI .

Under **Network**, click **Attach to Subnet** and select a subnet meeting the [Requirements](#).

Under **Boot Configuration**, select either **Legacy Boot** or **UEFI**.

Management

In the **Management** page of the **Create VM** wizard, click the **Timezone** drop-down list and select a timezone for the new virtual machine.

Review

In the **Review** page of the **Create VM** wizard, check the settings of the new virtual machine and edit them if required.

Configuring the boot mode on Nutanix

Depending on the selected boot mode (BIOS or UEFI), perform the following steps before booting the machine.


- [Selecting the boot order in the BIOS settings](#)
- [Importing the ELRepo key for UEFI boot](#)

Selecting the boot order in the BIOS settings

As explained in [Machine requirements](#), Cryptographic Security Platform requires two disks. Therefore, if your machine uses BIOS boot firmware, ensure the biggest disk is placed first in the boot order. Otherwise, the system will not boot.

Importing the ELRepo key for UEFI boot

If your machine uses the UEFI boot firmware, you must import and enroll the ELRepo key.


 For more details on enrolling the ELRepo key, see <https://elrepo.org/wiki/doku.php?id=secureboot>

To enroll the ELRepo key

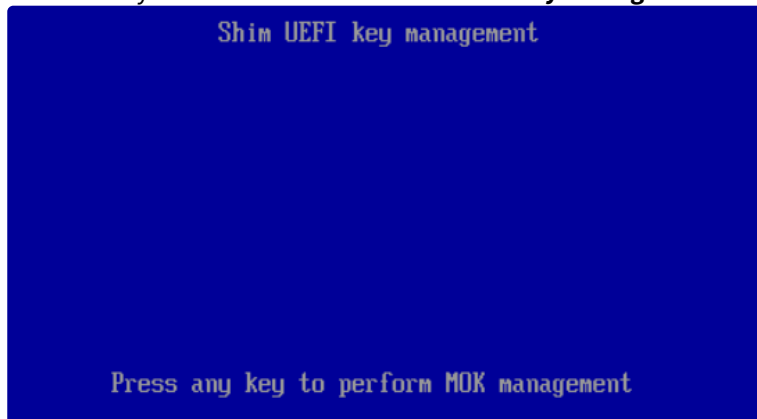
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

```
sudo mokutil --import /etc/pki/elrepo/SECURE-BOOT-KEY-elrepo.org.der
```

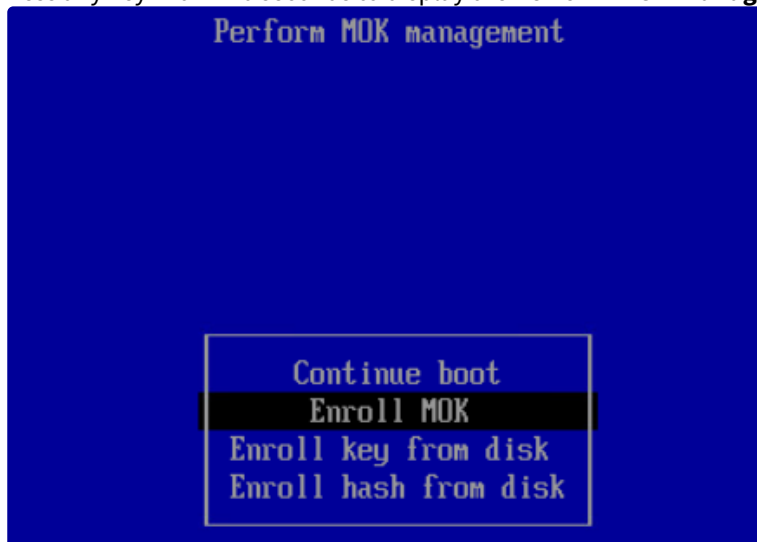
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

 The following operations do not support a remote console like an SSH client.

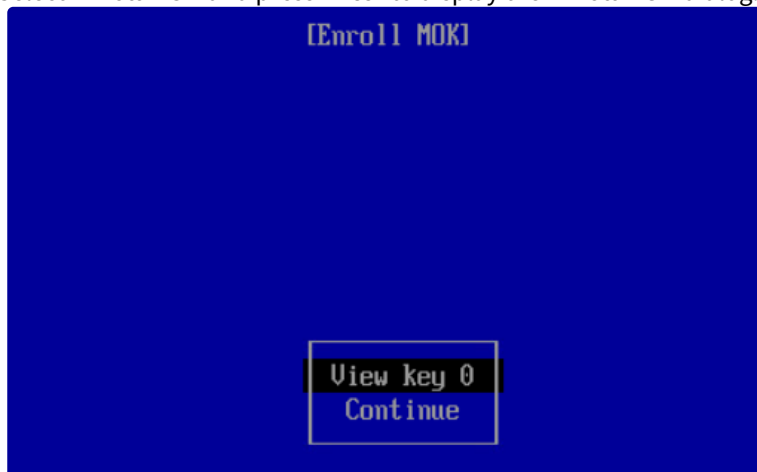
6. Reboot the system and wait for the **Shim UEFI key management** screen.



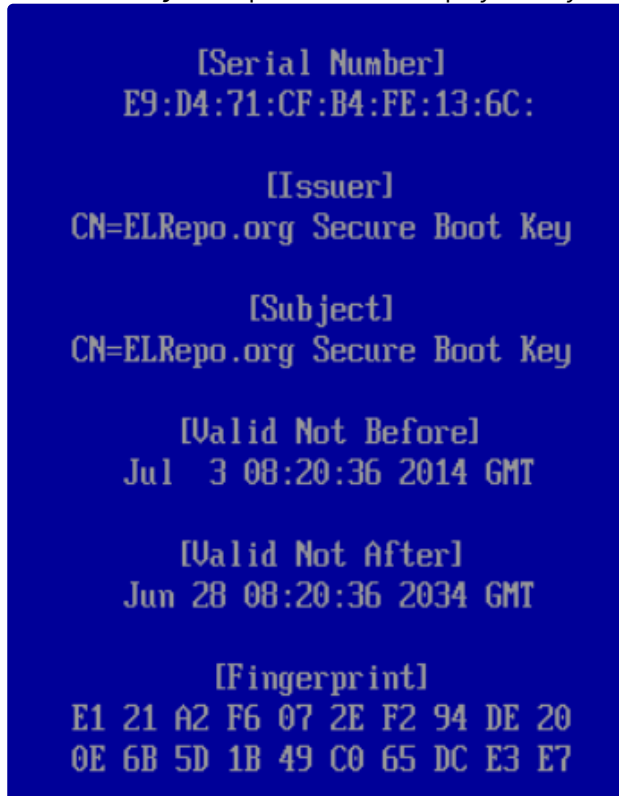
7. Press any key within 10 seconds to display the **Perform MOK management** dialog.



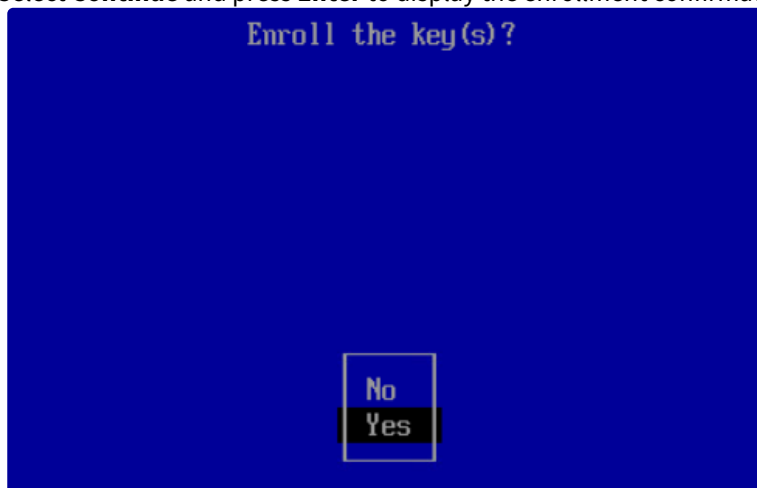
8. Select **Enroll MOK** and press **Enter** to display the **Enroll MOK** dialog.



9. Select **View key 0** and press **Enter** to display the key information.

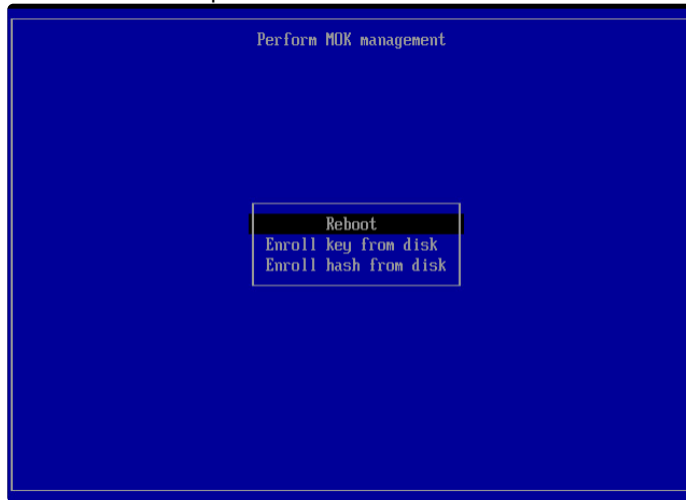


10. Check that the serial number is 0xe9d471cfb4fe136c .
11. Check that the SHA1 fingerprint is e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7 .
12. Press ESC to return to the **Enroll MOK** dialog.
13. Select **Continue** and press **Enter** to display the enrollment confirmation dialog.



14. Select **Yes** and press **Enter** to display the password form.
15. Type the key password you selected when importing the ELRepo key.
16. Press **Enter** to return to the **Perform MOK management** dialog.

17. Select **Reboot** and press **Enter**.



Installing the Cryptographic Security Platform ISO image on Proxmox

See below for installing and configuring the Cryptographic Security Platform image on a virtual machine hosted in Proxmox Virtual Environment.

To install and configure the Cryptographic Security Platform image on Proxmox Virtual Environment

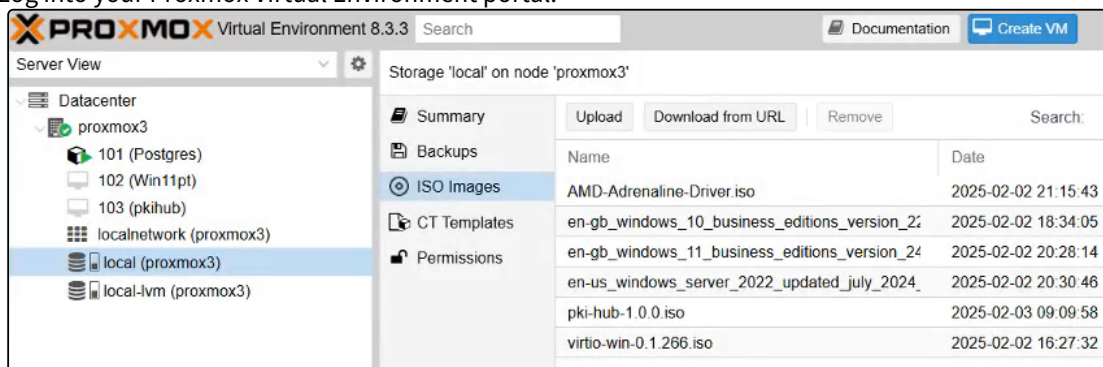
1. Download the ISO image, as explained in [Downloading the installation files](#).
2. Follow the below steps.
 - [Creating an virtual machine on Proxmox](#)
 - [Configuring the boot mode on Promox](#)
 - [Logging into Cryptographic Security Platform on Proxmox](#)
3. Configure the image installation as explained in [Configuring a Cryptographic Security Platform ISO image installation](#).

Creating an virtual machine on Proxmox

Follow the steps below to install the Cryptographic Security Platform ISO image in Proxmox Virtual Environment.

To create an Cryptographic Security Platform virtual machine on Proxmox Virtual Environment

1. Log into your Proxmox Virtual Environment portal.



2. Select a "local" node of your datacenter.
3. Click **Upload** in the menu bar.
4. Select the Cryptographic Security Platform ISO file in the **Upload** dialog.

5. Click the **Upload** button, and wait while the ISO file uploads.
6. Click the **Create VM** button to display the machine creation wizard.
7. In each step of this wizard, select the values described below.
 - [General](#)
 - [OS](#)
 - [System](#)
 - [Disks](#)
 - [CPU](#)
 - [Memory](#)
 - [Network](#)
8. In the navigation tree, select the identifier of the new machine.
9. Click the **Console** command to launch the machine.

General

Configure the following settings on this tab.

Field	Value
Note	The node on which to create the Virtual Machine
VM ID	The internal identifier of the new Virtual Machine
Name	A friendly name for the new Virtual Machine
Resource Pool	A resource pool to which the new Virtual Machine will belong. Optional value.

OS

On this tab:

1. Select the **Use CD/DVD disc image file (iso)** radio button.
2. Select **local** in **Storage**.
3. Select the uploaded ISO file.

System

On this tab, you can leave the default values.

Disks

On this tab, configure two disks with the requirements described in [Machine requirements](#).

 Click the **+Add** button to add the second disk.

CPU

On this tab, select the number of cores described in [Machine requirements](#).

Memory

On this tab, select the memory size described in [Machine requirements](#).

Network

On this tab, you can leave the default values.

Configuring the boot mode on Promox

Depending on the selected boot mode (BIOS or UEFI), perform the following steps before booting the machine.


- [Selecting the boot order in the BIOS settings](#)
- [Importing the ELRepo key for UEFI boot](#)

Selecting the boot order in the BIOS settings

As explained in [Machine requirements](#), Cryptographic Security Platform requires two disks. Therefore, if your machine uses BIOS boot firmware, ensure the biggest disk is placed first in the boot order. Otherwise, the system will not boot.

Importing the ELRepo key for UEFI boot

If your machine uses the UEFI boot firmware, you must import and enroll the ELRepo key.


 For more details on enrolling the ELRepo key, see <https://elrepo.org/wiki/doku.php?id=secureboot>

To enroll the ELRepo key

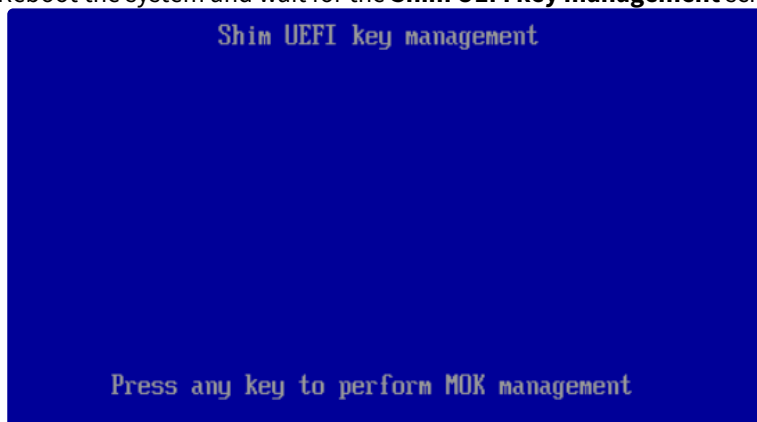
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

```
sudo mokutil --import /etc/pki/elrepo/SECURE-BOOT-KEY-elrepo.org.der
```

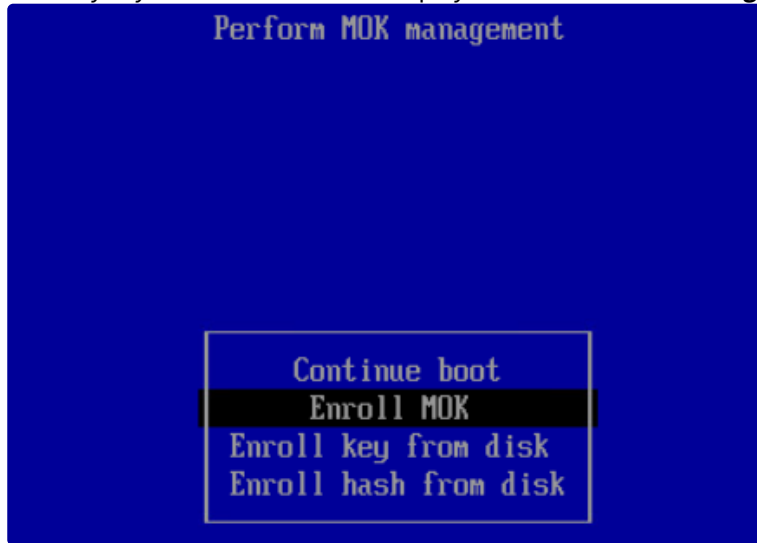
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

 The following operations do not support a remote console like an SSH client.

6. Reboot the system and wait for the **Shim UEFI key management** screen.



7. Press any key within 10 seconds to display the **Perform MOK management** dialog.



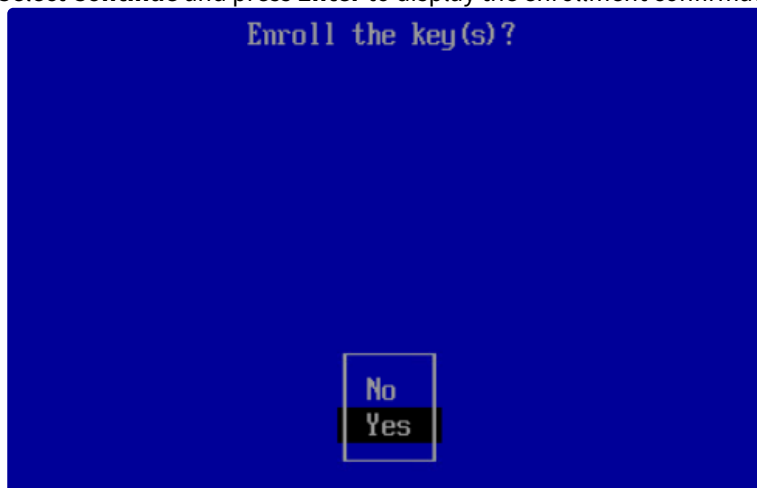
8. Select **Enroll MOK** and press **Enter** to display the **Enroll MOK** dialog.



9. Select **View key 0** and press **Enter** to display the key information.

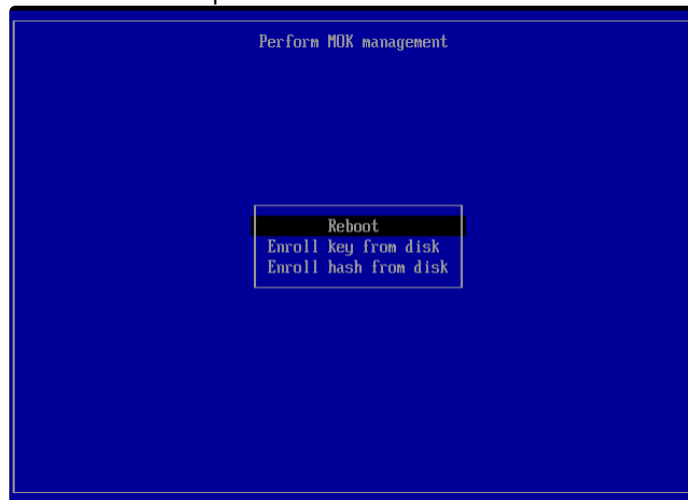


10. Check that the serial number is 0xe9d471cfb4fe136c .
11. Check that the SHA1 fingerprint is e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7 .
12. Press ESC to return to the **Enroll MOK** dialog.
13. Select **Continue** and press **Enter** to display the enrollment confirmation dialog.



14. Select **Yes** and press **Enter** to display the password form.
15. Type the key password you selected when importing the ELRepo key.
16. Press **Enter** to return to the **Perform MOK management** dialog.

17. Select **Reboot** and press **Enter**.



Logging into Cryptographic Security Platform on Proxmox

After installing the image on the machine, open a local or SSH session as the Cryptographic Security Platform administrator.

Name	Initial password
sysadmin	changeme

When prompted, change the initial password with a password meeting the requirements described in [Password policy CIS benchmarks](#).

Installing the Cryptographic Security Platform ISO image on VMware vSphere

See below for installing and configuring the Cryptographic Security Platform image on a virtual machine hosted in VMware vSphere.

To install and configure the Cryptographic Security Platform image on VMware vSphere

1. Download the ISO image, as explained in [Downloading the installation files](#).
2. Follow the below steps.
 - [Creating an Entrust Cryptographic Security Platform virtual machine on VMware vSphere](#)
 - [Configuring the boot mode on VMware vSphere](#)
 - [Logging into Cryptographic Security Platform on a VMware vSphere machine](#)
3. Configure the image installation as explained in [Configuring a Cryptographic Security Platform ISO image installation](#).

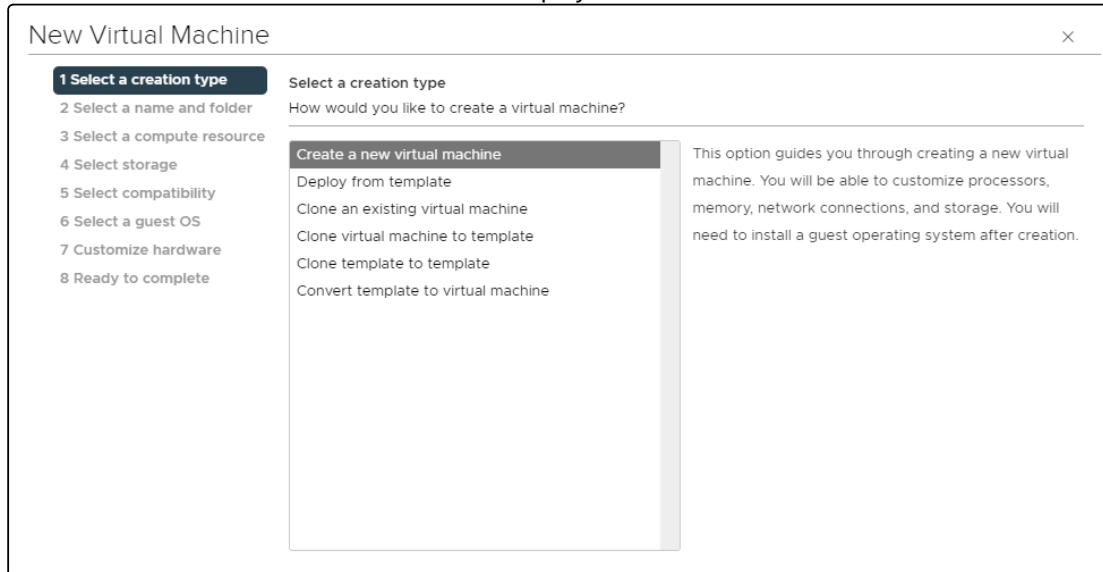
Creating an Entrust Cryptographic Security Platform virtual machine on VMware vSphere

Follow the steps below to install the Cryptographic Security Platform ISO image as a VMware vSphere virtual machine.

To create an Cryptographic Security Platform virtual machine on VMware vSphere

1. Log into your VMware vSphere portal.
2. Right-click on a node of the virtual machine navigation tree.

3. Select the **New Virtual Machine** command to display the machine creation wizard.



4. In each step of this wizard, select the values described below.

- [Select a creation type](#)
- [Select a name and folder](#)
- [Select a compute resource](#)
- [Select storage](#)
- [Select compatibility](#)
- [Select a guest OS](#)
- [Customize hardware / Virtual Hardware](#)
- [Customize hardware / VM Options](#)

Select a creation type

Configure the following settings.

Field	Value
Select a creation type	Select Create a new virtual machine .

Select a name and folder

Configure the following settings.

Field	Value
Virtual machine name	Write a name for the new virtual machine.
Location for the virtual machine	Select a folder for the new virtual machine.

Select a compute resource

Configure the following settings.

Field	Value
Select a compute resource	Select a computing resource for the new virtual machine.

Select storage

Configure the following settings.

Field	Value
Encrypt this virtual machine	Do not enable this option
Storage list	Select a storage resource for the new virtual machine.

Select compatibility

Configure the following settings.

Field	Value
Compatible with	Select ESXi 6.7 and later .

Select a guest OS

Configure the following settings.

Field	Value
Guest OS Family	Select Linux .
Guest OS Version	Select Oracle Linux 8 (64-bit) .

Customize hardware / Virtual Hardware

Configure the following settings in the **Virtual Hardware** tab of the **Customize hardware** page.

Field	Value
CPU	Select the number of cores recommended in Machine requirements .

Field	Value
Memory	Select the RAM size recommended in Machine requirements .
New Hard Disk	Select at least 1 TiB for the root disk, as explained in Machine requirements .
New Hard Disk	Click ADD NEW DEVICE > Hard disk and add a second disk for the <code>etcd</code> daemon. As explained in Machine requirements , this disk requires at least 15 GiB.
New CD/DVD Drive	Select the location of the ISO file.
New CD/DVD Drive > Status	Check the Connect At Power On box.

Customize hardware / VM Options

Configure the following settings in the **VM Options** tab of the **Customize hardware** page.

i See the next section [Configuring the boot mode on VMware vSphere](#) for how to configure the selected boot mode.

Field	Value	Description
Boot Options > Firmware	BIOS	Boot the machine with BIOS firmware.
	EFI	Boot the machine with UEFI firmware.

Configuring the boot mode on VMware vSphere

Depending on the selected boot mode (BIOS or UEFI), perform the following steps before booting the machine.

- [Selecting the boot order in the BIOS settings](#)
- [Importing the ELRepo key for UEFI boot](#)

Selecting the boot order in the BIOS settings

As explained in [Machine requirements](#), Cryptographic Security Platform requires two disks. Therefore, if your machine uses BIOS boot firmware, ensure the biggest disk is placed first in the boot order. Otherwise, the system will not boot.

Importing the ELRepo key for UEFI boot

If your machine uses the UEFI boot firmware, you must import and enroll the ELRepo key.

i For more details on enrolling the ELRepo key, see <https://elrepo.org/wiki/doku.php?id=secureboot>

To enroll the ELRepo key

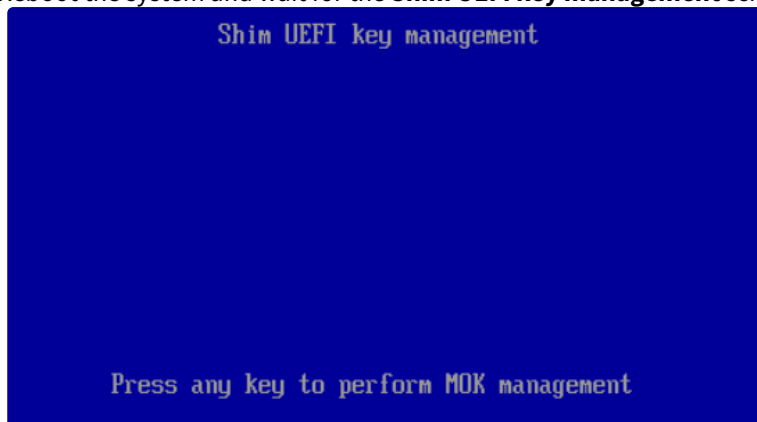
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

```
sudo mokutil --import /etc/pki/elrepo/SECURE-BOOT-KEY-elrepo.org.der
```

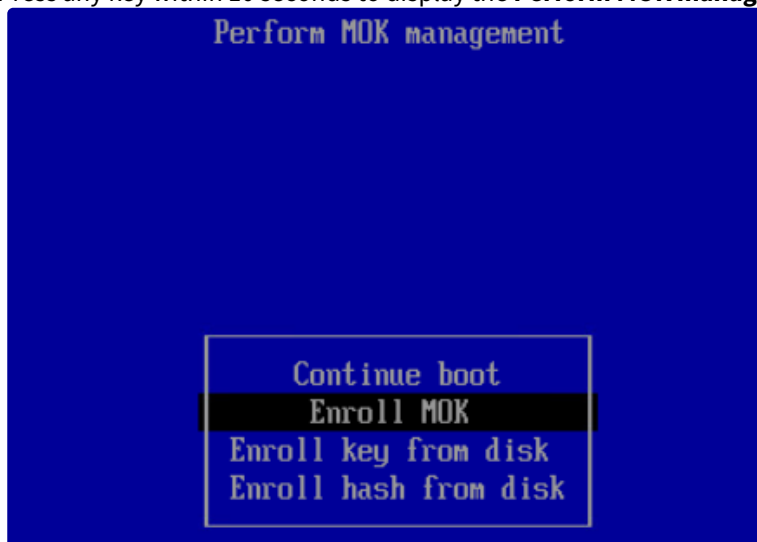
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

 The following operations do not support a remote console like an SSH client.

6. Reboot the system and wait for the **Shim UEFI key management** screen.



7. Press any key within 10 seconds to display the **Perform MOK management** dialog.



8. Select **Enroll MOK** and press **Enter** to display the **Enroll MOK** dialog.

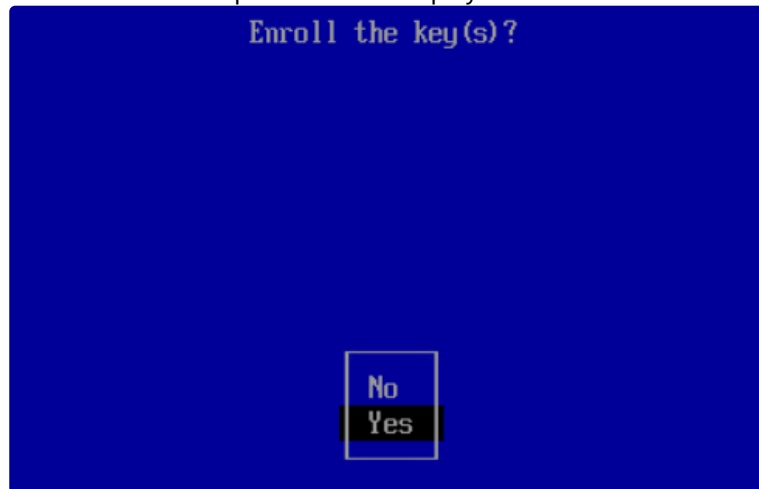


9. Select **View key 0** and press **Enter** to display the key information.

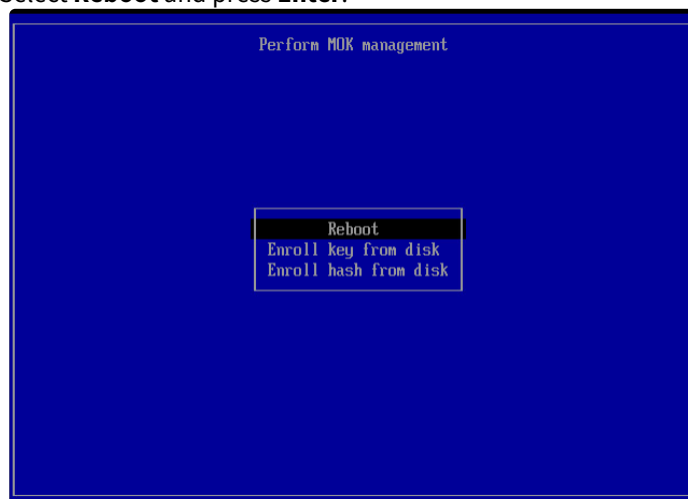


10. Check that the serial number is `0xe9d471cfb4fe136c`.
11. Check that the SHA1 fingerprint is `e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7`.
12. Press **ESC** to return to the **Enroll MOK** dialog.

13. Select **Continue** and press **Enter** to display the enrollment confirmation dialog.



14. Select **Yes** and press **Enter** to display the password form.
15. Type the key password you selected when importing the ELRepo key.
16. Press **Enter** to return to the **Perform MOK management** dialog.
17. Select **Reboot** and press **Enter**.



Logging into Cryptographic Security Platform on a VMware vSphere machine

After installing the image on the machine, open a local or SSH session as the Cryptographic Security Platform administrator.

Name	Initial password
sysadmin	changeme

When prompted, change the initial password with a password meeting the requirements described in [Password policy CIS benchmarks](#).

Configuring a Cryptographic Security Platform ISO image installation

Perform the following configuration steps after installing the Cryptographic Security Platform ISO image in the selected platform.

- [Configuring the connection of an ISO installation](#)
- [Configuring the hostname of a CSP PKI ISO installation](#)
- [Checking the connection of a Cryptographic Security Platform ISO installation](#)

Configuring the connection of an ISO installation

The following scenarios require manually configuring the connection as explained in this section.

- Your network does not use a DHCP (Dynamic Host Configuration Protocol) server.
- You want to overwrite the network configuration obtained from the DHCP server.

Skip this section otherwise.

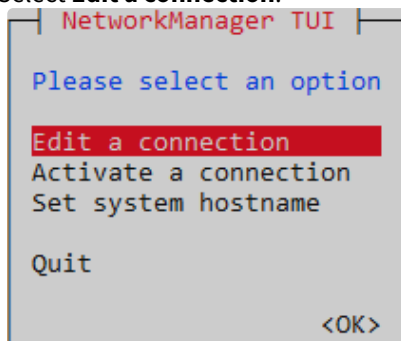
✗ After running the `clusterctl install` or `clusterctl node add` commands you cannot change the IP address or hostname of a node.

To configure the connection of a Cryptographic Security Platform ISO installation

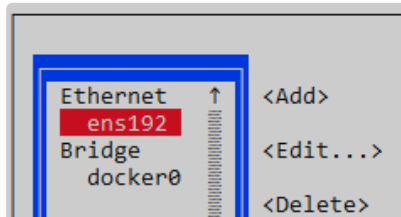
1. Log in to the machine locally as the `sysadmin` user.
2. Run the `nmtui` tool with `sudo` permissions.

```
sudo nmtui
```


3. Select **Edit a connection**.



4. Press **Enter** and select the Ethernet connection.




5. Press **Enter** to display the **Edit connection** dialog.
6. Change the **IPv4 CONFIGURATION** mode to **Manual**.
7. Select **<Show>** for **IPv4 CONFIGURATION**.

 As explained in [IP address requirements](#), Cryptographic Security Platform only supports IPv4 and disables IPv6 by default.


8. Press **Enter** to display the connection settings.
9. In the **Addresses** field, enter the preferred IP address and the subnet mask – for example:

```
192.168.100.4/24
```

10. In the **Gateway** field, enter the IP address of the default gateway for your network connection.
11. In the **DNS servers** field, enter the IP address of each server for DNS resolution. Separate multiple IP addresses with spaces or commas.

 As explained in [DNS requirements](#), Cryptographic Security Platform does not support accessing a DNS server through a proxy.


12. In the **Search domains** field, enter the domain names you want to use for DNS searches. Separate multiple domains with spaces or commas.

 Your system will automatically append the search domains to any unqualified domain names you use in your network, making it easier to access local resources without typing the full domain name every time.

13. Select **<OK>** and press **Enter**.
14. Select **<Back>** and press **Enter**.
15. Select **Quit** and press **Enter**.

Configuring the hostname of a CSP PKI ISO installation

See below for instructions on configuring the hostname of Cryptographic Security Platform.

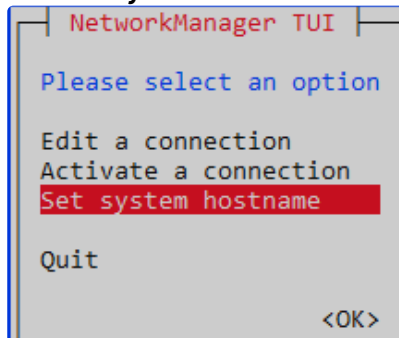
 After running the [clusterctl install](#) or [clusterctl node add](#) commands you cannot change the IP address or hostname of a node.

To configure the hostname

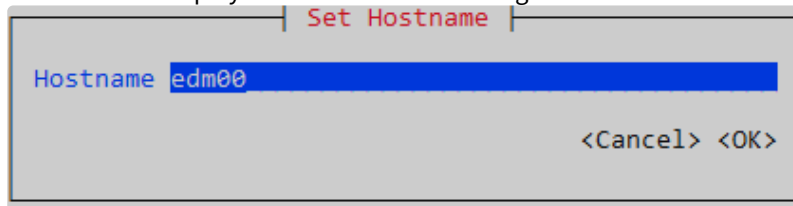
1. Log in to the Cryptographic Security Platform machine locally, as the `sysadmin` user.
2. Run the `nmtui` tool with `sudo` permissions.

```
sudo nmtui
```

3. Select **Set system hostname**.



4. Press **Enter** to display the **Set Hostname** dialog.



5. In the **Hostname** field, type an [RFC1123](#) compliant hostname – that is:
 - Must consist of lowercase alphanumeric characters, '-' or '.'
 - Must start and end with an alphanumeric character.
6. Select **<OK>** and press **Enter**.
7. Press **Enter** to confirm the hostname change.
8. Select **Quit** and press **Enter**.
9. Make the changes effective:
 - Reboot the machine, if you are using the local console
 - Open a new SSH session, if you are using remote SSH access.

Checking the connection of a Cryptographic Security Platform ISO installation

Run the `nmcli device status` command to check the connection of a machine – for example:

```
$ nmcli device status
DEVICE   TYPE      STATE                CONNECTION
ens192   ethernet  connected            ens192
docker0  bridge    connected (externally) docker0
lo        loopback  unmanaged            --
```

Check the state is `connected` for each connection.


Run the `ping` command to verify the host can send packets to other hosts.

```
ping <hostname>
```

Where `<hostname>` is the IP address or hostname of another host.

Installing the RAW image on AWS

See below for installing and configuring the Cryptographic Security Platform image in the Amazon Web Services (AWS) cloud.

 Refer to docs.aws.amazon.com for advanced configurations not covered in this guide, such as selecting the machine DNS.

To install and configure the Cryptographic Security Platform image in AWS

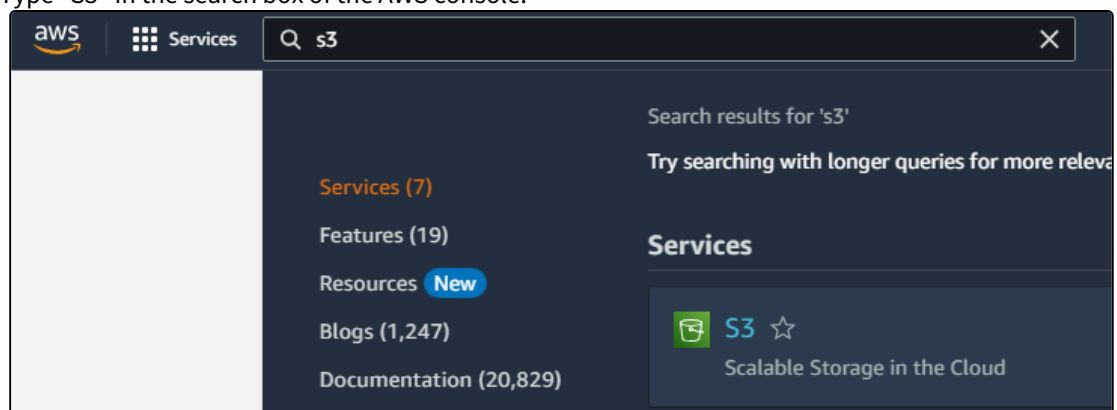
1. Download the Cryptographic Security Platform RAW image as explained in [Downloading the installation files](#).
2. Log into <https://console.aws.amazon.com> as a user with permission to:
 - Create and manage S3 buckets, roles, policies, snapshots, images, and EC2 instances.
 - Run AWS CLI commands using a locally installed AWS CLI or the AWS ShellCloud.
3. Perform the steps explained below.
 - [Creating an S3 bucket](#)
 - [Uploading the RAW image](#)
 - [Configuring the IAM policy](#)
 - [Creating an IAM role](#)
 - [Creating the snapshot configuration file](#)
 - [Preparing the command-line interface](#)
 - [Importing the snapshot](#)
 - [Creating an AMI from the snapshot](#)
 - [Creating the EC2 instance](#)
 - [Opening a session into AWS](#)
 - [Configuring the hostname on AWS](#)

Creating an S3 bucket

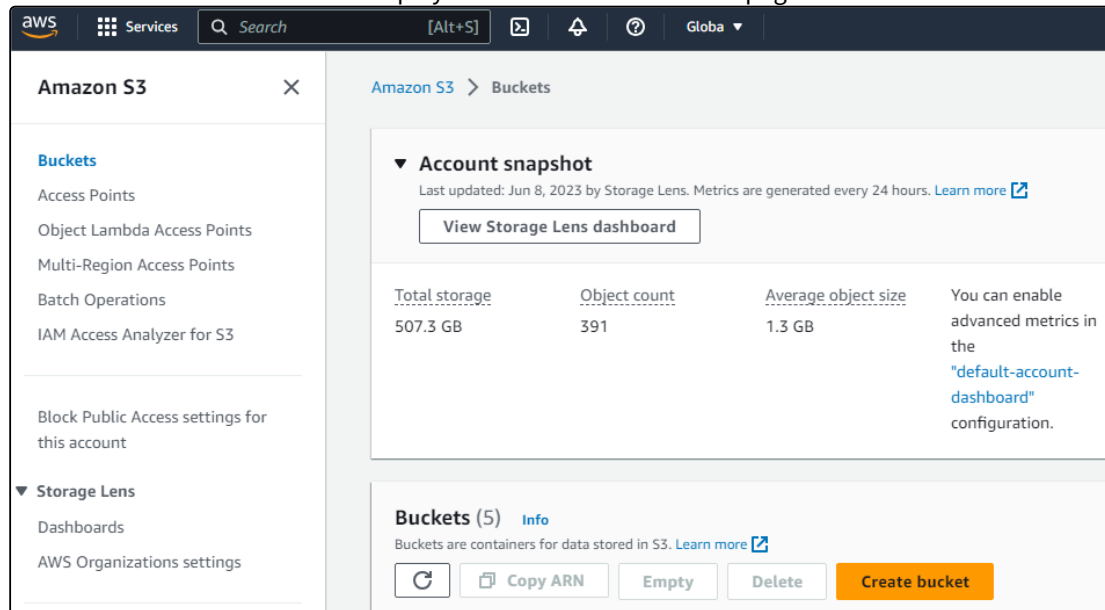
If you don't have an S3 bucket, create a new one as explained below.

To create an S3 bucket

1. Type "S3" in the search box of the AWS console.



2. Select **S3** in the search results to display the **Amazon S3 > Buckets** page.



3. Click **Create a bucket**.
4. Enter a name for the new bucket.
5. Select an AWS region for the bucket.

✗ All the resources created to deploy Cryptographic Security Platform in Amazon Web Service must share the same region.

6. For the other S3 settings, you can leave the default values.
 - Object Ownership
 - Block Public Access settings for this bucket
 - Bucket Versioning
 - Default encryption
 - Advanced settings
7. Click **Create bucket**.

Uploading the RAW image

Upload the Cryptographic Security Platform RAW image file to Amazon Web Services.

To upload the RAW image

1. Navigate to the **Amazon S3 page > Buckets** page of the AWS console.
2. Click the name of an S3 bucket. As explained in [Creating an S3 bucket](#), you can select an existing bucket or create a new one.
3. In the S3 bucket details page, click **Upload** to display the file upload form.
4. Click **Add Files**.
5. Select the Cryptographic Security Platform image file with **.raw** extension.
6. Click **Upload** at the bottom of the page to start the upload process.

Configuring the IAM policy

For granting permission to the S3 bucket, create an IAM (Identity and Access Management) policy or reuse an existing one.

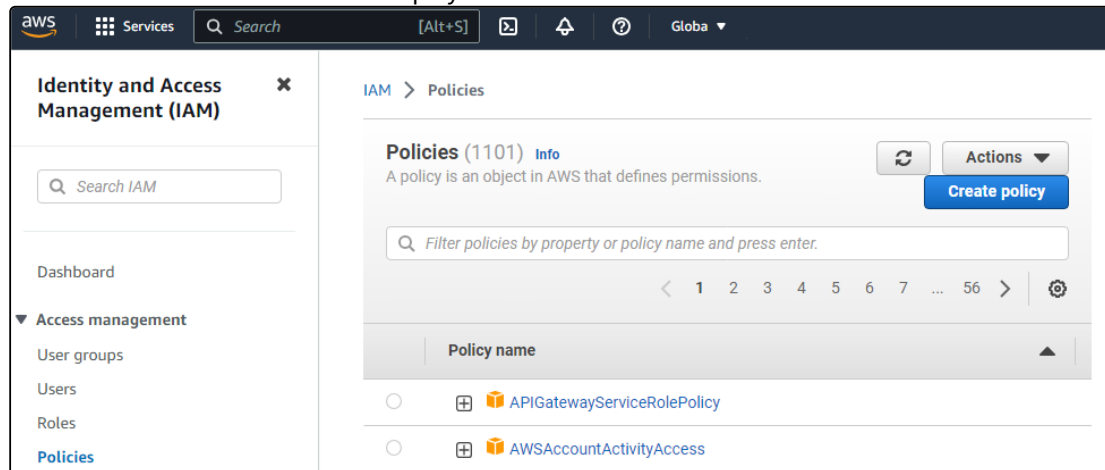
- [Creating a new IAM policy](#)
- [Updating an existing IAM policy](#)

Creating a new IAM policy

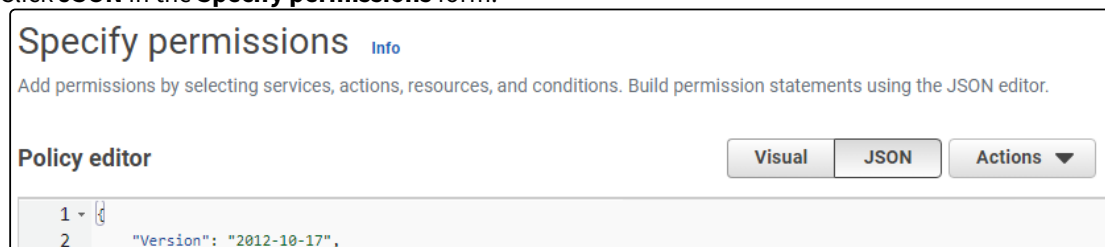
See below for creating an IAM policy granting permission to the S3 bucket.

To create an IAM policy

1. Type "IAM" in the search box of the AWS console.
2. Select **IAM** in the search results to display the IAM dashboard.



3. Select **Access management > Policies** in the navigation sidebar.
4. In the content pane, click the name of an existing IAM policy or click **Create policy** to create a new one.
5. Click **JSON** in the **Specify permissions** form.



6. Paste the following JSON code in the **Policy editor** field.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::$S3_BUCKET_NAME",
        "arn:aws:s3:::$S3_BUCKET_NAME/*"
      ]
    }
  ]
}
```

```

    ],
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
      ],
      "Resource": "*"
    }
  ]
}

```

7. In the JSON code, replace `$S3_BUCKET_NAME` with the name of the S3 bucket selected when [Creating an S3 bucket](#).
8. Click **Next**.
9. Enter a name and an optional description for the new policy.
10. Click **Create policy**.

Updating an existing IAM policy

See below for how to update an existing IAM policy for granting permission to the S3 bucket.

To update an IAM policy

1. Type "IAM" in the search box of the AWS console.
2. Select **IAM** in the search results to display the IAM dashboard.



3. Select **Access management > Policies** in the navigation sidebar.
4. In the content pane, click the **+** expand button for an existing IAM policy.
5. Click **Edit**.
6. In the policy editor field, add the following code to the `Resource` array.

```

"arn:aws:s3:::$S3_BUCKET_NAME",
"arn:aws:s3:::$S3_BUCKET_NAME/*"

```

7. In the code, replace `$S3_BUCKET_NAME` with the name of the S3 bucket selected when [Creating an S3 bucket](#).
8. Click **Next**.
9. Click **Save changes**.

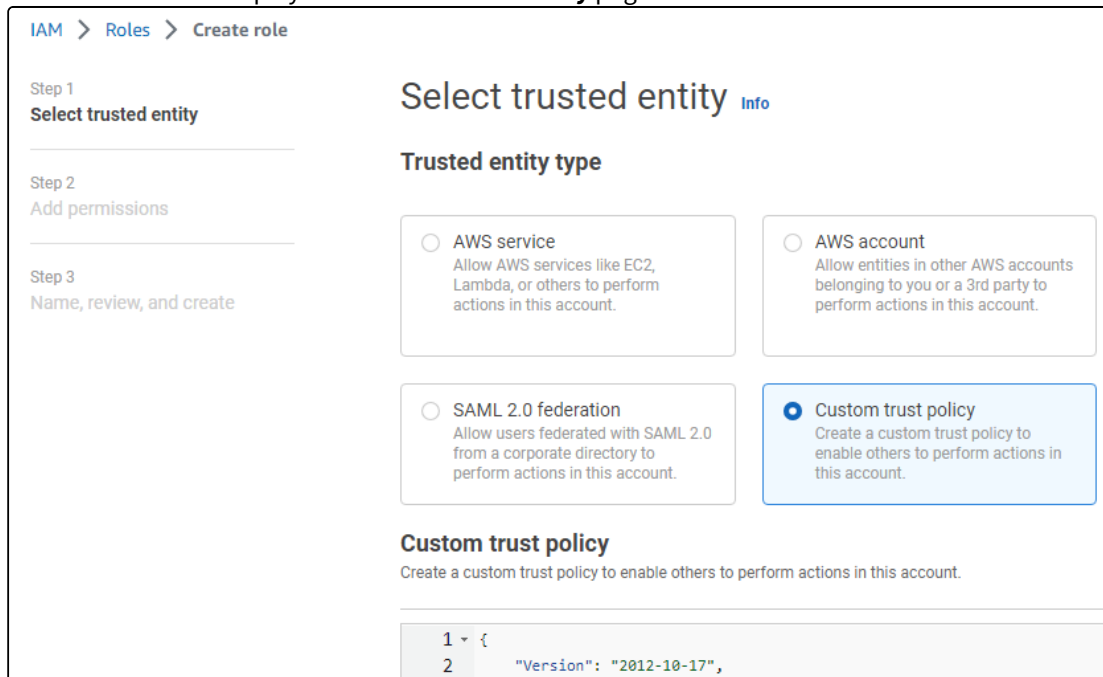
Creating an IAM role

Create an IAM (Identity and Access Management) role for the policy described in [Configuring the IAM policy](#).

✖ As indicated in the steps below, the value of the `sts:Externalid` field and the role name must both be exactly `vmimport`.

To create an IAM role

1. Type "IAM" in the search box.
2. Select IAM in the search results to display the IAM dashboard.
3. Select **Access management > Roles** in the navigation sidebar.
4. Click **Create role** to display the **Select trusted entity** page.



The screenshot shows the 'Select trusted entity' page in the AWS IAM console. The left sidebar indicates the path: IAM > Roles > Create role. The main area has a title 'Select trusted entity' with an 'Info' link. Under 'Trusted entity type', there are four radio button options: 'AWS service', 'AWS account', 'SAML 2.0 federation', and 'Custom trust policy'. The 'Custom trust policy' option is selected and highlighted in blue. Below this, there is a section for 'Custom trust policy' with a description: 'Create a custom trust policy to enable others to perform actions in this account.' At the bottom, there is a code editor with a JSON policy snippet:

```
1 {
2   "Version": "2012-10-17",
```

5. Under **Trusted entity type**, click **Custom trust policy**.
6. Paste the following code under **Custom trust policy**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vmie.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:Externalid": "vmimport"
        }
      }
    }
  ]
}
```

```
}  
  }  
]  
}
```

7. Click **Next**.
8. In the **Add permissions** page, select the policy described in [Configuring the IAM policy](#).
9. Click **Next** to display the **Role details** page.
10. In the **Role name** field, type `vmimport`.
11. Click **Create role**.

Creating the snapshot configuration file

In your local machine, create a `container.json` file with the following contents.

```
{  
  "Description": "Cryptographic Security Platform AMI file",  
  "Format": "raw",  
  "UserBucket": {  
    "S3Bucket": "$AWS_S3_BUCKET",  
    "S3Key": "$AMI_FILE"  
  }  
}
```

In the file contents, replace:

- `$AWS_S3_BUCKET` with the name of the S3 bucket described in [Creating an S3 bucket](#).
- `$AMI_FILE` with the name of the image file selected when [Uploading the RAW image](#).

For example:

```
{  
  "Description": "Cryptographic Security Platform AMI file",  
  "Format": "raw",  
  "UserBucket": {  
    "S3Bucket": "pki-hub-01",  
    "S3Key": "pki-hub-1.0.raw"  
  }  
}
```

Preparing the command-line interface

To run AWS commands in your machine, download and install the AWS CLI as explained in:

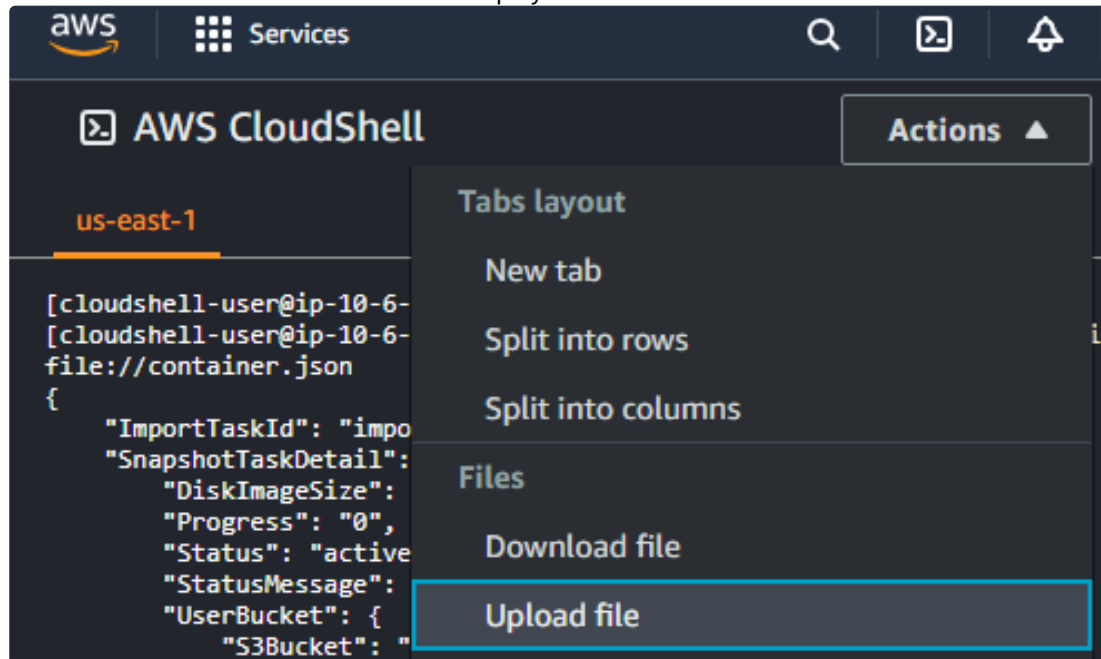
<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>

Alternatively, you can use the ShellCloud provided by the AWS console. This option requires uploading the configuration file as explained below.

To upload the snapshot configuration file

1. Type "shell" in the search box of the AWS console.

2. Select **CloudShell** in the search results to display the online AWS shell.



3. In the options menu, select **Actions > Upload file**.
4. Select the `container.json` file described in [Creating the snapshot configuration file](#).
5. Click **Upload**.

Importing the snapshot

Run the following AWS command to import the Cryptographic Security Platform image as an EC2 snapshot.

```
aws ec2 import-snapshot --disk-container file://container.json
```

For example:

```
$ aws ec2 import-snapshot --disk-container file://containers.json
{
  "ImportTaskId": "import-snap-03b38da24cb5fdde1",
  "SnapshotTaskDetail": {
    "DiskImageSize": 0.0,
    "Progress": "0",
    "Status": "active",
    "StatusMessage": "pending",
    "UserBucket": {
      "S3Bucket": "edm-01",
      "S3Key": "pki-hub-1.1.0_2025-01-06-10_38_16.raw"
    }
  },
  "Tags": []
}
```

Use the value of the `ImportTaskId` field to check the status of the import process.

```
aws ec2 describe-import-snapshot-tasks --import-task-ids <ImportTaskId>
```

For example:

```
aws ec2 describe-import-snapshot-tasks --import-task-ids import-
snap-03b38da24cb5fdde1
{
  "ImportSnapshotTasks": [
    {
      "ImportTaskId": "import-snap-03b38da24cb5fdde1",
      "SnapshotTaskDetail": {
        "DiskImageSize": 10740563968.0,
        "Format": "raw",
        "SnapshotId": "snap-03ea2ef99eb98d255",
        "Status": "completed",
        "UserBucket": {
          "S3Bucket": "edm-01",
          "S3Key": "pki-hub-1.1.0_2025-01-06-10_38_16.raw"
        }
      },
      "Tags": []
    }
  ]
}
```

In the command output, check the value of the `Status` field.

- If this value is `active`, rerun the command after 5 minutes to recheck the status.
- If this value is `completed`, the import process has already finished. Copy the `SnapshotId` value to use it in the next step [Creating an AMI from the snapshot](#).

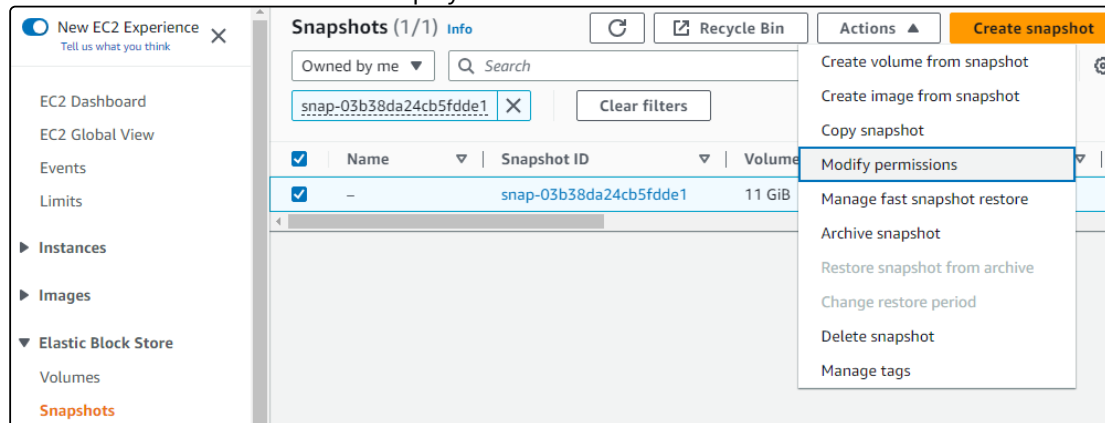
Creating an AMI from the snapshot

Create an Amazon Machine Image (AMI) from the imported snapshot.

To create the AMI

1. Type "EC2" in the search box.

2. Select **EC2** in the search results to display the EC2 dashboard.



3. Select **Elastic Block Store > Snapshots** in the navigation sidebar.
4. In the search box, paste the `SnapshotId` value returned when [Importing the snapshot](#).
5. Press **Enter**.
6. In the content pane, check the box for the newly imported snapshot.
7. In the options menu, select **Actions > Create image from snapshot**.
8. Configure the following settings.
 - [Image settings](#)
 - [Block device mappings](#)
9. Click **Create image**.

Image settings

Enter a name and an optional description for the image. For the other settings, you can leave the default values.

Block device mappings

Configure the root volume and add one for the `etcd` daemon. See below for the required settings.

Setting	Root volume	etdc volume
Size	1 TiB or more	15 GiB or more
Volume type	General Purpose SSD (gp3) or higher	General Purpose SSD (gp3) or higher

For the other settings, you can leave the default values.

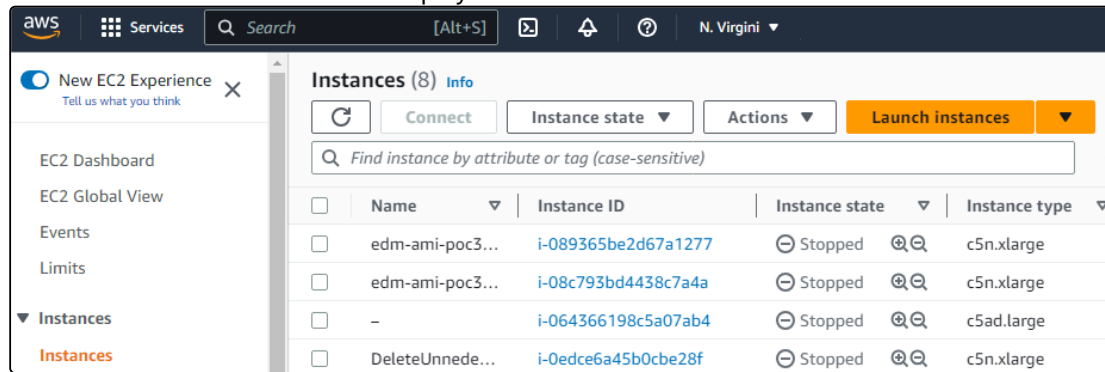
Creating the EC2 instance

Create an EC2 instance for running the Cryptographic Security Platform image.

To create the EC2 instance

1. Type "EC2" in the search box.

2. Select **IEC2** in the search results to display the EC2 dashboard.



3. Select **Instances > Instance** in the navigation sidebar.
4. In the options menu, click **Launch instance**.
5. Configure the following settings.
 - [Name and tags > Name](#)
 - [Application and OS Images \(Amazon Machine Image\)](#)
 - [Instance type](#)
 - [Key pair \(login\)](#)
 - [Network settings > Firewall \(security groups\)](#)
 - [Configure storage](#)
 - [Advanced Details > User data](#)
6. Click **Launch instance**.

Name and tags > Name

Enter a name for the new EC2 instance.

Application and OS Images (Amazon Machine Image)

Select the machine described in [Creating an AMI from the snapshot](#).

Instance type

Select the **c5n.2xlarge** instance type or higher.

Key pair (login)

Select an existing key pair, or create a new one for SSH connections.

Network settings > Firewall (security groups)

Select or create a security group with permission to open the ports described in [Required open ports](#).

i See <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html> for how to create a security group.


Configure storage

Select the default volume size or higher.

Advanced Details > User data

Paste the following code.


```
#!/bin/bash
/opt/entrust/scripts/configure-os.sh
```

 This code will allow the `sysadmin` Cryptographic Security Platform administrator to log in using the SSH key.


Opening a session into AWS

After creating and configuring the ECS instance:

1. Refresh the EC2 instance list until the instance status changes from **Initializing** to **2/2 checks passed**.
2. Wait a few minutes more.


You can then connect to the instance with SSH:

1. Copy the instance IP.
2. Open an SSH session into the instance.
3. Authenticate with the following credentials.
 - The username `sysadmin` of the default Cryptographic Security Platform administrator.
 - The SSH key selected when [Creating the EC2 instance](#).
4. When prompted, change the `changeme` initial password with a password meeting the requirements described in [Password policy CIS benchmarks](#).

 If you encounter an error during the initial connection, please try again after some time as the machine is currently being configured.

Configuring the hostname on AWS

See below for instructions on configuring the hostname of Cryptographic Security Platform.

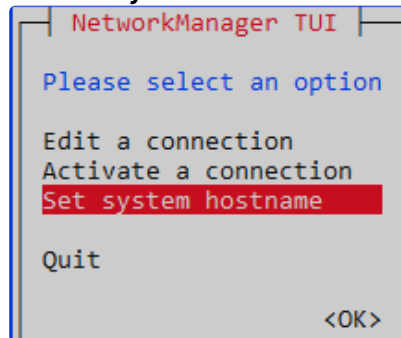
 After running the `clusterctl install` or `clusterctl node add` commands you cannot change the IP address or hostname of a node.

To configure the hostname

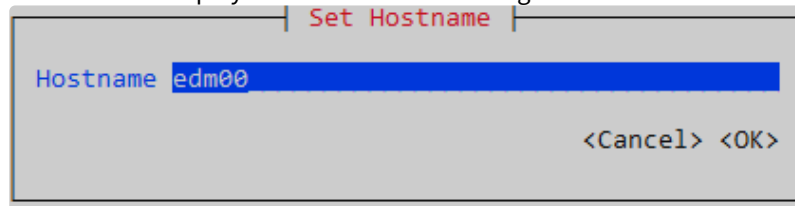
1. Log in to the Cryptographic Security Platform machine locally, as the `sysadmin` user.
2. Run the `nmtui` tool with `sudo` permissions.

```
sudo nmtui
```

3. Select **Set system hostname**.




4. Press **Enter** to display the **Set Hostname** dialog.



5. In the **Hostname** field, type an [RFC1123](#) compliant hostname – that is:
 - Must consist of lowercase alphanumeric characters, '-' or '.'
 - Must start and end with an alphanumeric character.
6. Select **<OK>** and press **Enter**.
7. Press **Enter** to confirm the hostname change.
8. Select **Quit** and press **Enter**.
9. Make the changes effective:
 - Reboot the machine, if you are using the local console
 - Open a new SSH session, if you are using remote SSH access.

Installing the VHD image on Azure

See below for installing and configuring a Cryptographic Security Platform image on the Microsoft Azure cloud.

 Refer to learn.microsoft.com/azure for advanced configurations not covered in this guide, such as selecting the machine DNS.

To install and configure the Cryptographic Security Platform image in Azure

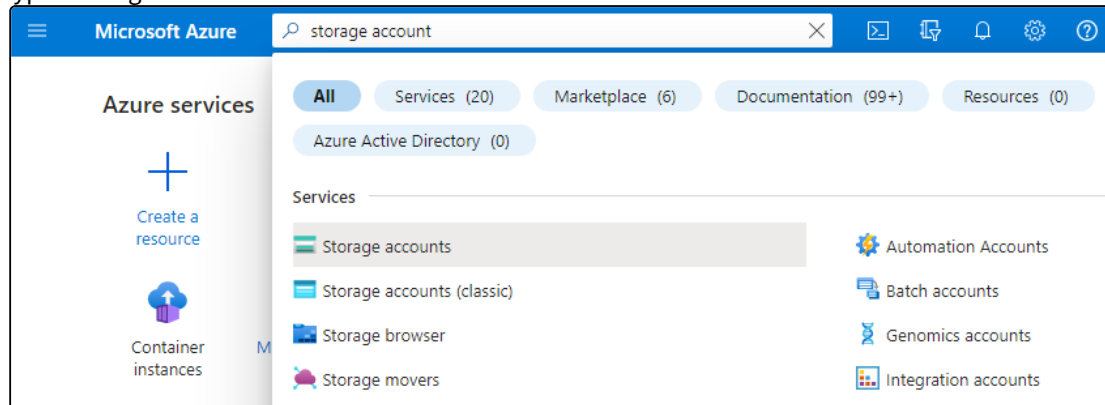
1. Download the Cryptographic Security Platform VHD image as explained in [Downloading the installation files](#).
2. Log into <https://portal.azure.com> as a user with permission to create and manage storage accounts, images, network rules, SSH keys, and virtual machines.
3. Perform the steps described below.
 - [Creating the Azure storage account](#)
 - [Uploading the VHD image file to Azure](#)
 - [Creating the Azure image](#)
 - [Creating the Azure network rules](#)
 - [Creating the SSH key for Azure](#)
 - [Creating the Azure virtual machine](#)
 - [Opening a session into Azure](#)
 - [Configuring the hostname on Azure](#)

Creating the Azure storage account

Select an existing Azure storage account or create a new one as explained below.

To create an Azure storage account

1. Type "storage accounts" in the Azure search bar.



2. Select **Storage accounts** in the search results.
3. Click **Create** on the **Storage accounts** page.
4. Configure the following settings on the **Create a storage account** page.
 - [Subscription](#)
 - [Resource group](#)
 - [Storage account name](#)
 - [Region](#)
5. Click **Review** to display the configured settings.
6. Click **Create** to create the storage account.

Subscription

Select your Azure user subscription.

Resource group

Select an existing resource group or create a new one.

✗ All the resources created to deploy Cryptographic Security Platform in Azure must share the same resource group.

Storage account name

Enter a name for the new storage account name.

Region

Select a region for the new storage account.

⚠ All the resources created to deploy Cryptographic Security Platform in Azure must share the same region.

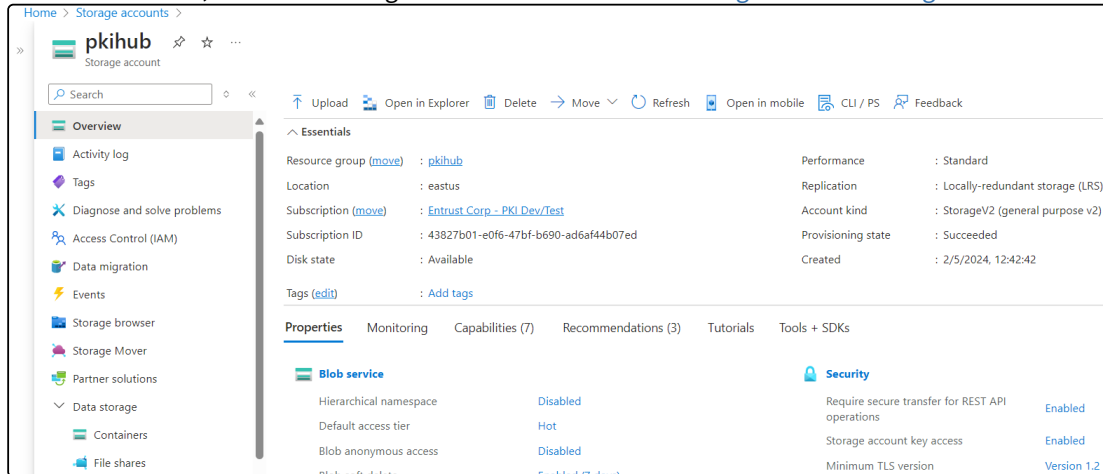
Uploading the VHD image file to Azure

Upload to Azure the Cryptographic Security Platform image file with `.vhd` extension.

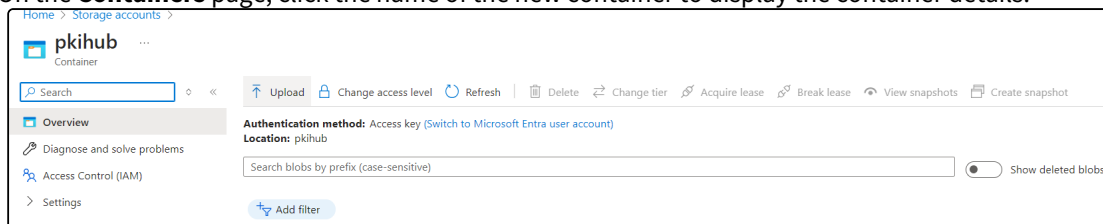
See [Downloading the installation files](#) for how to obtain this file.

To upload the VHD image file

1. In the Azure Portal, select the storage account described in [Creating the Azure storage account](#).



2. In the sidebar menu of the storage settings page, select **Data storage > Containers**.
3. On the **Containers** page, click **+ Container**
4. Enter a name for the new container and click **Create**.
5. On the **Containers** page, click the name of the new container to display the container details.



6. On the container details page, click **Upload**.
7. Select the Cryptographic Security Platform image file with **.vhd** extension and wait while the file uploads.

Creating the Azure image

Create an Azure image

- [Creating the Azure image with Azure Portal](#)
- [Creating the Azure image with Azure CLI](#)

Creating the Azure image with Azure Portal

See below for how to create the Entrust Development Manager image using the Azure Portal.

To create the image in the Azure Portal

1. Type "images" in the Azure Portal search bar.
2. Click **Images** on the search results.
3. Click **+ Create** on the **Images** page.
4. Configure the following settings in the **Create an image** page.
 - [Project details](#)
 - [Instance details](#)
 - [OS disk](#)

5. Click **Review + create** to validate the image settings.
6. Click **Create** to create the new image.

Project details

Configure the following settings under **Project details**.

Setting	Value
Subscription	Select your Azure subscription.
Resource group	Select the same resource group selected when Creating the Azure storage account .

Instance details

Configure the following settings under **Instance details**.

Setting	Value
Name	Enter a unique name for the new image.
Region	Select the same region selected when Creating the Azure storage account .

OS disk

Configure the following settings under **OS disk**.

Setting	Value
OS type	Select Linux .
Storage blob	Select the VHD image described in Uploading the VHD image file to Azure .
Account type	Select Standard SSD .
Host caching	Select Read-only .

Creating the Azure image with Azure CLI

Run the following command to create the image with the Azure command-line interface.

```
az image create --resource-group $GROUP --location $LOCATION --name $IMAGE \
```

```
--source $SOURCE --os-type linux --storage-sku Standard_LRS --os-disk-caching
ReadOnly
```

See the table below for a description of each parameter.

Option	Value
GROUP	The name of the resource group created in Creating the Azure storage account .
IMAGE	The name of the VHD image previously uploaded in Creating the Azure storage account .
LOCATION	The location of the resource group created in Creating the Azure storage account .
SOURCE	The OS disk source.

Creating the Azure network rules

Create a Network Security Group with rules granting access to the [Required open ports](#).


Creating the SSH key for Azure

Create or upload a key for authenticating the Azure machine administrator in remote SSH connections.

Creating the Azure virtual machine

Create an Azure Virtual Machine for running Cryptographic Security Platform.


- [Creating the Azure virtual machine with Azure Portal](#)
- [Creating the Azure virtual machine with Azure CLI](#)

 As explained in [IP address requirements](#), all the nodes of a multi-node installation require a static hostname and IP address.

Creating the Azure virtual machine with Azure Portal

When using the Azure portal to create the virtual machine, set the following configuration.

- [Basics](#)
- [Disk](#)
- [Networking](#)
- [Advanced](#)

 You can leave the default values for the settings not listed on this page.

Basics

Set the following values in the **Basics** tab of the **Create a virtual machine** page.

- [Project details](#)
- [Instance details](#)
- [Administrator account](#)
- [Inbound port rules](#)
- [Licensing type](#)

Project details

Set the following values under **Project details**.

Setting	Value
Subscription	Select your Azure subscription.
Resource group	Select the resource group described in Creating the Azure storage account .

Instance details

Set the following values under **Instance details**.

Setting	Value
Virtual machine name	Enter a name for the new virtual machine.
Region	Select the region shared by the rest of Azure resources.
Image	Select the image described in Creating the Azure image .
Size	Select one of the following: <code>Standard_D8s_v3</code> , <code>Standard_D8s_v4</code> , <code>Standard_D8ds_v4</code> , <code>Standard_F8s_v2</code> .

Administrator account

Set the following values under **Administrator account**.

Setting	Value
Authentication type	Select SSH public key .
SSH public key source	Select the key described in Creating the SSH key for Azure .

Setting	Value
Key pair name	Select the name of the key described in Creating the SSH key for Azure .

Inbound port rules

Set the following values under **Inbound port rules**.

Setting	Value
Public inbound ports	Select None .

Licensing type

Set the following values under **Licensing type**.

Setting	Value
License type	Select Other .

Disk

In the **Disk** tab of the **Create a virtual machine** page, configure the primary and secondary disks.

To configure the primary and secondary disks

1. Under **OS disk**, configure the values described in [OS disk](#).
2. Under **Data disks**, click **Create and attach a new disk**.
3. Under **Size**, click **Change size**.
4. In the **Select a disk size** page, configure the settings described in [Select a disk size](#).

OS disk

Set the following configuration for the primary disk.

Setting	Value
OS disk size	Select 1 TiB (P40) or higher
OS disk type	Select Premium SSD (locally-redundant storage) or higher

Select a disk size

Set the following configuration for the secondary disk.

Setting	Value
Storage type	Select Premium SSD (locally-redundant storage) or higher
Size	Select 15 GiB or higher
Performance tier	P40 or higher

Networking


Set the following values in the **Networking** tab of the **Create a virtual machine** page.

Setting	Value
NIC network security group	Select Advanced .
Configure network security group	Select the network security group described in Creating the Azure network rules .

Advanced

Paste the following code in the **Custom data** field of the **Advanced** tab.

```
#!/bin/bash
/opt/entrust/scripts/configure-os.sh
```

 This code will allow the `sysadmin` Cryptographic Security Platform administrator to log in using the SSH key.

Creating the Azure virtual machine with Azure CLI

Run the following command to create the virtual machine with the Azure command-line interface.

```
az vm create --resource-group $GROUP --location $LOCATION --name $VM --image $IMAGE
--size $SIZE --storage-sku Premium_LRS --os-disk-size-gb $DISK_SIZE --os-disk-caching
ReadOnly --data-disk-sizes-gb $EXTRA_DISK_SIZE --data-disk-caching ReadOnly --
authentication-type ssh --admin-username azureuser --ssh-key-name $SSH_KEY --nsg $NSG
--custom-data $CUSTOM_DATA
```

See below for a description of each parameter.

- `GROUP`
- `LOCATION`
- `VM`
- `IMAGE`

- [SIZE](#)
- [DISK_SIZE](#)
- [EXTRA_DISK_SIZE](#)
- [SSH_KEY](#)
- [NSG](#)
- [CUSTOM_DATA](#)

GROUP

The name of the resource group created in [Creating the Azure storage account](#).

LOCATION

The location of the resource group created in [Creating the Azure storage account](#).

VM

The name of the Virtual Machine that will be created.

IMAGE

The name of the VHD image previously uploaded in [Creating the Azure storage account](#).

SIZE

One of the following:

- Standard_D4s_v3
- Standard_D4ds_v5
- Standard_D4ds_v4
- Standard_D4as_v4
- Standard_F4s

DISK_SIZE

1024 GiB or more. For example:

```
--os-disk-size-gb 1024
```

EXTRA_DISK_SIZE

15 GiB or more. For example:

```
--data-disk-size-gb 15
```

SSH_KEY

The name of the SSH key pair created in [Creating the SSH key for Azure](#).


NSG

The network security group created in [Creating the Azure network rules](#).

CUSTOM_DATA

The path of a local text file with the following contents.

```
#!/bin/bash
/opt/entrust/scripts/configure-os.sh
```

 This code will allow the `sysadmin` Cryptographic Security Platform administrator to log in using the SSH key.


Opening a session into Azure

After creating and configuring the Azure virtual machine:

1. Refresh the page until the status changes from **Deployment is in progress** to **Your deployment is complete**.
2. Wait a few minutes more.


You can then connect to the virtual machine with SSH:

1. Copy the IP of the virtual machine.
2. Open an SSH session into the virtual machine
3. Authenticate with the following credentials.
 - The username `sysadmin` of the default Cryptographic Security Platform administrator.
 - The SSH key described in [Creating the SSH key for Azure](#).
4. When prompted, change the `changeme` initial password with a password meeting the requirements described in [Password policy CIS benchmarks](#).

 If you encounter an error during the initial connection, please try again after some time as the machine is currently being configured.

Configuring the hostname on Azure

See below for instructions on configuring the hostname of Cryptographic Security Platform.

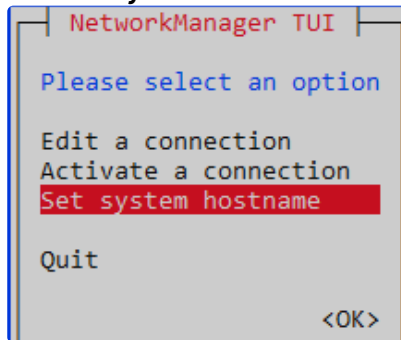
 After running the `clusterctl install` or `clusterctl node add` commands you cannot change the IP address or hostname of a node.

To configure the hostname

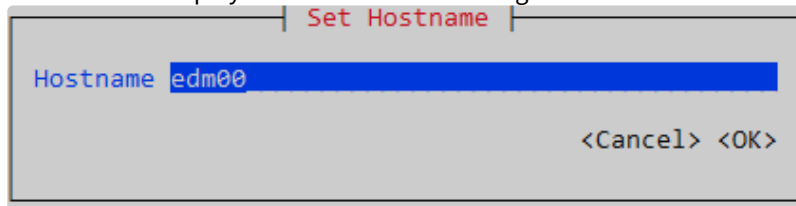
1. Log in to the Cryptographic Security Platform machine locally, as the `sysadmin` user.
2. Run the `nmtui` tool with `sudo` permissions.

```
sudo nmtui
```

3. Select **Set system hostname**.



4. Press **Enter** to display the **Set Hostname** dialog.



5. In the **Hostname** field, type an [RFC1123](#) compliant hostname – that is:
 - Must consist of lowercase alphanumeric characters, '-' or '.'
 - Must start and end with an alphanumeric character.
6. Select **<OK>** and press **Enter**.
7. Press **Enter** to confirm the hostname change.
8. Select **Quit** and press **Enter**.
9. Make the changes effective:
 - Reboot the machine, if you are using the local console
 - Open a new SSH session, if you are using remote SSH access.

Installing CSP

Run the `clusterctl install` command for installing Cryptographic Security Platform. This command supports `demo-mode` and `prod-mode` modes with the following differences.

Setting	demo-mode	prod-mode
Deployment type	Proof-of-concept deployments.	Production deployments.
Requirements	Does not need the disk performance requirements described in Machine requirements . Specifically, fsync latency is not an issue in this mode.	All the Requirements .
Supported number of nodes	One	One or more. See Required number of nodes for details.

Setting	demo-mode	prod-mode
Supported operations	You cannot perform the operations described in Joining nodes , Backing up the state , Recovering from disaster , or Restoring the state .	All
Supported updates	You cannot upgrade to a newer version or migrate to a multi-node installation.	All

See below for how to run these modes.

- demo-mode installations
- prod-mode installations on a single node
- prod-mode mode installations on several nodes

✖ The `clusterctl install` command validates the [Requirements](#) and throws an error if not met.

demo-mode installations

For a proof-of-concept installation, run `clusterctl install` on `demo-mode` in the machine where you have installed the Cryptographic Security Platform image (this mode only supports one node).

```
$ sudo clusterctl install --mode demo-mode
```

Installing done ██████████ 100 %

prod-mode installations on a single node

For a production environment installation on a single node, run `clusterctl install` with the default `prod-mode` in the machine where you have installed the Cryptographic Security Platform image.

```
$ sudo clusterctl install
Installing done ██████████ 100 %
```

prod-mode mode installations on several nodes

For a production environment installation on several nodes:

1. Run `clusterctl install` with the default `prod-mode` mode in only one of the machines where you have installed the Cryptographic Security Platform image.

```
$ sudo clusterctl install  
Installing done ██████████ 100 %
```


2. Follow the steps described in [Joining nodes](#) to add the remaining cluster nodes.

Joining nodes

If your Cryptographic Security Platform comprises more than one node, you need to join them on a cluster.

To join Cryptographic Security Platform nodes

1. In all the nodes:
 - a. Make sure the node meets the [Requirements](#).
 - b. If not yet installed, install the Cryptographic Security Platform image as explained in [Installing the image](#).
2. In one of the nodes:
 - a. Install Cryptographic Security Platform as explained in [Installing CSP](#).
 - b. Run `clusterctl node info` and copy the node IP address.
 - c. Run `clusterctl node join-token` and copy the node joining token.
3. In the rest of the nodes, perform the following steps sequentially.
 - a. Run the `clusterctl node add` command with the IP address and joining token previously obtained.
 - b. Wait for the command to complete before proceeding to join another node.

 Do not perform any operations on the cluster nodes until this operation completes.

4. Redeploy each deployed Entrust solution (if any) using either the `clusterctl solution deploy` command or the Management Console.

Replacing the default TLS certificate


During installation, Cryptographic Security Platform generates an insecure self-signed certificate for securing communications with Grafana, the Management Console, and the solution services. You must replace this certificate before running Cryptographic Security Platform in a production environment.

- [TLS certificate fields](#)
- [TLS certificate algorithms](#)
- [Issuing the TLS certificate](#)
- [Installing the TLS certificate](#)
- [Reusing as CA Gateway TLS certificate](#)

TLS certificate fields

Use the following fields to set the Cryptographic Security Platform hostname or IP address in the TLS certificate.

- Subject Alternative Name (SAN) extension.
- The Common Name (CN) field of the certificate subject.

 When both fields are present, the Subject Common Name is ignored.

TLS certificate algorithms

The Cryptographic Security Platform TLS certificate must be generated using either:

- The RSA algorithm with a key length of 2048 bits or more.
- The ECDSA algorithm with a P-256 elliptic curve.

Issuing the TLS certificate

Use your corporate PKI to issue the Cryptographic Security Platform TLS certificate.

Installing the TLS certificate

Run the `clusterctl certificate` command to install the Cryptographic Security Platform TLS certificate.

✖ When running Cryptographic Security Platform in high availability, also install the TLS certificate in the load balancer.

Reusing as CA Gateway TLS certificate

If the CA Gateway solution is deployed, you can use the same TLS certificate for Cryptographic Security Platform and CA Gateway.

ℹ See [Configuring and deploying CA Gateway](#) for selecting this TLS certificate in CA Gateway.

Configuring the proxy

Some solutions require outgoing connections – for example with:

- Entrust PKIaaS
- A third-party server integrated with the solution

If these connections pass through a proxy server, run the `clusterctl proxy set` command to configure this proxy server in Cryptographic Security Platform.

✖ As explained in [DNS requirements](#), Cryptographic Security Platform does not support accessing a DNS server through a proxy.

Changing the keyboard layout

The default keyboard layout for Cryptographic Security Platform Installations is `en-US`. Run the following command to list the available keyboard layouts.

```
localectl list-locales
```

Run the following command to set the `<layout>` keyboard layout.

```
sudo localectl set-keymap <layout>
```

For example:

```
$ sudo localectl set-keymap es-ES
```

Changing the operating system timezone

The default timezone for Cryptographic Security Platform Installations is UTC. Run the following command to list the available time zones.

```
timedatectl list-timezones
```

Run the following command to set the `<timezone>` timezone.

```
sudo timedatectl set-timezone <timezone>
```

For example

```
$ sudo timedatectl set-timezone Europe/Madrid
```

Configuring time synchronization

When [Installing CSP](#), the installation process automatically configures the built-in `chrony` service to use the NTP server provided by DHCP.

✖ In multi-node installations, all the nodes must have synchronized dates to prevent communication errors.

To modify this default configuration, edit the `chrony` configuration file in all the installation nodes.

```
/etc/chrony.conf
```

Do not modify the following lines in any case.

```
bindcmdaddress 0.0.0.0  
cmdallow all
```

ℹ See a reference of the `chrony` parameters at <https://chrony-project.org/doc/4.4/chrony.conf.html>

Manually starting starting the chrony service

Run the following command to manually start the `chrony` service.

```
sudo systemctl restart chronyd.service
```

⚠ Re-run this command after each node restart.

Configuring an nShield HSM

Perform the following configuration steps if any solution requires an Entrust nShield HSM (Hardware Security Module). Skip them if you intend to use an HSM from another vendor.

- [Selecting the platform for creating the Entrust nShield Security World](#)
- [Selecting the drivers for creating the Entrust nShield Security World](#)
- [Adding a cknfastrc file to the Entrust nShield Security World](#)
- [Configuring kmdata/config/config in Entrust nShield Security World](#)
- [Registering Cryptographic Security Platform nodes as Entrust nShield clients](#)
- [Integrating an nShield Trusted Verification Device](#)



For a complete guide on Security World, see <https://nshielddocs.entrust.com/security-world-docs/v12.80/connect-ug-nix/create-manage-security-world.html#CreatingSecurityWorld>

Selecting the platform for creating the Entrust nShield Security World

You can create the Entrust nShield Security World on the machine running the Timestamping Authority solution, or on another machine of your choice.

Selecting the drivers for creating the Entrust nShield Security World

Section [HSM requirements](#) details the version of the built-in client drivers Entrust solutions use to connect with Entrust nShield HSMs. To avoid potential incompatibilities, use client drivers of the same version when creating the Entrust nShield Security World.

Adding a cknfastrc file to the Entrust nShield Security World

To use the `cknfastrc` file in Timestamping Authority:

1. Copy the file into the Security World `kmdata` folder that will be imported later as part of the Timestamping Authority configuration.
2. Edit the file and add the following line:


```
CKNFAST_LOADSHARING=1
```

3. Save the file changes.

Configuring kmdata/config/config in Entrust nShield Security World

The following parameters in the `kmdata/config/config` file only support the default value.

Parameter	Default
impath_addr	0.0.0.0
impath_port	9004

 To use these default values, simply omit the parameters in the configuration.

Registering Cryptographic Security Platform nodes as Entrust nShield clients

Entrust nShield requires registering each Cryptographic Security Platform node as a client. When using an Entrust nShield HSM, repeat the below steps for each node.

To register an Cryptographic Security Platform node as Entrust nShield client

1. Run the client registration wizard as explained in <https://nshielddocs.entrust.com/security-world-docs/v12.80/connect-ug-nix/configure.html#ConfigureConnectClient>
2. When prompted **Please enter your client IP address**, type the node IP address and click **Yes**.
3. When prompted **Do you want to save the IP in the config?** click **Yes**.
4. When prompted **Please choose the client permissions** click **Unprivileged**.
5. When prompted **Do you want secure authentication enabled on this client?** click **No**.

Integrating an nShield Trusted Verification Device

The nShield Trusted Verification Device (TVD) is a USB-connected smart card reader that facilitates the authentication between the smart card and the HSM.

To integrate an nShield TVD

1. Set up the TVD as explained in <https://nshielddocs.entrust.com/security-world-docs/v13.6.5/tvd/intro.html>
2. Redeploy the solutions using an HSM to make changes effective. You can either use the Management Console or run the `clusterctl solution deploy` command.

6 Starting up the Management Console

Log into the web Management Console to import the license and create users as explained below.

- [Replacing the initial admin password](#)
- [Setting or updating the license](#)
- [Creating Management Console roles](#)
- [Creating Management Console users](#)
- [Integrating Identity providers](#)

Replacing the initial admin password

Log into the web Management Console and replace the initial password of the `admin` user.

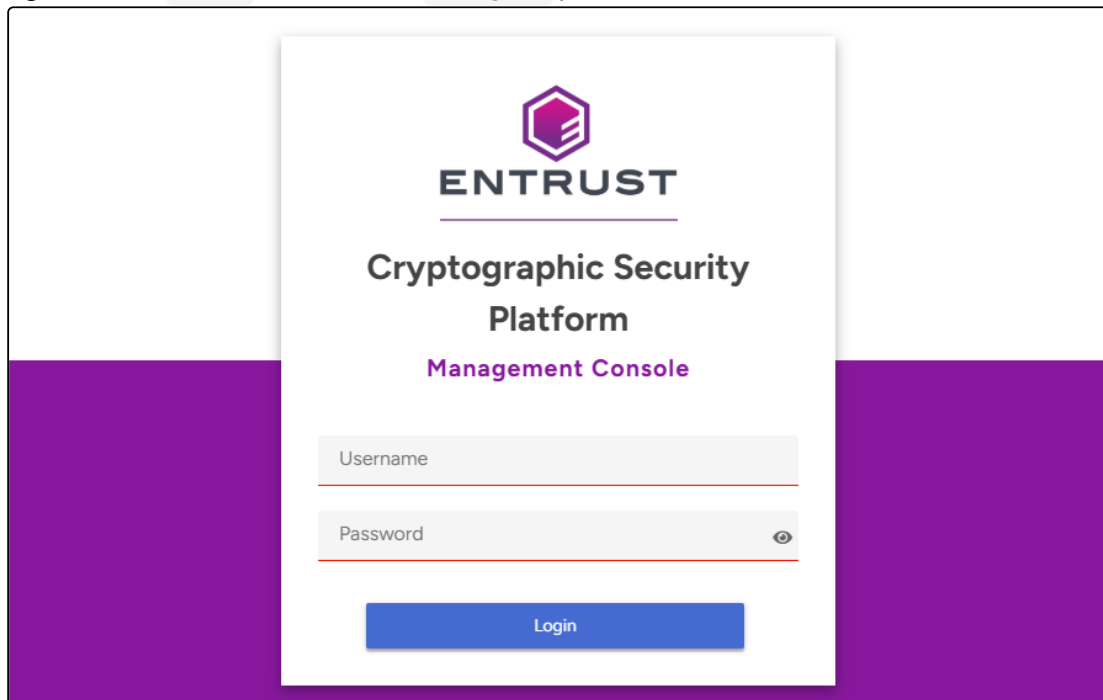
To replace the initial admin password

1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log in with the `admin` username and `changeme` password.



3. After the first login, you will be prompted to change these initial credentials. Fill in the **Change Password** form and click **SAVE**.

Setting or updating the license

The Cryptographic Security Platform license determines the Entrust solutions you are allowed to run on Cryptographic Security Platform. See below for how to set or update this license using the Management Console.

i Alternatively, you can set the license with the `clusterctl license import` command.

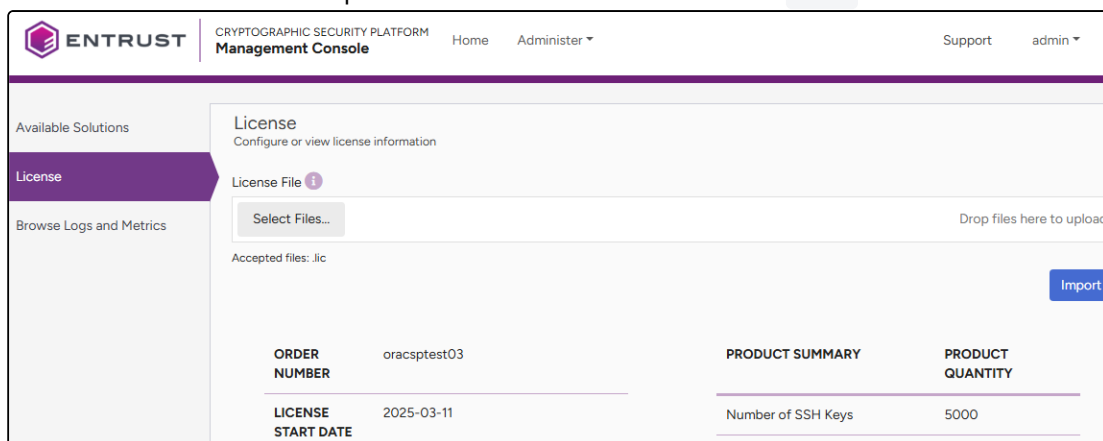
To set or update the license

1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log into the Management Console a user belonging to a role with license management permissions – for example, the initial `admin` administrator user.
3. Click **License** in the sidebar.
4. Click **Select File** in the content pane and select the license file with the `.lic` extension.



5. Check the details of the uploaded license.

Creating Management Console roles

Create roles to refine the permissions granted to Management Console users.

i Management Console users are not to be confused with operating system users with permissions on the operations described in [Command reference](#).

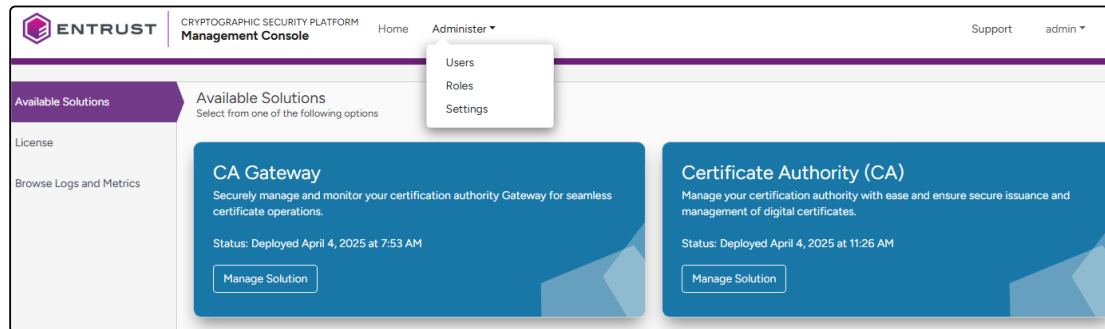
To create a Management Console role

1. Open the following URL in a Web browser.

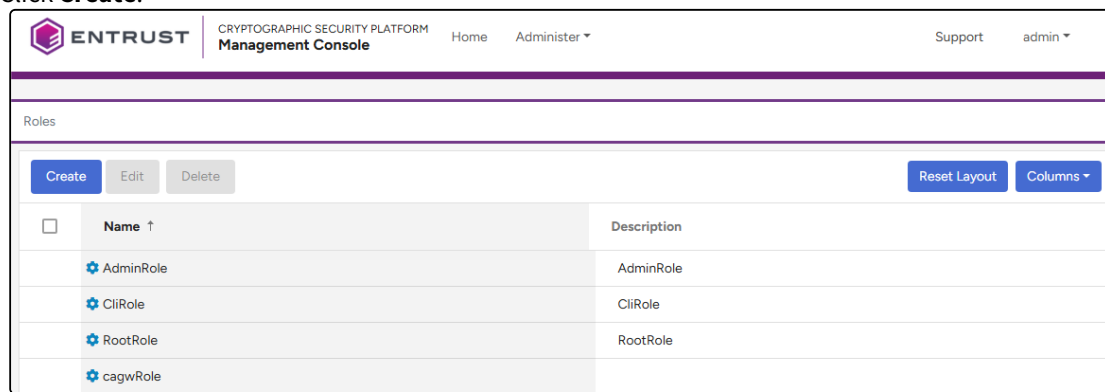
```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log into the Management Console a user belonging to a role with role management permissions – for example, the initial `admin` administrator user.
3. Select **Roles** in the **Administer** menu.



4. Click **Create**.



5. Complete the following fields in the **Create** form.
 - [Name](#)
 - [Description](#)
 - [Permissions](#)
6. Click **Create** to confirm the changes.

Name

A unique name for the role, at least two characters long.

Description

An optional description of the role.

Permissions

The permissions granted by the role

Category	Permission	Operation
Solutions	Manage and Operate Certificate Authority (CA)	See Managing Certificate Authority

Category	Permission	Operation
	Manage CA Gateway (CAGW)	See Managing CA Gateway
	Manage Certificate Enrollment Gateway (CEG)	See Managing Certificate Enrollment Gateway
	Manage Certificate Manager	See Managing Certificate Manager
	Manage Validation Authority (EVA)	See Managing Validation Authority
	Manage Timestamping Authority (TSA)	See Managing Timestamping Authority
Users	Manage Users	See Creating Management Console users
Roles	Manage Roles	The role creation and management operations described in this page
Identity Providers	Manage Identity Providers	See Integrating Identity providers

Creating Management Console users

Create users with permissions on the Management Console options.

i Management Console users are not to be confused with operating system users with permissions on the operations described in [Command reference](#).

To create a Management Console user

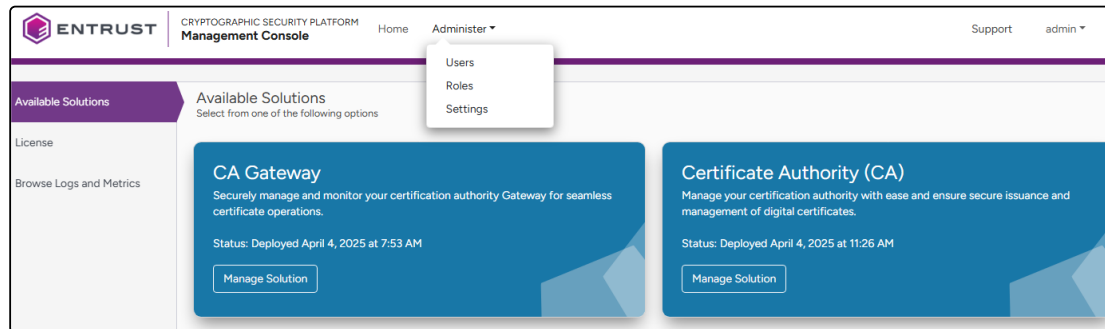
1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

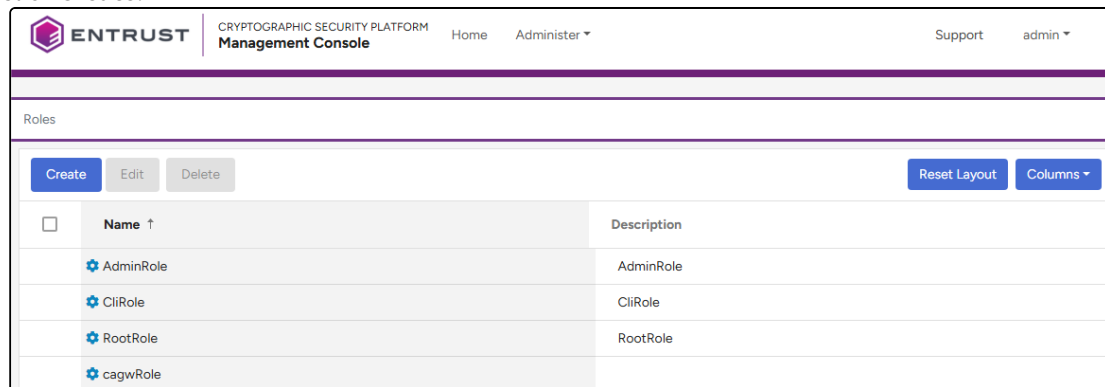
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log into the Management Console as a user belonging to a role with user management permissions – for example, the initial `admin` administrator user.

3. Select **Roles** in the **Administer** menu.



4. Click **Create**.



5. Complete the following fields in the **Create** form.

- [Name](#)
- [Email](#)
- [Password](#)
- [Confirm Password](#)
- [Roles](#)

6. Click **Create**.

Name

The name of the user. This name:

- Must be 3-13 characters long.
- Can only include lowercase letters, numbers, underscores (" _ "), and hyphens (" - ").
- Cannot match any of the following reserved words.
 - acs
 - ca
 - cas
 - crt
 - crlagent
 - crlresponder
 - deploy
 - idp
 - main
 - meteringca
 - operator
 - persistgc
 - pkihub

- pkihubidp
- scheduler
- schema
- schemas
- schemes
- vaagent

Email

The email address of the user.

Password

The user's password. This password must be at least 8 characters long and complex enough for the **Password Strength** bar to become green.

Confirm Password


Repeat the password.

Roles

The [Creating Management Console roles](#) granted to the user.

Integrating Identity providers

Integrate identity providers for the Management Console users to log in.

 Management Console users are not to be confused with operating system users with permissions on the operations described in [Command reference](#).

To integrate an identity provider

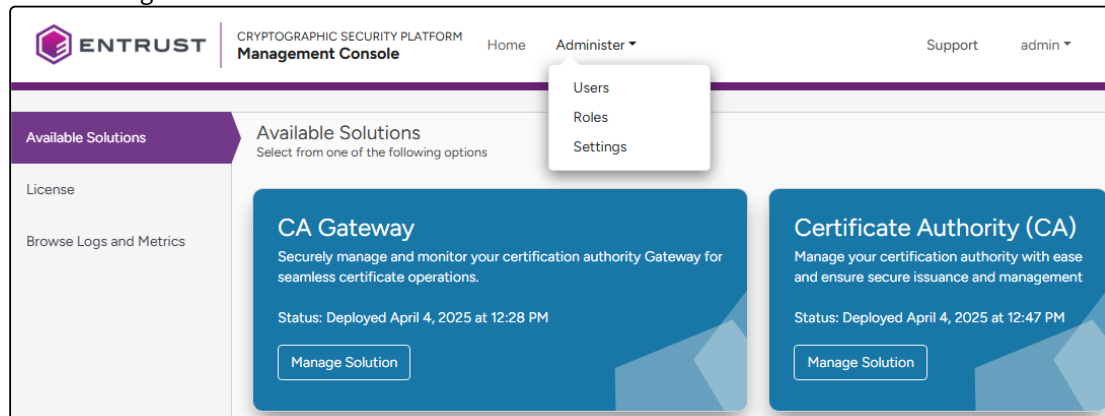
1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

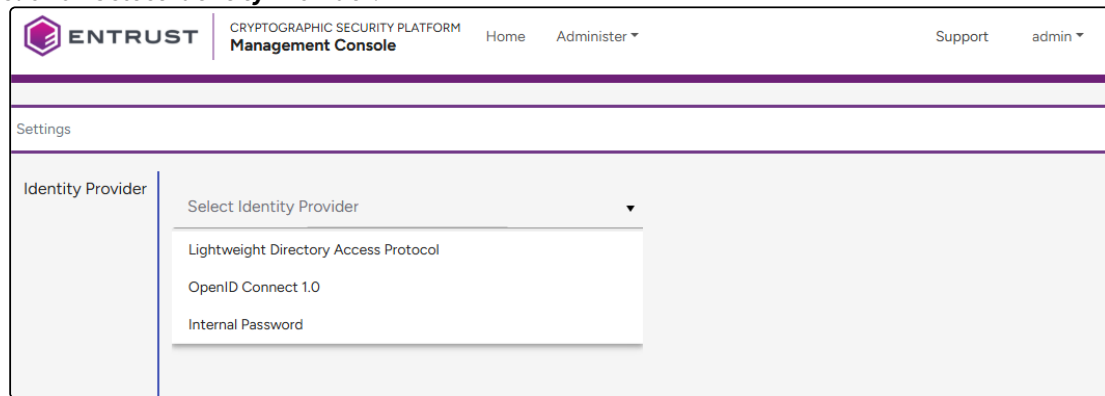
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log into the Management Console as a user belonging to a role with identity provider management permissions – for example, the initial `admin` administrator user.


3. Select Settings in the **Administer** menu.



4. Click on **Select Identity Provider**.



5. Select and configure one of the following mechanisms.
 - [Entrust Identity as a Service \(IDaaS\)](#)
 - [Internal password](#)
 - [Lightweight Directory Access Protocol](#)
 - [OpenID Connect 1.0](#)
6. Log out the Management Console.
7. Log into the Management Console using the new identity provider as authentication mode. This action will add the logged user to those described in [Creating Management Console users](#).
8. Click **Administer > Users** in the menu bar to manage the user and grant him roles.

 To manage users, you must log in as a user holding a role with the **Manage Users** permission.

Entrust Identity as a Service (IDaaS)

In the IDaaS administration interface, configure an OIDC Web application with the following settings.

Setting	Value
Subject Id Attribute	Type a unique user identifier.
ID Token Signing Algorithm	Select RS256 .

Setting	Value
Redirect URI(s)	Paste the value of the Redirect URL configuration setting described below.
Supported Scopes > Email address	Check this box
Require Consent	Uncheck this box.
User Info Signing Algorithm	None
Claims	Create a claim with the profile identifier. Set a group name as the value of each claim attribute.
Authentication decision	Select second factors as you wish and ensure users have the required authentications.
Groups	Create one group and add the users with login permissions.

In the Cryptographic Security Platform console, configure the following settings for an Entrust Identity as a Service (IDaaS) identity provider.

- [Active](#)
- [Name](#)
- [Redirect URL](#)
- [Client Secret](#)
- [Client ID](#)
- [Base IDaaS URL](#)
- [Required Group Attribute Name](#)
- [Required Group Name](#)
- [JWKS URL](#)
- [Authorization Endpoint](#)
- [Access Token Endpoint](#)
- [UserInfo Endpoint](#)
- [Logout Endpoint](#)

Active

Check this box to enable the identity provider.

Name

Type a provider name to display when logging into the Cryptographic Security Platform console.

Redirect URL

The URL to redirect to when the identity provider successfully authenticates a user. Cryptographic Security Platform automatically generates this value when you click **Save**. You must:

1. Copy this value from the Cryptographic Security Platform interface.
2. Paste this URL on the **Redirect URI(s)** field of the IDaaS interface.

When the Cryptographic Security Platform host URL changes, you must:

1. Re-type the **Client Secret** and **Client ID** values on the Cryptographic Security Platform console.
2. Click **Save**.
3. Copy the new **Redirect URL** value from the Cryptographic Security Platform console.
4. Paste this URL on the **Redirect URI(s)** field of the IDaaS interface.

Client Secret


Paste the client secret from the IDaaS OIDC application.

Client ID

Paste the client identifier from the IDaaS OIDC application.

Base IDaaS URL

Paste the account URL of the IDaaS OIDC application.

 When you enter this URL, the web browser interface fills in the rest of the URLs.

Required Group Attribute Name

Type the following attribute name.

profile

Required Group Name

Type the name of the group configured in the IDaaS OIDC application.

JWKS URL

Paste the JSON Web Key Set (JWKS) URL of your identity provider. For example:

`https://asacm.auth0.com/.well-known/jwks.json`

Authorization Endpoint

Paste the authorization endpoint of your identity provider. For example:

`https://asacm.auth0.com/authorize`

Access Token Endpoint

Paste the token endpoint of your identity provider. For example:

```
https://asacm.auth0.com/oauth/token
```

UserInfo Endpoint

Paste the `UserInfo` endpoint of your identity provider. For example:

```
https://asacm.auth0.com/userinfo
```

Logout Endpoint

Paste the logout URL of your identity provider. For example:

```
https://asacm.auth0.com/v2/logout
```

Internal password

The password authentication mechanism for the Web interface-registered administrators. Click the **Force Password Change** button if you want all the administrators to change the password at the next login.

Lightweight Directory Access Protocol

In the Lightweight Directory Access Protocol (LDAP) server, add the following attributes to the authorized users.

Attribute	Value
email	An email address to identify the user uniquely.
memberOf	The name of the group to which the user belongs. You can only omit this attribute if you also omit the Required Group Name setting described below.

In the Cryptographic Security Platform console, configure the following settings for an LDAP identity provider.


- [Active](#)
- [LDAP URI](#)
- [User DN Template](#)
- [Required Group Name](#)
- [LDAP SSL CA Bundle \(PEM\)](#)
- [Active Directory](#)
- [Active Directory Email Domain](#)
- [Active Directory Base Lookup DN](#)

Active

Check this box to enable the identity provider.

LDAP URI

Paste the URI of the LDAP or Active Directory server.

 When the URI does not include the LDAP port, 389 is assumed.

User DN Template

Enter a template for building the user's DN – for example:

```
uid={0},ou=users,dc=abccorp,dc=dev,dc=entrust,dc=com
```

Required Group Name


Enter the value of the `memberOf` LDAP attribute for users with login permissions. Enter the name of an LDAP group, not the full DN – for example, `CorpUser` grants access to members of an LDAP group with the following DN.

```
cn=CorpUser,ou=groups,dc=abccorp,dc=dev,dc=entrust,dc=com
```

Omit this optional field to authorize all LDAP users.

LDAP SSL CA Bundle (PEM)

Paste the certification chain of the LDAP server SSL certificate, as a bundle in PEM format.

 This parameter is mandatory for LDAPS connections when the LDAP server SSL certificate issuer is not a publicly trusted CA.

Active Directory

Check this box for configuring Active Directory-specific parameters.

Active Directory Email Domain

Enter the domain of the Active Directory email addresses.

Active Directory Base Lookup DN

Enter the root base for searching distinguished names in the Active Directory.

OpenID Connect 1.0

In the Cryptographic Security Platform console, configure the following settings for an OpenID Connect 1.0 identity provider.

- [Active](#)
- [Name](#)
- [Redirect URL](#)
- [Client Secret](#)
- [Client ID](#)
- [Required Group Attribute Name](#)
- [Required Group Name](#)
- [JWKS URL](#)
- [Authorization Endpoint](#)
- [Access Token Endpoint](#)
- [UserInfo Endpoint](#)
- [Logout Endpoint](#)

Active

Check this box to enable the identity provider.

Name

The identity provider name displayed when logging into the Cryptographic Security Platform console.

Redirect URL

The URL to redirect to when the identity provider successfully authenticates a user. Cryptographic Security Platform automatically generates this value when you click **Save**. You must:

1. Copy this value from the Cryptographic Security Platform console.
2. Paste this URL on the redirect URLs field of your IdP interface – for example, on the **Allowed Callback URLs** field of an auth0 identity provider.

When the Cryptographic Security Platform host URL changes, you must:

1. Re-type the **Client Secret** and **Client ID** values on the Cryptographic Security Platform console.
2. Click **Save**.
3. Copy the new **Redirect URL** value from the Cryptographic Security Platform console.
4. Paste this URL on the redirect URLs field of your IdP interface.

Client Secret

The client secret provided by your identity provider.

Client ID

The client identifier provided by your identity provider.

Required Group Attribute Name

The claim name provided by your identity provider for user access restriction. See below an example for Auth0.

```
https://asacm/group
```

This custom claim must start with `https` or `http` and cannot include a dot. For example:

```
function (user, context, callback){  
  context.idToken['https://asacm/group'] = user.app_metadata.group;  
  callback(null, user, context);  
}
```

See <https://auth0.com/docs/scopes/openid-connect-scopes> for how to create a custom claim.

Required Group Name

The claim value provided by your identity provider for user access restriction. See below an example for Auth0 where only users in the "admin" group have access permissions.

```
"app_metadata": {  
  "group": "admin"  
},
```

JWKS URL

The JSON Web Key Set (JWKS) URL of your identity provider. For example:

```
https://asacm.auth0.com/.well-known/jwks.json
```

Authorization Endpoint

The authorization endpoint of your identity provider. For example:

```
https://asacm.auth0.com/authorize
```

Access Token Endpoint

The token endpoint of your identity provider. For example:

```
https://asacm.auth0.com/oauth/token
```

UserInfo Endpoint

The UserInfo endpoint of your identity provider. For example:

`https://asacm.auth0.com/userinfo`

Logout Endpoint

The logout URL of your identity provider. For example:

`https://asacm.auth0.com/v2/logout`

7 Managing Certificate Authority

With the Certificate Authority solution, you can create and manage a PKI hierarchy comprising:

- Root Certificate Authorities, either created from scratch or imported.
- Subordinate Certificate Authorities, also known as *certificate issuing* Certificate Authorities.
- OCSP and CRL services to check the status of the issued certificates.
- CA gateway API for integration with Entrust and third-party client applications.

See below for configuring, deploying, and administrating the Certificate Authority solution.

- [Configuring and deploying Certificate Authority](#)
- [Creating Certificate Authority tenants](#)
- [Managing organizations](#)
- [Managing Certificate Authority instances](#)
- [Issuing certificates with Certificate Authority instances](#)
- [Changing the HSM vendor](#)

See [Browsing logs with Grafana](#) for how to browse Certificate Authority logs.

Configuring and deploying Certificate Authority

See below for configuring and deploying the Certificate Authority solution with the Management Console.

i Repeat the following steps each time a configuration update is required. Do not forget to click **Deploy** to make the changes effective.

To configure and deploy Certificate Authority with the Management Console

1. Open the following URL in a Web browser.

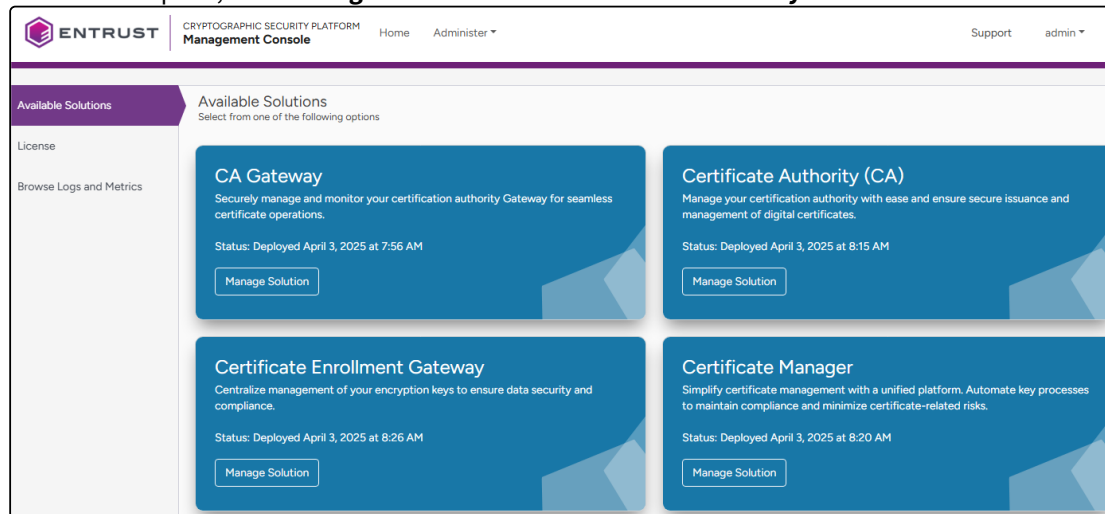
```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

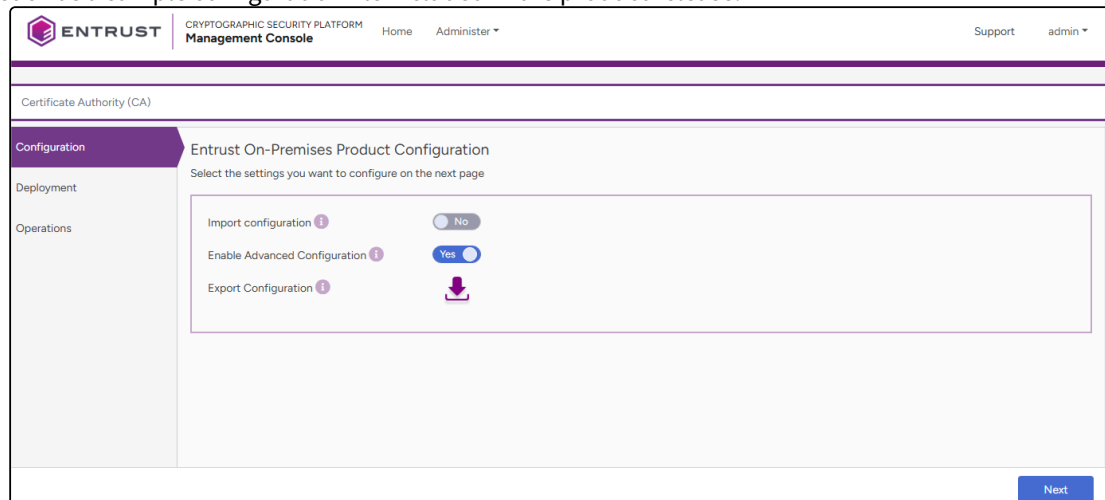
2. Log into the Management Console a user belonging to a role with permissions to manage Certificate Authorities – for example, the initial `admin` administrator user.

i See [Starting up the Management Console](#) for how to manage users and roles.

3. In the content pane, click **Manage Solution** under **Certificate Authority**.



4. Activate the **Import configuration** toggle switch if you want to import configuration settings from a file, such as a sample configuration file included in the product release.



5. Active the **Enable Advanced Configuration** if you want to configure the full set of configuration parameters supported by the solution.
6. Click **Next**.
7. Configure the solution settings described in the following sections.
 - [Database](#)
 - [HSM](#)
 - [General](#)
8. Click **Validate** to validate the configured settings.
9. Correct any detected configuration error until the **Validate** option displays no warnings.
10. Optionally, click the **Download** button to export the current configuration. You can later import this configuration using the already mentioned **Import configuration** toggle switch.
11. Click **Submit** and wait while Cryptographic Security Platform uploads the configuration and any attached file, such as a P12 file with authentication credentials.
12. Click **Deploy**.
13. Check the deployment information. Specifically, The **Important Information** field displays the URI of the online endpoints.

Database


Select the **Database** tab of the **Configuration** page to configure the connection with the external database.

- [Database URL](#)
- [Database Name](#)
- [Database username](#)
- [Database password](#)
- [Enable SSL mode for the PostgreSQL database](#)
- [CA Certificate\(s\)](#)

 See [Database requirements](#) for details on the external database.

Database URL

The IP address or Fully Qualified Domain Name (FQDN) of the database host.

 As explained in [Database SSL certificate](#), the SSL certificate for the database host must include the IP address or FQDN of the host.

Mandatory: Yes.

Database Name

The name of the database

Mandatory: Yes.

Database username

The username for connecting with the database.

Mandatory: Yes.


Database password

The password for connecting with the database.

Mandatory: Yes.

Enable SSL mode for the PostgreSQL database


yes to enable SSL security in the database connection; **no** otherwise.

 The **no** option is for testing environments only.

Mandatory: Yes.

CA Certificate(s)

The CA certificate chain for validating the database SSL certificate. Click **Select Files** to import each certificate file in PEM format and Base64 encoding.


 As explained in [Database SSL certificate](#), the SSL certificate for the database host must include the IP address or FQDN of the host.

Mandatory: When **Enable SSL mode for the PostgreSQL** database is **yes**.

HSM

Select the **HSM** tab of the **Configuration** page to configure the Hardware Security Module (HSM).

- [Vendor](#)
- [OCS \(Operator Card Set\) passphrase](#)
- [RFS \(remote file system\) host to download the nShield kmdata files](#)
- [Username to download the nShield files](#)
- [Password to download the nShield files](#)
- [Signing key unique identifier](#)

 After deploying Certificate Authority, you cannot switch between HSM and no-HSM, nor can you alter any HSM configuration set on this page. However, you can still make the changes described in [Administering nShield HSM integration](#).

Vendor


The identifier of the HSM manufacturer.

Vendor	Description
none	A built-in software PKCS #11 module (not recommended).
nshield	An Entrust nShield HSM. See HSM requirements for the supported versions.

Mandatory: Yes.

OCS (Operator Card Set) passphrase

The passphrase of the operator card set

 The OCS must be inserted during the first deployment to create the signing key. There has to be a quorum of 1.

Mandatory: Yes.

RFS (remote file system) host to download the nShield kmdata files

The domain name or the IP address of the host for downloading the kmdata configuration files of the HSM. The first deployment will make an SSH call to download these files from the RFS.

Mandatory: When the value of **Vendor** is **nShield**.

Username to download the nShield files

The username for logging into the host and downloading the kmdata configuration of the HSM.

Mandatory: When the value of **Vendor** is **nShield**.


Password to download the nShield files

The password for logging into the host and downloading the kmdata configuration of the HSM.

Mandatory: When the value of **Vendor** is **nShield**.

Signing key unique identifier

Choose a unique identifier consisting of only lowercase alphanumeric characters for the signing key created on deployment.

 After the first deployment, you must back up the configuration files – specifically the `kmdata.tar` file, which includes this key.

Mandatory: When the value of **Vendor** is **nShield**.


General

Select the **General** tab of the **Configuration** page to configure the CRL (Certificate Revocation List) generation.

- [Hostname](#)
- [CRL Generation \(in days\)](#)

Hostname

The public domain name or IP address of a node in the Cryptographic Security Platform cluster.

 This value can correspond to the domain name or IP address assigned by a proxy or load balancer that redirects traffic to the node.

Each CA instance will publish a non-partitioned Certificate Revocation List at the following URI.

```
http://{hostname}/crl/{organization}/{caid}/crl.crl
```

Where:

- `{hostname}` is the value of the **Hostname** field.
- `{organization}` is the name of the organization selected when [Managing Certificate Authority instances](#).
- `{caid}` is the CA identifier selected when [Managing Certificate Authority instances](#).

Mandatory: Yes.

CRL Generation (in days)

The number of days between each CRL issuance.

Mandatory: No. When omitting this value, the Certificate Authority solution does not issue CRLs.

Creating Certificate Authority tenants

Each tenant is a user who can manage organizations and Certificate Authorities.

i The tenant's user sessions expire after 30 minutes, requiring a re-login.

To create a tenant

1. Follow the steps in [Creating Management Console roles](#) to create a role with at least the **Manage and Operate Certificate Authority (CA)** permission.
2. Follow the steps in [Creating Management Console users](#) to create a user and grant him this role.

Managing organizations

Each organization is an independent partition for a set of Certificate Authorities. Before creating your PKI hierarchy of Certificate Authorities, you must create or select the organization they will belong to.

- [Creating an organization](#)
- [Joining an organization](#)
- [Leaving an organization](#)
- [Adding administrators to an organization](#)

i Certificate Authorities in different organization can share the same identifier.

Creating an organization

See below for creating a new organization for your PKI hierarchy of Certificate Authorities.

To create an organization

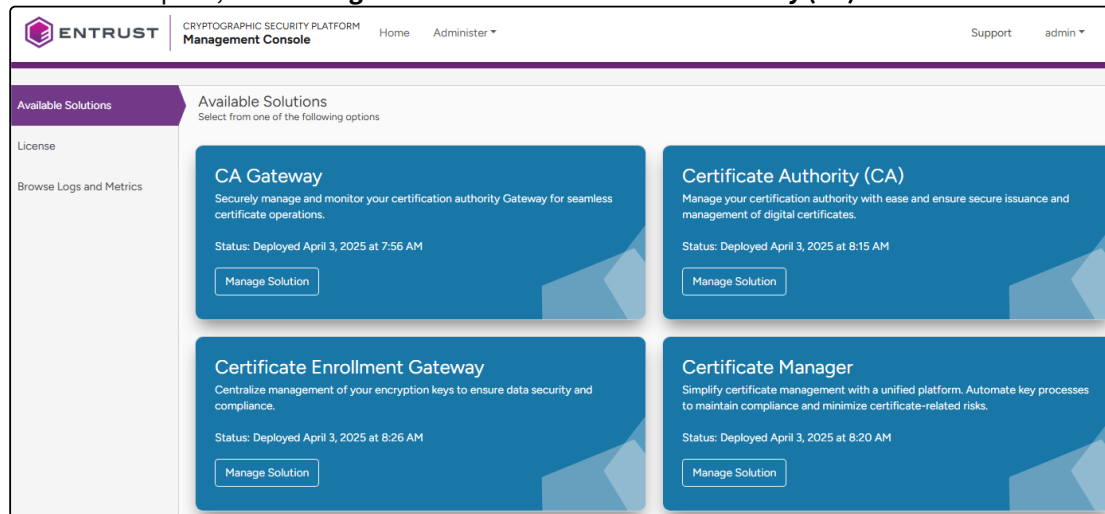
1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

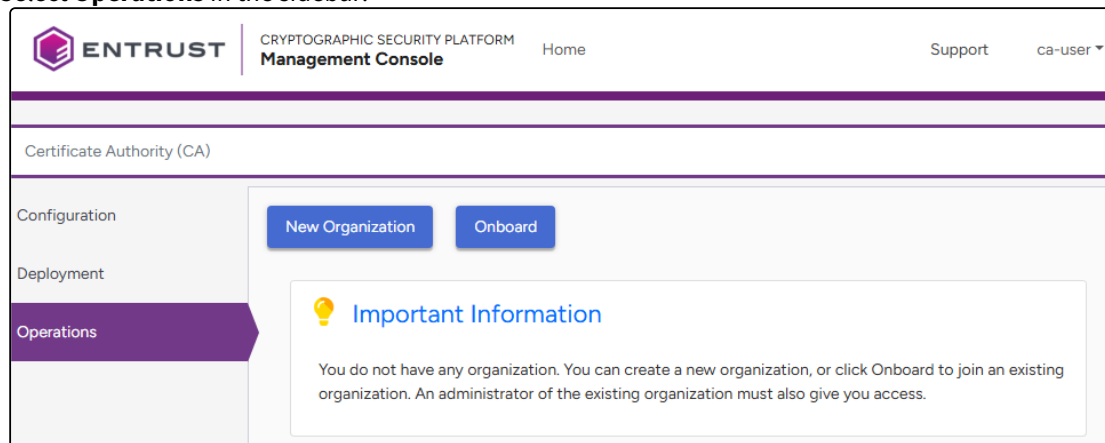
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log in to the Management Console as one of the users created in [Creating Certificate Authority tenants](#). This user will be the tenant of the new organization and the Certificate Authorities it contains.

- In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



- Select **Operations** in the sidebar.



- Click **New Organization**.
- Enter a name in the **Create Organization** dialog. This name:
 - Must be 3-14 characters long.
 - Can only include lowercase letters, numbers, underscores (" _"), and hyphens (" -").
 - Cannot match any of the reserved words:
 - acs
 - ca
 - cas
 - crl
 - crlagent
 - crlresponder
 - deploy
 - idp
 - main
 - meteringca
 - persistgc
 - pkihub
 - pkihubidp
 - scheduler
 - schema

- schemas
 - schemes
 - vaagent
- Click **Create** to create the organization. Your username will be added to the **Administrator** tab as the organization administrator.

Joining an organization

Instead of creating an organization for your PKI hierarchy, you can join an existing one.

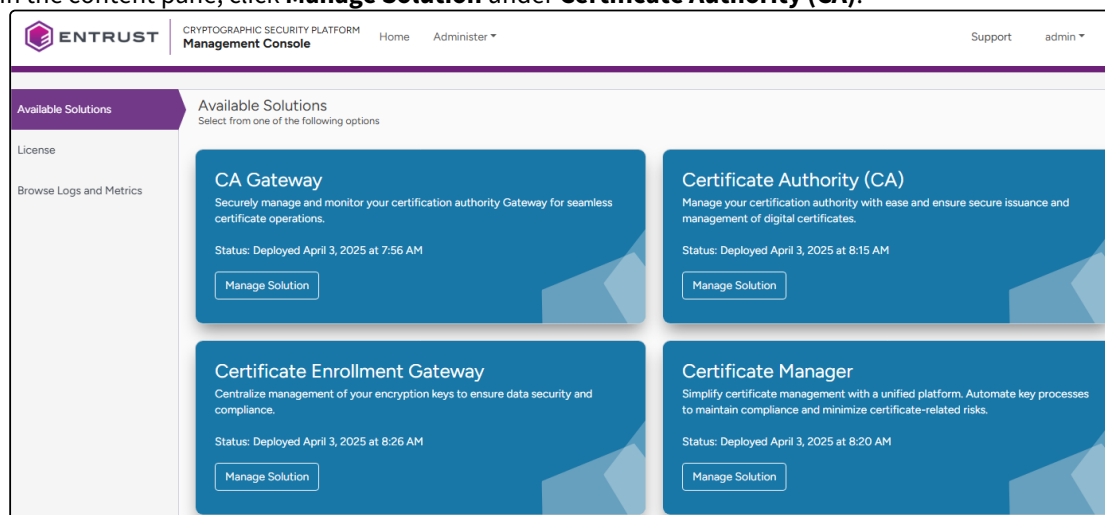
To join an organization

- Open the following URL in a Web browser.

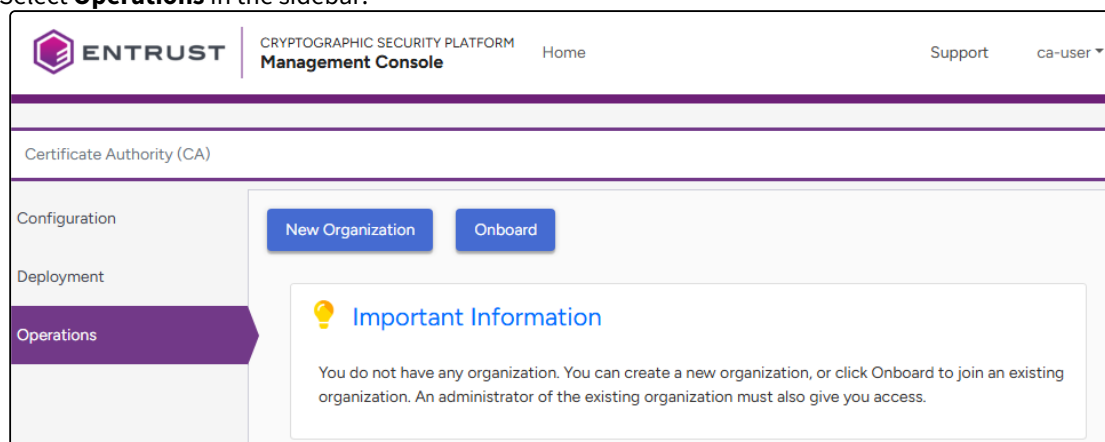
`https://<machine>/management-console`

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

- Log in to the Management Console as one of the users created in [Creating Certificate Authority tenants](#).
- In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



- Select **Operations** in the sidebar.



- Click **Onboard**.

6. Click **Join an Organization**.
7. Enter the name of an existing organization in the **Join Organization** dialog.
8. Click **Join**.

Leaving an organization

If no longer needed for your PKI hierarchy, you can leave an organization you have created or joined.

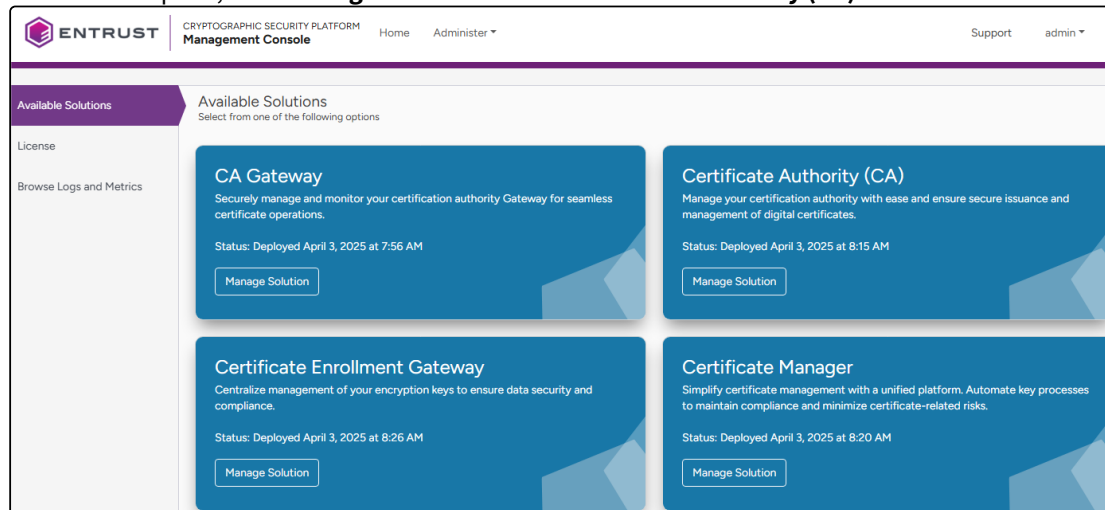
To leave organization

1. Open the following URL in a Web browser.

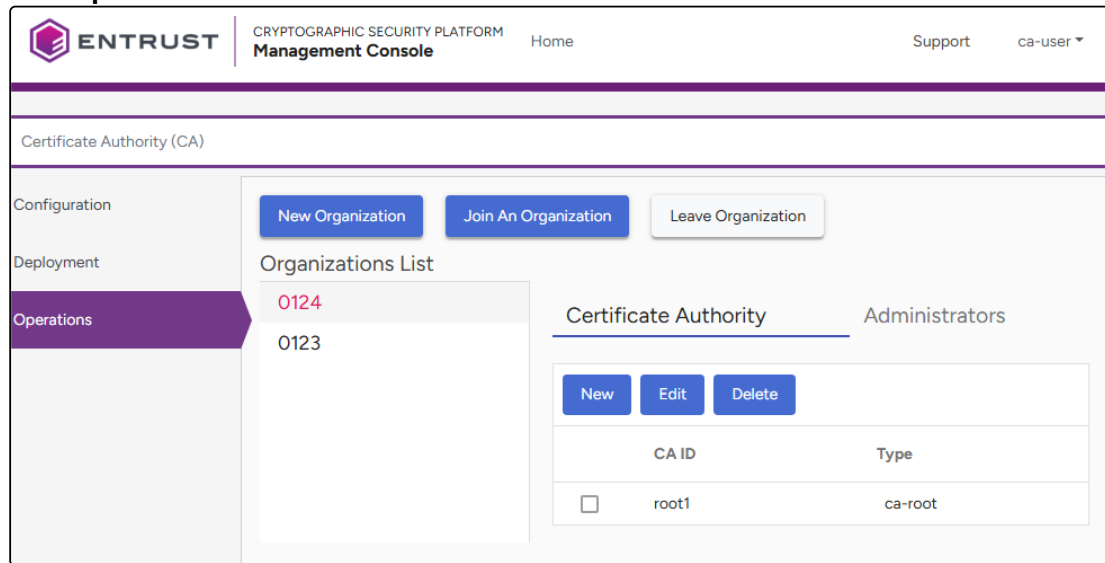
```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log in to the Management Console as one of the users created in [Creating Certificate Authority tenants](#).
3. In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



4. Select **Operations** in the sidebar.



5. Select an organization under **Organizations List**.
6. Click **Leave Organization**.
7. Click **Leave** in the **Leave Organization** confirmation dialog.

Adding administrators to an organization

After creating or joining an organization, you can add more administrators to this organization.

! For administrators to be added, you must previously register them as explained in [Creating Certificate Authority tenants](#).

To add administrators to an organization

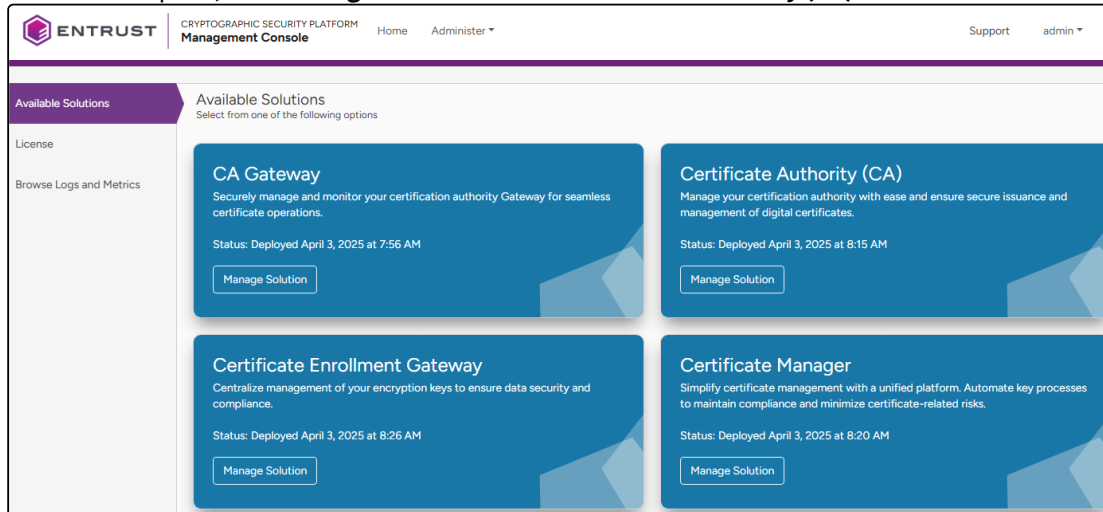
1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

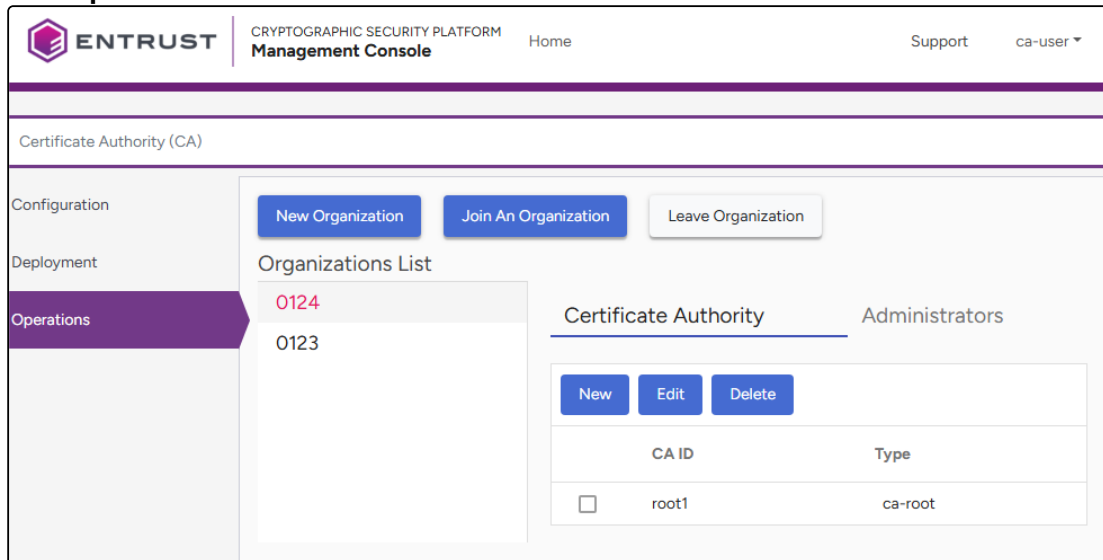
2. Log in to the Management Console as one of the users created in [Creating Certificate Authority tenants](#).

- In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



The screenshot shows the Entrust Management Console interface. The top navigation bar includes the Entrust logo, "CRYPTOGRAPHIC SECURITY PLATFORM Management Console", "Home", "Administer", "Support", and "admin". The left sidebar has "Available Solutions" selected. The main content area displays four solution cards: "CA Gateway", "Certificate Authority (CA)", "Certificate Enrollment Gateway", and "Certificate Manager". Each card includes a description, deployment status, and a "Manage Solution" button. The "Certificate Authority (CA)" card is the focus of the instruction.

- Select **Operations** in the sidebar.

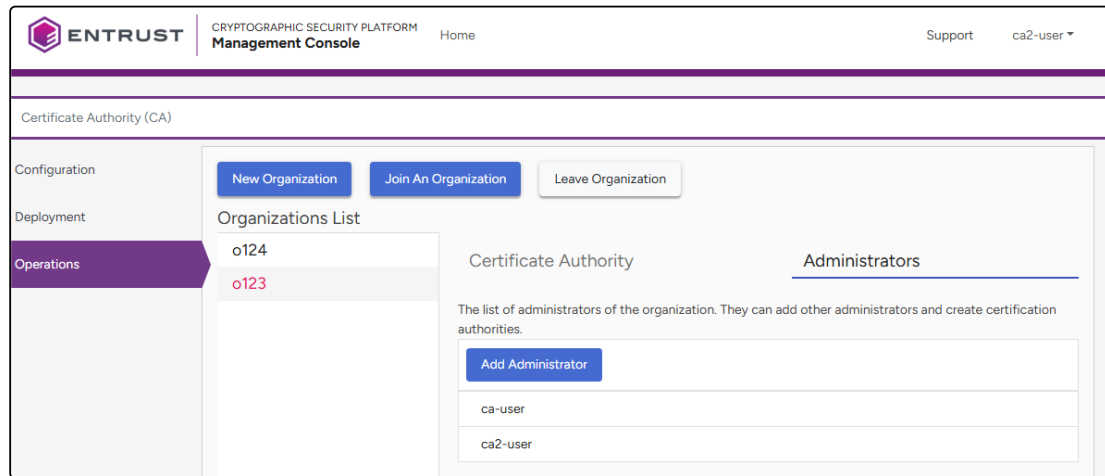


The screenshot shows the Entrust Management Console interface with the "Operations" sidebar selected. The main content area displays the "Certificate Authority (CA)" section. It includes buttons for "New Organization", "Join An Organization", and "Leave Organization". Below these is the "Organizations List" with two entries: "0124" (highlighted in red) and "0123". To the right, the "Certificate Authority" tab is active, showing a table of administrators.

CA ID	Type
<input type="checkbox"/> root1	ca-root

- Select an organization under **Organizations List**.
- Click the **Administrators** tab.

7. Click **Add Administrator**.



8. Click the administrator username in the **Add Administrator** dialog.
9. Click **Add**.

Managing Certificate Authority instances

With the Certificate Authority solution, you can create and manage a complete PKI hierarchy of Certificate Authorities (CAs).

- [Creating a root Certificate Authority](#)
- [Adding an external root Certificate Authority](#)
- [Creating an issuing Certificate Authority](#)
- [Deleting a Certificate Authority](#)
- [Editing Certificate Authority settings](#)

Creating a root Certificate Authority

See below for creating a root Certificate Authority (CA) with a self-signed certificate issued by the Certificate Authority solution.

To create a root Certificate Authority instance

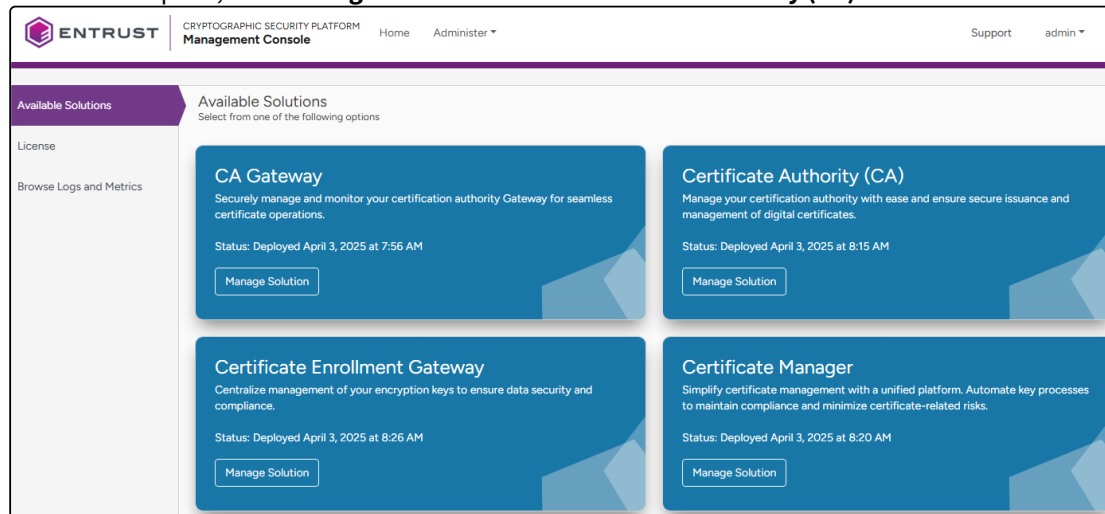
1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

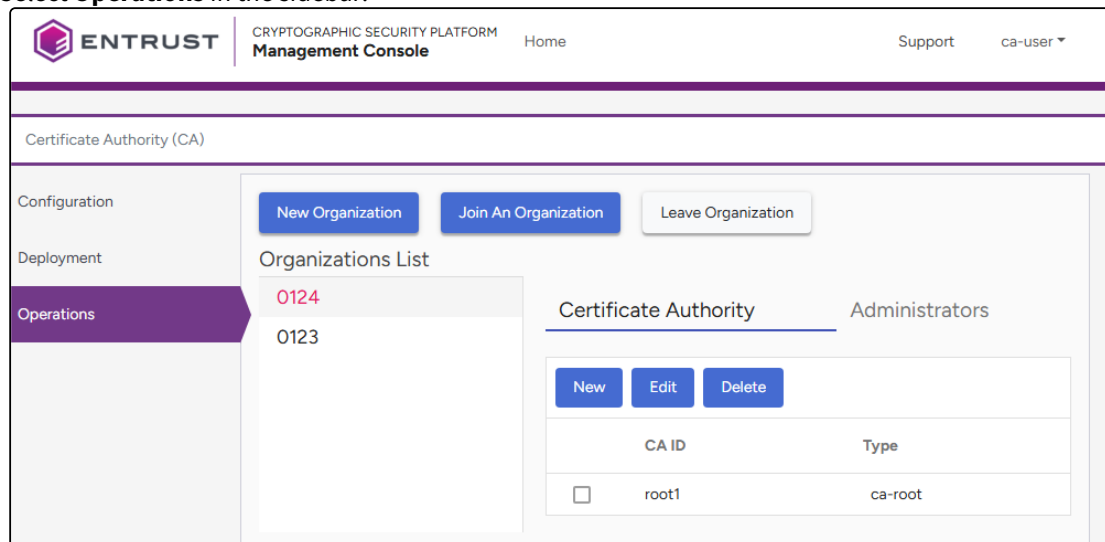
Where **<machine>** is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log in to the Management Console as one of the users created in [Creating Certificate Authority tenants](#). This user will be the tenant of the new root Certificate Authority.


- In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



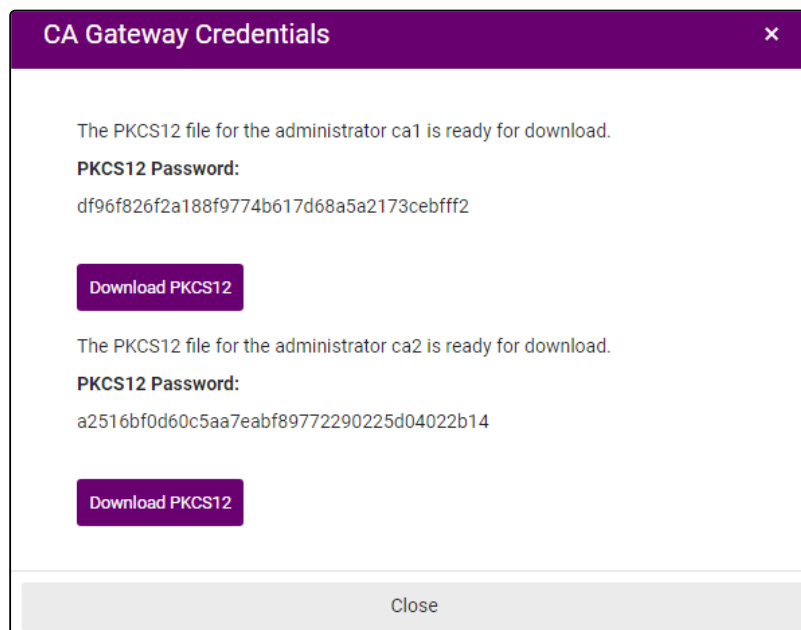
- Select **Operations** in the sidebar.



- Select an organization under **Organization List**.

 See [Managing organizations](#) for how to create or join an organization.

- Click **New** under **Certificate Authority**.
- Configure the following settings.
 - CA Type
 - CA ID
 - CA Key Type
 - Certificate Profiles
 - Expiration Date
 - Attributes
 - Auditors
 - Administrators
- Click **Submit** to create the new Certificate Authority.
- Copy the password of the client authentication PKCS #12 created for each new auditor or administrator (if any).



10. Click **Download PKCS12** to download the PKCS #12 files. Each PKCS #12 includes:
 - The certificate of the CA that issues the client certificates. This certificate is also available in the **Certificate Authority for CA Gateway Clients** tab.
 - A client certificate.
 - The private key of the client certificate.
11. Save the PKCS #12 files and passwords in a secure place, as you cannot obtain them later.

CA Type

Click **Root Certificate Authority**.

Mandatory: Yes.

CA ID

Type a unique identifier for the new Certificate Authority within its organization. This identifier:

- Must be 3-18 characters long.
- Can only include lowercase letters, numbers, underscores (" _"), and hyphens ("-").

 Do not reuse the identifier of a Certificate Authority for up to 24 hours after it has been deleted.


Mandatory: Yes.

CA Key Type

The type of key the new Certificate Authority will use to sign certificates.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256

Key algorithm	Signature algorithm
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

Mandatory: Yes.

Certificate Profiles

The profiles the Certificate Authority will support for issuing certificates. See the [Certificate profiles reference](#) for a description of each profile.

Mandatory: Select at least one profile.

Expiration Date

The expiration date for the certificate signing certificate of the Certificate Authority.

Mandatory: No. This value defaults to the following dates.

CA Type	Default expiration date
Root Certificate Authority	20 years after the certificate is issued
Issuing Certificate Authority	10 years after the certificate is issued

Attributes

The value of each attribute in the Distinguished Name (DN) of the Certificate Authority certificate.


Mandatory: Set at least the [CN](#) attribute of the Distinguished Name.

Auditors


Enter the names of the users who will have auditor permission on the Certificate Authority. For each name, you can:

- Enter a user name already assigned to another CA so that the user will have permissions on different CAs.

- Enter a new user.

 Upon CA creation, the Management Console only displays download buttons for the client authentication PKCS #12 of the new users.


Mandatory: No. When omitting this value, the Certificate Authority will not have users with only auditing permission.

 Use the trash icon to remove **Auditor** fields you do not want to fill out. Otherwise, they will display a **Please fill out this field** warning when you click **Save**.

Administrators

Enter the names of the users who will have administration permission on the Certificate Authority. For each name, you can:


- Enter a user name already assigned to another CA so that the user will have permissions on different CAs.
- Enter a new user.

 Upon CA creation, the Management Console only displays download buttons for the client authentication PKCS #12 of the new users.

Mandatory: Yes. Add the name of at least one administrator.

Adding an external root Certificate Authority

See below for adding an external root Certificate Authority (CA) – that is, a root Certificate Authority created outside the Certificate Authority solution.

 The following steps will ask you to have the certificate of this external CA at hand.

To add an external root Certificate Authority

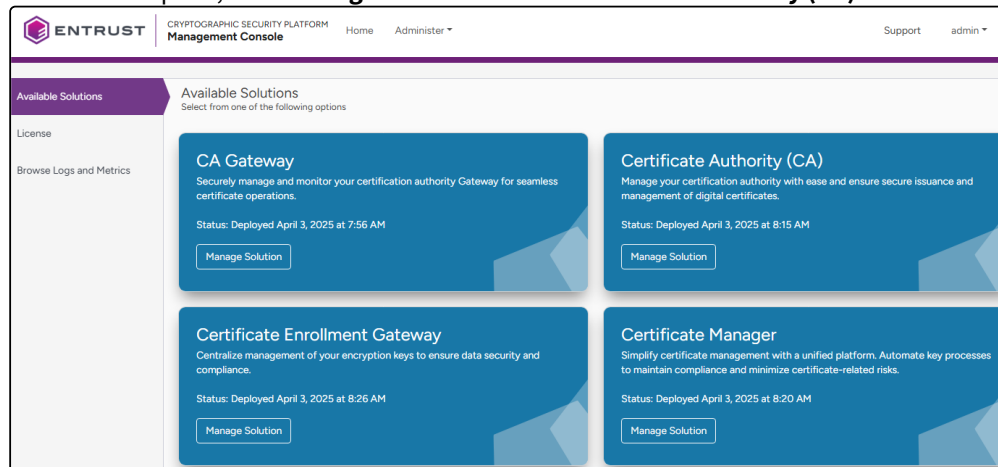
1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

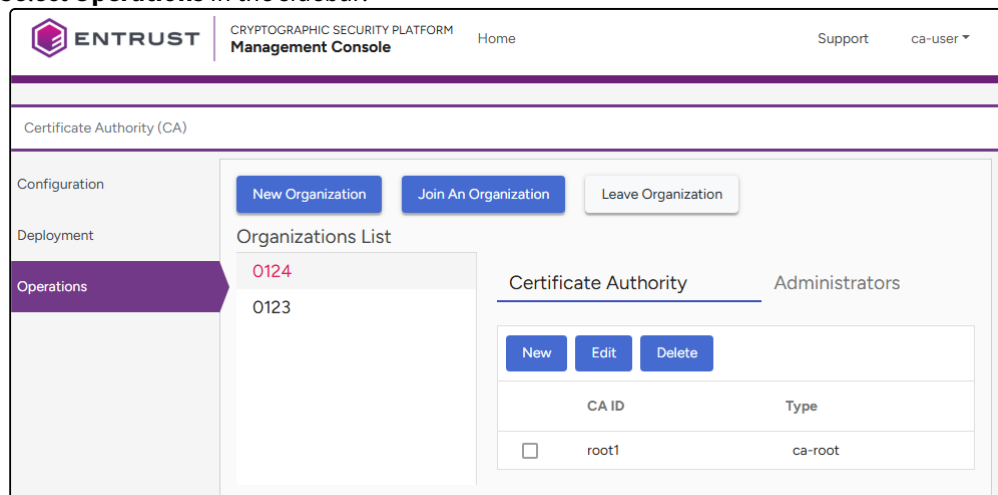
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log in to the Management Console as one of the users created in [Creating Certificate Authority tenants](#). This user will be the tenant of the new root external Certificate Authority.


3. In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



4. Select **Operations** in the sidebar.



5. Select an organization under **Organizations list**.

 See [Managing organizations](#) for how to create or join an organization.

6. Click **New** under **Certificate Authority**.
7. Configure the following settings.
 - [CA Type](#)
 - [CA ID](#)
 - [Self-Signed Root Certificate](#)
8. Click **Submit** to create the new Certificate Authority.

CA Type


Click **External Root Certificate Authority**.

Mandatory: Yes.

CA ID

Type a unique identifier for the new Certificate Authority within its organization. This identifier:

- Must be 3-18 characters long.
- Can only include lowercase letters, numbers, underscores (" _"), and hyphens (" -").

 Do not reuse the identifier of a Certificate Authority for up to 24 hours after it has been deleted.

Mandatory: Yes.

Self-Signed Root Certificate


Paste the PEM-encoded certificate signing certificate of the external CA – for example:

```
-----BEGIN CERTIFICATE-----
MIIEKjCCAxKgAwIBAgIEOGPe+DANBgkqhkiG9w0BAQUFADCbtDEUMBIGA1UEChMLRW50cnVzdC5u
ZXQxQDA+BgNVBASUN3d3dy5lbnRydXN0Lm5ldC9DUFNFmjaA00CBpbmNvcnAuIGJ5IHJlZi4gKGxp
bWl0cyBsaWFiLkxJTAjBgNVBASThChjKSAXOTk5IEVudHJ1c3QubmV0IExpbnWl0ZWQxMzAxBgNV
...
zX1XEC+bBAlahLVu2B064dae0Wx5XnkcFMXj0EyT02U87d89vqb1lRrDtRnDvV5bu/8j72gZyxKT
J1wDLW8w0B62GqzeWvfRqqgnpv55gcR5mTNXuhKwqeBCbJPKVt7+bYQLCIt+jerXmCHG8+c8eS9e
nNFMFY3h7CI3zJpDC5fcgJCNS2ebb0gIFVbPv/Erff6adulZkMV8gzURZVE=
-----END CERTIFICATE-----
```

Mandatory: Yes.

Creating an issuing Certificate Authority

See below for creating a certificate issuing or *subordinate* Certificate Authority (CA).

-  If the root CA of the new issuing CA is an external root CA, you must have the certificate issued by the root CA for the issuing CA at hand.

To create an issuing Certificate Authority

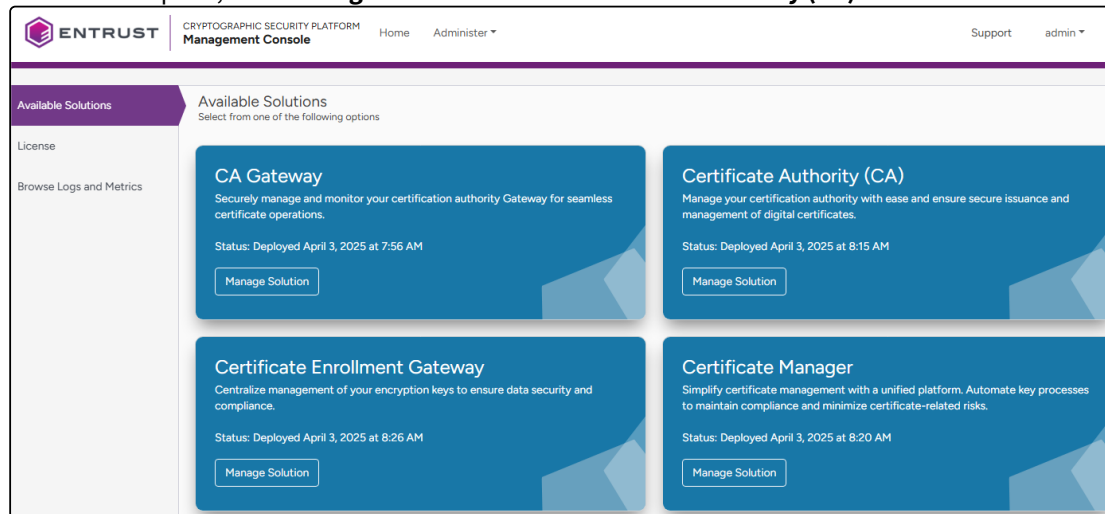
1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

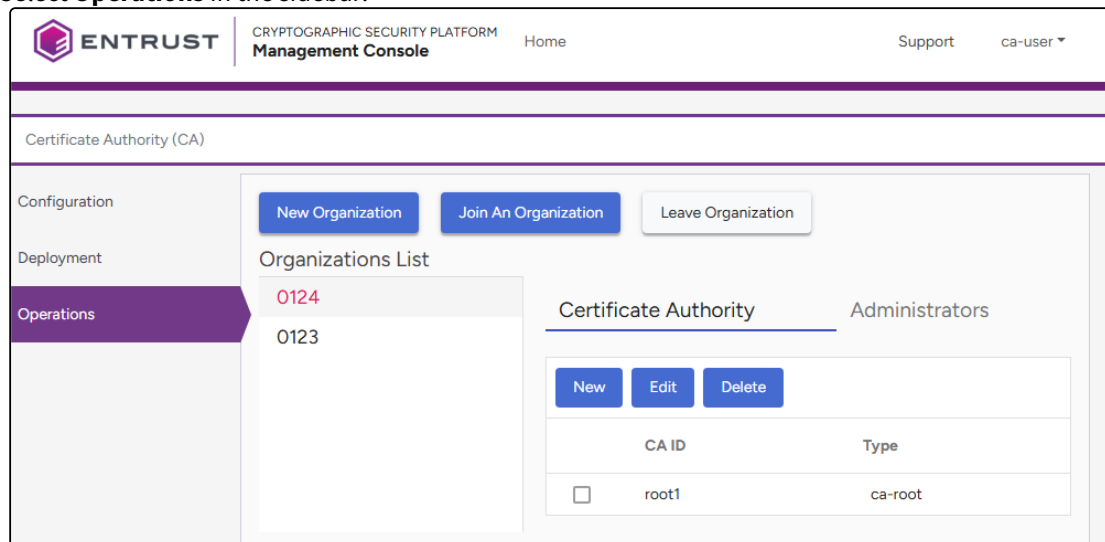
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log in to the Management Console as one of the users created in [Creating Certificate Authority tenants](#). This user will be the tenant of the new issuing Certificate Authority.


- In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



- Select **Operations** in the sidebar.

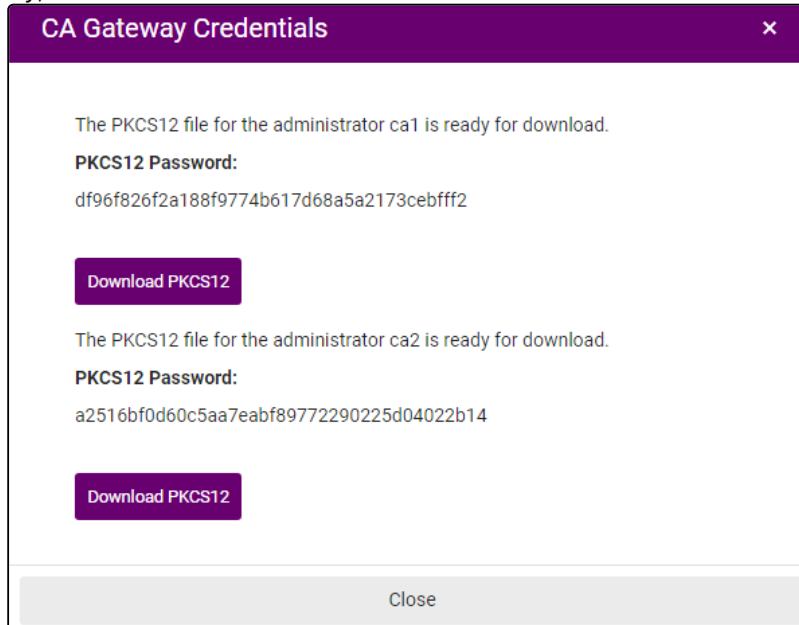


- Select an organization under **Organizations list**.

 See [Managing organizations](#) for how to create or join an organization.

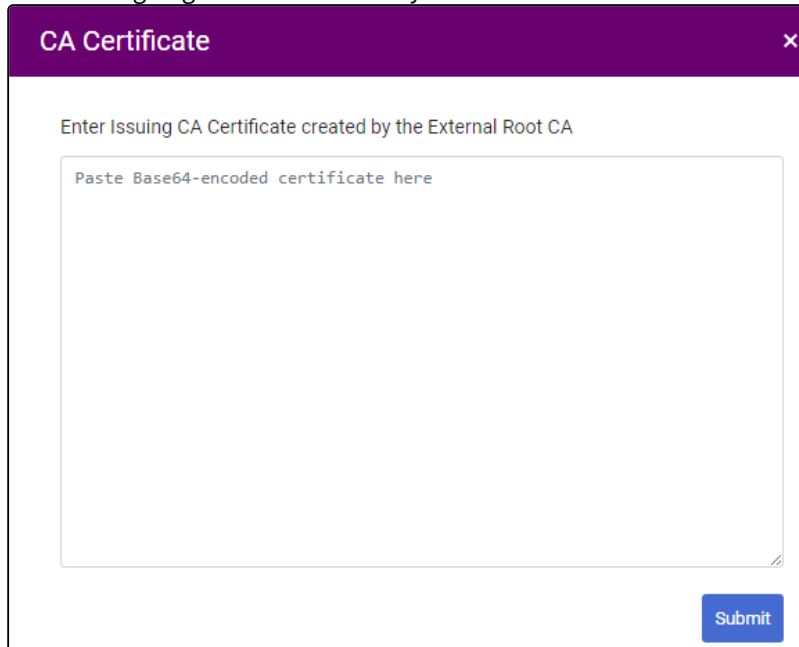
- Click **New** under **Certificate Authority**.
- Configure the following settings.
 - CA Type
 - CA ID
 - CA Key Type
 - Certificate Profiles
 - Issuer CA ID
 - Expiration Date
 - Attributes
 - Auditors
 - Administrators
 - OCSP Key Type
- Click **Submit** to create the new Certificate Authority.

9. Copy the password of the client authentication PKCS #12 created for each new auditor or administrator (if any).



The dialog box is titled "CA Gateway Credentials" with a close button (X) in the top right corner. It contains two sections for downloading PKCS12 files. The first section states: "The PKCS12 file for the administrator ca1 is ready for download." followed by "PKCS12 Password:" and the password "df96f826f2a188f9774b617d68a5a2173cebfff2". Below this is a blue "Download PKCS12" button. The second section states: "The PKCS12 file for the administrator ca2 is ready for download." followed by "PKCS12 Password:" and the password "a2516bf0d60c5aa7eabf89772290225d04022b14". Below this is another blue "Download PKCS12" button. At the bottom of the dialog is a grey "Close" button.

10. Click **Download** to download the PKCS #12 files. Each PKCS #12 includes:
 - The certificate of the CA that issues the client certificates. This certificate is also available in the **Certificate Authority for CA Gateway Clients** tab.
 - A client certificate.
 - The private key of the client certificate.
11. Save the PKCS #12 files and passwords in a secure place, as you cannot obtain them later.
12. If the root CA of the new issuing CA is an external root CA, click **Upload certificate** and paste a PEM-encoded certificate signing certificate issued by the root CA.



The dialog box is titled "CA Certificate" with a close button (X) in the top right corner. It contains the text "Enter Issuing CA Certificate created by the External Root CA". Below this is a large text area with the placeholder text "Paste Base64-encoded certificate here". At the bottom right of the dialog is a blue "Submit" button.

CA Type


Click **Issuing Certificate Authority**.

Mandatory: Yes.

CA ID

Type a unique identifier for the new Certificate Authority within its organization. This identifier:

- Must be 3-18 characters long.
- Can only include lowercase letters, numbers, underscores (" _"), and hyphens (" -").


 Do not reuse the identifier of a Certificate Authority for up to 24 hours after it has been deleted.

Mandatory: Yes.

CA Key Type

The type of key the new Certificate Authority will use to sign certificates.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

Mandatory: Yes.

Certificate Profiles

The profiles the Certificate Authority will support for issuing certificates. See the [Certificate profiles reference](#) for a description of each profile.

Mandatory: Select at least one profile.

Issuer CA ID

The identifier of the root Certificate Authority.

Mandatory: Yes.

Expiration Date

The expiration date for the certificate signing certificate of the Certificate Authority.

Mandatory: No. This value defaults to the following dates.

CA Type	Default expiration date
Root Certificate Authority	20 years after the certificate is issued
Issuing Certificate Authority	10 years after the certificate is issued

Attributes


The value of each attribute in the Distinguished Name (DN) of the Certificate Authority certificate.

Mandatory: Set at least the **CN** attribute of the Distinguished Name.


Auditors

Enter the names of the users who will have auditor permission on the Certificate Authority. For each name, you can:

- Enter a user name already assigned to another CA so that the user will have permissions on different CAs.
- Enter a new user.

 Upon CA creation, the Management Console only displays download buttons for the client authentication PKCS #12 of the new users.


Mandatory: No. When omitting this value, the Certificate Authority will not have users with only auditing permission.

 Use the trash icon to remove **Auditor** fields you do not want to fill out. Otherwise, they will display a **Please fill out this field** warning when you click **Save**.

Administrators

Enter the names of the users who will have administration permission on the Certificate Authority. For each name, you can:

- Enter a user name already assigned to another CA so that the user will have permissions on different CAs.
- Enter a new user.

 Upon CA creation, the Management Console only displays download buttons for the client authentication PKCS #12 of the new users.

Mandatory: Yes. Add the name of at least one administrator.

OCSF Key Type

The type of key to sign OCSF responses at the following endpoint.


```
http://{pkihub}/ocsp/{organization}/{caid}
```

- `{pkihub}` is the domain name or IP address of the machine running Cryptographic Security Platform.
- `{organization}` is the identifier of the CA organization.
- `{caid}` is the value of the **CA ID** field.

Mandatory: Yes.

Deleting a Certificate Authority

See below for deleting a Certificate Authority (CA).

 Before deleting a root CA you must delete all its subordinate CAs.

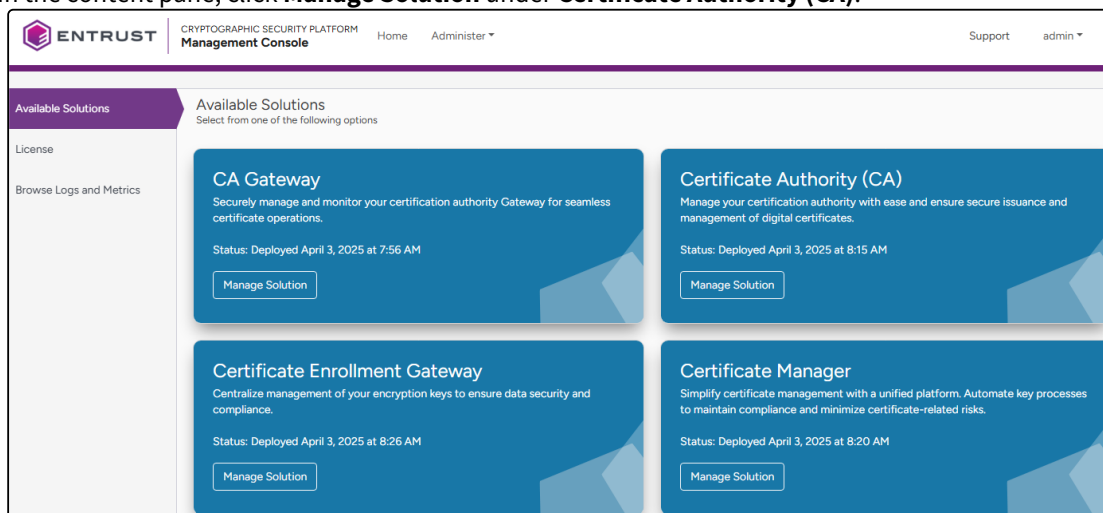
To delete a Certificate Authority

1. Open the following URL in a Web browser.

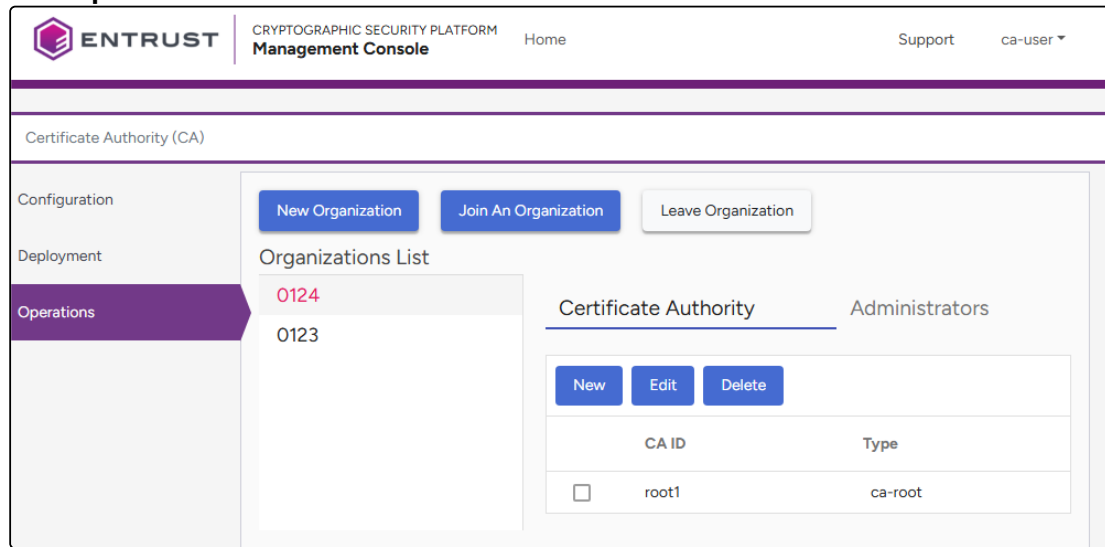
```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log in to the Management Console as one of the users created in [Creating Certificate Authority tenants](#). This user will be the tenant of the new issuing Certificate Authority.
3. In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



4. Select **Operations** in the sidebar.



5. Select an organization under **Organizations list**.
6. Select a CA under **Certificate Authority**.
7. Click **Delete**.
8. Click **Delete** in the **Delete CA** confirmation dialog.

Editing Certificate Authority settings

See below for editing the settings of a Certificate Authority (CA).

To edit a Certificate Authority

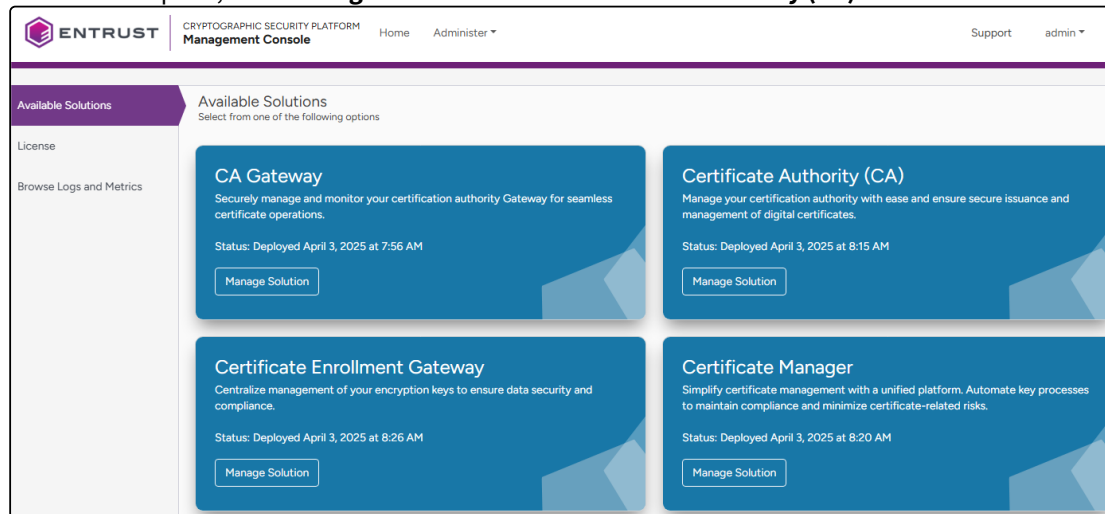
1. Open the following URL in a Web browser.

`https://<machine>/management-console`

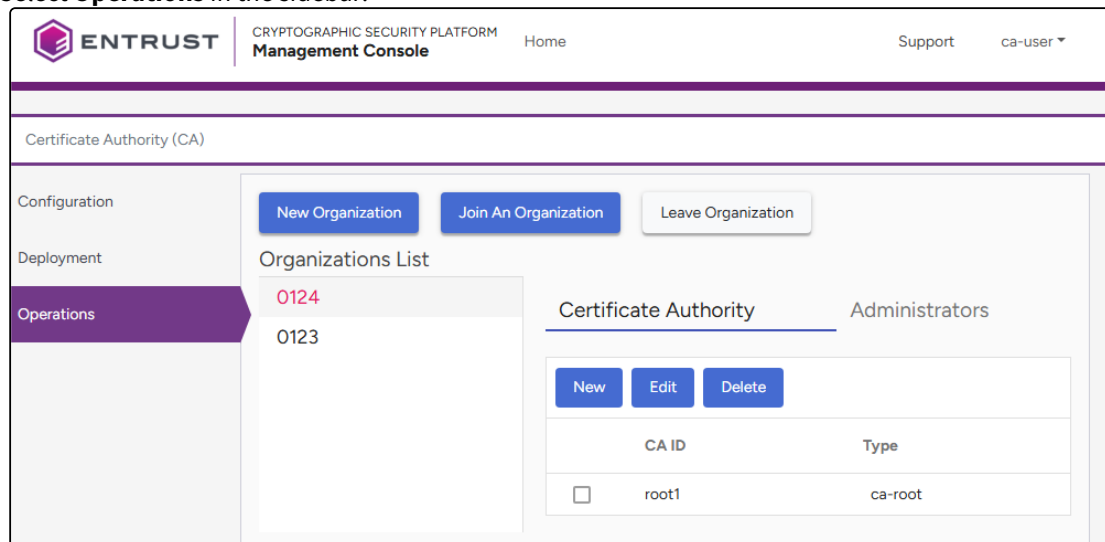
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log in to the Management Console as one of the users created in [Creating Certificate Authority tenants](#). This user will be the tenant of the new issuing Certificate Authority.

3. In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



4. Select **Operations** in the sidebar.



5. Select an organization under **Organizations list**.
6. Select a CA under **Certificate Authority**.
7. Click **Edit** to display the CA settings in the **Edit Certificate Authority** dialog. Of these settings, you can only edit the following ones:
 - [Certificate Profiles](#)
 - [Auditors](#)
 - [Administrators](#)

Meaning that you cannot modify any setting of an External Root Certificate Authority.

Certificate Profiles


The profiles the Certificate Authority will support for issuing certificates. See the [Certificate profiles reference](#) for a description of each profile.

Mandatory: Select at least one profile.


Auditors

Enter the names of the users who will have auditor permission on the Certificate Authority. For each name, you can:

- Enter a user name already assigned to another CA so that the user will have permissions on different CAs.
- Enter a new user.

 Upon CA creation, the Management Console only displays download buttons for the client authentication PKCS #12 of the new users.


Mandatory: No. When omitting this value, the Certificate Authority will not have users with only auditing permission.

 Use the trash icon to remove **Auditor** fields you do not want to fill out. Otherwise, they will display a **Please fill out this field** warning when you click **Save**.

Administrators

Enter the names of the users who will have administration permission on the Certificate Authority. For each name, you can:

- Enter a user name already assigned to another CA so that the user will have permissions on different CAs.
- Enter a new user.

 Upon CA creation, the Management Console only displays download buttons for the client authentication PKCS #12 of the new users.

Mandatory: Yes. Add the name of at least one administrator.

Issuing certificates with Certificate Authority instances

To issue certificates with a Certificate Authority instance, you must send requests to the embedded CA Gateway. See below for the supported modes.

- [Issuing certificates with a REST client](#)
- [Issuing certificates with Certificate Manager](#)

Issuing certificates with a REST client

See below for issuing certificates with the REST API exposed by the embedded CA Gateway of the Certificate Authority solution.

To issue certificates with a REST client

1. Install a REST client.
2. As the client credential, select the administrator PKCS #12 automatically generated when [Managing Certificate Authority instances](#).
3. Import the Swagger specification, which is available at the following endpoint.

```
https://{pkihub}:7443/cagw
```

Where `{pkihub}` is the hostname or IP address of the machine hosting Cryptographic Security Platform.

4. Send a REST requests to the issuing CA endpoint – for example:

```
curl --request POST --header "Accept: application/json" --header "Content-Type: application/json" -d @enrollments.json --cert-type P12 --cert $P12:$PWD https://$PKIHUB:7443/cagw/v1/certificate-authorities/$ORG_ID~$CA_ID/enrollments | jq .
```

Where :

- `$P12` is the path of the PKCS#12 file.
- `$PWD` is the password of the PKCS 12 file.
- `$PKIHUB` is the hostname or IP address of the machine hosting Cryptographic Security Platform.
- `$ORG_ID` is the identifier of the organization to which the CA belongs.
- `$CA_ID` is the identifier of the issuing CA.

Issuing certificates with Certificate Manager

See below for instructions on adding the embedded CA Gateway service, provided by the Certificate Authority solution, to Certificate Manager. Once added, Certificate Manager will support requesting certificates from all CA instances.

To add a CA Gateway instance to Certificate Manager

1. Install a Certificate Manager instance as explained in [Managing Certificate Manager](#).
2. Log into the Certificate Manager management console as explained in [Using Certificate Manager](#).
3. In the menu bar, select **Control > CA Gateways**.
4. On the **CA Gateways** page, click **Add**.
5. Configure the following values in the **Add** dialog.
 - [Name](#)
 - [CA Gateway URL](#)
 - [Required PKCS#12 File](#)
 - [Required PKCS#12 Password](#)
 - [Optional PKCS#12 Truststore File](#)

Add

Name

Owner
fake@fake.com

Description

CA Gateway URL
https://apibeta.managed.entrust.com:8080/cagw

Required PKCS#12 File

Select Files...
Drop files here to upload

The client PKCS#12 file to access CA Gateway

Required PKCS#12 Password

The password of the client PKCS#12 file

Optional PKCS#12 Truststore File

Select Files...
Drop files here to upload

An optional truststore that can be used to override the built-in truststore when using a private certificate authority (CA)

Optional Truststore Password

The password of the truststore file

Verify
Verify the CA Gateway connection

Add
Cancel

6. Click **Add** to confirm the CA Gateway creation.

Name

Write a name for the CA Gateway instance in Certificate Manager.

CA Gateway URL

Enter the following URL:

https://<hostname>:7443/cagw

Where **<hostname>** is the domain name or IP address of the machine hosting Cryptographic Security Platform.

Required PKCS#12 File

Click **Select Files** and import the administrator PKCS #12 that is automatically generated when .

Required PKCS#12 Password

Enter the PKCS#12 password that is automatically displayed when [Managing Certificate Authority instances](#).

Optional PKCS#12 Truststore File

Click **Select Files** and import PKCS#12 containing the certification chain of the TLS certificate described in [Replacing the default TLS certificate](#).

i To put the certification chain on a PKCS #12 file, you can use free tools such as <https://keystore-explorer.org>

Changing the HSM vendor

As explained in [Configuring and deploying Certificate Authority](#), the **Vendor** field of the [HSM](#) configuration page allows selecting the following Hardware security modules.

Vendor	Description
none	A built-in software PKCS #11 module (not recommended).
nshield	An Entrust nShield HSM. See HSM requirements for the supported versions.

On test environments, you can change the **Vendor** parameter value of an already deployed Certificate Authority solution.

- [Changing vendor from none to nShield](#)
- [Changing vendor from nShield to none](#)

Changing vendor from none to nShield

See below for changing the value of the **Vendor** parameter from **none** to **nShield**.

To change the vendor from none to nShield


1. Create a new database meeting the [Database requirements](#), or recreate the public schema of the database.
2. Run the following command.

```
sudo kubectl delete namespace pkihub-v202410180954
```

3. Set the **Vendor** field of the [HSM](#) configuration page to **nShield**.
4. Save the configuration.
5. Redeploy the solution.

Changing vendor from nShield to none

See below for changing the value of the **Vendor** parameter from **nShield** to **none**.

 Use `pkihub` as solution identifier when running the `clusterctl solution config export` and `clusterctl solution config import` commands.

To change the vendor from nShield to none

1. Create a new database meeting the [Database requirements](#), or recreate the public schema of the database.
2. Run the following command.

```
sudo kubectl delete namespace pkihub-v202410180954
```

3. Set the **Vendor** field of the [HSM](#) configuration page to **none**.
4. Save the configuration.
5. Export the configuration files with the `clusterctl solution config export` command.
6. Delete the `config` folder of the HSM installation.
7. Delete the `kmdata.tar` file of the HSM installation.
8. Import the configuration files with the `clusterctl solution config import` command.
9. Redeploy the solution.

8 Managing Certificate Manager

See below for configuring, deploying, and administering the Certificate Manager solution.

- [Certificate Manager architecture](#)
- [Configuring and deploying Certificate Manager](#)
- [Using Certificate Manager](#)
- [Certificate Manager API](#)
- [Certificate Manager error reference](#)
- [Migrating Certificate Manager database to an external host](#)

See [Browsing logs with Grafana](#) for how to browse Certificate Manager logs.

Certificate Manager architecture

Certificate Manager has three sets of capabilities:

- The **find capabilities** inventory certificates across your organization (through network discovery) and automated certificate import (from CA databases and cloud services).
- The **control capabilities** centrally manage policy, issuance & access to public and private certificates regardless of vendor. Perform manual operations as necessary to issue, renew, and revoke certificates.
- The **automation capabilities** push keys and certificates to endpoints, with fully managed rotation and certificate profile management.
- The **report capabilities** provide organizational, issue notifications, and reports to remind certificate owners of actions they need to take.

i Administrators can customize Certificate Manager to meet enterprise needs like access permissions, system metadata, notifications, or report branding.

The high-level architecture integrates the following main components.

- [Discovery Scanners](#)
- [Entrust CA Gateway](#)
- [Certificate Manager](#)

Discovery Scanners

Certificate Manager Discovery Scanners:

- Search your enterprise's networks or portions of networks for the most recent information about deployed certificates.
- Record each certificate's location, type, algorithms, and expiry, regardless of the certificate issuer.

Discovery Scanners are typically deployed on your premises, inside corporate firewalls, to access the internal private servers. However, only Discovery Scanners require this kind of deployment; you can deploy the other Certificate Manager components in a less restrictive environment.

When started, a Discovery Scanner:

1. Contacts Certificate Manager to get the policy and scan configuration.
2. Launches the Certificate Manager scheduling process for scanning.
3. Executes one or more configured scans according to the calendar schedule and priority.
4. Periodically polls Certificate Manager for any policy and or configuration updates.

i Discovery Scanners run a custom-built version of Nmap to scan ports, capture the returned SSL certificate chain, and transmit scan results to Certificate Manager for processing.

Entrust CA Gateway

Through Entrust CA Gateway, Entrust solutions obtain a direct feed of issued certificates from each supported Certificate Authority (CA). See the following table for the CA Gateway deployment required by each type of CA.

CA type	CA Gateway deployment
Certificate Authority running on Cryptographic Security Platform	Create a Certificate Authority instance, as explained in Managing Certificate Authority , and select the built-in CA Gateway service of this CA.
External Certificate Authority	Start up the Entrust CA Gateway solution and connect it with the external CA as explained Managing CA Gateway .

Certificate Manager

Certificate Manager is a container-based set of services amenable to either customer premises or commercial cloud hosting. Certificate Manager provides:

- An API interface to the companion Certificate Manager browser UI.
- The underlying certificate database.
- The necessary background processes.

Configuring and deploying Certificate Manager

See below for configuring and deploying Certificate Manager with the Management Console.

i Repeat the following steps each time a configuration update is required. Do not forget to click **Deploy** to make the changes effective.

To configure and deploy Certificate Manager with the Management Console

1. Open the following URL in a Web browser.

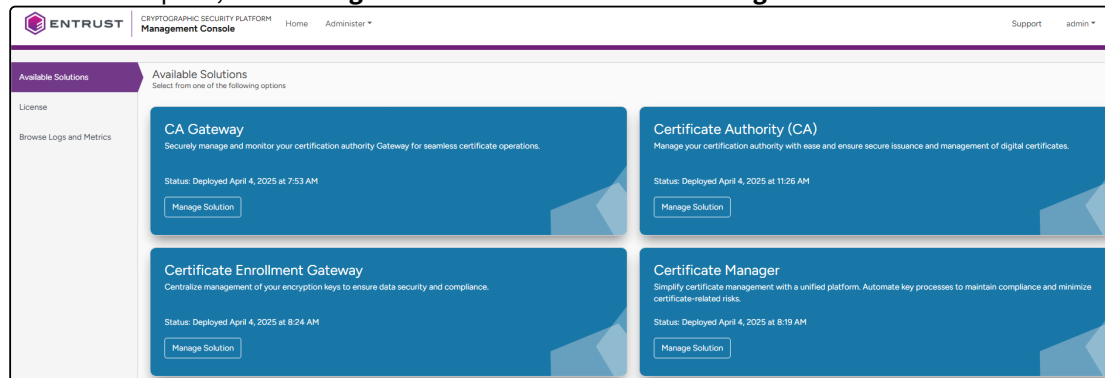
```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

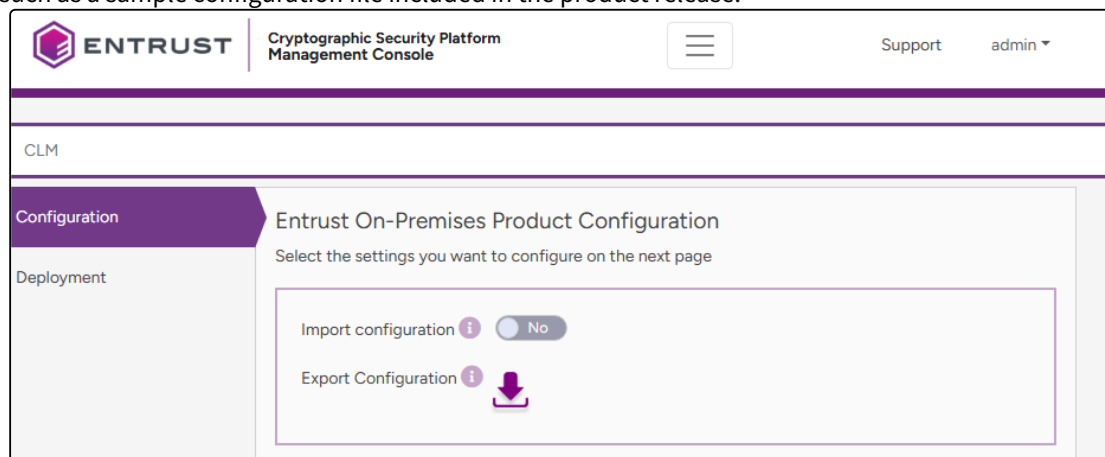
2. Log into the Management Console a user belonging to a role with Certificate Manager management permissions – for example, the initial `admin` administrator user.

i See [Starting up the Management Console](#) for how to manage users and roles.

3. In the content pane, click **Manage Solution** under **Certificate Manager**.



4. Activate the **Import configuration** toggle switch if you want to import configuration settings from a file, such as a sample configuration file included in the product release.



1. Click **Next**.
2. Configure the solution settings described in the following sections.
 - [CM Hostname](#)
 - [Discovery Scanner version](#)
 - [Initial Administrator Username](#)
 - [Initial Administrator Password](#)
 - [Initial Administrator Email](#)
 - [Name of the PostgreSQL Database](#)
 - [Database User Name](#)
 - [Database User Password](#)
 - [Host of the PostgreSQL database](#)
 - [External database port](#)
 - [SSLMode for the PostgreSQL external database](#)
 - [CA Certificate\(s\)](#)
3. Click **Validate** to validate the configured settings.
4. Correct any detected configuration error until the **Validate** option displays no warnings.
5. Optionally, click the **Download** button to export the current configuration. You can later import this configuration using the already mentioned **Import configuration** toggle switch.
6. Click **Submit** and wait while Cryptographic Security Platform uploads the configuration and any attached file, such as a P12 file with authentication credentials.
7. Click **Deploy**.

CM Hostname

The base hostname of the Kubernetes Ingress routing to the application.

Mandatory: Yes.

Discovery Scanner version

The version of the Entrust Discover Scanner integrated with Certificate Manager.

Mandatory: No. Skip this field when Certificate Manager is not integrated with Discover Scanner.

Initial Administrator Username

The username of the initial administrator.

Mandatory: Yes.

Initial Administrator Password

A temporary password for the initial administrator. Ensure that this temporary password does not include special characters such as '#', '!', or '*'.



After the initial login, the administrator will be prompted to create a new password that meets a specific set of password strength requirements

Mandatory: Yes.

Initial Administrator Email

The email address of the initial administrator.

Mandatory: Yes.

Name of the PostgreSQL Database

The name of an external PostgreSQL database.

Mandatory: Yes.

Database User Name

The user name of the external PostgreSQL database.

Mandatory: Yes.

Database User Password

The user password of the external PostgreSQL database.




Do not include special characters such as "#", "!", or "*" in the user password.

Mandatory: Yes.

Host of the PostgreSQL database

The IP address or Fully Qualified Domain Name (FQDN) of the database host.

 As explained in [Database SSL certificate](#), the SSL certificate for the database host must include the IP address or FQDN of the host.

Mandatory: Yes.

External database port

The connection port with the external PostgreSQL database.

Mandatory: Yes.

SSLMode for the PostgreSQL external database

The SSL mode for connecting with the external PostgreSQL database. Supported values are:

- require
- verify-ca
- verify-full


See <https://www.postgresql.org/docs/current/libpq-ssl.html> for a description of each mode.

 Any of the supported PostgreSQL modes requires enabling SSL.

Mandatory: Yes.

CA Certificate(s)

The CA certificate for validating the database SSL certificate. Click **Select Files** to import a file containing this certificate in PEM format and Base64 encoding.

 As explained in [Database SSL certificate](#), the SSL certificate for the database host must include the IP address or FQDN of the host.

Mandatory: When the **SSLMode for the PostgreSQL external database** value is one of the following.

- verify-ca
- verify-full

Using Certificate Manager

Once deployed, you can use Certificate Manager to manage certificate issuance and lifecycle.

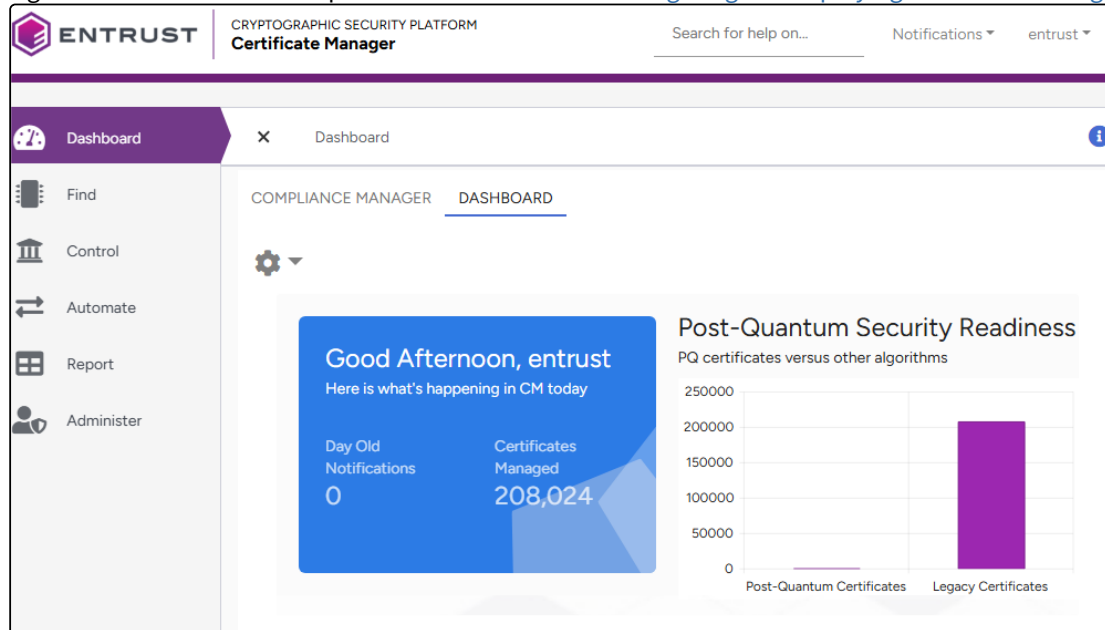
To manage certificates with Certificate Manager

1. Open a web browser in the following URL.

```
https://<host>/cm
```

Where `<host>` is the value of the hostname or IP address selected when [Configuring and deploying Certificate Manager](#).

2. Login with the username and password selected when [Configuring and deploying Certificate Manager](#).



3. Select the interface options described in the following sections.
 - [Dashboard](#)
 - [Find](#)
 - [Control](#)
 - [Automate](#)
 - [Report](#)
 - [Administer](#)
 - [Menu options](#)

Dashboard

Select **Dashboard** in the sidebar to manage the following settings.

- [Compliance Manager](#)
- [Dashboard](#)

Compliance Manager

Entrust Compliance Manager provides:

- Centralized visibility of cryptographic assets.
- Fine-grained control of all cryptographic keys and secrets regardless of the vault locations.

See below for adding and managing a connection between Certificate Manager and Compliance Manager.



To add and manage a connection with Compliance Manager

1. Create and download a data source connection as explained in the Compliance Manager documentation.
2. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to manage connections with Compliance Manager.

3. Click the **Dashboard** command in the sidebar menu.
4. Select the **COMPLIANCE MANAGER** tab.
 - If no connection has already been added, click **Get Started** on the content page.
 - If any connection has already been added, click **Enter New Configuration** to add a new one.
5. Under **Data Source Name**, enter a unique identifier for the Certificate Manager instance in Certificate Manager.
6. Click **Select Files** and select the data source connection file obtained in the first step. Alternatively, you can check the **Manually input connection details** box and enter each connection setting.
7. Click **Verify** to check the connection and fix any reported issues.
8. Click **Create** to add the connection. Certificate Manager will begin replicating certificate data to Compliance Manager within a minute.

Dashboard

Get an overview of the Certificate Manager operation with informational widgets.

 A widget with no data to display will only include a description of the widget. This same description is available when clicking the  icon at the top-right corner.

To browse and manage Certificate Manager widgets

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to browse widgets.
2. Click the **Dashboard** command in the sidebar menu.
3. Select the **DASHBOARD** tab.
4. Click the gear icon to display the **Dashboard Preferences** menu.
5. Under **Widgets**, add or remove the following widgets.
 - [Authorities](#)
 - [Discovery](#)
 - [Expiring Certificates](#)
 - [Post Quantum Certificates](#)
 - [Reports Today](#)
 - [Signature Algorithm](#)
 - [Today's Summary](#)
 - [Certificate Requests](#)
 - [Domains](#)
 - [Key Algorithm](#)
 - [Report retention](#)
 - [Scheduled Renewals](#)
 - [Sources](#)
 - [Top 10 Certificate Issuers](#)
6. Under **Layout**, select your preferred number of columns to display the selected widgets.

Authorities

This widget lists the [Authorities](#) and the number of [Certificates](#) associated with each, including the authority certificate. Click the number beside an authority to browse the certificates issued by this authority.

Discovery

This widget lists the connections that failed during certificate discovery.

Expiring Certificates

This widget displays the number of [Certificates](#) matching the **Expiring Soon** system report. Click this number to browse these certificates.

 See in [Designing a report](#) how to select the number of certificates in this widget.

Post Quantum Certificates

This widget displays different metrics on the post-quantum-ready certificates, such as the security level or the algorithms.

Reports Today

This widget shows information on the [Reports](#) programmed for the current day.

Signature Algorithm

This widget lists the number of certificates issued with each supported signature algorithm.


Today's Summary

This widget summarizes the Certificate Manager state in 3 columns.

- The left column displays the number of notifications in the last 24 hours, and the number of certificates managed by Certificate Manager.
- The **Post-Quantum Security Readiness** central column displays the number of legacy vs post-quantum certificates.
- The right column includes a three-dashes carousel to cycle different widgets.
 - **Activity this week:** Number of issued certificates, scheduled renewals, and archived certificates.
 - **Plugins:** Number of plugins of each type (key management, certificate destination, certificate source, notifications).
 - **Sources:** Configured certificate sources.
 - **Missed connections:** Missed connections with discovery agents and sources.

Certificate Requests

This widget displays the certificate requests created by the user.

 Users with the [global_admin](#) role can see the requests created by all users.

Domains


This widget lists the number of [Domains](#) in each state (inactive, expiring, pending, or active). Click the number beside a state to browse the domains in this state.

Key Algorithm

This widget lists the number of certificates issued with each supported key algorithm.

Report retention

This widget lists the [Reports](#) that will expire in the coming days.

 See in [Editing a report schedule](#) how to update the report retention period.

Scheduled Renewals

This widget displays the number of [Certificates](#) matching the **Renewing Soon** system filter (a number in red indicates that at least one certificate failed a previous renewal attempt). Click this number to browse these certificates.

 See in [Designing a report](#) how to select the number of certificates in this widget.

Sources

This widget lists the failed connections with the certificate sources.

Top 10 Certificate Issuers

This widget lists the 10 top certificate issuers and the number of certificates issued by each one, not counting an issuer self-signed certificate. Hover the mouse over the chart to check the number of certificates issued by a certificate issuer, click **Certificates** to browse the certificate details.

Find


The Discovery Scanner scanning tool finds the certificates exposed on IP ports of your corporate network, usually TLS certs. Typically, you will:

1. Download Discovery Scanner from the Entrust website: <https://www.entrust.com/resources/certificate-solutions/tools/entrust-discovery-scanner>
2. Set up one Discovery Scanner for each network you wish to scan.
3. Configure scans to instruct the Discovery Scanner on the network range and ports to check.

Thus, each Discovery Scanner can run multiple scans, and you can run as few or many scans as you like. Normally, customers run one scan for each segment of their network.

The Certificate Manager Web browser interface centralizes the Discovery Scanner configuration and management. Discovery Scanners periodically connect to Certificate Manager and send up reports of the certificates found. Certificate Manager collects this information and presents it in the certificate view. Using the information collected, the administrator can track:

- The basic information derived from the certificate.
- The expiry notices (automatically created). Certificate Manager administrators can program rules for populating these notices to certificate holders.
- The domains where the certificate was discovered.
- The public certificate.
- The certificate chain.

 You can also connect Certificate Manager with external scan tools using the Certificate Manager API.

To manage discovery scanners, click **Find** in the sidebar and select the following options.

- [Launch](#)
- [Discovery](#)
- [Endpoints](#)

Launch

Select **Find > Launch** to display the discovery insights page. You can:

- Check the number of [Discovery Scanners](#) and create new ones

- Check the number of [Endpoints](#) and go to the browsing grid.
- Click the tags under **Related Topics** to learn about different topics.

Discovery

Select **Find > Discovery** to manage discovery scanners.

- [Browsing Discovery Scanners](#)
- [Creating a Discovery Scanner](#)
- [Editing a Discovery Scanner](#)
- [Checking the Discovery Scanner connection](#)
- [Configuring the scans of a Discovery Scanner](#)
- [Deleting Discovery Scanners](#)

Browsing Discovery Scanners

See below for browsing the details of the registered Discovery Scanners.

To browse Discovery Scanners

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Find > Discovery**.
3. Define Discovery Scanner views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. For each Discovery Scanner, browse the following settings.
 - [Name](#)
 - [Description](#)
 - [Scanner Version](#)
 - [Last Seen](#)
 - [Owner](#)

Name


The unique identifier of the Discovery Scanner.

Description

The purpose or usage of the scanner.

Scanner Version

The release version number of the Discovery Scanner. This field is only informed after the first execution of the Discovery Scanner.


 If you observe old scanners running in your environment, contact your IT organization or PKI management for an upgrade (please note that the scanner version numbering is separate from Certificate Manager).

Last Seen

The date of the last connection with Certificate Manager. This field is only informed after the first execution of the Discovery Scanner.

Owner


The username of the scanner owner.

 The user who creates the scanner is automatically made the owner. You can later edit this field and assign ownership to someone else.

Creating a Discovery Scanner


See below for how to create a Discovery Scanner in Certificate Manager.

To create a Discovery Scanner

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Find > Discovery**.
3. Click **Create** to configure the following settings.
 - [Agent Name](#)
 - [Owner](#)
 - [Description](#)
 - [Poll Frequency](#)
4. Click **Create** to confirm the Discovery Scanner registration.
5. In the main grid, click the plus button  of the new scanner.
6. Copy the **Server URL** or **Access Token** displayed in the Discovery Scanner Details. You will need one of these values when running the Discovery Scanner.

Agent Name


A unique identifier for the Discovery Scanner.

 If a Discovery Scanner already exists with the same name, it will be overwritten.

Mandatory: Yes

Owner

The username of the scanner owner.

 The user who creates the scanner is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

The purpose or usage of the scanner.


Mandatory: No

Poll Frequency

The number of minutes between each Discovery Scanner connection with Certificate Manager for checking:

- Configuration updates.
- Requests to run scans immediately.

This optional value defaults to 1 to remain responsive to updates.

 Periodic polling checking is an inexpensive operation from a networking and computing standpoint.

Mandatory: Yes

Editing a Discovery Scanner


See below for how to edit Discovery Scanner settings.

To edit a Discovery Scanner

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Find > Discovery**.
3. In the main grid, select one of the listed Discovery Scanners.
4. Click **Edit** to update the following settings.
 - [Agent Name](#)
 - [Owner](#)
 - [Description](#)
 - [Poll Frequency](#)

Agent Name


A unique identifier for the Discovery Scanner.

 If a Discovery Scanner already exists with the same name, it will be overwritten.

Mandatory: Yes

Owner

The username of the scanner owner.

 The user who creates the scanner is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

The purpose or usage of the scanner.


Mandatory: No

Poll Frequency

The number of minutes between each Discovery Scanner connection with Certificate Manager for checking:

- Configuration updates.
- Requests to run scans immediately.


This optional value defaults to 1 to remain responsive to updates.

 Periodic polling checking is an inexpensive operation from a networking and computing standpoint.

Mandatory: Yes

Checking the Discovery Scanner connection

See below for how to check the connections of the Discovery Scanners with Certificate Manager.

 If you upgrade from a prior Certificate Manager release and observe Scanner versions older than 1.5.1, you must upgrade them before they connect.

To check the Discovery Scanners connection

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Find > Discovery**.
3. Inspect the **Scanner Version** and **Last Seen** entries. Once the Discovery Scanner runs, Certificate Manager will update these entries to confirm the operation.

Configuring the scans of a Discovery Scanner

See below for creating and managing the scan configurations for a Discovery Scanner.

- [Creating the first scan configuration of a Discovery Scanner](#)
- [Adding a scan configuration to a Discovery Scanner](#)
- [Copying the scan configuration of a Discovery Scanner](#)
- [Running a scan configuration](#)
- [Deleting a scan configuration](#)

Creating the first scan configuration of a Discovery Scanner

See below for creating the first scan configuration of a Discovery Scanner.

To create the first configuration of a Discovery Scanner

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Find > Discovery**.
3. Click on the **Discovery Scanner** checkbox.
4. Click **Configure**.
5. In the **Configure** dialog, configure the following scan settings.
 - [Scan Name](#)
 - [Description](#)
 - [Priority](#)
 - [Custom Ports](#)
 - [Custom Hosts](#)
 - [Schedule / Run Frequency](#)
 - [Advanced / Hosts to Exclude](#)
 - [Advanced / Resolve Hostnames](#)
 - [Advanced / Check If Host's Alive First](#)
 - [Advanced / Host Order](#)
 - [Advanced / Scan Rate](#)
6. Click **Save**.

Scan Name

The name of the scan configuration.

Description

A brief description of the scan configuration.

Priority

If scans might overlap, this setting determines which scan (if any) should take precedence. Use this setting to avoid impacting the performance of other scheduled scans by over-stressing network bandwidth.

Priority	Scan execution
Low	Only run if no high or normal priority scan is running. Thus, when starting a normal or high-priority scan, low-priority scans stop executing until the other, higher-priority scans finish.
High	Always. Suspend any other normal or low-priority scans until they are complete.
Normal	When no high-priority scan runs, any normal-priority scans can run simultaneously.

✖ Some configurations can prevent low-priority scans from running at all.

Custom Ports

The ports to run the certificate scan for every host listed in the **Custom Hosts** field. This field supports 255 characters in one of the following syntaxes.

- An individual port. For example 1443
- A comma-separated list of ports. For example 1400, 1443
- A port range. For example, 1400-1443

Please use a second scan if you require more space to specify ports.

✖ The certificate scan will fail when providing invalid custom ports.

Custom Hosts

The hosts to scan for certificates. The value of this setting supports the following syntaxes.

Syntax	Example
An individual hostname	www.example.com
An individual IP address	192.51.100.20
A comma-separated list of IP addresses or hostnames	www.example.com ,192.51.100.2
A range of IP addresses using CIDR notation	192.51.100.0/24
A range of IP addresses, using a dash to separate the range	192.51.100.0-24

Schedule / Run Frequency

Select:

- **Manual** to run the scans when manually triggered.
- **Hourly, Daily, Weekly, Monthly**, to run the scans periodically at the specified moment.

Advanced / Hosts to Exclude

List of the hosts excluded from the scan, in any of the following formats.

`192.0.2.0-100``192.0.2.0/24``www.example.com``www.example.com/16`

Advanced / Resolve Hostnames

Configure the hostname resolution.

Option	Hostname resolution
Always	Performs a reverse DNS lookup of the hostname before contacting each host.
Never	Do not resolve hostnames. Select this option for better performance.

Advanced / Check If Host's Alive First

Select whether to ping the hosts to check whether they are alive.

Option	Scanned hosts
Check node before scan	Only the hosts that respond to an initial ping.
Assume all hosts are alive	All hosts. The agent will attempt to perform scans on every host until the scan is successful or it times out. Select this option if the ping response is disabled in some hosts.

Advanced / Host Order

Select the scan order.

Option	Scan order
Normal	Order in which hosts appear in the list.
Randomized	Random order. This option slows the scan rate but prevents false alarms triggered by intrusion detection systems.

Advanced / Scan Rate

Select the rate of the queries executed by each scan to discover certificates.

✖ Higher rates are resource-consuming and can trigger false alarms in intrusion detection systems.

Scan Rate	Initial scan delay (ms)	Max attempts to reach host port	Max time before sending another probe (ms)	Max scan delay (ms)
Slowest	300000	10	300000	300000
Slower	15000	10	15000	15000
Slow	400	10	10000	1000
Normal	0	10	10000	1000
Aggressive	0	6	1250	10
Very Aggressive	0	2	300	5

Adding a scan configuration to a Discovery Scanner

After [Creating the first scan configuration of a Discovery Scanner](#), you can add new scan configurations as explained below.

To add a scanner configuration to a Discovery Scanner

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Find > Discovery**.
3. In the content pane, click the checkbox of the Discovery Scanner for which you want to add a configuration.
4. Click **Configure**.
5. In the **Configure** dialog, click **New**.
6. Configure the following scan settings.
 - [Scan Name](#)
 - [Description](#)
 - [Priority](#)
 - [Custom Ports](#)
 - [Custom Hosts](#)

- [Schedule / Run Frequency](#)
- [Advanced / Hosts to Exclude](#)
- [Advanced / Resolve Hostnames](#)
- [Advanced / Check If Host's Alive First](#)
- [Advanced / Host Order](#)
- [Advanced / Scan Rate](#)

7. Click **Save**.

Scan Name

The name of the scan configuration.

Description

A brief description of the scan configuration.

Priority

If scans might overlap, this setting determines which scan (if any) should take precedence. Use this setting to avoid impacting the performance of other scheduled scans by over-stressing network bandwidth.

Priority	Scan execution
Low	Only run if no high or normal priority scan is running. Thus, when starting a normal or high-priority scan, low-priority scans stop executing until the other, higher-priority scans finish.
High	Always. Suspend any other normal or low-priority scans until they are complete.
Normal	When no high-priority scan runs, any normal-priority scans can run simultaneously.

✖ Some configurations can prevent low-priority scans from running at all.

Custom Ports

The ports to run the certificate scan for every host listed in the **Custom Hosts** field. This field supports 255 characters in one of the following syntaxes.

- An individual port. For example 1443
- A comma-separated list of ports. For example 1400, 1443
- A port range. For example, 1400-1443

Please use a second scan if you require more space to specify ports.

✖ The certificate scan will fail when providing invalid custom ports.

Custom Hosts

The hosts to scan for certificates. The value of this setting supports the following syntaxes.

Syntax	Example
An individual hostname	www.example.com
An individual IP address	192.51.100.20
A comma-separated list of IP addresses or hostnames	www.example.com ,192.51.100.2
A range of IP addresses using CIDR notation	192.51.100.0/24
A range of IP addresses, using a dash to separate the range	192.51.100.0-24

Schedule / Run Frequency

Select:

- **Manual** to run the scans when manually triggered.
- **Hourly, Daily, Weekly, Monthly**, to run the scans periodically at the specified moment.

Advanced / Hosts to Exclude

List of the hosts excluded from the scan, in any of the following formats.

192.0.2.0-100

192.0.2.0/24

www.example.com

www.example.com/16

Advanced / Resolve Hostnames

Configure the hostname resolution.

Option	Hostname resolution
Always	Performs a reverse DNS lookup of the hostname before contacting each host.
Never	Do not resolve hostnames. Select this option for better performance.

Advanced / Check If Host's Alive First

Select whether to ping the hosts to check whether they are alive.

Option	Scanned hosts
Check node before scan	Only the hosts that respond to an initial ping.
Assume all hosts are alive	All hosts. The agent will attempt to perform scans on every host until the scan is successful or it times out. Select this option if the ping response is disabled in some hosts.

Advanced / Host Order

Select the scan order.

Option	Scan order
Normal	Order in which hosts appear in the list.
Randomized	Random order. This option slows the scan rate but prevents false alarms triggered by intrusion detection systems.

Advanced / Scan Rate


Select the rate of the queries executed by each scan to discover certificates.

✗ Higher rates are resource-consuming and can trigger false alarms in intrusion detection systems.

Scan Rate	Initial scan delay (ms)	Max attempts to reach host port	Max time before sending another probe (ms)	Max scan delay (ms)
Slowest	300000	10	300000	300000
Slower	15000	10	15000	15000
Slow	400	10	10000	1000
Normal	0	10	10000	1000
Aggressive	0	6	1250	10
Very Aggressive	0	2	300	5

Copying the scan configuration of a Discovery Scanner

See below for how to copy a scan configuration into a different Discovery Scanner.

 The copy option does not support copying a scan configuration into the same Discovery Scanner.

To copy a scan configuration

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Find > Discovery**.
3. In the content pane, click the checkbox of the Discovery Scanner of the configuration you want to copy.
4. Click **Configure**.
5. In the top list of the **Configure** dialog, select the scan configuration you want to copy.
6. Click **Copy**.
7. In the **Save to** list, select the Discovery Scanner to which you want to assign the scan configuration. This list does not include the Discovery Scanner of the copied configuration.
8. Configure the following scan settings.
 - [Scan Name](#)
 - [Description](#)
 - [Priority](#)
 - [Custom Ports](#)
 - [Custom Hosts](#)
 - [Schedule / Run Frequency](#)
 - [Advanced / Hosts to Exclude](#)
 - [Advanced / Resolve Hostnames](#)
 - [Advanced / Check If Host's Alive First](#)
 - [Advanced / Host Order](#)
 - [Advanced / Scan Rate](#)
9. Click **Save**.

Scan Name

The name of the scan configuration.

Description

A brief description of the scan configuration.

Priority

If scans might overlap, this setting determines which scan (if any) should take precedence. Use this setting to avoid impacting the performance of other scheduled scans by over-stressing network bandwidth.

Priority	Scan execution
Low	Only run if no high or normal priority scan is running. Thus, when starting a normal or high-priority scan, low-priority scans stop executing until the other, higher-priority scans finish.
High	Always. Suspend any other normal or low-priority scans until they are complete.

Priority	Scan execution
Normal	When no high-priority scan runs, any normal-priority scans can run simultaneously.

✖ Some configurations can prevent low-priority scans from running at all.

Custom Ports

The ports to run the certificate scan for every host listed in the **Custom Hosts** field. This field supports 255 characters in one of the following syntaxes.

- An individual port. For example 1443
- A comma-separated list of ports. For example 1400, 1443
- A port range. For example, 1400-1443

Please use a second scan if you require more space to specify ports.

✖ The certificate scan will fail when providing invalid custom ports.

Custom Hosts

The hosts to scan for certificates. The value of this setting supports the following syntaxes.

Syntax	Example
An individual hostname	www.example.com
An individual IP address	192.51.100.20
A comma-separated list of IP addresses or hostnames	www.example.com ,192.51.100.2
A range of IP addresses using CIDR notation	192.51.100.0/24
A range of IP addresses, using a dash to separate the range	192.51.100.0-24

Schedule / Run Frequency

Select:

- **Manual** to run the scans when manually triggered.
- **Hourly, Daily, Weekly, Monthly**, to run the scans periodically at the specified moment.

Advanced / Hosts to Exclude

List of the hosts excluded from the scan, in any of the following formats.

192.0.2.0-100

192.0.2.0/24

www.example.com

www.example.com/16

Advanced / Resolve Hostnames

Configure the hostname resolution.

Option	Hostname resolution
Always	Performs a reverse DNS lookup of the hostname before contacting each host.
Never	Do not resolve hostnames. Select this option for better performance.

Advanced / Check If Host's Alive First

Select whether to ping the hosts to check whether they are alive.

Option	Scanned hosts
Check node before scan	Only the hosts that respond to an initial ping.
Assume all hosts are alive	All hosts. The agent will attempt to perform scans on every host until the scan is successful or it times out. Select this option if the ping response is disabled in some hosts.

Advanced / Host Order

Select the scan order.

Option	Scan order
Normal	Order in which hosts appear in the list.
Randomized	Random order. This option slows the scan rate but prevents false alarms triggered by intrusion detection systems.

Advanced / Scan Rate

Select the rate of the queries executed by each scan to discover certificates.

✖ Higher rates are resource-consuming and can trigger false alarms in intrusion detection systems.

Scan Rate	Initial scan delay (ms)	Max attempts to reach host port	Max time before sending another probe (ms)	Max scan delay (ms)
Slowest	300000	10	300000	300000
Slower	15000	10	15000	15000
Slow	400	10	10000	1000
Normal	0	10	10000	1000
Aggressive	0	6	1250	10
Very Aggressive	0	2	300	5

Running a scan configuration

See below for how to trigger a scan execution without waiting for the defined schedule.

ℹ The triggered scan will start upon the next poll.

To run a scan configured in a Discovery Scanner

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Find > Discovery**.
3. In the content pane, click the checkbox of the Discovery Scanner of the configuration you want to run.
4. Click **Configure**.
5. In the top list of the **Configure** dialog, select the scan configuration you want to run.
6. Click **Schedule Scan Now** to add the scan to the execution queue.

Deleting a scan configuration

See below for how to delete a scan configuration from a Discovery Scanner.

To delete a scan configuration

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Find > Discovery**.
3. In the content pane, click the checkbox of the Discovery Scanner of the configuration you want to delete.
4. Click **Configure**.
5. In the top list of the **Configure** dialog, select the scan configuration you want to delete.
6. Click **Delete**.

Deleting Discovery Scanners

See below for removing Discovery Scanners from Certificate Manager.

To delete Discovery Scanners

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Find > Discovery**.
3. In the main grid, select one or more Discovery Scanners.
4. Click **Delete** to remove the selected Discovery Scanners.

Endpoints

See below for browsing the Certificate Manager endpoints where Discovery Scanner instances discover certificates.

To browse endpoints

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Control > Endpoints**.
3. Define endpoint views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. Check the following settings for each endpoint.
 - [Host Name](#)
 - [Port](#)
 - [Location](#)
 - [Owner](#)
 - [Service](#)
 - [Service Vendor](#)
 - [Service Vendor Version](#)
 - [Cipher Suites](#)
 - [OS Type](#)

Host Name

The name of the endpoint host.

Port

The endpoint port.

Location

The location of the certificate on the host machine.

Owner

The email address of the person responsible for the endpoint.

Service

The service exposed on the endpoint.

Service Vendor

The vendor of the service exposed on the endpoint.

Service Vendor Version

The version of the vendor services exposed on the endpoint.

Cipher Suites

The list of cipher suites that a service accepts

OS Type

The operating system type of the endpoint.

Control

With the Certificate Manager control capabilities, you can centrally view and manage your certificate authorities and certificates. Click **Control** in the sidebar and select the following options.

- [Launch](#)
- [CA Gateways](#)
- [Authorities](#)
- [Key Managers](#)
- [Custom Fields](#)
- [Public Enrollment Forms](#)
- [Requests For Approval](#)
- [My Certificate Requests](#)
- [Certificates](#)
- [Certificate History](#)
- [Domains](#)

Launch

Select **Control > Launch** to view the control insights page. You can:

- Check the number of [CA Gateways](#) and configure new ones
- Check the number of [Authorities](#) and configure new ones.
- Click the corresponding link to browse:
 - [Certificates](#)
 - [Custom Fields](#)
 - [Public Enrollment Forms](#)
 - [Requests For Approval](#)
 - [Domains](#)
 - [Key Managers](#)
- Click the tags under **Related Topics** to learn about different topics.

CA Gateways

Through Entrust CA Gateway, Certificate Manager obtains a direct feed of issued certificates from each supported certificate authority (CA).

- [Browsing CA Gateway instances](#)
- [Adding a CA Gateway instance](#)
- [Editing a CA Gateway instance](#)
- [Deleting a CA Gateway instance](#)

Certificate Manager can request certificates from all the CAs managed by a CA Gateway instance.

Browsing CA Gateway instances

See below for browsing the CA Gateway instances added to Certificate Manager.

To browse CA Gateway instances

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with the **Manage CA Gateway (CAGW)** permission.
2. Go to **Control > CA Gateways**.
3. Define CA Gateway views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. For each CA Gateway in the main grid, check the following settings.
 - [Name](#)
 - [Owner](#)
 - [Description](#)
 - [Active](#)
 - [CA Gateway URL](#)

Name

A unique identifier for the CA Gateway instance in Certificate Manager.

Owner

The email address of the person responsible for the CA Gateway instance.



The user who adds the CA Gateway is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description


A description of the CA Gateway instance.

Active

✔ if the CA Gateway is enabled in Certificate Manager; ✖ otherwise.

CA Gateway URL

The URL of the CA Gateway host.

 For Entrust Managed PKI systems, your Entrust contact will provide the URL.

Adding a CA Gateway instance

See below for adding a CA Gateway instance to Certificate Manager.

To add a CA Gateway

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with the **Manage CA Gateway (CAGW)** permission.
2. Go to **Control > CA Gateways**.
3. Click **Add** to configure the following settings.
 - [Name](#)
 - [Owner](#)
 - [Description](#)
 - [CA Gateway URL](#)
 - [Required PKCS#12 File](#)
 - [Required PKCS#12 Password](#)
 - [Optional PKCS#12 Truststore File](#)
 - [Optional Truststore Password](#)
4. Click **Verify** to check the connection with the CA Gateway.


Name

A unique identifier for the CA Gateway instance in Certificate Manager.

Mandatory: Yes

Owner

The email address of the person responsible for the CA Gateway instance.

 The user who adds the CA Gateway is automatically made the owner. You can later edit this field and assign ownership to someone else.

Mandatory: Yes


Description

A description of the CA Gateway instance.

Mandatory: No

CA Gateway URL

The URL of the CA Gateway host.

 For Entrust Managed PKI systems, your Entrust contact will provide the URL.

Mandatory: Yes

Required PKCS#12 File

The PKCS#12 file containing the keys and the certificate that Certificate Manager must present to the CA Gateway instance for accessing the CAs. This PKCS#12 file is either:

- Generated when configuring your CA Gateway instance,
- Provided by Entrust for API access to your Entrust Managed PKI service.

Mandatory: Yes

Required PKCS#12 Password

The password of the PKCS#12 file.

Mandatory: Yes

Optional PKCS#12 Truststore File

A truststore that will override the built-in truststore when using a private CA.

Mandatory: No

Optional Truststore Password

The password of the optional PKCS#12 truststore.

Mandatory: When selecting an **Optional PKCS#12 Truststore File**.

Editing a CA Gateway instance

See below for editing the settings of a CA Gateway instance.

To edit a CA Gateway

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with the **Manage CA Gateway (CAGW)** permission.
2. Go to **Control > CA Gateways**.
3. In the main grid, select a CA Gateway instance.
4. Click **Edit** to check or update the following settings.
 - [Active](#)
 - [Name](#)
 - [Owner](#)
 - [Description](#)
 - [CA Gateway URL](#)
 - [Required PKCS#12 File](#)
 - [Required PKCS#12 Password](#)
 - [Optional PKCS#12 Truststore File](#)
 - [Optional Truststore Password](#)
 - [PKCS#12 Expiry Date](#)
 - [PKCS#12 Subject DN](#)
5. Click **Verify** to check the connection with the CA Gateway.

Active

Check this box to enable the CA Gateway in Certificate Manager; uncheck otherwise.


Name

A unique identifier for the CA Gateway instance in Certificate Manager.

Mandatory: Yes

Owner

The email address of the person responsible for the CA Gateway instance.

 The user who adds the CA Gateway is automatically made the owner. You can later edit this field and assign ownership to someone else.

Mandatory: Yes


Description

A description of the CA Gateway instance.

Mandatory: No

CA Gateway URL

The URL of the CA Gateway host.

 For Entrust Managed PKI systems, your Entrust contact will provide the URL.

Mandatory: Yes

Required PKCS#12 File

The PKCS#12 file containing the keys and the certificate that Certificate Manager must present to the CA Gateway instance for accessing the CAs. This PKCS#12 file is either:

- Generated when configuring your CA Gateway instance,
- Provided by Entrust for API access to your Entrust Managed PKI service.

Mandatory: Yes

Required PKCS#12 Password

The password of the PKCS#12 file.

Mandatory: Yes

Optional PKCS#12 Truststore File

A truststore that will override the built-in truststore when using a private CA.

Mandatory: No

Optional Truststore Password

The password of the optional PKCS#12 truststore.

Mandatory: When selecting an **Optional PKCS#12 Truststore File**.

PKCS#12 Expiry Date


The expiry date of the certificate in the **Required PKCS#12 File**.

PKCS#12 Subject DN

The subject's Distinguished Name of the certificate in the **Required PKCS#12 File**.

Deleting a CA Gateway instance

See below for deleting CA Gateway instances from Certificate Manager.

-  Certificate Manager will preserve all certificates associated with the removed CA Gateway but no longer update their status.

To delete CA Gateway instances

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with the **Manage CA Gateway (CAGW)** permission.
2. Go to **Control > CA Gateways**.
3. In the main grid, select one or more CA Gateway instances.
4. Click **Delete** to remove the selected CA Gateway instances from Certificate Manager.

Authorities

Certificate Manager integrates authorities for certificate issuance and subsequent lifecycle management.

- [Browsing authorities](#)
- [Adding authorities](#)
- [Editing an authority](#)
- [Deleting authorities](#)

Browsing authorities

See below for browsing the authorities added to Certificate Manager.

To browse authorities


1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create authorities.
2. Go to **Control > Authorities**.
3. Define authority views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. For each authority in the main grid, browse the following settings.
 - [Name](#)
 - [Owner](#)
 - [Description](#)
 - [Active](#)
 - [Subject DN](#)

Name

A unique identifier for the authority.

Owner

The username of the person responsible for the authority.

 The user who adds the authority is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the authority.

Active

 if the authority is enabled in Certificate Manager;  otherwise.

Subject DN

The Distinguished Name (DN) of the authority certificate subject.

Adding authorities

See below for adding an authority to Certificate Manager.

To add an authority

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create authorities.
2. Go to **Control > Authorities**.
3. Click **Add** to configure the following settings.
 - [Name](#)
 - [Owner](#)
 - [Description](#)
 - [CA Gateway](#)
 - [Found CA\(s\)](#)
 - [Certificate Authority](#)
4. Click **Add**.


Name

A unique identifier for the authority.

Mandatory: Yes

Owner

The username of the person responsible for the authority.

 The user who adds the authority is automatically made the owner. You can later edit this field and assign ownership to someone else.

Mandatory: Yes

Description

A description of the authority.

Mandatory: No

CA Gateway

The [CA Gateway](#) instance managing the authority.

Mandatory: Yes

Found CA(s)

Check the number of authorities managed by the selected CA Gateway.

Certificate Authority

Select one of the authorities managed by the CA Gateway.

Mandatory: Yes

Editing an authority

See below for editing the settings of an Authority.

To edit an authority

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create authorities.
2. Go to **Control > Authorities**.
3. In the main grid, select one of the listed authorities.
4. Click **Edit** to check or update the following settings.
 - [Active](#)
 - [Owner](#)
 - [Description](#)
 - [CA Gateway](#)
 - [ID in CA Gateway](#)

Active

Check to enable the Authority in Certificate Manager; uncheck otherwise.

Owner

The username of the person responsible for the authority.



The user who adds the authority is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the authority.

CA Gateway

The [CA Gateway](#) instance managing the authority.


Mandatory: Yes

ID in CA Gateway

The authority identifier in CA Gateway.

Deleting authorities

See below for deleting Authorities from Certificate Manager.

 Certificate Manager will preserve all the certificates associated with the removed Authority but no longer update their status.

To deleting Authorities

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create Authorities.
2. Go to **Control > Authorities**.
3. In the main grid, select one or more Authorities.
4. Click **Delete** to remove the selected Authorities from Certificate Manager.

Key Managers

Key managers generate key pairs and certificate signing requests (CSRs) for certificate authorities to issue certificates.

- [Browsing key managers](#)
- [Creating a key manager](#)
- [Editing a key manager](#)
- [Deleting key managers](#)

Browsing key managers

See below for browsing the key managers added to Certificate Manager.

To browse Key Managers

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to view key managers.
2. Go to **Control > Key Managers**.
3. Define key manager views,.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. For each key manager in the main grid, browse the following settings.
 - [Label](#)
 - [Description](#)
 - [Plugin](#)
 - [Associated Certificates](#)
 - [Owner](#)

- [Authorization Tags](#)

Label

A descriptive name of the key manager.

Description

A description of the key manager.

Plugin

The plugin for connecting with the key manager.

Associated Certificates

The number of certificates issued for the key manager keys. Click this value to browse these certificates on the [Certificates](#) page.

Owner

The username of the person responsible for the key manager.



The user who adds the key manager is automatically made the owner. You can later edit this field and assign ownership to someone else.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the key manager.

Creating a key manager

See below for adding a key manager to Certificate Manager.

- [Creating a F5 BIG-IP key manager](#)
- [Creating a KMIP key manager](#)

Creating a F5 BIG-IP key manager

See below for using F5 BIG-IP certificate management services as a key management server.

To create a F5 BIG-IP key manager

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create key managers.
2. Go to **Control > Key Managers**.
3. Click **Create** to configure the following settings.
 - [Label](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
 - [Plugin Type](#)
 - [Host](#)
 - [Port](#)
 - [Partition/Path](#)
 - [Username](#)

- [Password](#)
- [Host CA Bundle \(PEM\)](#)
- [Key Type](#)
- [Key Length](#)
- [Curve Name](#)
- [Security Type](#)
- [Enable hostname verification](#)
- [Allow private key export](#)

4. Click **Verify** to check the connection with the key manager.


Label

A descriptive name of the key manager.

Mandatory: Yes

Owner

The username of the person responsible for the key manager.

 The user who adds the key manager is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the key manager.

Mandatory: No

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the key manager.

Mandatory: No

Plugin Type

Select **F5-BIG-IP-KMS-Plugin**.

Mandatory: Yes.

Host


The URL of the F5 BIG-IP server host. For example:

`https://f5.entrust.com`

Mandatory: Yes

Port

The port for accessing the F5 BIG-IP service.

 The default F5 BIG-IP port is 443.

Mandatory: Yes


Partition/Path

The partition and path, in the following syntax


```
<partition>/<path>
```

Where:

- `<partition>` is the name of a F5 BIG-IP server partition.

 The user must have access to this partition.


- `<path>` is the path of a subdirectory within the partition.

 Both values are case sensitive.

Mandatory: Yes

Username

The username for authenticating in the F5 BIG-IP server.

 The selected user must have an administrator role for the given partition in the F5 BIG-IP server.

Mandatory: Yes

Password

The password for authenticating to the F5 BIG-IP server.

Mandatory: Yes

Host CA Bundle (PEM)

The certification chain of the F5 BIG-IP server, as a bundle in PEM format.

Mandatory: Yes

Key Type

The type of keys managed by the F5 BIG-IP server:

- RSA
- EC
- DSA.

Mandatory: Yes.

Key Length

The bit length of the generated keys.

Mandatory: When **Key Type** is RSA or DSA.

Curve Name

The name of the elliptic curve.

Mandatory: When **Key Type** is EC.

Security Type

The type of security for generating the keys:

- FIPS Enabled Key
- Normal Key

Mandatory: No. This optional value defaults to Normal Key.

Enable hostname verification

Check this box for validating the F5 BIG-IP server certificate in each connection.

Allow private key export

Check this box to allow exporting the private key from the key manager – for example, to push the same certificate and key to other destinations.

 The key manager server must support key export.

Creating a KMIP key manager

See below for using any key management server meeting the Key Management Interoperability Protocol (KMIP).

To create a KMIP key manager

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create key managers.
2. Go to **Control > Key Managers**.
3. Click **Create** to configure the following settings.
 - [Label](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
 - [Plugin Type](#)
 - [KMIP Server URL](#)
 - [Client Credential file format](#)
 - [Key Algorithm](#)
 - [Key Size](#)
 - [Digital Signature Algorithm](#)
 - [Start Date](#)
 - [Enable hostname verification](#)
 - [KMIP Version](#)
 - [Allow private key export](#)
4. Click **Verify** to check the connection with the key manager.


Label

A descriptive name of the key manager.

Mandatory: Yes

Owner

The username of the person responsible for the key manager.

 The user who adds the key manager is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the key manager.

Mandatory: No

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the key manager.

Mandatory: No

Plugin Type

Select **KMIP-KeyManagement-Plugin**.

Mandatory: Yes

KMIP Server URL

The URL of the KMIP server.

```
https://<host>:<port>/kmip
```

Where:

- `<host>` is the hostname or IP address of the KMIP server.
- `<port>` is the port of the KMIP server.

For example:

```
https://172.30.141.241:5696/kmip
```


Mandatory: Yes

Client Credential file format

The file format for importing the client credentials. When selecting **PKCS#12**, configure the following additional parameters.

Parameter	Value
Client PKCS#12	A PKCS#12 file containing the key pair, certificate, and certification chain of the client.
PKCS 12 and Key Password	The password of the PKCS#12 file and the private key of the client.

When selecting **PEM**, configure the following additional parameters.

 The parameters below do not support encrypted PEM keys.

Parameter	Value
Client Key & Certificate	A file in PEM format containing the private key and certificate of the client.
CA Certificate Chain	A file in PEM format containing the certification chain of the client certificate.

Mandatory: Yes

Key Algorithm

The algorithm for generating the keys.

Mandatory: No. This optional value defaults to RSA (the only supported option).

Key Size

The bit size of the generated keys.

Mandatory: No. This optional value defaults to 2048 (the only supported option).

Digital Signature Algorithm

The algorithm for signing the certificate requests:

- SHA256
- SHA512

Mandatory: No. This optional value defaults to SHA256.

Start Date

The starting date for the background job that synchronizes the certificate states in Certificate Manager with the certificate states in the KMIP server.


Mandatory: Yes

Enable hostname verification

Check this box for validating the KMIP server certificate in each connection.

KMIP Version

The version used by the KMIP server.

 The dropdown menu only lists supported versions.

Mandatory: Yes

Allow private key export

Check this box to allow exporting the private key from the key manager – for example, to push the same certificate and key to other destinations.

 The key manager server must support key export.

Editing a key manager

See below for editing the settings of a key manager.

To edit a key Manager


1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to edit key managers.
2. Go to **Control > CA Gateways**.
3. In the main grid, select one of the key managers.
4. Click **Edit** to update the following settings.
 - [Label](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
 - [Plugin](#)
5. Click **Verify** to check the connection with the key manager.

Label

A descriptive name of the key manager.

Owner

The username of the person responsible for the key manager.

 The user who adds the key manager is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the key manager.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the key manager.

Plugin

The settings of the plugin selected when creating the key manager.

- [Creating a F5 BIG-IP key manager](#)
- [Creating a KMIP key manager](#)

Deleting key managers

See below for deleting key managers from Certificate Manager.

To delete key managers

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to delete key managers.

2. Go to **Control > CA Gateways**.
3. In the main grid, select one or more key managers.
4. Click **Delete** to remove the selected key managers from Certificate Manager.

Custom Fields

Customers can define custom fields for their organization and associate them with each certificate. These fields:

- Are available when managing [Certificates](#) or [Reports](#).
- Support string, numeric, date, list, email, and boolean data types.
- Hold specific people or teams accountable for each certificate and endpoint.
- Prevent accidental outages and risks caused by expiring certificates and insufficient algorithm strength.

See below for how to manage custom fields.

- [Browsing custom fields](#)
- [Creating a custom field](#)
- [Editing a custom field](#)
- [Deleting custom fields](#)

Browsing custom fields

See below for browsing the available custom fields.

To browse custom fields

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Control > Custom Fields**.
3. Define custom field views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. For each custom field, browse the following settings.
 - [ID](#)
 - [Display Order](#)
 - [Label](#)
 - [Active](#)
 - [Required](#)
 - [Data Type](#)
 - [List Values](#)
 - [Validation Expression](#)
 - [Help Message](#)

ID

The field identifier.

Display Order

The field position in the **Create Certificate** form. To rearrange, drag and drop a row by clicking and dragging the row's handle ≡.

Label

The label of the field in the **Create Certificate** form.

Active

✓ if the custom field is enabled in Certificate Manager; ✗ otherwise. Only active fields are available when:

- [Creating a certificate](#)
- [Editing a single certificate](#)
- [Browsing certificates](#)
- [Creating Reports](#).

Required

✓ if the custom field is mandatory; ✗ otherwise.

Data Type

The data type of the field value.

✗ After creating the custom field, you can only modify this setting if not present in issued certificates.

List Values

The list values separated by commas, when **Data Type** is **List**.

✗ After creating the custom field, you can only modify this setting if not present in issued certificates.

Validation Expression

The regular expression the field value must match.

⚠ Validation of Unicode values is not supported.

Help Message

The hover text displayed in the **Create Certificate** form.

Creating a custom field

See below for creating a custom field.

To create a custom field

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Control > Custom Fields**.
3. Click **Create** and configure the following settings.
 - [Label](#)
 - [Required](#)
 - [Data Type](#)

- [List Values](#)
- [Validation Expression](#)
- [Help Message](#)

Label

The label of the field in the **Create Certificate** form.

Mandatory: Yes

Required

Check this box to make the custom field mandatory; uncheck otherwise.

Data Type

The data type of the field value.

✗ After creating the custom field, you can only modify this setting if not present in issued certificates.

Mandatory: Yes

List Values

The list values separated by commas, when **Data Type** is **List**.

✗ After creating the custom field, you can only modify this setting if not present in issued certificates.

Mandatory: No

Validation Expression

The regular expression the field value must match.

⚠ Validation of Unicode values is not supported.

Mandatory: No

Help Message

The hover text displayed in the **Create Certificate** form.

Mandatory: No

Editing a custom field

See below for how to edit the settings of a custom field.

To edit a custom field

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Control > Custom Fields**.
3. In the main grid, select a custom field.
4. Click **Edit** to modify the following settings.
 - [Active](#)
 - [Label](#)
 - [Required](#)

- [Data Type](#)
 - [List Values](#)
 - [Validation Expression](#)
 - [Help Message](#)
5. Check the consistency of the new settings with the existing reports (as explained in [Updating a report design](#))
 6. Re-create the certificate views (as explained in [Browsing certificates](#)).

Active

Check this box to enable the custom field in Certificate Manager; uncheck otherwise. Only active fields are available when:

- [Creating a certificate](#)
- [Editing a single certificate](#)
- [Browsing certificates](#)
- [Creating Reports](#).

Label

The label of the field in the **Create Certificate** form.

Mandatory: Yes

Required

Check this box to make the custom field mandatory; uncheck otherwise.

Data Type

The data type of the field value.

✗ After creating the custom field, you can only modify this setting if not present in issued certificates.

Mandatory: Yes

List Values

The list values separated by commas, when **Data Type** is **List**.

✗ After creating the custom field, you can only modify this setting if not present in issued certificates.

Mandatory: No

Validation Expression

The regular expression the field value must match.

⚠ Validation of Unicode values is not supported.

Mandatory: No

Help Message

The hover text displayed in the **Create Certificate** form.

Mandatory: No

Deleting custom fields

See below for deleting custom fields.

To delete custom fields

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Control > Custom Fields**.
3. In the main grid, select one or more custom fields.
4. Click **Delete** to remove the selected custom fields.

Public Enrollment Forms

Public enrollment forms are HTML forms in publicly accessible URLs for non-registered users to enroll certificates without a Certificate Manager administrator account.

- [Browsing public enrollment forms](#)
- [Creating a public enrollment form](#)
- [Editing a public enrollment form](#)
- [Deleting public enrollment forms](#)
- [Using public enrollment forms](#)



See [General](#) for how to disable user access to public enrollment forms.

Browsing public enrollment forms

See below for browsing public enrollment forms.

To browse public enrollment forms

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority configured in the public enrollment form.
 - A [Certificate Role](#) for the same certificate authority and certificate profile configured in the public enrollment form.
2. Go to **Control > Public Enrollment Forms**.
3. Define public enrollment form views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. For each public enrollment form in the main grid, browse the following settings.
 - [Name](#)
 - [Description](#)
 - [Active](#)
 - [Authority](#)
 - [Profile](#)
 - [Owner](#)
 - [URL](#)

Name

The identifier of the public enrollment form.

Description

A description of the public enrollment form.

Active

✓ if the public enrollment form is publicly accessible; ✗ **No** otherwise.

Authority


The Authority to issue the enrolled certificates.

Profile

The certificate authority profile to issue the enrolled certificates.

Owner

The email address of the person responsible for the public enrollment form.

 The user who creates the public enrollment form is automatically made the owner. You can later edit this field and assign ownership to someone else.

URL

Click **Copy** to copy the public URL of the public enrollment form.

Creating a public enrollment form

See below for creating a public enrollment form.

To create a public enrollment form

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority you will configure in the public enrollment form.
 - A [Certificate Role](#) for the same certificate authority and certificate profile you will configure in the public enrollment form.
2. Go to **Control > Public Enrollment Forms**.
3. Click **Create** to configure the following configuration parameters.
 - [Name](#)
 - [Owner](#)
 - [Description](#)
 - [Custom Fields](#)
 - [Authority](#)
 - [Profile](#)
 - [Profile Key Type](#)
 - [Override required key type](#)
 - [Select allowed key types](#)
 - [Minimum RSA Key Length](#)
4. Click **Create** to expose the generated form on the Internet.
5. Click **Copy** on the main grid to obtain the public URL.


Name

The identifier of the public enrollment form.

Mandatory: Yes

Owner

The email address of the person responsible for the public enrollment form.

 The user who creates the public enrollment form is automatically made the owner. You can later edit this field and assign ownership to someone else.

Mandatory: Yes

Description

A description of the public enrollment form.

Mandatory: No

Custom Fields

The [Custom Fields](#) whose value will be requested by the public enrollment form.

Mandatory: No

Authority

The Authority to issue the enrolled certificates.

Mandatory: Yes

Profile

The certificate authority profile to issue the enrolled certificates.

Mandatory: Yes

Profile Key Type

The key type specified by the **Profile**, if any.

Mandatory: Yes

Override required key type

Whether to override the **Profile Key Type** and allow different key types.

Profile	Field visibility
A PKCS #12 profile (the CA generates the keys)	Never displayed.
A CSR profile	Only displayed when Profile Key Type is Unspecified .

Mandatory: When requested by the selected **Profile**.

Select allowed key types

The key types supported by the Certificate Signing Requests.

Profile	Field visibility
A PKCS #12 profile (the CA generates the keys)	Never displayed.
A CSR profile	Only displayed when Profile Key Type is Unspecified or Override key type is enabled.

Mandatory: When requested by the selected **Profile**.

Minimum RSA Key Length

The minimum bit length for the RSA-type keys.

Profile	Field visibility
A PKCS #12 profile (the CA generates the keys)	Never displayed.
A CSR profile	Always displayed.

Mandatory: When requested by the selected **Profile**.

Editing a public enrollment form

See below for editing the settings of a public enrollment form.

To edit a public enrollment form

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority configured in the public enrollment form.
 - A [Certificate Role](#) for the same certificate authority and certificate profile configured in the public enrollment form.
2. Go to **Control > Public Enrollment Forms**.
3. Go to **Control > Custom fields**.
4. In the main grid, select a custom field.
5. click **Edit** to update the following settings.
 - [Active](#)
 - [Name](#)
 - [Owner](#)
 - [Description](#)
 - [Custom Fields](#)
 - [Authority](#)
 - [Profile](#)
 - [Profile Key Type](#)
 - [Override required key type](#)
 - [Select allowed key types](#)
 - [Minimum RSA Key Length](#)

Active


Check this box for the public enrollment form to be accessible; uncheck otherwise.

Name

The identifier of the public enrollment form.

Owner

The email address of the person responsible for the public enrollment form.

 The user who creates the public enrollment form is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the public enrollment form.

Custom Fields

The [Custom Fields](#) whose value will be requested by the public enrollment form.

Authority

The Authority to issue the enrolled certificates.

Profile

The certificate authority profile to issue the enrolled certificates.

Profile Key Type

The key type specified by the **Profile**, if any.

Override required key type

Whether to override the **Profile Key Type** and allow different key types.

Profile	Field visibility
A PKCS #12 profile (the CA generates the keys)	Never displayed.
A CSR profile	Only displayed when Profile Key Type is Unspecified .

Mandatory: When requested by the selected **Profile**.

Select allowed key types

The key types supported by the Certificate Signing Requests.

Profile	Field visibility
A PKCS #12 profile (the CA generates the keys)	Never displayed.
A CSR profile	Only displayed when Profile Key Type is Unspecified or Override key type is enabled.

Mandatory: When requested by the selected **Profile**.

Minimum RSA Key Length

The minimum bit length for the RSA-type keys.

Profile	Field visibility
A PKCS #12 profile (the CA generates the keys)	Never displayed.
A CSR profile	Always displayed.

Mandatory: When requested by the selected **Profile**.

Deleting public enrollment forms

See below for deleting public enrollment forms.

To delete public enrollment forms


1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority configured in the public enrollment forms.
 - A [Certificate Role](#) for the certificate authority and certificate profile configured in the public enrollment form.
2. Go to **Control > Public Enrollment Forms**.
3. In the main grid, select one or more public enrollment forms.
4. Click **Delete** to remove the selected public enrollment forms.

Using public enrollment forms

As explained below, end-users can request certificates using public enrollment forms.

To request a certificate using a public enrollment form

1. Ask the administrator for the public link generated when [Creating a public enrollment form](#).

 The administrator must share this link out-of-band because the form does not require access credentials.

2. Fill in the form fields.
3. Submit the form.
4. Copy the link displayed on the submission information page
5. Use this link to check the request processing status and eventually download the certificate.

Requests For Approval

Manage the "internal" and "external" pending certificate requests.

Request type	Description
Internal	Created as explained in Making a certificate request by registered Administrators logged in to Certificate Manager.
External	Created by non-registered users from a Public Enrollment Form configured by an Administrator and published to a publicly accessible URL.

See below for the supported operations.

- [Browsing pending requests](#)
- [Approving a pending certificate request](#)
- [Rejecting a pending certificate request](#)




The default retention period for certificate requests is 365 days. See [General](#) for how to change this period.

Browsing pending requests

See below for browsing the certificate issuance and renewal requests.

To browse pending requests

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority configured in the requests.
 - A [Certificate Role](#) for the certificate authority and certificate profile configured in the requests.
2. Go to **Control > Requests For Approval**.
3. Define request views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. In the main grid, click the plus button  to display the full details of a request. See below a reference of each field displayed on the grid or the request details.
 - [Request Type](#)
 - [Associated Certificate](#)
 - [Actions](#)
 - [Key Manager](#)
 - [Request ID](#)
 - [BASIC INFO](#)
 - [DESTINATIONS](#)
 - [ACCESS TAGS](#)
 - [CUSTOM FIELDS](#)

- [CSR INFORMATION](#)
- [CERTIFICATES](#)
- [REPLACES](#)

Request Type

The type of request.

Value	Request type
Internal request	Request created as explained in Making a certificate request or Requesting a certificate renewal .
<public_form>	Request created by non-registered users using the Public Enrollment Form with <public_form> name.

Associated Certificate

The issued certificate (if any).


Actions

The actions supported by the pending request

- [Approving a pending certificate request](#)
- [Rejecting a pending certificate request](#)

Key Manager

The Key Manager that will generate the key pair, if any.

 This field is only available in PKCS#12 requests.

Request ID

The request identifier.

 Certificate Manager automatically generates this value.

BASIC INFO

Click the plus button  and select the **BASIC INFO** tab to display additional basic information.

Setting	Description
Requestor	The email address entered by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request .

Setting	Description
Description	The certificate description entered by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request .
Status	The status of the certificate requests are Pending, Approved and Rejected.
Comment	The reason behind rejecting a certificate request, if request gets rejected.
Date Created	The date when an end-user requested the certificate using a Public Enrollment Form published online, or an administrator requested the certificate as explained in Making a certificate request .
Last Modified	The date of the latest request modification, whether it should be request creation, request approval or request rejection.
Authority	The issuing certificate authority configured in a Public Enrollment Form published online, or selected by an administrator as explained in Making a certificate request .
Profile	The certificate authority profile configured for a Public Enrollment Form published online, or selected by an administrator as explained in Making a certificate request .
Subject DN	The distinguished name (DN) of the certificate subject as defined or included in the certificate signing request (CSR) pasted by an end-user on a Public Enrollment Form published online, or pasted by an administrator as explained in Making a certificate request .
SAN	The subject alternative name (SAN) entered by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request .
Subject Variables	The certificate subject variables, if required by the selected profile defined by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request .

DESTINATIONS


Click the plus button  and select the **DESTINATIONS** tab to display the destination an administrator selected when [Making a certificate request](#).

ACCESS TAGS

Click the plus button  and select the **ACCESS TAGS** tab to display the [Certificate Access Tags](#):


- Entered by an administrator as explained in [Making a certificate request](#).
- Entered by an administrator when approving the certificate request.

CUSTOM FIELDS

Click the plus button  and select the **CUSTOM FIELDS** tab to display the [Custom Fields](#) an administrator entered when [Making a certificate request](#).

CSR INFORMATION

Click the plus button  and select the **CSR INFORMATION** tab to display additional request information.

 The selected certificate profile sets all the values described in the following table.


Setting	Description
Subject	The Distinguished Name (DN) of the certificate subject.
Public Key Algorithm	The name or OID of the certificate public key algorithm.
Public Key Size	The size in bits of the certificate public key.
Public Key Exponent	The exponent of the public key, if any.
Signature Algorithm	The name or OID of the certificate signing algorithm.
Attributes	The extension attributes present in the request (if any): Subject Alternative Names (SAN), Key Usages, Basic Constraints...
EC Curve	The name of Elliptic Curve (EC), if the public key uses Elliptic Curve Cryptography (ECC).

CERTIFICATES

Click the plus button  and select the **CERTIFICATES** tab to display the request PEM encoding of:

- The certificate.
- The certificate certification chain.
- The certificate signing request (CSR).

REPLACES

Click the plus button  and select the **REPLACES** tab to display the renewed certificate, if the request is a renewal request.

Approving a pending certificate request

See below for approving a certificate issuance or renewal request.

To approve a request

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority configured in the requests.
 - A [Certificate Role](#) for the certificate authority and certificate profile configured in the request.
2. Go to **Control > Requests For Approval**.
3. In the main grid, click **Select Action > Approve** for the pending certificate request.
4. In the **Approve** form, update the value of the [Certificate Access Tags](#) and certificate [Custom Fields](#).
5. Click **Approve** to:
 - Issue the certificate, if the selected profile processes a CSR.
 - Mark the request as **Approved**, if the selected profile is a PKCS#12 profile. See [Issuing a PKCS #12](#) to issue the certificate.

Rejecting a pending certificate request

See below for rejecting a certificate issuance or renew request.


To reject a pending certificate request

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - A [<ca>_admin](#) role for the certificate authority configured in the request.
 - A [Certificate Role](#) for the certificate authority and certificate profile configured in the request.
2. Go to **Control > Requests For Approval**.
3. In the main grid, click **Select Action > Reject** for a pending certificate request.
4. In the **Reject** form, add a mandatory comment on the reason for rejecting the request.
5. Click **Reject**.

My Certificate Requests

Create and browse your certificate requests.

- [Browsing my certificate requests](#)
- [Issuing a PKCS #12](#)
- [Making a certificate request](#)

 The default retention period for certificate requests is 365 days. See [General](#) for how to change this period.

Browsing my certificate requests

See below for browsing your certificate issuance and renewal requests.

To browse your certificate requests

1. Log in as an administrator with a [Certificate Role](#) for the CA and certificate profile configured in the requests.
2. Go to **Control > My Certificate Requests**.
3. Define request views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.

- Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. In the main grid, click the plus button **+** to display the full details of a request. See below a reference of each field displayed on the grid or the request details.
- [Associated Certificate](#)
 - [Actions](#)
 - [Key Manager](#)
 - [Request ID](#)
 - [BASIC INFO](#)
 - [DESTINATIONS](#)
 - [ACCESS TAGS](#)
 - [CUSTOM FIELDS](#)
 - [CSR INFORMATION](#)
 - [CERTIFICATES](#)
 - [REPLACES](#)

Associated Certificate

The issued certificate (if any).

Actions

The [Issuing a PKCS #12](#) action supported by the request

Key Manager

The Key Manager that will generate the key pair, if any.

i This field is only available in PKCS#12 requests.

Request ID

The request identifier.

i Certificate Manager automatically generates this value.

BASIC INFO

Click the plus button **+** and select the **BASIC INFO** tab to display additional basic information.

Setting	Description
Requestor	The email address entered by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request .

Setting	Description
Description	The certificate description entered by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request .
Status	The status of the certificate requests are Pending, Approved and Rejected.
Comment	The reason behind rejecting a certificate request, if request gets rejected.
Date Created	The date when an end-user requested the certificate using a Public Enrollment Form published online, or an administrator requested the certificate as explained in Making a certificate request .
Last Modified	The date of the latest request modification, whether it should be request creation, request approval or request rejection.
Authority	The issuing certificate authority configured in a Public Enrollment Form published online, or selected by an administrator as explained in Making a certificate request .
Profile	The certificate authority profile configured for a Public Enrollment Form published online, or selected by an administrator as explained in Making a certificate request .
Subject DN	The distinguished name (DN) of the certificate subject as defined or included in the certificate signing request (CSR) pasted by an end-user on a Public Enrollment Form published online, or pasted by an administrator as explained in Making a certificate request .
SAN	The subject alternative name (SAN) entered by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request .
Subject Variables	The certificate subject variables, if required by the selected profile defined by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request .

DESTINATIONS


Click the plus button  and select the **DESTINATIONS** tab to display the destination an administrator selected when [Making a certificate request](#).

ACCESS TAGS

Click the plus button  and select the **ACCESS TAGS** tab to display the [Certificate Access Tags](#):


- Entered by an administrator as explained in [Making a certificate request](#).
- Entered by an administrator when approving the certificate request.

CUSTOM FIELDS

Click the plus button  and select the **CUSTOM FIELDS** tab to display the [Custom Fields](#) an administrator entered when [Making a certificate request](#).

CSR INFORMATION

Click the plus button  and select the **CSR INFORMATION** tab to display additional request information.

 The selected certificate profile sets all the values described in the following table.


Setting	Description
Subject	The Distinguished Name (DN) of the certificate subject.
Public Key Algorithm	The name or OID of the certificate public key algorithm.
Public Key Size	The size in bits of the certificate public key.
Public Key Exponent	The exponent of the public key, if any.
Signature Algorithm	The name or OID of the certificate signing algorithm.
Attributes	The extension attributes present in the request (if any): Subject Alternative Names (SAN), Key Usages, Basic Constraints...
EC Curve	The name of Elliptic Curve (EC), if the public key uses Elliptic Curve Cryptography (ECC).

CERTIFICATES

Click the plus button  and select the **CERTIFICATES** tab to display the request PEM encoding of:

- The certificate.
- The certificate certification chain.
- The certificate signing request (CSR).

REPLACES

Click the plus button  and select the **REPLACES** tab to display the renewed certificate, if the request is a renewal request.

Issuing a PKCS #12

See below for issuing a PKCS #12 containing a certificate and a key pair.

To issue a PKCS #12

1. Log in as an administrator with a [Certificate Role](#) for a CA and a set of profiles.
2. Go to **Control > My Certificate Requests**.
3. Browse for requests with:
 - A profile that supports PKCS #12 generation.
 - The **Approval** status. See [Approving a pending certificate request](#) for how to approve a request.
4. In the main grid, click **Select Action > Issue PKCS12** for a certificate request.
5. Wait until a notification in the bottom right corner of the Certificate Manager UI announces the PKCS #12 issuance.
6. Click the download link in the notification, You can also download the PKCS #12 from:
 - The list of notifications in the top-right **Notifications** menu.
 - The certificates view described in [Browsing certificates](#).

Making a certificate request

See below for requesting a certificate using the Certificate Manager administration UI.

To make a certificate request

1. Log in as an administrator with a [Certificate Role](#) for a CA and a set of profiles.
2. Go to **Control > My Certificate Requests**.
3. Click **Make Request**
4. Fill in the following forms of the **Make Request** wizard.
 - [General](#)
 - [Destinations](#)
 - [Profile Options](#)
 - [Renewal](#)
5. Click **Create** to create the certificate request.

General

Configure the following settings in **General** form of the **Make Request** wizard.

- [Owner](#)
- [Description](#)
- [<custom>](#)
- [Access Tags](#)
- [Certificate Authority](#)
- [Certificate Profile](#)
- [Use a key manager \(KMS\) to generate the key pair](#)

Owner

The email address of the person responsible for the certificate – for example, the Web server operator.

Mandatory: Yes

Description

A brief description of the certificate purpose.

Mandatory: No

[<custom>](#)

Business-specific [Custom Fields](#) defined by your organization.

Mandatory: No

Access Tags

One or several [Certificate Access Tags](#).



[Certificate Roles](#) with any of these tags will grant permissions on the certificate.

Mandatory: No

Certificate Authority

The certificate authority that issues the certificate. See [Authorities](#) for how to register certificate authorities.

Mandatory: Yes

Certificate Profile

The certificate profile the certificate authority applies to issue the certificate. For certificates to be published in [Destinations](#), consider the following profile limitations.

Destination	Limitations
Apache	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).
Azure	Does not support issuing certificates from a CSR.
Nginx	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).



The selected certificate profile must be configured in CA Gateway for the Certificate Authority.


Mandatory: Yes

Use a key manager (KMS) to generate the key pair

To generate the certificate key pair with a key manager, check this box and select a key manager from the **Key Manager** list.


For the key managers described in [Creating a F5 BIG-IP key manager](#), also configure the settings in the table below.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

 See [Key Managers](#) for creating key managers and techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Destinations


If required by the certificate profile, add one or more [Destinations](#) to publish the issued certificate.

 If you selected a [Key Manager](#), ensure the **Allow private key export** option is enabled on this Key Manager to add additional destinations for this certificate.

To add a destination

1. In the **Destinations** list, select a destination previously created as explained in the following sections.
 - [Creating a HashiCorp Vault destination](#)
 - [Creating a Microsoft IIS web server destination](#)
 - [Creating an Apache web server destination](#)
 - [Creating an AWS Certificate Manager destination](#)
 - [Creating an Azure Key Vault destination](#)
 - [Creating an F5 BIG-IP destination](#)
 - [Creating an Nginx web server destination](#)
 - [Creating an SFTP destination](#)

2. Click **Add** to confirm the selection.


 Apache and Nginx destinations do not support adding several destinations or other key managers.

3. If required, configure destination-specific parameters.
 - [F5 BIG-IP destination-specific settings](#)
 - [Microsoft IIS destination-specific settings](#)

F5 BIG-IP destination-specific settings

Configure the following additional settings when adding a destination of the F5 BIG-IP type.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

 See techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.


Microsoft IIS destination-specific settings

When adding a destination of the Microsoft IIS type, enter one or more site bindings in the **Site bindings** field. Define each binding with a line in the following syntax.

```
<name>;<host>;<port>
```

Where:

- `<name>` is the website name
- `<host>` is the website hostname or IP address
- `<port>` is the port for connecting to the website.

 Select a certificate profile with "Web Server" or dual usage (key encipherment and digital signature) to deploy the certificate successfully.

Profile Options

Configure the following settings in the **Profile Options** form of the **Make Request** wizard.


- [Certificate Signing Request \(CSR\)](#)
- [Password](#)
- [Subject Variable Requirements](#)
- [Subject Alternative Names](#)
- [Expected Subject DN](#)

Certificate Signing Request (CSR)

The PEM or Base64 encoding of a CSR (Certificate Signing Request).

This field is only present when the selected certificate profile issues certificates from CSR. In this issuance mode:

- The user generates the key pair and the CSR.
- The CA processes the CSR and issues the certificate.
- The user downloads the certificate.

 When selecting Apache, Nginx, or Microsoft IIS certificate destinations, Certificate Manager ignores any client-generated CSR and uses instead a CSR generated at the destination along with the key pair.

Password

A password for the generated P12.

This field is only present when the selected certificate profile issues certificates in P12 files. In this issuance mode:


1. The CA generates the key pair.
2. The user downloads both the certificate and the private key in a P12 file protected with the selected password.

Subject Variable Requirements

Variable values to build:

- The subject's distinguished name for the CSR, if using a Key Manager.
- The expected subject's distinguished name otherwise.

This field is mandatory when required by the selected profile.

 Certificate renewals reuse the value of Subject variables, such as Subject DN, entered at issuance. Thus, the value of these variables is read-only during renewal.

Subject Alternative Names

The list of subject alternative names (SAN) for the certificate.

Expected Subject DN

The Subject DN (Distinguished Name) that Certificate Manager will generate using the configured values. This field is read-only.

Renewal

If supported by the selected profile, you can check the **Auto Renewal** box and configure the following settings.

- [Renewal Period](#)
- [PKCS12 Password](#)

Renewal Period

The day the certificate must be renewed, as a number of days before the certificate expiry. For a certificate that expires in E days and a **Renewal Period** set to P, the renewal starts in E-P days. At 12:00 AM UTC every day, a background process collects the certificates that:

- Must be renewed the same day because E-P=0
- Failed a previous renewal because E-P<0

For example, to force a certificate renewal the next day, set a P value equal to E-1 before 12:00 AM UTC. At 12:00 AM UTC, E-P will equal 0, and the certificate will be included in the renewal queue for that day.

i The restrictions imposed by Apache, Nginx, or Microsoft IIS destinations on other issuance modes do not affect automated renewal. Specifically, these destinations support automated renewal with client-side generated keys and CSRs.

PKCS12 Password

The password of the PKCS #12 for delivering the certificate and its private key in the selected **Destinations**.

i This password is encrypted and stored in the application database.

Certificates

The certificates managed by Certificate Manager come from one or more of the origins below.

Certificate origin	See section
Detected by the Discovery Scanners	Find
Imported into Certificate Manager	Importing certificates
Imported into Certificate Manager using the Certificate Manager API	Certificate Manager API
Issued using the Certificate Manager Web browser interface	Creating a certificate

Certificate origin	See section
Provided by a source and inserted with source synchronization operations	Sources
Imported with key manager synchronization operations	Key Managers

Operations you can take include:

- [Browsing certificates](#)
- [Creating a certificate](#)
- [Automating certificate renewal](#)
- [Manually renewing a certificate](#)
- [Requesting a certificate renewal](#)
- [Editing a single certificate](#)
- [Editing certificates in bulk](#)
- [Revoking a certificate](#)
- [Revoking certificates in bulk](#)
- [Releasing a certificate from hold](#)
- [Exporting a certificate](#)
- [Importing certificates](#)
- [Archiving certificates](#)
- [Archiving certificates in bulk](#)

Browsing certificates

See below for browsing the certificates managed by Certificate Manager.

To browse certificates

1. Go to **Control > Certificates**.
2. Click **Show Insights** at the top-right to display information such as:
 - The total number of issued certificates.
 - The total number of certificates issued, expired, renewed, suspended, revoked, or archived.
 - The number of post-quantum certificates issued, expired, renewed, suspended, revoked, or archived.
3. Define grid certificate views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. Select **Update > Save As** to save the view. Alternatively, you can click **Update** to overwrite the currently selected view.

 Grid records in boldface correspond to post-quantum certificates.

5. For each certificate in the main grid, check the following parameters.
 - [Common Name](#)
 - [Key Algorithm](#)

- [Key Algorithm Security Level](#)
- [Owner](#)
- [Revocation Reason](#)
- [Signature Algorithm](#)
- [Access Tags](#)
- [Actions](#)
- [Auto Renew](#)
- [Compliance Last Evaluated](#)
- [Compliance Result](#)
- [Compliance Result Last Modified](#)
- [Description](#)
- [Domains](#)
- [Endpoints](#)
- [Expires](#)
- [Issuer](#)
- [Key Length](#)
- [Key Manager](#)
- [Key State](#)
- [Last Modified](#)
- [Name](#)
- [Serial Number](#)
- [Signing Algorithm Security Level](#)
- [Source Type](#)
- [Subject Alternative Names](#)
- [Valid From](#)
- [Validity](#)
- [Certificate Details](#)

Common Name

The common name (CN) of the certificate subject. In SSL/TLS certificates, this value usually matches the **Domains** value.

Key Algorithm

The algorithm used to generate the key pair.

Key Algorithm Security Level

The security of the key algorithm.

Level	Description
1	Basic security (AES-128 equivalent)
2	Moderate security (SHA-256 equivalent)
3	High security (AES-192 equivalent)
4	Very high security (SHA-384 equivalent)

Level	Description
5	Highest security (AES-256 equivalent)

Owner

The email address of the person responsible for the certificate – for example, the Web server operator.

Revocation Reason

The revocation reason, when the value of the **Validity** column is **Revoked**.

Signature Algorithm

The hash signature algorithm.

Access Tags

One or several [Certificate Access Tags](#).

 [Certificate Roles](#) with any of these tags will grant permissions on the certificate.

Actions

The actions supported by the certificate. See the following sections for details.

- [Editing a single certificate](#)
- [Exporting a certificate](#)
- [Automating certificate renewal](#)
- [Manually renewing a certificate](#)
- [Revoking a certificate](#)
- [Archiving certificates](#)

Auto Renew

 if the automatic renewal is enabled as explained in [Automating certificate renewal](#);  otherwise.

Compliance Last Evaluated

The time and date of the latest key evaluation performed by the [Compliance Manager](#).

Compliance Result

The result of the latest key evaluation performed by the [Compliance Manager](#).

Compliance Result Last Modified

The date and time of the latest change in the result of the key evaluation performed by the [Compliance Manager](#).

Description

A brief description of the certificate purpose.

Domains

The [Domains](#) certified by the SSL/TLS certificate.

Endpoints

The host and port where a discovery scan discovered the certificate.

Expires

The **Not After** date of the certificate.

Issuer


The common name (CN) of the certificate issuer.

Key Length

The length of the certificate key.

Key Manager

The Key Manager, if a Key Manager generated the key pair.

 See [Key Managers](#) for how to create key managers.

Key State

The validity state of the key.

Last Modified

The time and date of the latest [Key State](#) modification.

Name

The concatenation of the following certificate field values.

- [Common Name](#)
- [Issuer](#)
- Hash

Serial Number

The serial number (SN) of the certificate.

Signing Algorithm Security Level

The security of the hash signing algorithm.

Level	Description
1	Basic security (AES-128 equivalent)
2	Moderate security (SHA-256 equivalent)

Level	Description
3	High security (AES-192 equivalent)
4	Very high security (SHA-384 equivalent)
5	Highest security (AES-256 equivalent)

Source Type

The type of the certificate [Source](#).

Subject Alternative Names

The list of subject alternative names (SAN) of the certificate.

Valid From

The **Not Before** date of the certificate.

Validity


The certificate status:

- Empty for certificates from unknown sources (because either imported or discovered);
- **Issued** for certificates from known sources and still valid;
- **Revoked** for certificates from known sources and already revoked as explained in [Revoking a certificate](#).

Certificate Details

Click the plus button  to display the following certificate details.

- [BASICS](#)
- [ACCESS TAGS](#)
- [CUSTOM FIELDS](#)
- [EXISTING DESTINATIONS](#)
- [RENEWAL DESTINATIONS](#)
- [DOMAINS](#)
- [REPLACES](#)
- [ENDPOINTS](#)
- [CERTIFICATES](#)

 The details view for post-quantum certificates displays a shield badge in the top-right corner.

BASICS


The following certificate information.

Setting	Description
Certificate Authority	The Subject's DN (Distinguished Name) of the issuing CA certificate.

Setting	Description
Source Type	The type of the certificate Source .
Serial	The serial number (SN) of the certificate.
Valid From	The Not Before date of the certificate.
Valid To	The Not After date of the certificate.
Last Modified	The time and date of the latest Key State modification.
SAN	The list of subject alternative names (SAN) of the certificate.
Key Length	The length of the certificate key.
Signature Algorithm	The hash signature algorithm and the Signing Algorithm Security Level
Key Algorithm	The key-pair generation algorithm and the Key Algorithm Security Level .
Validity	The certificate status: Empty for certificates from unknown sources (because either imported or discovered); Issued for certificates from known sources and still valid; Revoked for certificates from known sources and already revoked as explained in Revoking a certificate .
Requested Properties	Additional properties included in the certificate request.

ACCESS TAGS

The list of [Certificate Access Tags](#).

 The [Certificate Roles](#) with any of these tags will grant permissions on the certificate.

CUSTOM FIELDS

The business-specific [Custom Fields](#) defined by your organization.

EXISTING DESTINATIONS

The list of [Destinations](#) where Certificate Manager has pushed the certificate.

RENEWAL DESTINATIONS

The list of [Destinations](#) where Certificate Manager will push the certificate upon auto-renewal.

DOMAINS

The **DOMAINS** tab to display the list of certified domains.

REPLACES

The certificate renewed by the current certificate.

ENDPOINTS

The [Endpoint](#) where a Discovery Scanner discovered the certificate (if any).

Setting	Description
Host Name	The name of the endpoint host.
Port	The endpoint port.
Service	The service exposed on the endpoint.
Service Vendor	The vendor of the service exposed on the endpoint.
Service Vendor Version	The version of the vendor services exposed on the endpoint.
Cipher Suites	The list of cipher suites that a service accepts.
OS Type	The operating system type of the endpoint.
Completed	The time and date the certificate discovery scan was completed.

CERTIFICATES

The PEM encoding of:

- The certificate.
- The certificate certification chain.
- The certificate signing request (CSR).

Creating a certificate

See below for creating a certificate in Certificate Manager.

To create a certificate

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority that will issue the certificate.

- A [Certificate Role](#) with permissions to create certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. Click **Create**.
4. Fill in the following forms of the **Create** wizard.
 - [General](#)
 - [Destinations](#)
 - [Profile Options](#)
 - [Renewal](#)
5. Click **Create** to create the certificate.
6. Wait until a notification in the bottom right corner of the Certificate Manager UI announces the certificate issuance.
7. Click the download link in the notification. You can also download the certificate from:
 - The list of notifications in the top-right **Notifications** menu.
 - The certificates view described in [Browsing certificates](#).

General

Configure the following settings in the **General** form of the **Create** wizard.

- [Owner](#)
- [Description](#)
- [<custom>](#)
- [Access Tags](#)
- [Certificate Authority](#)
- [Certificate Profile](#)
- [Use a key manager \(KMS\) to generate the key pair](#)

Owner

The email address of the person responsible for the certificate – for example, the Web server operator.

Mandatory: Yes

Description

A brief description of the certificate purpose.

Mandatory: No

<custom>

Business-specific [Custom Fields](#) defined by your organization.

Mandatory: No

Access Tags

One or several [Certificate Access Tags](#).



[Certificate Roles](#) with any of these tags will grant permissions on the certificate.

Mandatory: No

Certificate Authority


The certificate authority that issues the certificate. See [Authorities](#) for how to register certificate authorities.

Mandatory: Yes

Certificate Profile

The certificate profile the certificate authority applies to issue the certificate. For certificates to be published in [Destinations](#), consider the following profile limitations.

Destination	Limitations
Apache	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).
Azure	Does not support issuing certificates from a CSR.
Nginx	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).

 The selected certificate profile must be configured in CA Gateway for the Certificate Authority.


Mandatory: Yes

Use a key manager (KMS) to generate the key pair

To generate the certificate key pair with a key manager, check this box and select a key manager from the **Key Manager** list.


For the key managers described in [Creating a F5 BIG-IP key manager](#), also configure the settings in the table below.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

 See [Key Managers](#) for creating key managers and techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Destinations

If required by the certificate profile, add one or more [Destinations](#) to publish the issued certificate.


 If you selected a [Key Manager](#), ensure the **Allow private key export** option is enabled on this Key Manager to add additional destinations for this certificate.

To add a destination

1. In the **Destinations** list, select a destination previously created as explained in the following sections.
 - [Creating a HashiCorp Vault destination](#)
 - [Creating a Microsoft IIS web server destination](#)

- [Creating an Apache web server destination](#)
- [Creating an AWS Certificate Manager destination](#)
- [Creating an Azure Key Vault destination](#)
- [Creating an F5 BIG-IP destination](#)
- [Creating an Nginx web server destination](#)
- [Creating an SFTP destination](#)

2. Click **Add** to confirm the selection.

 Apache and Nginx destinations do not support adding several destinations or other key managers.


3. If required, configure destination-specific parameters.

- [F5 BIG-IP destination-specific settings](#)
- [Microsoft IIS destination-specific settings](#)

F5 BIG-IP destination-specific settings

Configure the following additional settings when adding a destination of the F5 BIG-IP type.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

 See techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.


Microsoft IIS destination-specific settings

When adding a destination of the Microsoft IIS type, enter one or more site bindings in the **Site bindings** field. Define each binding with a line in the following syntax.

```
<name>;<host>;<port>
```

Where:

- `<name>` is the website name
- `<host>` is the website hostname or IP address
- `<port>` is the port for connecting to the website.

 Select a certificate profile with "Web Server" or dual usage (key encipherment and digital signature) to deploy the certificate successfully.

Profile Options

Configure the following settings in the **Profile Options** form of the **Create** wizard.

- [Certificate Signing Request \(CSR\)](#)
- [Password](#)
- [Requested Properties](#)


- [Subject Alternative Names](#)
- [Subject DN for CSR](#)

Certificate Signing Request (CSR)

The PEM or Base64 encoding of a CSR (Certificate Signing Request).

This field is only present when the selected certificate profile issues certificates from CSR. In this issuance mode:

- The user generates the key pair and the CSR.
- The CA processes the CSR and issues the certificate.
- The user downloads the certificate.

 When selecting Apache, Nginx, or Microsoft IIS certificate destinations, Certificate Manager ignores any client-generated CSR and uses instead a CSR generated at the destination along with the key pair.

Password

A password for the generated P12.

This field is only present when the selected certificate profile issues certificates in P12 files. In this issuance mode:

1. The CA generates the key pair.
2. The user downloads both the certificate and the private key in a P12 file protected with the selected password.

Requested Properties

Additional properties of the selected profile (if any).

Subject Alternative Names

The list of subject alternative names (SAN) for the certificate.

Subject DN for CSR

The distinguished name of the certificate subject. This field is mandatory when:

- The selected certificate profile issues certificates from CSRs, and
- The **Use Subject DN from CSR** checkbox is not marked.

Renewal

If supported by the selected profile, you can check the **Auto Renewal** box and configure the following settings.


- [Renewal Period](#)
- [PKCS12 Password](#)

Renewal Period

The day the certificate must be renewed, as a number of days before the certificate expiry. For a certificate that expires in E days and a **Renewal Period** set to P, the renewal starts in E-P days. At 12:00 AM UTC every day, a background process collects the certificates that:


- Must be renewed the same day because E-P=0
- Failed a previous renewal because E-P<0

For example, to force a certificate renewal the next day, set a P value equal to E-1 before 12:00 AM UTC. At 12:00 AM UTC, E-P will equal 0, and the certificate will be included in the renewal queue for that day.

 The restrictions imposed by Apache, Nginx, or Microsoft IIS destinations on other issuance modes do not affect automated renewal. Specifically, these destinations support automated renewal with client-side generated keys and CSRs.


PKCS12 Password

The password of the PKCS #12 for delivering the certificate and its private key in the selected **Destinations**.

 This password is encrypted and stored in the application database.

Automating certificate renewal

See below for automating the successive renewals of a certificate.

 As explained in [Creating a certificate](#), you can configure the certificate renewal on certificate creation.

To automate the renewal of a certificate

1. Log in as an administrator with one of the following roles.
 - The `<ca>_admin` role for the certificate authority that will renew the certificate.
 - A [Certificate Role](#) with permission to create certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. In the main grid, click **Select Action > Automate** for the certificate.
4. Configure the following settings.
 - [Certificate Authority](#)
 - [Certificate Profile](#)
 - [Destinations](#)
 - [Key Manager](#)
 - [Renewal](#)

Certificate Authority

The certificate authority that issues the certificate. See [Authorities](#) for how to register certificate authorities.


Certificate Profile

The certificate profile the certificate authority applies to issue the certificate.

 The selected certificate profile must be configured in CA Gateway for the certificate authority.

Destinations

If required by the certificate profile, add one or more [Destinations](#) to publish the issued certificate.


 If you selected a [Key Manager](#), ensure the **Allow private key export** option is enabled on this Key Manager to add additional destinations for this certificate.

To add a destination

1. In the **Destinations** list, select a destination previously created as explained in the following sections.
 - [Creating a HashiCorp Vault destination](#)

- [Creating a Microsoft IIS web server destination](#)
- [Creating an Apache web server destination](#)
- [Creating an AWS Certificate Manager destination](#)
- [Creating an Azure Key Vault destination](#)
- [Creating an F5 BIG-IP destination](#)
- [Creating an Nginx web server destination](#)
- [Creating an SFTP destination](#)

2. Click **Add** to confirm the selection.

 Apache and Nginx destinations do not support adding several destinations or other key managers.


3. If required, configure destination-specific parameters.

- [F5 BIG-IP destination-specific settings](#)
- [Microsoft IIS destination-specific settings](#)

F5 BIG-IP destination-specific settings

Configure the following additional settings when adding a destination of the F5 BIG-IP type.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

 See techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.


Microsoft IIS destination-specific settings

When adding a destination of the Microsoft IIS type, enter one or more site bindings in the **Site bindings** field. Define each binding with a line in the following syntax.

```
<name>;<host>;<port>
```

Where:

- `<name>` is the website name
- `<host>` is the website hostname or IP address
- `<port>` is the port for connecting to the website.


 Select a certificate profile with "Web Server" or dual usage (key encipherment and digital signature) to deploy the certificate successfully.

Key Manager (auto)

If required by the certificate profile, select the key manager that will generate the key pair.

For the key managers described in [Creating a F5 BIG-IP key manager](#), also configure the settings in the table below.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

 See [Key Managers](#) for creating key managers and techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Renewal

If supported by the selected profile, you can check the **Auto Renewal** box and configure the following settings.


- [Renewal Period](#)
- [PKCS12 Password](#)

Renewal Period

The day the certificate must be renewed, as a number of days before the certificate expiry. For a certificate that expires in E days and a **Renewal Period** set to P, the renewal starts in E-P days. At 12:00 AM UTC every day, a background process collects the certificates that:


- Must be renewed the same day because E-P=0
- Failed a previous renewal because E-P<0

For example, to force a certificate renewal the next day, set a P value equal to E-1 before 12:00 AM UTC. At 12:00 AM UTC, E-P will equal 0, and the certificate will be included in the renewal queue for that day.

 The restrictions imposed by Apache, Nginx, or Microsoft IIS destinations on other issuance modes do not affect automated renewal. Specifically, these destinations support automated renewal with client-side generated keys and CSRs.

PKCS12 Password

The password of the PKCS #12 for delivering the certificate and its private key in the selected **Destinations**.

 This password is encrypted and stored in the application database.

Manually renewing a certificate

See below for manually renewing a certificate before its expiry date.

To manually renew a certificate

1. Log in as an administrator with one of the following roles.
 - The [<ca>_admin](#) role for the certificate authority that will renew the certificate.
 - A [Certificate Role](#) with permission to renew certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. In the main grid, click **Select Action > Renew** for a certificate.
4. Fill in the following forms of the Create wizard.
 - [General](#)

- [Destinations](#)
 - [Profile Options](#)
 - [Automate Options](#)
5. Click **Renew** to renew the certificate.
 6. Wait until a notification in the bottom right corner of the Certificate Manager UI announces the certificate issuance.
 7. Click the download link in the notification. You can also download the certificate from:
 - The list of notifications in the top-right **Notifications** menu.
 - The certificates view described in [Browsing certificates](#).

General

Configure the following settings in the **General** form of the **Renew** wizard.

- [Owner](#)
- [Description](#)
- [<custom>](#)
- [Access Tags](#)
- [Certificate Authority](#)
- [Certificate Profile](#)
- [Use a key manager \(KMS\) to generate the key pair](#)

Owner

The email address of the person responsible for the certificate – for example, the Web server operator.

Description

A brief description of the certificate purpose.

<custom>

Business-specific [Custom Fields](#) defined by your organization.

Access Tags

One or several [Certificate Access Tags](#).



[Certificate Roles](#) with any of these tags will grant permissions on the certificate.

Certificate Authority


The certificate authority that issues the certificate. See [Authorities](#) for how to register certificate authorities.

Certificate Profile

The certificate profile the certificate authority applies to issue the certificate. For certificates to be published in [Destinations](#), consider the following profile limitations.

Destination	Limitations
Apache	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).

Destination	Limitations
Azure	Does not support issuing certificates from a CSR.
Nginx	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).


 The selected certificate profile must be configured in CA Gateway for the Certificate Authority.

Use a key manager (KMS) to generate the key pair

To generate the certificate key pair with a key manager, check this box and select a key manager from the **Key Manager** list.


For the key managers described in [Creating a F5 BIG-IP key manager](#), also configure the settings in the table below.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

 See [Key Managers](#) for creating key managers and techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.


Destinations

If required by the certificate profile, add one or more [Destinations](#) to publish the issued certificate.

 If you selected a [Key Manager](#), ensure the **Allow private key export** option is enabled on this Key Manager to add additional destinations for this certificate.

To add a destination

1. In the **Destinations** list, select a destination previously created as explained in the following sections.
 - [Creating a HashiCorp Vault destination](#)
 - [Creating a Microsoft IIS web server destination](#)
 - [Creating an Apache web server destination](#)
 - [Creating an AWS Certificate Manager destination](#)
 - [Creating an Azure Key Vault destination](#)
 - [Creating an F5 BIG-IP destination](#)
 - [Creating an Nginx web server destination](#)
 - [Creating an SFTP destination](#)
2. Click **Add** to confirm the selection.

 Apache and Nginx destinations do not support adding several destinations or other key managers.


3. If required, configure destination-specific parameters.

- [F5 BIG-IP destination-specific settings](#)
- [Microsoft IIS destination-specific settings](#)

F5 BIG-IP destination-specific settings

Configure the following additional settings when adding a destination of the F5 BIG-IP type.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

 See techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.


Microsoft IIS destination-specific settings

When adding a destination of the Microsoft IIS type, enter one or more site bindings in the **Site bindings** field. Define each binding with a line in the following syntax.

```
<name>;<host>;<port>
```

Where:

- `<name>` is the website name
- `<host>` is the website hostname or IP address
- `<port>` is the port for connecting to the website.

 Select a certificate profile with "Web Server" or dual usage (key encipherment and digital signature) to deploy the certificate successfully.

Profile Options

Configure the following settings in the **Profile Options** form of the **Renew** wizard.

- [Certificate Signing Request \(CSR\)](#)
- [Password](#)
- [Subject DN for CSR](#)
- [Subject Variable Requirements](#)
- [Subject Alternative Names](#)

Certificate Signing Request (CSR)

The PEM or Base64 encoding of a CSR (Certificate Signing Request).

This field is only present when the selected certificate profile issues certificates from CSR. In this issuance mode:

- The user generates the key pair and the CSR.
- The CA processes the CSR and issues the certificate.
- The user downloads the certificate.

i When selecting Apache, Nginx, or Microsoft IIS certificate destinations, Certificate Manager ignores any client-generated CSR and uses instead a CSR generated at the destination along with the key pair.

Password

A password for the generated P12.

This field is only present when the selected certificate profile issues certificates in P12 files. In this issuance mode:

1. The CA generates the key pair.
2. The user downloads both the certificate and the private key in a P12 file protected with the selected password.

Subject DN for CSR

The distinguished name of the certificate subject. This field is mandatory when:

- The selected certificate profile issues certificates from CSRs, and
- The **Use Subject DN from CSR** checkbox is not marked.

Subject Variable Requirements

Variable values to build:

- The subject's distinguished name for the CSR, if using a Key Manager.
- The expected subject's distinguished name otherwise.

This field is mandatory when required by the selected profile.

i Certificate renewals reuse the value of Subject variables, such as Subject DN, entered at issuance. Thus, the value of these variables is read-only during renewal.

Subject Alternative Names

The list of subject alternative names (SAN) for the certificate.

Renewal

If supported by the selected profile, you can check the **Auto Renewal** box and configure the following settings.

- [Renewal Period](#)
- [PKCS12 Password](#)

Renewal Period

The day the certificate must be renewed, as a number of days before the certificate expiry. For a certificate that expires in E days and a **Renewal Period** set to P, the renewal starts in E-P days. At 12:00 AM UTC every day, a background process collects the certificates that:

- Must be renewed the same day because E-P=0
- Failed a previous renewal because E-P<0

For example, to force a certificate renewal the next day, set a P value equal to E-1 before 12:00 AM UTC. At 12:00 AM UTC, E-P will equal 0, and the certificate will be included in the renewal queue for that day.

i The restrictions imposed by Apache, Nginx, or Microsoft IIS destinations on other issuance modes do not affect automated renewal. Specifically, these destinations support automated renewal with client-side generated keys and CSRs.

PKCS12 Password

The password of the PKCS #12 for delivering the certificate and its private key in the selected **Destinations**.

i This password is encrypted and stored in the application database.

Requesting a certificate renewal

See below for requesting the renewal of a certificate.

To request the renewal of a certificate

1. Log in as an administrator with one of the following roles.
 - The [<ca>_admin](#) role for the certificate authority that will renew the certificate.
 - A [Certificate Role](#) with request permission for the same certificate authority and selected certificate profile.
2. Go to **Control > Certificates**.
3. In the main grid, click **Select Action > Request Renew** for a certificate.
4. Fill in the following forms of the **Renew** wizard.
 - [General](#)
 - [Destinations](#)
 - [Profile options](#)
 - [Automate Options](#)
5. Click **Create** to create the certificate renewal request.
6. Browse the request status as explained in [Browsing my certificate requests](#) and [Browsing pending requests](#).

General

Configure the following settings in the **General** form of the **Renewal** wizard.

- [Owner](#)
- [Description](#)
- [<custom>](#)
- [Access Tags](#)
- [Certificate Authority](#)
- [Certificate Profile](#)
- [Use a key manager \(KMS\) to generate the key pair](#)

Owner

The email address of the person responsible for the certificate – for example, the Web server operator.

Description

A brief description of the certificate purpose.

<custom>

Business-specific [Custom Fields](#) defined by your organization.

Access Tags

One or several [Certificate Access Tags](#).

 [Certificate Roles](#) with any of these tags will grant permissions on the certificate.


Certificate Authority

The certificate authority that issues the certificate. See [Authorities](#) for how to register certificate authorities.

Certificate Profile

The certificate profile the certificate authority applies to issue the certificate. For certificates to be published in [Destinations](#), consider the following profile limitations.

Destination	Limitations
Apache	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).
Azure	Does not support issuing certificates from a CSR.
Nginx	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).


 The selected certificate profile must be configured in CA Gateway for the Certificate Authority.

Use a key manager (KMS) to generate the key pair

To generate the certificate key pair with a key manager, check this box and select a key manager from the **Key Manager** list.


For the key managers described in [Creating a F5 BIG-IP key manager](#), also configure the settings in the table below.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

 See [Key Managers](#) for creating key managers and techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Destinations


If required by the certificate profile, add one or more [Destinations](#) to publish the issued certificate.

 If you selected a [Key Manager](#), ensure the **Allow private key export** option is enabled on this Key Manager to add additional destinations for this certificate.

To add a destination

1. In the **Destinations** list, select a destination previously created as explained in the following sections.
 - [Creating a HashiCorp Vault destination](#)
 - [Creating a Microsoft IIS web server destination](#)
 - [Creating an Apache web server destination](#)
 - [Creating an AWS Certificate Manager destination](#)
 - [Creating an Azure Key Vault destination](#)
 - [Creating an F5 BIG-IP destination](#)
 - [Creating an Nginx web server destination](#)
 - [Creating an SFTP destination](#)

2. Click **Add** to confirm the selection.


 Apache and Nginx destinations do not support adding several destinations or other key managers.

3. If required, configure destination-specific parameters.
 - [F5 BIG-IP destination-specific settings](#)
 - [Microsoft IIS destination-specific settings](#)

F5 BIG-IP destination-specific settings

Configure the following additional settings when adding a destination of the F5 BIG-IP type.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

 See techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.


Microsoft IIS destination-specific settings

When adding a destination of the Microsoft IIS type, enter one or more site bindings in the **Site bindings** field. Define each binding with a line in the following syntax.

```
<name>;<host>;<port>
```

Where:

- `<name>` is the website name
- `<host>` is the website hostname or IP address
- `<port>` is the port for connecting to the website.

 Select a certificate profile with "Web Server" or dual usage (key encipherment and digital signature) to deploy the certificate successfully.

Profile Options

Configure the following settings in the **Profile Options** form of the **Renewal** wizard.


- [Certificate Signing Request \(CSR\)](#)
- [Password](#)
- [Subject Variable Requirements](#)
- [Subject Alternative Names](#)

Certificate Signing Request (CSR)

The PEM or Base64 encoding of a CSR (Certificate Signing Request).

This field is only present when the selected certificate profile issues certificates from CSR. In this issuance mode:

- The user generates the key pair and the CSR.
- The CA processes the CSR and issues the certificate.
- The user downloads the certificate.

 When selecting Apache, Nginx, or Microsoft IIS certificate destinations, Certificate Manager ignores any client-generated CSR and uses instead a CSR generated at the destination along with the key pair.

Password

A password for the generated P12.

This field is only present when the selected certificate profile issues certificates in P12 files. In this issuance mode:


1. The CA generates the key pair.
2. The user downloads both the certificate and the private key in a P12 file protected with the selected password.

Subject Variable Requirements

Variable values to build:

- The subject's distinguished name for the CSR, if using a Key Manager.
- The expected subject's distinguished name otherwise.

This field is mandatory when required by the selected profile.

 Certificate renewals reuse the value of Subject variables, such as Subject DN, entered at issuance. Thus, the value of these variables is read-only during renewal.

Subject Alternative Names

The list of subject alternative names (SAN) for the certificate.

Renewal

If supported by the selected profile, you can check the **Auto Renewal** box and configure the following settings.


- [Renewal Period](#)
- [PKCS12 Password](#)

Renewal Period

The day the certificate must be renewed, as a number of days before the certificate expiry. For a certificate that expires in E days and a **Renewal Period** set to P, the renewal starts in E-P days. At 12:00 AM UTC every day, a background process collects the certificates that:


- Must be renewed the same day because E-P=0
- Failed a previous renewal because E-P<0

For example, to force a certificate renewal the next day, set a P value equal to E-1 before 12:00 AM UTC. At 12:00 AM UTC, E-P will equal 0, and the certificate will be included in the renewal queue for that day.

 The restrictions imposed by Apache, Nginx, or Microsoft IIS destinations on other issuance modes do not affect automated renewal. Specifically, these destinations support automated renewal with client-side generated keys and CSRs.

PKCS12 Password

The password of the PKCS #12 for delivering the certificate and its private key in the selected **Destinations**.

 This password is encrypted and stored in the application database.

Editing a single certificate

See below for editing the settings of a single certificate.

To edit a single certificate

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority that issued the certificate.
 - A [Certificate Role](#) with permission to edit certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. In the main grid, click **Select Action > Edit** for one of the listed certificates.
4. Update the value of the following editable certificate settings.
 - [Owner](#)
 - [Description](#)
 - [Access Tags](#)
 - [<custom>](#)

Owner

The email address of the person responsible for the certificate – for example, the Web server operator.

Description

A brief description of the certificate purpose.

Access Tags

One or several [Certificate Access Tags](#).

 [Certificate Roles](#) with any of these tags will grant permissions on the certificate.

<custom>


Business-specific [Custom Fields](#) defined by your organization.

Editing certificates in bulk

See below for editing certificate settings in bulk.

To edit certificates in bulk

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority that issued the certificates.
 - A [Certificate Role](#) with permission to edit certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. Click **Bulk Actions**.
4. In the **Select bulk actions** drop-down list, select **Edit**.
5. Configure a filter for the certificates you want to edit. Use the filter options to combine several filters.
6. In the **Select field** drop-down list, select the name of an editable field.
 - [Owner](#)
 - [Description](#)
 - [Access Tags](#)
 - [<custom>](#)
7. In the **Value** drop-down list, type a new value for the selected field.
8. Click **Add**. You can optionally select and add more fields to modify.
9. Click **Save** to add all the certificates matching the filter to the edit background task.

 An [INFO](#) log will indicate the number of updated certificates upon task completion.

Owner

The email address of the person responsible for the certificate – for example, the Web server operator.

Description

A brief description of the certificate purpose.

Access Tags

One or several [Certificate Access Tags](#).

 [Certificate Roles](#) with any of these tags will grant permissions on the certificate.

<custom>

Business-specific [Custom Fields](#) defined by your organization.


Revoking a certificate

See below for revoking the validity of a certificate before the certificate expiration date.

To revoke a certificate

1. Log in as an administrator with one of the following roles:
 - The [global_admin](#) role.

- The `<ca>_admin` role for the certificate authority that issued the certificate.
 - A [Certificate Role](#) with permission to revoke certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
 3. In the main grid, click **Select Action > Revoke** for the certificate.
 4. In the **Revocation Reason** list of the **Revoke** dialog, select the revocation reason.

 ECS Certificate Authorities do not support the **On Hold** revocation reason.


5. In the **Comment** field, add an optional comment on the revocation reason.
6. Click **Save**.

Revoking certificates in bulk

See below for revoking certificates in bulk.


To revoking certificates in bulk

1. Log in as an administrator with one of the following roles.
 - The `global_admin` role.
 - The `<ca>_admin` role for the certificate authority that issued the certificates.
 - A [Certificate Role](#) with permission to revoke certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. Click **Bulk Actions**.
4. In the **Select bulk actions** drop-down list, select **Revoke**.
5. Configure a filter for the certificates you want to edit. Use the filter options to combine several filters.
6. In the **Revocation Reason** drop-down list, select the reason for revoking certificates.
7. In the **Comment** text box, provide a comment for revoking certificates.
8. Click **Save** to add all the certificates matching the filter to the revocation background task.

 An `INFO` log will indicate the number of revoked certificates upon task completion.

Releasing a certificate from hold

See below for releasing a certificate from hold – that is, reenabling a certificate previously revoked with the **Certificate Hold** reason.

 This operation is only available when supported by the issuing CA.

To release a certificate from hold


- Log in as an administrator with one of the following roles:
 - The `global_admin` role.
 - The `<ca>_admin` role for the certificate authority that issued the certificate.
 - A [Certificate Role](#) with permission to unhold certificates for the same certificate authority and certificate profile.
- Go to **Control > Certificates**.
- In the main grid, click **Select Action > Unhold** for the certificate.

Exporting a certificate

See below for exporting a certificate to a file.

To export a certificate

1. Log in as an administrator with either:
 - A `global_admin` role.
 - The `<ca>_admin` role for the certificate authority that issued the certificate.
2. Go to **Control > Certificates**.
3. In the main grid, click **Select Action > Export** for the certificate.
4. In the **Export format** list, select one of the following values.
 - [PEM - Base64 encoded public certificate and private key \(.pem\)](#)
 - [PKCS12 - Encrypted public certificate and private key \(.p12\)](#)
 - [DER - Binary encoded public certificate \(.der\)](#)
5. In the **Export Filename** field, enter a name for the exported file. Certificate Manager provides a default name that you may override.

 Exported files will go to your browser's download directory.


6. Select the elements to include in the generated file.
 - The **Include Public Certificate** checkbox is available for all formats.
 - The **Include Certificate Chain** checkbox is available for PEM and PKCS#12 formats.
 - The **Include Private Key** checkbox is available for PEM and PKCS#12 formats.

PEM - Base64 encoded public certificate and private key (.pem)

Select this format to export the base64 encoding of the public certificate and private key. Run the following command to view the file after exporting.


```
openssl x509 -in cert.pem -text -noout
```

You'll find that the PEM format consists of a set of blocks delimited with BEGIN and END markers.

 PEM files are not encrypted, so you should be cautious when exporting the private key.

PKCS12 - Encrypted public certificate and private key (.p12)

Select this format to export the certificate, the chain, and the private key in PKCS #12 file. When selecting this format, the **Export** dialog displays an additional **Password** field to enter a password for protecting the PCKS #12 contents.

 No password strength rules are applied since some uses require simple or no password.

Run the following command to decrypt and view the file.

```
openssl pkcs12 -in cert.p12 -info
```


DER - Binary encoded public certificate (.der)

Select this format to export a binary DER-encoded file typically used for public certificates, so Certificate Manager limits the options here. Run the following command to view the file contents.

```
openssl x509 -in cert.der -inform der -text -noout
```

Importing certificates

See below for importing certificates from file.

 Importing PKCS#12 files is not supported.

To import certificates

1. Log in as an administrator with one of the following roles:
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority that issued the certificates.
 - A [Certificate Role](#) with permissions to import certificates.
2. Go to **Control > Certificates**.
3. Click the **Import** button to configure the following settings.
 - [Owner](#)
 - [Description](#)
 - [Certificate\(s\)](#)
 - [<custom>](#)
 - [Access Tags](#)
4. Click **Import** to confirm the certificate import.

 The import will fail if any of the certificates already exist in Certificate Manager.

Owner


The email address of the person responsible for the certificate – for example, the Web server operator.

Description

A brief description of the certificate purpose.


Certificate(s)

Click **Select Files** to import public certificate files in PEM, DER, or base64 encoding.

 Any file may include the certificate chain in the same file.

<custom>

Business-specific [Custom Fields](#) defined by your organization.

 When importing many certificate files, the selected custom fields will apply to all the imported certificates.

Access Tags

One or several [Certificate Access Tags](#).

 [Certificate Roles](#) with any of these tags will grant permissions on the certificate.

Archiving certificates

See below for archiving a certificate.

i Once archived, Certificate Manager will omit the certificate from the [Browsing certificates](#) results and the generated [Reports](#). See [Restoring archived certificates](#) for how to unarchive certificates.

To archive a certificate

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority that issued the certificates.
 - A [Certificate Role](#) with permissions to archive certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. In the main grid, click **Select Action > Archive** for the certificate.
4. Click **Save** in the confirmation dialog.

Archiving certificates in bulk

See below for archiving certificates in bulk.

To archive certificates in bulk

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority that issued the certificates.
 - A [Certificate Role](#) with permission to archive certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. Click **Bulk Actions**.
4. In the **Select bulk actions** drop-down list, select **Archive**.
5. Configure a filter for the certificates you want to edit. Use the filter options to combine several filters.
6. Click **Save** to add all the certificates matching the filter to the archiving background task.

i An **INFO** log will indicate the number of archived certificates upon task completion.

Certificate History

Browse the actions performed on certificates, and optionally restore archived certificates.

- [Browsing the certificate history](#)
- [Restoring archived certificates](#)

Browsing the certificate history

See below for browsing the actions performed on the managed certificates.

To browse the certificate history

1. Go to **Control > Certificate History**.
2. Click **Show Insights** at the top-right to display detailed charts on the certificate history.
3. Define grid views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.

- Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. For each action log, check the following parameters in the certificate history grid.
- [Logged At](#)
 - [Certificate Name](#)
 - [Username](#)
 - [Action](#)

Logged At

The time and date of the logged operation.

Certificate Name

The certificate identifier. This value concatenates the following certificate fields:

- Common Name
- Issuer
- Valid from
- Valid to

When another certificate has the same name, the certificate serial number is appended to make the name unique.

Username

The name of the administrator that performed the operation.

Action

The logged certificate action:

- Created
- Destination Error
- Edited
- Revoked
- Deleted
- Held
- Unheld
- Archived
- Restored
- Source Sync
- Discovered
- Imported

Restoring archived certificates

See below for restoring certificates previously archived as explained in [Archiving certificates](#).



Once restored, Certificate Manager will include the certificates in the [Browsing certificates](#) results and the generated [Reports](#).

To restore archived certificates

1. Log in as an administrator with either:
 - The [global_admin](#) role.

- The `<ca>_admin` role for the certificate authority that issued the certificate.
2. Go to **Control > Certificate History**.
 3. Select one or several logs with the **Action** column set to **Archive**.
 4. Click **Restore** to restore the certificates.

Domains

Register the domains for which the certificate authorities are authorized to issue EV (Extended validation) or OV (Organization Validation) SSL/TLS certificates.

- [Browsing domains](#)
- [Registering a domain](#)
- [Checking a domain status](#)
- [Re-verifying a domain](#)

Browsing domains

See below for browsing domains.

To browse domains

1. Log in as an administrator with either:
 - The `global_admin` role.
 - The `<ca>_admin` role for the certificate authority that issues the domain certificates.
2. Go to **Control > Domains**.
3. Define domain views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the `<column>` column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.

 When filtering domains, the menu in the **Authority** column allows filtering by single certificate authority only.

4. Check the domain settings described in the following sections.
 - [Domain](#)
 - [Authority](#)
 - [Owner](#)
 - [Next step](#)
 - [OV Eligible](#)
 - [OV Expiry](#)
 - [EV Eligible](#)
 - [EV Expiry](#)
 - [Verification status](#)
 - [Verification method](#)
 - [Last Updated On](#)
 - [DNS Token](#)
 - [Record Domain](#)
 - [Record Type](#)

- [Web Server Token](#)
- [Web Server URL](#)
- [Email](#)

Domain


The domain name.

Authority

The certificate authority that will verify the domain.

Owner



The username of the domain owner.

 The user who adds the domain is automatically made the owner. You can later edit this field and assign ownership to someone else.


Next step

The next step for verifying the domain.



OV Eligible

 if the domain certificates can be OV certificates;  otherwise.


OV Expiry

The expiration date for the OV-issued certificates, when **OV Eligible** is .

EV Eligible

 if the domain certificates can be EV certificates;  otherwise.

EV Expiry

The expiration date for the EV-issued certificates, when **EV Eligible** is .

Verification status

The status of the domain verification process.

Verification method

The method for verifying the domain.

Method	Description
Email	Send a confirmation email to one of the following: the email address listed on the DNS Server's TXT, the email address listed on the CAA record, the contacts on the WHOIS record who authorize issuing certificates for the domain.

Method	Description
DNS	Generate a random value that you must post to your domain DNS record. Once detected, your domain is validated.
Manual	Require some action on the administrator's part to prove domain ownership or control. Site administrators will be contacted to explain the different domain validation options. We recommend using self-service domain verification methods because this option may result in delays.
Web	Generate a random value you must post on a server hosting web content for the domain in question. Once detected, your domain is validated.

Last Updated On

The date of the last domain verification.

DNS Token

The DNS token, when **Verification Method** is **DNS**.

Record Domain

The record for verifying the domain (if any).

Record Type

The type of **Record Domain**.

Web Server Token

The web server token, when **Verification Method** is **Web Server**.

Web Server URL

The web server token, when **Verification Method** is **Web Server**.

Email

The email address to be used when the **Verification Method** is **Email**. You can:

- Select an email address in the DNS record.
- Select an email address in the WHOIS record.
- Select a standard CA/Browser forum address.
- Enter the email address manually.

Registering a domain

See below for registering a domain. Once registered, Certificate Manager can issue certificates for the domain.

To register a domain

1. Log in as an administrator with either:
 - The `global_admin` role.
 - The `<ca>_admin` role for the certificate authority that issues the domain certificates.


2. Go to **Control > Domains**.
3. Click **Register** to configure the following settings.
 - [Domain](#)
 - [Owner](#)
 - [Authority](#)
 - [Verification method](#)
 - [Email](#)
4. Follow the instructions in the **Next Step** column.

Domain

The domain name.

Owner

The username of the domain owner.

 The user who adds the domain is automatically made the owner. You can later edit this field and assign ownership to someone else.

Authority

The certificate authority that will verify the domain.

Verification method

The method for verifying the domain.

Method	Description
Email	Send a confirmation email to one of the following: the email address listed on the DNS Server's TXT, the email address listed on the CAA record, the contacts on the WHOIS record who authorize issuing certificates for the domain.
DNS	Generate a random value that you must post to your domain DNS record. Once detected, your domain is validated.
Manual	Require some action on the administrator's part to prove domain ownership or control. Site administrators will be contacted to explain the different domain validation options. We recommend using self-service domain verification methods because this option may result in delays.
Web	Generate a random value you must post on a server hosting web content for the domain in question. Once detected, your domain is validated.

Email

The email address to be used when the **Verification Method** is **Email**. You can:

- Select an email address in the DNS record.
- Select an email address in the WHOIS record.

- Select a standard CA/Browser forum address.
- Enter the email address manually.

Checking a domain status

See below for checking the status of a domain.

To check the status of a domain

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - The [<ca>_admin](#) role for the certificate authority that issues the domain certificates.
2. Go to **Control > Domains**.
3. Select a domain.
4. Click **Check Status** to update the following domain information,
 - [Next step](#)
 - [OV Eligible](#)
 - [EV Eligible](#)
 - [Verification status](#)
 - [Last Updated On](#)

Next step

The next step for verifying the domain.

OV Eligible

✓ if the domain certificates can be OV certificates; ✗ otherwise.

EV Eligible

✓ if the domain certificates can be EV certificates; ✗ otherwise.

Verification status

The status of the domain verification process.

Last Updated On

The date of the last domain verification.

Re-verifying a domain

See below for running new verifications on an existing domain.

To re-verify a domain

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Control > Domains**.
3. Select a domain.
4. Click **Re-Verify**.
5. Configure the following settings.
 - [Domain](#)
 - [Authority](#)
 - [Verification method](#)
 - [Email](#)
6. Submit the domain re-verify request.
7. Follow the instructions in the **Next Step** column.

Domain

The domain name.

Authority

The certificate authority that will verify the domain.

Verification method

The method for verifying the domain.

Method	Description
Email	Send a confirmation email to one of the following: the email address listed on the DNS Server's TXT, the email address listed on the CAA record, the contacts on the WHOIS record who authorize issuing certificates for the domain.
DNS	Generate a random value that you must post to your domain DNS record. Once detected, your domain is validated.
Manual	Require some action on the administrator's part to prove domain ownership or control. Site administrators will be contacted to explain the different domain validation options. We recommend using self-service domain verification methods because this option may result in delays.
Web	Generate a random value you must post on a server hosting web content for the domain in question. Once detected, your domain is validated.

Email

The email address to be used when the **Verification Method** is **Email**. You can:

- Select an email address in the DNS record.
- Select an email address in the WHOIS record.
- Select a standard CA/Browser forum address.
- Enter the email address manually.

Automate

With the Certificate Manager automation capabilities, you can automate the integration of certificate sources and destinations. Click **Automate** in the sidebar and select the following options.

- [Launch](#)
- [Sources](#)
- [Destinations](#)
- [Rules and Actions](#)

Launch

Go to **Automate > Launch** to view the control insights page. You can:

- Click the corresponding link to browse:
 - [Sources](#)
 - [Destinations](#)
 - [Rules and Actions](#)
- Click the tags under **Related Topics** to learn about different topics.

Sources

A source is a connection for Certificate Manager to obtain certificates. Certificate Manager calls each source periodically to obtain new certificates and update the state of existing certificates known by the source. Currently, each source is called every 30 minutes.

- [Browsing sources](#)
- [Creating a source](#)
- [Editing a source](#)
- [Deleting sources](#)

✖ If a source did not fetch certificates from a source due to an incorrect start date for synchronization, delete the source and create a new source with a correct start date.

Certificate Manager associates the obtained certificates with known certificate authorities.

- For certificates associated with a certificate authority, Certificate Manager administrators can take action through the certificate authority connections.
- For certificates not issued by a known certificate authority, Certificate Manager administrators cannot take action, but Certificate Manager can still perform notification and reporting functions.

ℹ When removing a source, Certificate Manager preserves all certificates synchronized by the source.

Browsing sources

See below for browsing the sources added to Certificate Manager.

To browse sources

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to browse sources.
2. Go to **Automate > Sources**.
3. Click **Show Insights** at the top-right to display the number of sources for each plugin.
4. Define source views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
5. For each source in the main grid, browse the following settings.
 - [Label](#)
 - [Description](#)
 - [Plugin](#)

- [Associated Certificates](#)
- [Last Run](#)
- [Owner](#)
- [Authorization Tags](#)

Label

A descriptive name of the source.

Description

A description of the source purpose.

Plugin

The plugin for connecting with the source.

Associated Certificates


The number of certificates obtained via the source. Click this value to browse these certificates on the [Certificates](#) page.

Last Run

The date of the last connection with the source.

Owner

The username of the source owner. The user who creates the source is automatically made the owner of both the source and the source certificates.

 You can later edit this field and assign ownership to someone else.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Creating a source

See below for adding a certificate source to Certificate Manager.

- [Creating a F5 BIG-IP source](#)
- [Creating an Azure Key Vault source](#)
- [Creating a CA Gateway source](#)

Creating a F5 BIG-IP source

See below for creating a source that imports certificates from an F5 BIG-IP certificate management service.

To create a F5 BIG-IP source

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create sources.
2. Go to **Automate > Sources**.
3. Click **Create** to configure the following settings.
 - [Label](#)
 - [Owner](#)

- [Description](#)
- [Authorization Tags](#)
- [Select Source Type](#)
- [Host](#)
- [Port](#)
- [Partition/Path](#)
- [Username](#)
- [Password](#)
- [Host CA Bundle \(PEM\)](#)
- [Enable hostname verification](#)

4. Click **Verify** for Certificate Manager to verify all the settings. Some plugins might ask for additional configuration settings after verification.


Label

A descriptive name of the source.

Mandatory: Yes

Owner

The username of the source owner. The user who creates the source is automatically made the owner of both the source and the source certificates.

 You can later edit this field and assign ownership to someone else.

Description

A description of the source purpose.

Mandatory: No

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Mandatory: No

Select Source Type

Select **Azure-KeyVault-Source-Plugin**.

Mandatory: Yes

Host


The URL of the F5 BIG-IP server host. For example:

`https://f5.entrust.com`

Mandatory: Yes

Port

The port for accessing the F5 BIG-IP service.

 The default F5 BIG-IP port is 443.

Mandatory: Yes


Partition/Path

The partition and path, in the following syntax


`<partition>/<path>`

Where:

- `<partition>` is the name of a F5 BIG-IP server partition.

 The user must have access to this partition.


- `<path>` is the path of a subdirectory within the partition.

 Both values are case sensitive.

Mandatory: Yes

Username

The username for authenticating in the F5 BIG-IP server.

 The selected user must have an administrator role for the given partition in the F5 BIG-IP server.

Mandatory: Yes

Password

The password for authenticating to the F5 BIG-IP server.

Mandatory: Yes

Host CA Bundle (PEM)

The certification chain of the F5 BIG-IP server, as a bundle in PEM format.


Mandatory: Yes

Enable hostname verification

Check this box for validating the F5 BIG-IP server certificate in each connection.

Creating an Azure Key Vault source

See below for creating a source that imports your Azure Key Vault certificates.

 This source is only available when installing the corresponding plugin.

To create an Azure Key Vault source

1. Log in as an administrator with either:

- The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create sources.
2. Go to **Automate > Sources**.
 3. Click **Create** to configure the following settings.
 - [Label](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
 - [Select Source Type](#)
 - [Key Vault URL](#)
 - [Client ID](#)
 - [Client Secret](#)
 - [Tenant ID](#)
 4. Click **Verify** for Certificate Manager to verify all the settings. Some plugins might ask for additional configuration settings after verification.


Label

A descriptive name of the source.

Mandatory: Yes

Owner

The username of the source owner. The user who creates the source is automatically made the owner of both the source and the source certificates.

 You can later edit this field and assign ownership to someone else.

Description

A description of the source purpose.

Mandatory: No

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Mandatory: No

Select Source Type

Select **Azure-KeyVault-Source-Plugin**.

Mandatory: Yes

Key Vault URL


The URL of the Azure Vault.

Mandatory: Yes

Client ID

The Application ID displayed on the Azure portal. See the following guide to register an application, create a new application secret and configure access policies on Azure key vault resource.

<https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

 The Azure Key Vault plugin needs the following certificate permissions: create, update, get, list, import, and delete.

Mandatory: Yes

Client Secret

The Application API Key generated in the Azure portal.

Mandatory: Yes


Tenant ID

The Tenant ID displayed in the Azure portal.

Mandatory: Yes

Creating a CA Gateway source

See below for creating a source that connects Certificate Manager with the CAs managed by an Entrust CA Gateway instance.

 If the CA you want to connect is an Entrust Certificate Authority initialized in a pre-8.4.10 release, please run the backfill script before creating the source to correct any missing or incorrect certificate event.

To create a CA Gateway source

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [user_defined](#) role with permission to create sources.
2. Go to **Automate > Sources**.
3. Click **Create** to configure the following settings.
 - [Label](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
 - [Select Source Type](#)
 - [CA Gateway URL](#)
 - [Verify server certificate](#)
 - [Required PKCS#12 File](#)
 - [Required PKCS#12 Password](#)
 - [Optional PKCS#12 Truststore File](#)
 - [Optional Truststore Password](#)
4. Click **Verify** for Certificate Manager to verify all the settings. Some plugins might ask for additional configuration settings after verification.


Label

A descriptive name of the source.

Mandatory: Yes

Owner

The username of the source owner. The user who creates the source is automatically made the owner of both the source and the source certificates.

 You can later edit this field and assign ownership to someone else.

Description

A description of the source purpose.

Mandatory: No

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Mandatory: No


Select Source Type

Select **CAGW-Source-Plugin**.

Mandatory: Yes

CA Gateway URL

The URL of the CA Gateway host.

 For Entrust Managed PKI systems, your Entrust contact will provide the URL.

Mandatory: Yes

Verify server certificate

Check this box to verify the CA Gateway server certificate.

Required PKCS#12 File

The PKCS#12 file containing the keys and the certificate that Certificate Manager must present to the CA Gateway instance for accessing the CAs. This PKCS#12 file is either:

- Generated when configuring your CA Gateway instance,
- Provided by Entrust for API access to your Entrust Managed PKI service.

Mandatory: Yes

Required PKCS#12 Password

The password of the PKCS#12 file.

Mandatory: Yes

Optional PKCS#12 Truststore File

A truststore that will override the built-in truststore when using a private CA.

Mandatory: No

Optional Truststore Password

The password of the optional PKCS#12 truststore.

Mandatory: When selecting an **Optional PKCS#12 Truststore File**.

Editing a source

See below for editing the settings of a source.

To edit a source

1. Log in as an administrator with either.
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to edit sources.
2. Go to **Automate > Sources**.
3. In the main grid, select one of the sources.
4. Click **Edit** to update the source settings already described in [Creating a source](#).
 - [Creating a F5 BIG-IP source](#)
 - [Creating an Azure Key Vault source](#)
 - [Creating a CA Gateway source](#)
5. Click **Verify** to check the connection with the source.

Deleting sources

See below for removing sources from Certificate Manager.

To delete sources

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to delete sources.
2. Go to **Automate > Sources**.
3. In the main grid, select one or more sources.
4. Click **Delete** to remove the selected sources from Certificate Manager.

Destinations

A destination is a connection for Certificate Manager to push certificates to services, servers, or devices (on issuance and renewal). Certificate Manager pushes the created certificates:

- Immediately (manual mode).
- On a calendar based on predefined renewal periods (automated mode).

Certificate Manager is always responsible for initiating the actions that push certs to destinations.

- [Browsing destinations](#)
- [Creating a destination](#)
- [Editing a destination](#)
- [Deleting destinations](#)

Browsing destinations

See below for browsing the destinations created in Certificate Manager.

To browse destinations

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to browse destinations.
2. Go to **Automate > Destinations**.
3. Define destination views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.

- Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. For each destination in the main grid, browse the following settings.
- [ID](#)
 - [Label](#)
 - [Description](#)
 - [Plugin](#)
 - [Associated Certificates](#)
 - [Owner](#)
 - [Authorization Tags](#)

ID

A destination identifier for automation with the API.

Label

A descriptive name of the destination.

Description

A description of the destination purpose.

Plugin

The plugin for connecting to the destination.

Associated Certificates

The number of certificates sent to the destination. Click this value to browse these certificates on the [Certificates](#) page.

Owner

The username of the destination owner.



The user who adds the destination is automatically made the owner. You can later edit this field and assign ownership to someone else.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Creating a destination


See below for creating destinations where to push certificates.

- [Creating a HashiCorp Vault destination](#)
- [Creating a Microsoft IIS web server destination](#)
- [Creating an Apache web server destination](#)
- [Creating an AWS Certificate Manager destination](#)

- [Creating an Azure Key Vault destination](#)
- [Creating an F5 BIG-IP destination](#)
- [Creating an Nginx web server destination](#)
- [Creating an SFTP destination](#)

Creating a HashiCorp Vault destination

Create this destination to store the issued certificates on HashiCorp Vault.

 HashiCorp Vault is a tool to manage secrets and encryption keys securely.

To create a Hashicorp Vault destination in Certificate Manager


1. Log in as an administrator with one of the following roles:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create destinations.
2. Go to **Automate > Destinations**.
3. Click **Create** to configure the following settings.
 - [Label](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
 - [Select Destination Type](#)
 - [Vault URL](#)
 - [Vault SSL CA Bundle \(PEM\)](#)
 - [Vault KV API Version](#)
 - [Authentication Method](#)
 - [Token](#)
 - [Vault Mount](#)
 - [Vault Path](#)
 - [Object Name](#)
 - [Bundle Chain](#)
 - [SAN Filter](#)
4. Click **Verify** to check the connection with the destination.

Label

A descriptive name of the destination.

Owner

The username of the destination owner.

 The user who adds the destination is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the destination purpose.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Select Destination Type

Select the following value.

Hashicorp-Vault-Destination-Plugin

Vault URL

The URL of the vault instance.

Vault SSL CA Bundle (PEM)

The certification chain of the Vault's SSL certificate, as a bundle in PEM format.

Vault KV API Version

The version of the Vault KV mount point.

Authentication Method

The authentication method. Only the token method is supported.

Token

A Vault authentication token with "Vault Mount" write privileges.

Vault Mount

The path of the Vault KV secrets engine. For example, a certificate with this distinguished name:

"C=CA,S=Ontario,L=Kanata,O=Entrust,OU=Sales,CN=vaultcert"

Is stored with the corresponding private key in this path:

dev/vaultcert/Sales/Entrust/Ontario/Kanata/CA/
vaultcert_Sales_Entrust_Ontario_Kanata_CA

When setting the following configuration.

Setting	Value
Vault Mount	dev
Vault Path	"{CN}/{OU}/{O}/{S}/{L}/{C}"
Object Name	"{CN}{OU}{O}{S}{L}_{C}"

Vault Path

A template for generating certificate paths from the following fields of the certificate distinguished names: CN, OU, O, S, L, C.

Object Name

A template for generating certificate entries from the following fields of the certificate distinguished names: CN, OU, O, S, L, C.

Bundle Chain

The storage format for the private key, the certificate, and the certificate chain. See below for a description of each supported format.

Nginx

```
crt: <certificate> + "\n" + <cert_chain>
key: <private_key>
```

Apache

```
crt: <certificate>
chain: <cert_chain>
key: <private_key>
```

PEM

```
pem: <certificate>+ "\n" + <cert_chain> + "\n" + <private_key>
```

No chain


```
crt: <certificate>
key: <private_key>
```

SAN Filter

A regular expression to filter out certificates by subject alternative name (SAN). Certificate Manager will discard a certificate when the certificate SAN does not match this regular expression.

Creating a Microsoft IIS web server destination

Create this destination to install the issued certificates as the server TLS certificate of a Microsoft IIS web server.

 On certificate issuance, Certificate Manager ignores any user-provided CSR and uses instead a CSR generated at the destination along with the key pair.

To create a Microsoft IIS web server destination in Certificate Manager

1. Configure a Microsoft IIS web server as explained in [Microsoft IIS web server prerequisites](#).
2. Log into Certificate Manager as an administrator with one of the following roles:
 - The [global_admin](#) role.

- A `<user_defined>` role with permission to create destinations.
3. Go to **Automate > Destinations**.
 4. Click **Create** and set the [Microsoft IIS web destination settings](#).
 5. Click **Verify** to check the connection with the destination.


Microsoft IIS web server prerequisites

Perform the following operations in the Microsoft IIS web server.

- [Checking basic authentication support](#)
- [Configuring HTTPS for WinRM](#)

Checking basic authentication support

Ensure the Microsoft Windows Remote Management WinRM service supports basic authentication, which is the only authentication the IIS plugin for Certificate Manager supports.

 Future releases will support other authentication methods.

To check if the WinRM service supports basic authentication

1. Launch PowerShell in the Microsoft Windows server.
2. Run the following command.

```
winrm get winrm/config/client/auth
```

3. Check the command output includes the "Basic = true" line. For example:

```
Auth
  Basic = true
  Digest = true
  Kerberos = true
  Negotiate = true
  Certificate = true
  CredSSP = false
```

Configuring HTTPS for WinRM


Run the following command to check if HTTPS is enabled for the WinRM (Windows Remote Management) protocol.

```
winrm get winrm/config/Listener?Address=*&Transport=HTTPS
```

If the command raises an error, configure HTTPS for WinRM as explained below.

To configure HTTPS for WinRM

1. Issue a certificate for WinRM.

 Self-signed certificates will work for testing purposes but will fail certificate validation.

2. Launch PowerShell in the Microsoft Windows server.
3. Import a `.pfx` or PKCS#12 file containing the issued new certificate, the certificate chain, and the private key for WinRM. For example:

```
Import-PfxCertificate -FilePath "C:\Path\To\winrm.pfx" -CertStoreLocation Cert:
\LocalMachine\My
```

4. Delete the existing configuration, if any.

```
winrm delete winrm/config/Listener?Address=**Transport=HTTPS
```

5. Set the WinRM new certificate. For example:

```
winrm create winrm/config/Listener?Address=**Transport=HTTPS
'@{Hostname="examplehost";
CertificateThumbprint="d6013136de9f9d18244ac3bca392ce206d57fe38"}'
```

Microsoft IIS web destination settings

In the Certificate Manager web console, configure the following settings of a Microsoft IIS web server destination.


- [Label](#)
- [Owner](#)
- [Description](#)
- [Authorization Tags](#)
- [Select Destination Type](#)
- [Host](#)
- [User](#)
- [Password](#)
- [Validate Windows Remote Management \(WinRM\) Certificate](#)
- [CA Certificate](#)

Label

A descriptive name of the destination.

Owner

The username of the destination owner.

 The user who adds the destination is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the destination purpose.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Select Destination Type

Select the following value.

IIS-Server-Plugin

Host

The hostname or IP address of the Microsoft IIS web server.

User

The name of a user with permission to use the Microsoft IIS web server.

Password

The password of the selected user.

Validate Windows Remote Management (WinRM) Certificate

Check this box to validate the certificate of the Windows Remote Management (WinRM) service, Certificate Manager will use this service to install the issued certificate.

CA Certificate

The PEM encoding of the CA certificate chain for validating the WinRM certificate. This value is only mandatory when checking the **Validate Windows Remote Management (WinRM) Certificate** box.

Creating an Apache web server destination

Create this destination to install the issued certificates as the server TLS certificate of an Apache web server. Note that:

- On certificate issuance, Certificate Manager ignores any user-provided CSR and uses instead a CSR generated at the destination along with the key pair.
- On renewal, the operating system timestamp may remain the same, but the contents of the certificate are always updated.

See below for how to create an Apache web server destination.

To create an Apache web server destination in Certificate Manager

1. If not already installed, install Python 3.9 or newer on the Nginx web server.
2. Log in as an administrator with one of the following roles:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create destinations.
3. Go to **Automate > Destinations**.
4. Click **Create** to configure the following settings.
 - [Label](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
 - [Select Destination Type](#)
 - [Host](#)
 - [User](#)
 - [Password](#)
 - [Private Key File](#)
 - [Private Key Password](#)
 - [Certificate Destination](#)
 - [Is sudo access required?](#)

- [Sudo password](#)
- [Restart the Apache web server](#)


5. Click **Verify** to check the connection with the destination.
6. Check the fingerprint of the host key displayed after the verification.
7. If you trust the key, click **Create** to confirm the destination creation.

Label

A descriptive name of the destination.

Owner

The username of the destination owner.

 The user who adds the destination is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the destination purpose.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Select Destination Type

Select the following value.

Apache-Webserver-Plugin

Host

The hostname or IP address of the machine hosting the web server.

User

The username for opening an SSH session in the machine hosting the web server.

Password

The user password for opening an SSH session in the machine hosting the web server. Skip this optional parameter if the user will authenticate with a private key.

Private Key File

Click **Select File** to import a keystore containing the user's private key. Skip this optional parameter if the user will authenticate with a password.

Private Key Password

The password of the keystore containing the user's private key. Skip this optional parameter if the user will authenticate with a password.

Certificate Destination

The path of the certificate and the key in the machine hosting the Apache web server, Select **default** to publish the certificate and the key in the following default paths.

OS	Certificate path	Key path
Debian	/etc/ssl/certs/localhost.crt	/etc/ssl/private/localhost.key
Redhat	/etc/pki/tls/certs/localhost.crt	/etc/pki/tls/private/localhost.key.

Select **customized** to set the certificate and key path in the following fields.


- Destination Certificate Path
- Destination Key Path

Is sudo access required?

Check this box if pushing the certificate and the key in the destination requires `sudo` access.


Sudo password

The password of a user with `sudo` permission. Skip this field if **Is sudo access required?** is not checked,

 This password is typically the SSH password of the user selected in the **User** field.


Restart the Apache web server

Whether to restart the web server after pushing the certificate and the key. If you select **Yes**, enter the TLS port of the host machine in the additional **HTTPS Port** field.

 The standard TLS port is 443.

Creating an AWS Certificate Manager destination

Create this destination to store the issued certificates on the AWS Certificate Manager (ACM).

 This destination is only available when installing the corresponding plugin.

To create an AWS Certificate Manager destination

1. Configure an AWS IAM service as explained in [AWS Certificate Manager prerequisites](#).
2. Log into Certificate Manager as an administrator with one of the following roles:
 - The `global_admin` role.
 - A `<user_defined>` role with permission to create destinations.
3. Go to **Automate > Destinations**.
4. Click **Create** and set the [AWS Certificate Manager destination settings](#).
5. Click **Verify** to check the connection with the destination.

AWS Certificate Manager prerequisites

In the AWS IAM service, use `AWSCertificateManagerFullAccess` from [AWS-managed policies](#) or create a customer-managed policy with at least the following permissions.

- GetCertificate

- ImportCertificate
- RenewCertificate
- ListCertificates.
- AddTagsToCertificate

AWS Certificate Manager destination settings

In the Certificate Manager web console, configure the following settings of an AWS Certificate Manager destination.


- [Label](#)
- [Owner](#)
- [Description](#)
- [Authorization Tags](#)
- [Select Destination Type](#)
- [Region](#)
- [Access Key ID](#)
- [Secret Key](#)

Label

A descriptive name of the destination.

Owner

The username of the destination owner.

 The user who adds the destination is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the destination purpose.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Select Destination Type

Select the following value.

azure-destination-plugin

Region

The AWS region,

Access Key ID

The identifier of the AWS IAM access key.

Secret Key

The identifier of the AWS IAM secret key.

Creating an Azure Key Vault destination

Create this destination to store the issued certificates on Azure Key Vault.

i Azure Key Vault is a cloud service offered by Microsoft for securely storing and accessing secrets such as API keys, passwords, certificates, and cryptographic keys.

To create an Azure Key Vault destination

1. Configure an Azure Key Vault as explained in [Azure Key Vault prerequisites](#).
2. Log into Certificate Manager as an administrator with one of the following roles:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create destinations.
3. Go to **Automate > Destinations**.
4. Click **Create** and set the [Azure Key Vault destination settings](#).
5. Click **Verify** to check the connection with the destination.

Azure Key Vault prerequisites

In the Azure Key Vault, register an application and create a new application secret as explained in

<https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

Configure an access policy with backup, delete, get, list, create, and update permissions. For example, run:

```
az keyvault set-policy --name azure-key-vault-dest --spn $AZURE_CLIENT_ID --  
certificate-permissions backup delete get list create update
```

Azure Key Vault destination settings

In the Certificate Manager web console, configure the following settings of an Azure Key Vault destination.

- [Label](#)
- [Owner](#)
- [Description](#)
- [Authorization Tags](#)
- [Select Destination Type](#)
- [Key Vault URL](#)
- [Client ID](#)
- [Client Secret](#)
- [Tenant ID](#)
- [Certificate Name](#)

Label

A descriptive name of the destination.

Owner

The username of the destination owner.

i The user who adds the destination is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the destination purpose.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Select Destination Type

Select the following value.

azure-destination-plugin

Key Vault URL

The URL of the Azure Vault.

Client ID

The Application ID generated when creating the destination in Azure Vault.

Client Secret

The Application API Key generated when Creating a destination in Azure.

Tenant ID


The Tenant ID generated when Creating a destination in Azure.

Certificate Name

The certificate name in the destination (as an alphanumeric string).

Creating an F5 BIG-IP destination

Create this destination to store the issued certificates on F5 BIG-IP.

 BIG-IP by F5 provides a secure vault to store passwords and passphrases.

To create a BIG-IP destination in Certificate Manager

1. Log in as an administrator with one of the following roles:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create destinations.
2. Go to **Automate > Destinations**.
3. Click **Create** to configure the following settings.
 - [Label](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
 - [Select Destination Type](#)
 - [Host](#)
 - [Port](#)
 - [Partition/Path](#)
 - [Username](#)
 - [Password](#)
 - [Host CA Bundle \(PEM\)](#)

- [Enable hostname verification](#)


4. Click **Verify** to check the connection with the destination.

Label

A descriptive name of the destination.

Owner

The username of the destination owner.

 The user who adds the destination is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the destination purpose.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Select Destination Type

Select the following value.

F5-BIG-IP-Destination-Plugin

Host

The URL of the F5 BIG-IP server host. For example:

https://f5.entrust.com

Mandatory: Yes

Port

The port for accessing the F5 BIG-IP service.

 The default F5 BIG-IP port is 443.

Mandatory: Yes


Partition/Path

The partition and path, in the following syntax


<partition>/<path>

Where:

- **<partition>** is the name of a F5 BIG-IP server partition.

 The user must have access to this partition.

- `<path>` is the path of a subdirectory within the partition.

 Both values are case sensitive.

Mandatory: Yes

Username

The username for authenticating in the F5 BIG-IP server.

 The selected user must have an administrator role for the given partition in the F5 BIG-IP server.

Mandatory: Yes

Password

The password for authenticating to the F5 BIG-IP server.

Mandatory: Yes

Host CA Bundle (PEM)

The certification chain of the F5 BIG-IP server, as a bundle in PEM format.

Mandatory: Yes

Enable hostname verification

Check this box for validating the F5 BIG-IP server certificate in each connection.

Creating an Nginx web server destination

Create this destination to install the issued certificates as the server TLS certificate of an Nginx web server. Note that:

- On certificate issuance, Certificate Manager ignores any user-provided CSR and uses instead a CSR generated at the destination along with the key pair.
- On renewal, the operating system timestamp may remain the same, but the contents of the certificate are always updated.

See below for how to create an Nginx web server destination.

To create an Nginx web server destination in Certificate Manager

1. If not already installed, install Python 3.9 or newer on the Nginx web server.
2. Log in as an administrator with one of the following roles:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create destinations.
3. Go to **Automate > Destinations**.
4. Click **Create** to configure the following settings.
 - [Label](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
 - [Select Destination Type](#)

- [Host](#)
- [User](#)
- [Password](#)
- [Private Key File](#)
- [Private Key Password](#)
- [Certificate Destination](#)
- [Is sudo access required?](#)
- [Sudo password](#)
- [Restart the Nginx web server](#)

5. Click **Verify** to check the connection with the destination.
6. Check the fingerprint of the host key displayed after the verification.
7. If you trust the key, click **Create** to confirm the destination creation.

Label

A descriptive name of the destination.

Owner

The username of the destination owner.



The user who adds the destination is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the destination purpose.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Select Destination Type

Select the following value.

Nginx-Webserver-Plugin

Host

The hostname or IP address of the machine hosting the web server.

User

The username for opening an SSH session in the machine hosting the web server.

Password

The user password for opening an SSH session in the machine hosting the web server. Skip this optional parameter if the user will authenticate with a private key.

Private Key File

Click **Select File** to import a keystore containing the user's private key. Skip this optional parameter if the user will authenticate with a password.

Private Key Password

The password of the keystore containing the user's private key. Skip this optional parameter if the user will authenticate with a password.

Certificate Destination

The path of the certificate and the key in the machine hosting the Nginx web server, Select **default** to publish the certificate and the key in the following default paths.

OS	Certificate path	Key path
Debian	/etc/ssl/certs/nginx.crt	/etc/ssl/private/nginx.key.
Redhat	/etc/pki/tls/certs/nginx.crt	/etc/pki/tls/private/nginx.key

Select **customized** to set the certificate and key path in the following fields.


- Destination Certificate Path
- Destination Key Path

Is sudo access required?

Check this box if pushing the certificate and the key in the destination requires `sudo` access.


Sudo password

The password of a user with `sudo` permission. Skip this field if **Is sudo access required?** is not checked,

 This password is typically the SSH password of the user selected in the **User** field.


Restart the Nginx web server

Whether to restart the web server after pushing the certificate and the key. If you select **Yes**, enter the TLS port of the host machine in the additional **HTTPS Port** field.

 The standard TLS port is 443.

Creating an SFTP destination

Create this destination to post the issued certificates using the SFTP protocol.

 SFTP destinations are a general-purpose way to deploy certificates and private keys to servers supporting the SFTP protocol, such as servers running the sshd process.

To create an SFTP destination in Certificate Manager

1. Log in as an administrator with one of the following roles:
 - The `global_admin` role.
 - A `<user_defined>` role with permission to create destinations.
2. Go to **Automate > Destinations**.
3. Click **Create** to configure the following settings.
 - `Label`

- [Owner](#)
- [Description](#)
- [Authorization Tags](#)
- [Select Destination Type](#)
- [Host](#)
- [Port](#)
- [User](#)
- [Password](#)
- [Private Key File](#)
- [Private Key Password](#)
- [Destination Path](#)
- [Export Format](#)
- [Export Separate Chain](#)

4. Click **Verify** to check the connection with the destination.

Label

A descriptive name of the destination.

Owner

The username of the destination owner.



The user who adds the destination is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the destination purpose.

Authorization Tags

A list of authorization tags. The [Custom Roles](#) with any of these tags will grant permissions on the source.

Select Destination Type

Select the following value.

SFTP-Destination-Plugin

Host

The hostname or IP of the destination server.

Port

The server port for SFTP.

User

The name of the SFTP user.

Password

The password of the SFTP user.

 Certificate Manager will use the password if you provide a value for both **Password** and **Private Key File**.

Private Key File

The PEM file containing the private key for SFTP authentication. Click **Choose Files** to import this file.

 Certificate Manager will use the password if you provide a value for both **Password** and **Private Key File**.

Private Key Password

The password of the private key for SFTP authentication.

Destination Path

The server directory path where Certificate Manager will push the certificates and keys. For each certificate with the `<cn>` common name, a `<cn>` subdirectory will include:

- The certificate
- The private key
- The certificate chain.

Existing files will be overwritten.

 The paths in these subdirectories do not support aliases.

Export Format

The format of the files containing the certificates and keys.

- PEM
- PKCS #12

Export Separate Chain

When **Export Format** is **PEM**:

- Check this checkbox for saving the certificate chain in a separate PEM file
- Uncheck this checkbox (default value) to save the certificate chain in the same PEM file containing the key and the certificate.

When **Export Format** is **P12**, the generated PKCS #12 file always contains the certificate chain.

Editing a destination

See below for editing the settings of a destination.

To edit a destination

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to edit destinations.
2. Go to **Automate > Destinations**.
3. In the main grid, select one of the destinations.
4. Click **Edit** to update the settings already described in [Creating a destination](#).
 - [Creating a HashiCorp Vault destination](#)
 - [Creating a Microsoft IIS web server destination](#)

- [Creating an Apache web server destination](#)
- [Creating an AWS Certificate Manager destination](#)
- [Creating an Azure Key Vault destination](#)
- [Creating an F5 BIG-IP destination](#)
- [Creating an Nginx web server destination](#)
- [Creating an SFTP destination](#)

5. Click **Verify** to check the connection with the destination.

Deleting destinations

See below for removing destinations from Certificate Manager.

To delete destinations

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to delete destinations.
2. Go to **Automate > Destinations**.
3. In the main grid, select one or more destinations.
4. Click **Delete** to remove the selected destinations from Certificate Manager.

Rules and Actions

For certificates about to expire and not yet renewed using Certificate Manager, the following default rules will send an email notification 30, 15, and 2 days before the expiration date.

- Default 30 Day Certificate Expiry Notification to Certificate Owner
- Default 15 Day Certificate Expiry Notification to Certificate Owner
- Default 2 Day Certificate Expiry Notification to Certificate Owner

See the following sections for how to create and manage additional rules.

- [Browsing rules](#)
- [Creating a rule](#)
- [Editing a rule](#)
- [Deleting rules and actions](#)

Browsing rules

See below for browsing rules

To browse rules

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - A [<ca>_admin](#) role.
 - A [<user_defined>](#) role with permission to view rules.
2. Go to **Automate > Rules & Actions**.
3. Define rule views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.

- Click the refresh icon to rerun the query with the current filters.
4. For each rule in the main grid, browse the following settings.
- [Name](#)
 - [Description](#)
 - [Rule Type](#)
 - [Owner](#)
 - [Authorization Tags](#)

Name

The rule name.

Description

A description of the rule purpose.


Rule Type

The type of event triggering the rule.

- Administration Event
- Certificate Automated Renewal Failure
- Certificate Automated Renewal Success
- Certificate Expiry

Owner

The username of the rule owner. The user who creates the rule is automatically made the owner.

 The user who creates the rule is automatically made the owner. You can later edit this field and assign ownership to someone else.

Authorization Tags

A list of authorization tags. A [<user_defined>](#) role with any of these tags will grant permissions on the source.

Creating a rule

See below for creating a rule.

To create a rule

1. Log in as an administrator with one of the following roles:
 - The [global_admin](#) role.
 - A [<ca>_admin](#) role.
 - A [<user_defined>](#) role with permission to create rules.
2. Go to **Automate > Rules & Actions**.
3. Click **Create** to configure the following settings.
 - [Name](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
 - [Notify When](#)
 - [Action](#)
 - [Email Source](#)


Name

The rule name.

Mandatory: Yes

Owner

The username of the rule owner. The user who creates the rule is automatically made the owner.

 The user who creates the rule is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the rule purpose.

Mandatory: No

Authorization Tags

A list of authorization tags. A `<user_defined>` role with any of these tags will grant permissions on the source.

Mandatory: Yes

Notify When

The type of event triggering the rule.

- Administration Event
- Certificate Automated Renewal Failure
- Certificate Automated Renewal Success
- Certificate Expiry

Mandatory: Yes

Action

The triggered action.

 Currently, only **Email Notification** is supported.

Email Source

The email addresses of the notification recipients.

Address Source	Email addresses
Address Book	The email addresses selected in the static Address Book of Certificate Manager.
Address Book entry in Custom Field	All the email addresses in an address book set as Custom Field.

Address Source	Email addresses
Email in Custom Field	The email address in a Custom Field.
Certificate Owner	The email address configured in the Owner field of the certificate.

Mandatory: Yes

Editing a rule

See below for editing the settings of a rule.

To edit a rule

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to edit destinations.
2. Go to **Automate > Rule & Actions**.
3. In the main grid, select one of the rules.
4. Click **Edit** to update the following settings.
 - [Name](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
 - [Email Source](#)

Name

The rule name.

Mandatory: Yes

Owner

The username of the rule owner. The user who creates the rule is automatically made the owner.

i The user who creates the rule is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the rule purpose.

Mandatory: No

Authorization Tags

A list of authorization tags. A [<user_defined>](#) role with any of these tags will grant permissions on the source.

Mandatory: No

Email Source

The email addresses of the notification recipients.

Address Source	Email addresses
Address Book	The email addresses selected in the static Address Book of Certificate Manager.
Address Book entry in Custom Field	All the email addresses in an address book set as Custom Field.
Email in Custom Field	The email address in a Custom Field.
Certificate Owner	The email address configured in the Owner field of the certificate.

Mandatory: Yes

Deleting rules and actions

See below for deleting rules and actions.

To delete rules and actions

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to delete destinations.
2. Go to **Automate > Rules & Actions**.
3. In the main grid, select one or more rules.
4. Click **Delete** to remove the selected rules.

Report

Certificate Manager includes extensive reporting capabilities optimized for the automated production and dissemination of management notifications and reports. Click **Report** in the sidebar and select the following options.

- [Launch](#)
- [Designer](#)
- [Report Schedules](#)
- [History](#)

Launch

Go to **Report > Launch** to view the control insights page. You can:

- Click the corresponding link to manage:
 - The report [Designer](#)
 - [The Report Schedules](#)
 - [The report History](#)
- Click the tags under **Related Topics** to learn about different topics.

Designer

You can design the reports Certificate Manager periodically generates with updated information on the managed certificates. Report design and scheduling are separated to use one design for multiple reports.

- [Browsing reports](#)
- [Creating a report](#)
- [Editing a report](#)
- [Designing a report](#)
- [Updating a report design](#)
- [Deleting reports](#)

Browsing reports

See below for browsing reports.

To browse reports

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [Custom Role](#) with permission to view reports.
2. Go to **Report > Designer**.
3. Define report views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. For each report in the main grid, browse the following settings.
 - [Report Name](#)
 - [Description](#)
 - [Schedules](#)
 - [Next Scheduled Run](#)
 - [Owner](#)
 - [Authorization Tags](#)
 - [Actions](#)

Report Name

The name of the report.

- Reports with the "This is a system report" mouseover text are predefined reports visible for all users – for example, in the [Dashboard \(widget\)](#).
- Reports with the "This is a public report" mouseover text have been created by an administrator, as explained in [Creating a report](#).

Description

A description of the report.

Schedules


The number of scheduled generations for the report. Click this number to browse these schedules on the [Report Schedules](#) page.

Next Scheduled Run

The name and date of the next programmed [Report Schedule](#) for the report.

Owner

The username of the report owner. The user who creates the report is automatically made the owner. The report owner can always view, edit, or delete the report.

 You can later edit this field and assign ownership to someone else.

Authorization Tags

The optional authorization tags for managing the report. Authorization tags are defined as part of a [<user_defined>](#) role and selected here to give explicit control over a report. Users possessing a role referencing the same tag can use, edit, or delete this report. These permissions are in addition to any users with roles enabling them to view, edit, or delete reports globally.

Actions

The actions supported by the report. Select:

- **Design** for [Designing a report](#)
- **Manage Schedules** for managing the [report Schedules](#) for this report.

Creating a report

See below for creating a report.

To create a report

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [Custom Role](#) with permission to create reports.
2. Go to **Report > Designer**.
3. Click **Create** to configure the following settings.
 - [Report Name](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)


Report Name

The name of the report.

Mandatory: Yes

Owner

The username of the report owner. The user who creates the report is automatically made the owner. The report owner can always view, edit, or delete the report.

 You can later edit this field and assign ownership to someone else.

Description

A description of the report.

Mandatory: No

Authorization Tags

The optional authorization tags for managing the report. Authorization tags are defined as part of a [<user_defined>](#) role and selected here to give explicit control over a report. Users possessing a role referencing the same tag can use, edit, or delete this report. These permissions are in addition to any users with roles enabling them to view, edit, or delete reports globally.

Mandatory: No

Editing a report

See below for editing the settings of a report.

To edit a report

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [Custom Role](#) with permission to edit reports.
2. Go to **Report > Designer**.
3. In the main grid, select one of the reports.
4. Click **Edit** to update the following settings.
 - [Report Name](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)


Report Name

The name of the report.

Mandatory: Yes

Owner

The username of the report owner. The user who creates the report is automatically made the owner. The report owner can always view, edit, or delete the report.

 You can later edit this field and assign ownership to someone else.

Description

A description of the report.

Mandatory: No

Authorization Tags

The optional authorization tags for managing the report. Authorization tags are defined as part of a [<user_defined>](#) role and selected here to give explicit control over a report. Users possessing a role referencing the same tag can use, edit, or delete this report. These permissions are in addition to any users with roles enabling them to view, edit, or delete reports globally.

Mandatory: No

Designing a report


See below for designing a report.

To design a report

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create reports.
2. Click **Report > Designer**.
3. In the main grid, click **Select Action > Design** for the report.
4. Configure the report as already explained in [Browsing certificates](#).
5. Click **Update** to save the report design.
6. Click **Preview > <format>** to download a report preview in the [<format>](#) file format.
7. Configure the report schedule, as explained in [Report Schedules](#).
8. Configure the report branding, as explained in [reports](#).

Updating a report design

See below for updating the design of a report

 Certificate Manager automatically updates the report design when modifying or deleting [Custom Fields](#). However, you must verify the performed changes and fix any inconsistencies. Otherwise, the generated reports may not contain the expected data, or the report generation can fail.

To update a report design


1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to create reports.
2. Go to **Report > Designer**.
3. In the report entry, click **Select Action > Design**. If the report design includes modified Custom Fields, a warning message will ask you to review the automatic changes.
4. Check or modify the following settings.
 - [Name](#)
 - [Owner](#)
 - [Description](#)
 - [Authorization Tags](#)
5. Click **Update**.

Name

The name of the report schedule.

Owner

The username of the report owner. The user who creates the report is automatically made the owner. The report owner can always view, edit, or delete the report.

 You can later edit this field and assign ownership to someone else.

Description


A description of the report.

Authorization Tags

The optional authorization tags for managing the report. Authorization tags are defined as part of a [<user_defined>](#) role and selected here to give explicit control over a report. Users possessing a role referencing the same tag can use, edit, or delete this report. These permissions are in addition to any users with roles enabling them to view, edit, or delete reports globally.

Deleting reports

See below for deleting reports.

 Certificate Manager will display an error message when deleting a report displayed in the dashboard [Dashboard](#).

To delete reports

1. Log in as an administrator with one of the following roles.
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to delete reports.
2. Go to **Report > Designer**.
3. In the main grid, select one or more reports.
4. Click **Delete** to remove the selected reports.

Report Schedules

See the following sections for how to manage generation schedules for each report.

- [Browsing report schedules](#)
- [Creating a report schedule](#)
- [Editing a report schedule](#)
- [Deleting report schedules](#)

Browsing report schedules

See below for browsing report schedules.

To browse report schedules

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to view reports.
2. Go to **Report > Report Schedules**.
3. Define report schedule views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.

- Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. For each report schedule in the main grid, browse the following settings.
- [Report name](#)
 - [Schedule Name](#)
 - [Description](#)
 - [Recipients](#)
 - [Schedule End](#)
 - [Next Run](#)
 - [Enabled](#)
 - [Owner](#)

Report name

The name of the scheduled report. See [Designer](#) for how to manage reports.

Schedule Name

The name of the report schedule.

Description

A brief description of the report schedule.

Recipients

The email addresses of the report recipients.

Schedule End

The end date for the report generation and sending.

Next Run

The date for the next report generation.

Enabled

✔ if the report schedule is active; ✖ otherwise.

Owner

The username of the report schedule owner.



The user who creates the report schedule is automatically made the owner. You can later edit this field and assign ownership to someone else.

Creating a report schedule

See below for creating report schedules.

To create a report schedule

1. Log in as an administrator with either:
 - The [global_admin](#) role.

- A [<user_defined>](#) role with permission to create reports.
- 2. Go to **Report > Report Schedules**.
- 3. Click **Create** to configure the following settings.
 - [Enabled](#)
 - [Associated Report](#)
 - [Name](#)
 - [Description](#)
 - [Report Format](#)
 - [Send report only when there are records](#)
 - [Effective End Date](#)
 - [Repeat](#)
 - [Recipients](#)

Enabled

Check this box to enable report generation; uncheck otherwise.

Associated Report

The report you want to schedule. See [Designer](#) for how to manage reports.

Mandatory: Yes

Name

The name of the report schedule.

Mandatory: Yes

Description

A brief description of the report schedule.

Report Format

The file format for the generated report :

- CSV
- PDF
- Microsoft Excel
- Microsoft Word

Mandatory: Yes

Send report only when there are records

Check this box to send reports only when not empty.

Effective End Date

The end date for the report generation and sending.

Mandatory: No. This optional value defaults to **Never Expire**.


Repeat

The frequency for report generation and sending.

Mandatory: Yes

Recipients

The email addresses of the report recipients. The email selection dialog includes all the addresses in the [Address Book](#).

 If a recipient changes his email address in the [Address Book](#) after creating the report, edit the report and select the new email address. The **Edit** dialog warns of these changes displaying the old addresses of the recipients you must reselect.

Mandatory: Yes

Editing a report schedule

See below for editing the settings of a report schedule.

To edit a report schedule

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to edit reports.
2. Go to **Report > Report Schedules**.
3. In the main grid, select one of the report schedules.
4. Click **Edit** to update the following settings.
 - [Enabled](#)
 - [Name](#)
 - [Description](#)
 - [Report Format](#)
 - [Send report only when there are records](#)
 - [Effective End Date](#)
 - [Repeat](#)
 - [Recipients](#)

Enabled

Check this box to enable report generation; uncheck otherwise.

Name

The name of the report schedule.

Mandatory: Yes

Description

A brief description of the report schedule.

Mandatory: No

Report Format

The file format for the generated report :

- CSV
- PDF
- Microsoft Excel
- Microsoft Word

Mandatory: Yes

Send report only when there are records

Check this box to send reports only when not empty.

Effective End Date

The end date for the report generation and sending.

Mandatory: No. This optional value defaults to **Never Expire**.

Repeat

The frequency for report generation and sending.

Mandatory: Yes

Recipients

The email addresses of the report recipients. The email selection dialog includes all the addresses in the [Address Book](#).



If a recipient changes his email address in the [Address Book](#) after creating the report, edit the report and select the new email address. The **Edit** dialog warns of these changes displaying the old addresses of the recipients you must reselect.

Mandatory: Yes

Deleting report schedules

See below for deleting report schedules.

To delete report schedules

1. Log in as an administrator with either:
 - The [global_admin](#) role.
 - A [<user_defined>](#) role with permission to delete reports.
2. Go to **Report > Report Schedules**.
3. In the main grid, select one or more report schedules.
4. Click **Delete** to remove the selected report schedules.

History

See below for how to manage the reports generated for each report design.

- [Browsing generated reports](#)
- [Deleting generated reports](#)
- [Downloading generated reports](#)

Browsing generated reports

See below for how to browse the reports generated for each report design.

To browse generated reports

1. Go to **Report > History**.
2. Define generated report views.
 - Unfold the **Columns** list to select the properties you want to display as columns.

- Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
3. For each report design, check the following settings.
- [Report name](#)
 - [Description](#)
 - [Total generated](#)

Report name

The name provided when creating the report as explained in [Creating a report](#).

Description

The description provided when creating the report as explained in [Creating a report](#).


Total generated

The number of reports generated for the report design. See [Report Schedules](#) for how to schedule report generation.

Deleting generated reports

See below for how to delete reports generated for a report design.


To delete generated reports

1. Go to **Report > History**.
2. Click the plus button  for a report design.
3. Select one or more generated reports and click **Delete** to delete them.

Downloading generated reports

See below for how to download reports generated for a report design.

To download generated reports

1. Go to **Report > History**.
2. Click the plus button  for a report design.
3. Click **Download** to download a report generated for the design.

Administer

Certificate Manager provides extensive user and credential management capabilities. Click **Administer** in the sidebar and select the following options.

- [Launch](#)
- [Administrators](#)
- [Address Book](#)
- [Audit Log](#)
- [API Tokens](#)
- [Certificate Access Tags](#)

- [Roles](#)
- [Settings](#)

Launch

Go to **Administer > Launch** to display the administration insights page. On this page, you can:

- Click the different page links to manage the following entities.
 - [Administrators](#)
 - [Address Book](#)
 - [Audit Log](#)
 - [API Tokens](#)
 - [Certificate Access Tags](#)
 - [Roles](#)
 - [Settings](#)
- Click the tags under **Related Topics** to learn about different topics.

Administrators

See the following sections for how to register and manage Certificate Manager administrators.

- [Browsing administrators](#)
- [Creating an administrator](#)
- [Editing an administrator](#)
- [Deleting administrators](#)



Administrators are the only users allowed to access the Certificate Manager Web browser interface.

As explained in [Settings](#), Certificate Manager administrators can also register via an IdP. Initially, these users will have the following settings.

Setting	Value
Name	The name of the administrator.
Email	The email that will uniquely identify the administrator in the IdP-initiated logins.
Active	Yes
Roles	An empty list of roles. An administrator with the global_admin must add the required roles.

Browsing administrators

See below for browsing the Certificate Manager administrators.

To browse Certificate Manager administrators

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Administer > Administrators**.

3. Select **Show Insights** at the top-right and click **View Accounts** for each predefined filter:
 - New Accounts
 - Deactivated Accounts
 - Idle Accounts.
4. Define grid views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
5. For each administrator in the grid, browse the following settings.
 - [Username](#)
 - [Email](#)
 - [Active](#)
 - [Roles](#)
 - [Account Profile](#)

Username

The unique identifier of the Certificate Manager administrator.

Email

The email address of the Certificate Manager administrator. This address

- Will uniquely identify the administrator in the IdP-initiated logins.
- Is automatically added to the [Address Book](#) when creating the administrator.

Active

✔ if the Certificate Manager administrator is enabled; ✖ otherwise.

Roles

The list of [Roles](#) granted to the Certificate Manager administrator.

Account Profile

Click **View Profile** in the administrators grid to display details on an administrator profile.

- The number of managed [CA Gateways](#).
- The number of managed [Authorities](#).
- The total number of issued [Certificates](#), including details on the number of certificates expiring in 7 days and the number of scheduled renewals.
- The time and date of the last login.
- The granted [Roles](#).
- The managed [Certificate Access Tags](#).
- The number of managed [Discovery Agents](#).
- The number of requested workflows.

Use the **Change User** list to display details of another profile without returning to the administrators grid.

Creating an administrator

See below for creating a Certificate Manager administrator.

To create a Certificate Manager administrator

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Administer > Administrators**.
3. Click **Create**.
4. Configure the following settings.
 - [Username](#)
 - [Email](#)
 - [Password](#)
 - [Confirm Password](#)
 - [Password Strength](#)
 - [Require New Password](#)
 - [Roles](#)

Username

The unique identifier of the Certificate Manager administrator.

Mandatory: Yes

Email

The email address of the Certificate Manager administrator. This address

- Will uniquely identify the administrator in the IdP-initiated logins.
- Is automatically added to the [Address Book](#) when creating the administrator.

Mandatory: Yes

Password

The password of the Certificate Manager administrator. This password:

- Must have a strength level of 3 or 4.
- Can be later modified by the registered administrator.

Mandatory: Yes


Confirm Password

Retype the Certificate Manager administrator password.

Mandatory: Yes

Password Strength

The strength of the typed password.

 The administrator creation will fail unless this field displays a green line to confirm the password strength.

Require New Password

Check this box for the Certificate Manager administrator to change the password at the next login. See in [Internal password](#) how to force a password change for all administrators.

Roles

The list of [Roles](#) granted to the Certificate Manager administrator.

Mandatory: No

Editing an administrator

See below for editing the settings of a Certificate Manager administrator.

To edit a Certificate Manager administrator

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Administer** > **Administrators**.
3. In the main grid, select one of the administrators.
4. Click **Edit** to update the following settings.
 - [Active](#)
 - [Username](#)
 - [Email](#)
 - [Password](#)
 - [Confirm Password](#)
 - [Password Strength](#)
 - [Require New Password](#)
 - [Roles](#)

Active

Check this box to enable the Certificate Manager administrator; uncheck otherwise.

Username

The unique identifier of the Certificate Manager administrator.

Mandatory: Yes

Email

The email address of the Certificate Manager administrator. This address

- Will uniquely identify the administrator in the IdP-initiated logins.
- Is automatically added to the [Address Book](#) when creating the administrator.

Mandatory: Yes

Password

The password of the Certificate Manager administrator. This password:

- Must have a strength level of 3 or 4.
- Can be later modified by the registered administrator.

Mandatory: Yes


Confirm Password

Retype the Certificate Manager administrator password.

Mandatory: Yes

Password Strength

The strength of the typed password.

 The administrator creation will fail unless this field displays a green line to confirm the password strength.

Require New Password

Check this box for the Certificate Manager administrator to change the password at the next login. See in [Internal password](#) how to force a password change for all administrators.

Roles

The list of [Roles](#) granted to the Certificate Manager administrator.

Deleting administrators

See below for deleting Certificate Manager administrators.

To delete Certificate Manager administrators

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Administer > Administrators**.
3. In the main grid, select one or more administrators.
4. Click **Delete** to remove the selected administrators.

Address Book

The address book contains:

- The addresses of the [Administrators](#).
- Manually-added addresses.

These addresses are available when defining [Rules and Actions](#).

- [Browsing the address book](#)
- [Creating an address](#)
- [Importing addresses](#)
- [Editing an address](#)
- [Deleting addresses](#)

Browsing the address book

See below for browsing the Certificate Manager address book.

To browse the address book

1. Go to **Administer > Address Book**.
2. Define address book views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.

- Click the refresh icon to rerun the query with the current filters.
3. For each address book, browse the following settings.
- [Name](#)
 - [Description](#)
 - [Address](#)
 - [Address Type](#)

Name

The name of the address holder.

Description

A description of the address holder.

Address

One of several email addresses, depending on the **Address Type**.

 Email addresses of the **Administrator Address** type cannot be edited or deleted.

Address Type

The type of address.

Address Type	Contents
Single Address	A single email address.
List of Addresses	A list of email addresses.
Administrator Address	The email address automatically added when creating the Administrator.

Creating an address

See below for adding an address to the Certificate Manager address book.

To create an address

1. Go to **Administer > Address Book**.
2. Click **Create** to configure the following settings.
 - [Name](#)
 - [Description](#)
 - [Address Type](#)

Name

The name of the address holder.

Mandatory: Yes

Description

A description of the address holder.

Mandatory: No

Address Type

The type of address. Select:

- **Single Address** to enter a single email address in the **Address** field.
- **List of Addresses** to select multiple addresses in the address book.

Mandatory: Yes

Importing addresses

See below for importing addresses into the Certificate Manager address book.

To import addresses

1. Go to **Administer > Address Book**.
2. Click **Import**,
3. In the **Address Type** list, select one of the following values.
 - [Single Address](#)
 - [List of Addresses](#)
4. Click **Select Files** and select the CSV file containing the addresses.
5. Review the data displayed in the **Import** dialog.
6. Click **Submit**.

Single Address

Import one or multiple addresses from a CSV (Comma Separated File) file. Each line in this file must match the following format.

```
<name>, <description>, <address>
```

Where:

- `<name>` is the name of the address holder.
- `<description>` is the description of the address holder.
- `<address>` is a single address.

For example:

```
Anna Smith, ABC Security Officer, anna.smith@abc.com  
John Doe, ABC Administrator, john.doe@abc.com
```

List of Addresses

Import one or multiple addresses from a CSV (Comma Separated File) file. Each line in this file must match the following format.

```
<name>, <description>, <addresses>
```


Where:

- `<name>` is the name of the address holder.
- `<description>` is the description of the address holder.
- `<addresses>` is either a single address or a list of addresses separated by semicolons (";").

For example:

```
Anna Smith, ABC Security Officer, anna.smith@abc.com  
John Doe, ABC Administrator, john.doe@abc.com; jdoe@abcom; admin@abc.com
```

Editing an address

See below for editing an address.

To edit an address

1. Go to **Administer > Address Book**.
2. In the main grid, select one of the addresses.
3. Click **Edit** to update the following settings.
 - [Name](#)
 - [Description](#)
 - [Address](#)

Name

The name of the address holder.

Description

A description of the address holder.


Address

One of several email addresses, depending on the **Address Type**.

 Email addresses of the **Administrator Address** type cannot be edited or deleted.

Deleting addresses

See below for deleting addresses.

 Email addresses of the **Administrator Address** type cannot be deleted.

To delete addresses

1. Go to **Administer > Address Book**.
2. In the main grid, select one or more addresses.
3. Click **Delete** to delete the selected addresses.

Audit Log

Audit the actions performed in Certificate Manager.

To audit logs

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Administer > Audit Log**.
3. Define log views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. On the main grid, check the following log details.
 - **Performed By:** The identifier of the user or internal component that performed the event.
 - **Logged At:** The event time and date.
 - **Logs:** A summary description of the event.
 - **Audit Code:** The internal code of the audit log. See below for the supported values.
 - [Administration logs](#)
 - [Authentication and authorization logs](#)
 - [Automation logs](#)
 - [Certificate logs](#)
 - [Certificate policy logs](#)
 - [Control logs](#)
 - [Destination logs](#)
 - [Public form logs](#)
 - [Source logs](#)

Administration logs

The following logs record administration events.

Audit Code	Log
AUDIT_1114	Events retention period set to <code><retention_period></code> days
AUDIT_1115	Reports settings updated. Retention period: <code><retention_period></code> , Copyright text <code><copyright_text></code>
AUDIT_1116	Plugin <code><plugin_name></code> updated. State set to <code><plugin_active_state></code>
AUDIT_1117	Public Enrollment Forms <code><general_setting_enabled/disabled></code>

Audit Code	Log
AUDIT_1119	Address <code><address_name></code> updated
AUDIT_1120	Single address created: <code><address_name></code>
AUDIT_1121	Mapped address created: <code><address_name></code>
AUDIT_1122	List of addresses created: <code><address_name></code>
AUDIT_1124	Address deleted: <code><address_name></code>
AUDIT_1125	Address <code><address_name></code> removed from rules
AUDIT_1126	Address <code><address_name></code> removed from schedules
AUDIT_1127	New addresses imported in list of address <code><address_name></code>
AUDIT_1128	Imported single address <code><address_name></code>
AUDIT_1129	Imported list of addresses <code><address_name></code>
AUDIT_1168	License with order number: <code><order_number></code> , Revision number: <code><revision_number></code> uploaded
AUDIT_1169	License with order number: <code><order_number></code> , Revision number: <code><revision_number></code> updated.
AUDIT_1170	Entitlement usage updated for <code><consumption_type></code> . Usage count: <code><usage_count></code>

Authentication and authorization logs

The following logs record authentication and authorization events.

Audit Code	Log
AUDIT_1010	Auth provider <auth_provider_name> registered
AUDIT_1011	Auth provider <auth_provider_name> updated
AUDIT_1012	LDAP login failed for user: <username>
AUDIT_1013	LDAP login failed as user: <username> is not in the required group: <auth_provider_registration_group_name> , dn: <email>
AUDIT_1017	API token created for user <username>
AUDIT_1018	API token deleted for user <username>
AUDIT_1023	Roles updated for user <username>
AUDIT_1030	API token deleted for user <username>
AUDIT_1031	API token updated for user <username>
AUDIT_1032	All API tokens deleted for user <username>
AUDIT_1033	All API tokens deactivated for user <username>
AUDIT_1036	Created initial user with username: <username> .
AUDIT_1037	Created user with username: <username> .
AUDIT_1039	Created LDAP user with username: <username> .
AUDIT_1040	Created external user username: <username> .
AUDIT_1041	Deleted user: <username> .

Audit Code	Log
AUDIT_1042	Updated user: <code><username></code> .
AUDIT_1043	Updated LDAP user: <code><username></code> .
AUDIT_1044	Updated external user: <code><username></code> .
AUDIT_1046	Updated account password for user: <code><username></code> .
AUDIT_1047	Updated last login for user: <code><username></code> .
AUDIT_1048	Successful login by User: <code><username></code> .
AUDIT_1057	Failed login attempt for user: <code><username></code>
AUDIT_1058	Failed login attempt for user: <code><username></code>
AUDIT_1059	Maximum login attempts exceeded. Rejected login attempt for user: <code><username></code>
AUDIT_1060	Login denied. Tenant id not found for user <code><username></code>
AUDIT_1061	Global role created: <code><role_name></code>
AUDIT_1062	Custom role created: <code><role_name></code>
AUDIT_1063	Custom role updated: <code><role_name></code>
AUDIT_1064	Authority role created: <code><role_name></code>
AUDIT_1065	Composite role created: <code><role_name></code>
AUDIT_1066	Role deleted: <code><role_name></code>
AUDIT_1067	Role updated: <code><role_name></code>

Audit Code	Log
AUDIT_1068	Role <code><role_name></code> assigned to user <code><username></code> .
AUDIT_1069	Role <code><role_name></code> unassigned from user <code><username></code> .
AUDIT_1070	Certificate role created: <code><role_name></code>
AUDIT_1071	Certificate role updated: <code><role_name></code>
AUDIT_1092	Failed login attempt for user: <code><username></code> . User is not active.
AUDIT_1093	Failed login attempt. User does not exist.

Automation logs

The following logs record rule and report events.

Audit Code	Log
AUDIT_1201	<code><rule_type></code> Rule created: <code><rule_name></code>
AUDIT_1205	<code><rule_type></code> Rule updated: <code><rule_name></code>
AUDIT_1209	<code><rule_type></code> Rule deleted: <code><rule_name></code>
AUDIT_1250	Generated certificate report: <code><rule_name></code>
AUDIT_1251	Created report: <code><rule_name></code>
AUDIT_1252	Updated report: <code><rule_name></code>
AUDIT_1253	Deleted report: <code><rule_name></code>
AUDIT_1254	Report Schedule <code><schedule_name></code> deleted

Audit Code	Log
AUDIT_1255	Report Schedule <code><schedule_name></code> created for report <code><rule_name></code>
AUDIT_1256	Report Schedule <code><schedule_name></code> updated
AUDIT_1257	Delete report execution at <code><executed_at></code> for report <code><rule_name></code>
AUDIT_1258	Successfully renewed certificate <code><cert_name></code> (Serial Number: <code><cert_sn></code>)

Certificate logs

The following logs record certificate events.

Audit Code	Log
AUDIT_1434	Certificate <code><cert_name></code> (Serial Number: <code><cert_sn></code>) archived
AUDIT_1435	Certificate <code><cert_name></code> (Serial Number: <code><cert_sn></code>) unarchived
AUDIT_1436	Certificate <code><cert_name></code> (Serial Number: <code><cert_sn></code>) revoked
AUDIT_1437	Certificate <code><cert_name></code> (Serial Number: <code><cert_sn></code>) released from hold
AUDIT_1472	Custom Field created: <code><custom_field_name></code> .
AUDIT_1473	Custom Field deleted: <code><custom_field_name></code> .
AUDIT_1474	Custom Field updated: <code><custom_field_name></code> .
AUDIT_1480	Certificate exported: Common Name <code><cert_name></code> , Serial Number <code><decimal_cert_sn></code> , export type: <code><export_type></code>

Audit Code	Log
AUDIT_1491	<number_of_updated_certs> certificates queued for bulk update.
AUDIT_1492	New certificate issued by authority: <authority_name> . (Common Name: <cert_name> , Serial Number: <cert_sn >)
AUDIT_1493	Certificate <cert_name> (Serial Number: <cert_sn >) updated
AUDIT_1494	Certificate <cert_name> (Serial Number: <decimal_cert_sn >) imported
AUDIT_1498	Certificate view <view_name> created.
AUDIT_1499	Certificate view <view_name> updated.
AUDIT_1500	Certificate view <view_name> deleted.

Certificate policy logs

The following logs record Access Tags events.

Audit Code	Log
AUDIT_1481	Certificate Access Tag <access_tag_name> created.
AUDIT_1482	Certificate Access Tag <access_tag_name> updated.
AUDIT_1483	Certificate Access Tag <access_tag_name> deleted.

Control logs

The following logs record events on authorities, key managers, and discovery scanners.

Audit Code	Log
AUDIT_1301	CA Gateway added: <cagw_name>

Audit Code	Log
AUDIT_1302	CA Gateway updated: <cagw_name>
AUDIT_1303	CA Gateway deleted: <cagw_name>
AUDIT_1304	Authority added: <auth_name>
AUDIT_1305	Authority updated: <auth_name>
AUDIT_1306	Authority deleted: <auth_name>
AUDIT_1371	Successfully uploaded certificate with Private key Id: <priv_key_id> and Public key Id: <pub_key_id> to KMS using plugin: <plugin_name>
AUDIT_1375	Key pair deactivated at Key Manager <plugin_name> , Private key id: <priv_key_id> , Public key id: <pub_key_id>
AUDIT_1376	Verification request submitted for domain <domain_name> to authority <auth_name>
AUDIT_1377	Key manager with plugin <plugin_name> created: <key_manager_name>
AUDIT_1378	Key manager updated: <key_manager_name>
AUDIT_1379	Key manager deleted: <key_manager_name>
AUDIT_1382	Status updated for domain <Domain name> from authority <auth_name>
AUDIT_1383	Re-verify request submitted for domain <domain_name> to authority <auth_name>
AUDIT_1384	Discovery scanner added: <disco_agent_name>

Audit Code	Log
AUDIT_1385	Discovery scanner updated: <disco_agent_name>
AUDIT_1386	Discovery scanner deleted: <disco_agent_name>
AUDIT_1387	<num_of_disco_agent_scans> Scan configurations updated for discovery scanner <disco_agent_name>
AUDIT_1388	Discovery scanner <disco_agent_name> policy updated, new polling frequency: <disco_agent_poll_freq> seconds

Destination logs

The following logs record destination events.

Audit Code	Log
AUDIT_1495	Destination <dest_name> created.
AUDIT_1496	Destination <dest_name> updated.
AUDIT_1497	Destination <dest_name> deleted.

Public form logs

The following logs record Public Enrollment Form events.

Audit Code	Log
AUDIT_1504	Public form <pub_form_name> created.
AUDIT_1505	Public form <pub_form_name> updated.
AUDIT_1506	Public form <pub_form_name> deleted.
AUDIT_1507	Certificate request (ID: <cert_request_id>) of requester <requester> (IP: <remote_ip>) is rejected.

Audit Code	Log
AUDIT_1508	Certificate request (ID: <cert_request_id>) of requester <requester> (IP: <remote_ip>) is approved.
AUDIT_1509	Certificate request (ID: <cert_request_id>) of requester <requester> (IP: <remote_ip>) is already approved.
AUDIT_1510	Certificate request (ID: <cert_request_id>) of requester <requester> (IP: <remote_ip>) is already rejected.
AUDIT_1511	Error rejecting certificate request (ID: <cert_request_id>) of requester <requester> (IP: <remote_ip>).
AUDIT_1512	Error approving certificate request (ID: <cert_request_id>) of requester <requester> (IP: <remote_ip>).
AUDIT_1513	New Certificate request created.
AUDIT_1514	Certificate request (ID: <cert_request_id>) of requester <requester> (IP: <remote_ip>) is cancelled.
AUDIT_1515	New Certificate request created with key algorithm <key_alg>, key size <Key size> (IP: <remote_ip>)
AUDIT_1516	New Certificate request created key algorithm <key_alg>, (IP: <remote_ip>)
AUDIT_1517	New Certificate request created with key algorithm <key_alg>, OID <pub_key_info_alg> (IP: <remote_ip>).
AUDIT_1518	Deleted <num_cert_requests_deleted> certificate requests last modified <cert_request_retention> days ago.
AUDIT_1519	Certificate request (ID: <cert_request_id>) of requester <requester> (IP: <remote_ip>) with CA side key generation (profile: <profile_id>) is marked approved.

Audit Code	Log
AUDIT_1520	Certificate request (ID: <cert_request_id>) of requester <requester> (IP: <remote_ip>) is already issued.
AUDIT_1521	Pkcs12 for Certificate Request (ID: <cert_request_id>) of requester <requester> (IP: <remote_ip>) with CA side key generation (profile: <profile_id>) is issued.

Source logs

The following logs record source events.

Audit Code	Log
AUDIT_1501	Source deleted: <source_name>
AUDIT_1502	Source with plugin <plugin_name> created: <source_name>
AUDIT_1503	Source updated: <source_name>

API Tokens

With API tokens, you can programmatically interface to the [Certificate Manager API](#).

- [Browsing API tokens](#)
- [Creating an API token](#)
- [Deleting API tokens](#)

Each API token is associated with the user who created that token. Therefore, all actions taken through the API are associated with that person and inherit the person's roles.

Browsing API tokens

See below for browsing API tokens.

To browse API tokens

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Administer > API Tokens**.
3. Define API token views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.

- Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. Browse the following settings for each API token in the main grid.
- [Owner](#)
 - [Label](#)
 - [Token ID](#)
 - [Issued At](#)
 - [Expires At](#)
 - [Roles](#)
 - [Token](#)

Owner

The administrator who created the API token.

Label

An optional description of the API token usage.

Token ID

The identifier automatically generated when creating the API token.

Issued At

The API token creation date.

Expires At

The API token expiration date.

Roles

The roles with permissions to use the API token.



Certificate Manager automatically fills this list with the roles of the administrator that creates the API token.

Token

Click **Copy** to copy the API token. Use this value as the bearer token in the authorization header for the Certificate Manager external API requests.

Creating an API token

See below for creating an API token.

To create an API token

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Administer > API Tokens**.
3. Click **Create to** configure the following settings.
 - [Label](#)
 - [Expires At](#)

4. In the main grid, click **Copy** to copy the API token. Use this value as the bearer token in the authorization header for the Certificate Manager external API requests.

Label

An optional description of the API token usage.

Mandatory: Yes

Expires At

The API token expiration date.

Mandatory: No. This optional value defaults to **Never**.

Deleting API tokens

See below for deleting API tokens.


To delete API tokens

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Administer > API Tokens**.
3. In the main grid, select one or more API tokens.
4. Click **Delete** to delete the selected API tokens.

Certificate Access Tags

Certificate access tags allow granting role permissions on groups of certificates.

- [Browsing certificate access tags](#)
- [Creating a certificate access tag](#)
- [Editing a certificate access tag](#)
- [Deleting Certificate Access Tags](#)

 As explained in [Editing a single certificate](#), you can edit certificates in bulk to add certificate access tags.

Browsing certificate access tags

See below for browsing certificate access tags.

To browse certificate access tags

1. Go to **Administer > Certificate Access Tag**.
2. Define certificate access tag views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
3. Browse the following settings for each certificate access tag in the main grid.
 - [Label](#)
 - [Owner](#)


- [Description](#)

Label

A unique identifier for the certificate access tag.

Owner

The username of the certificate access tag owner. The user who creates the certificate access tag is automatically made the owner.

 You can later edit this field and assign ownership to someone else.

Description

An optional description of the tag purpose.

Creating a certificate access tag

See below for creating and adding a certificate access tag.

To create a certificate access tag

1. Go to **Administer > Certificate Access Tag**.
2. Click **Create** to configure the following settings.
 - [Label](#)
 - [Owner](#)
 - [Description](#)
3. Click **Create** to create a new certificate access tag.
4. Create a [Certificate Role](#).
5. In the role settings, select the new tag.
6. Create a certificate as explained in [Certificates](#).
7. In the certificate settings, select the new tag.


Label

A unique identifier for the certificate access tag.

Mandatory: Yes

Owner

The username of the certificate access tag owner. The user who creates the certificate access tag is automatically made the owner.

 You can later edit this field and assign ownership to someone else.

Description

An optional description of the tag purpose.

Mandatory: No

Editing a certificate access tag

See below for editing the settings of a certificate access tag.

To edit a certificate access tag

1. Go to **Administer > Certificate Access Tags**.
2. In the main grid, select one of the certificate access tags.
3. Click **Edit** to update the following settings.
 - [Label](#)
 - [Owner](#)
 - [Description](#)

Label

A unique identifier for the certificate access tag.

Mandatory: Yes

Owner

The username of the certificate access tag owner. The user who creates the certificate access tag is automatically made the owner.



You can later edit this field and assign ownership to someone else.

Description

An optional description of the tag purpose.

Mandatory: No

Deleting Certificate Access Tags

See below for deleting certificate access tags.

To delete certificate access tags

1. Go to **Administer > Certificate Access Tags**.
2. In the main grid, select one or more certificate access tags.
3. Click **Delete** to delete the selected certificate access tags.

Roles

Certificate Manager provides the following role operations to grant permissions to users.

- [Browsing roles](#)
- [Creating a role](#)
- [Editing a role](#)
- [Deleting roles](#)

An administrator can have no assigned roles as well. However, in such cases, the administrator can still exercise some capabilities in Certificate Manager, like:

- Browse imported and discovered [Certificates](#).
- [Audit Log](#).
- Manage owned [Sources](#), [Destinations](#), and [Reports](#).
- Create [Certificate Access Tags](#).

Administrators can hold more than one role. For instance, they might have permission to manage two, but not all, of the organization's CAs, and therefore hold two roles, one for each of the two CAs.

Browsing roles

See below for browsing user roles in Certificate Manager.

To browse roles

1. Log in as an administrator with either:
 - The [global_admin](#) role to browse all the roles.
 - The [<ca>_admin](#) role to browse [Certificate Roles](#).
2. Go to **Administer > Roles**
3. Define role views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. In the main grid, browse the roles.
 - [<ca>_admin](#)
 - [<user_defined>](#)
 - [global_admin](#)
 - [Operator Role](#)
 - [renewal_daemon](#)

<ca>_admin

Certificate Manager automatically generates a [<ca>_admin](#) role when adding a certificate authority with the [<ca>](#) name. See below for the permissions granted by this role.

- [Find permissions](#)
- [Control permissions](#)
- [Automate permissions](#)
- [Report permissions](#)
- [Administer permissions](#)

Find permissions

Administrators with the [<ca>_admin](#) role have no permission to use the [Find](#) menu.

Control permissions

Administrators with the [<ca>_admin](#) role have the following permissions on the menu options under [Control](#).

Menu option	Operation	<ca>_admin permissions
CA Gateways	Browsing CA Gateway instances	✓
	Adding a CA Gateway instance	✓

Menu option	Operation	<ca>_admin permissions
	Editing a CA Gateway instance	✓
	Deleting a CA Gateway instance	✓
Authorities	Browsing authorities	The <ca> authority only.
	Adding authorities	✗
	Editing an authority	The <ca> authority only.
	Deleting authorities	The <ca> authority only.
Key Managers	Browsing key managers	Only own-created.
	Creating a key manager	✓
	Editing a key manager	Only own-created.
	Deleting key managers	Only own-created.
Custom Fields	Browsing custom fields	✗
	Creating a custom field	✗
	Editing a custom field	✗
	Deleting custom fields	✗
Public Enrollment Forms	Browsing public enrollment forms	Only forms requesting certificates to the <ca> authority.
	Creating a public enrollment form	Only forms requesting certificates to the <ca> authority.
	Editing a public enrollment form	Only forms requesting certificates to the <ca> authority.

Menu option	Operation	<ca>_admin permissions
	Deleting public enrollment forms	Only forms requesting certificates to the <ca> authority.
Requests For Approval	Browsing pending requests	Only requests for the <ca> authority.
	Approving a pending certificate request	Only requests for the <ca> authority.
	Rejecting a pending certificate request	Only requests for the <ca> authority.
My Certificate Requests	Browsing my certificate requests	✗
	Making a certificate request	✗
Certificates	Browsing certificates	Only certificates issued by the <ca> authority.
	Creating a certificate	Only certificates issued by the <ca> authority.
	Automating certificate renewal	Only certificates issued by the <ca> authority.
	Manually renewing a certificate	Only certificates issued by the <ca> authority.
	Editing a single certificate	Only certificates issued by the <ca> authority.
	Editing certificates in bulk	Only certificates issued by the <ca> authority.
	Revoking a certificate	Only certificates issued by the <ca> authority.
	Releasing a certificate from hold	Only certificates issued by the <ca> authority.

Menu option	Operation	<ca>_admin permissions
	Exporting a certificate	Only certificates issued by the <ca> authority.
	Importing certificates	Only certificates issued by the <ca> authority.
	Archiving certificates	Only certificates issued by the <ca> authority.
Endpoints	Browsing Endpoints	✗
Certificate History	Browsing the certificate history	Only certificates issued by the <ca> authority.
	Restoring archived certificates	Only certificates issued by the <ca> authority.
Domains	Browsing domains	Only domains certified by the <ca> authority.
	Registering a domain	Only domains certified by the <ca> authority.
	Checking a domain status	Only domains certified by the <ca> authority.
	Re-verifying a domain	Only domains certified by the <ca> authority.

Automate permissions

Administrators with the <ca>_admin role have the following permissions on the menu options under [Automate](#).

Menu option	Operation	<ca>_admin permissions
Sources	Browsing sources	✗
	Creating a source	✗

Menu option	Operation	<ca>_admin permissions
	Editing a source	✗
	Deleting sources	✗
Destinations	Browsing destinations	✗
	Creating a destination	✗
	Editing a destination	✗
	Deleting destinations	✗
Rules and Actions	Browsing rules	Only rules for certificates issued by the <ca> authority.
	Creating a rule	Only rules for certificates issued by the <ca> authority.
	Editing a rule	Only rules for certificates issued by the <ca> authority.
	Deleting rules and actions	Only rules for certificates issued by the <ca> authority.

Report permissions

Administrators with the <ca>_admin role have the following permissions on the menu options under [Report](#).

Menu option	Operation	<ca>_admin permissions
Designer	Browsing reports	Only reports on certificates issued by the <ca> authority.
	Creating a report	✗
	Editing a report	Only reports on certificates issued by the <ca> authority.

Menu option	Operation	<ca>_admin permissions
	Designing a report	Only reports on certificates issued by the <ca> authority.
	Updating a report design	Only reports on certificates issued by the <ca> authority.
	Deleting reports	Only reports on certificates issued by the <ca> authority.
Report Schedules	Browsing report schedules	Only reports on certificates issued by the <ca> authority.
	Creating a report schedule	Only reports on certificates issued by the <ca> authority.
	Editing a report schedule	Only reports on certificates issued by the <ca> authority.
	Deleting report schedules	Only reports on certificates issued by the <ca> authority.
History	Browsing generated reports	Only reports on certificates issued by the <ca> authority.
	Deleting generated reports	Only reports on certificates issued by the <ca> authority.
	Downloading generated reports	Only reports on certificates issued by the <ca> authority.

Administer permissions

Administrators with the <ca>_admin role have the following permissions on the menu options under [Administer](#).

Menu option	Operation	<ca>_admin permissions
Administrators	Browsing administrators	✓

Menu option	Operation	<ca>_admin permissions
	Creating an administrator	✗
	Editing an administrator	✗
	Deleting administrators	✗
Address Book	Browsing the address book	✓
	Creating an address	✗
	Importing addresses	✗
	Editing an address	✗
	Deleting addresses	✗
Audit Log	Browsing Logs	✗
API Tokens	Browsing API tokens	Only own-created.
	Creating an API token	✓
	Deleting API tokens	Only own-created.
Certificate Access Tags	Browsing certificate access tags	✓
	Creating a certificate access tag	✓
	Editing a certificate access tag	✓
	Deleting Certificate Access Tags	✓
Roles	Browsing roles	Only Certificate Roles for issuing certificates with the <ca> authority.

Menu option	Operation	<ca>_admin permissions
	Creating a role	Only a Certificate Role for issuing certificates with the <code><ca></code> authority.
	Editing a role	Only Certificate Roles for issuing certificates with the <code><ca></code> authority.
	Deleting roles	Only Certificate Roles for issuing certificates with the <code><ca></code> authority.
Settings	General	✗
	Identity Provider	✗
	Reports	✗
	License	✗
	Plugins	✗

<user_defined>

A [Certificate Role](#) or [Custom Role](#) created by an administrator as explained in [Creating a role](#).

global_admin

This role for major configuration tasks is granted to the first administrator created during the system deployment. See below for the permissions granted by this role.

- [Find permissions](#)
- [Control permissions](#)
- [Automate permissions](#)
- [Report permissions](#)
- [Administer permissions](#)

Find permissions

Administrators with the `global_admin` role have the following permissions on the menu options under [Find](#).

Menu option	Operation	global_admin permissions
Discovery	Browsing Discovery Scanners	✓
	Creating a Discovery Scanner	✓
	Editing a Discovery Scanner	✓
	Checking the Discovery Scanner connection	✓
	Creating the first scan configuration of a Discovery Scanner	✓
	Deleting Discovery Scanners	✓

Control permissions

Administrators with the `global_admin` role have the following permissions on the menu options under [Control](#).

Menu option	Operation	global_admin permissions
CA Gateways	Browsing CA Gateway instances	✓
	Adding a CA Gateway instance	✓
	Editing a CA Gateway instance	✓
	Deleting a CA Gateway instance	✓
Authorities	Browsing authorities	✓
	Adding authorities	✓
	Editing an authority	✓
	Deleting authorities	✓
Key Managers	Browsing key managers	✓
	Creating a key manager	✓

Menu option	Operation	global_admin permissions
	Editing a key manager	✓
	Deleting key managers	✓
Custom Fields	Browsing custom fields	✓
	Creating a custom field	✓
	Editing a custom field	✓
	Deleting custom fields	✓
Public Enrollment Forms	Browsing public enrollment forms	✗
	Creating a public enrollment form	✗
	Editing a public enrollment form	✗
	Deleting public enrollment forms	✗
Requests For Approval	Browsing pending requests	✗
	Approving a pending certificate request	✗
	Rejecting a pending certificate request	✗
My Certificate Requests	Browsing my certificate requests	✗
	Making a certificate request	✗
Certificates	Browsing certificates	✓
	Creating a certificate	✗
	Automating certificate renewal	✗

Menu option	Operation	global_admin permissions
	Manually renewing a certificate	✗
	Editing a single certificate	✓
	Editing certificates in bulk	✓
	Revoking a certificate	✗
	Releasing a certificate from hold	✗
	Exporting a certificate	✓
	Importing certificates	✓
	Archiving certificates	✓
Endpoints	Browsing Endpoints	✓
Certificate History	Browsing the certificate history	✓
	Restoring archived certificates	✓
Domains	Browsing domains	✓
	Registering a domain	✓
	Checking a domain status	✓
	Re-verifying a domain	✓

Automate permissions

Administrators with the `global_admin` role have the following permissions on the menu options under [Automate](#).

Menu option	Operation	global_admin permissions
Sources	Browsing sources	✓

Menu option	Operation	global_admin permissions
	Creating a source	✓
	Editing a source	✓
	Deleting sources	✓
Destinations	Browsing destinations	✓
	Creating a destination	✓
	Editing a destination	✓
	Deleting destinations	✓
Rules and Actions	Browsing rules	✓
	Creating a rule	✓
	Editing a rule	✓
	Deleting rules and actions	✓

Report permissions

Administrators with the `global_admin` role have the following permissions on the menu options under [Report](#).

Menu option	Operation	global_admin permissions
Designer	Browsing reports	✓
	Creating a report	✓
	Editing a report	✓
	Designing a report	✓
	Updating a report design	✓

Menu option	Operation	global_admin permissions
	Deleting reports	✓
Report Schedules	Browsing report schedules	✓
	Creating a report schedule	✓
	Editing a report schedule	✓
	Deleting report schedules	✓
History	Browsing generated reports	✓
	Deleting generated reports	✓
	Downloading generated reports	✓

Administer permissions

Administrators with the `global_admin` role have the following permissions on the menu options under [Administer](#).


Menu option	Operation	global_admin permissions
Administrators	Browsing administrators	✓
	Creating an administrator	✓
	Editing an administrator	✓
	Deleting administrators	✓
Address Book	Browsing the address book	✓
	Creating an address	✓
	Importing addresses	✓
	Editing an address	✓

Menu option	Operation	global_admin permissions
	Deleting addresses	✓
Audit Log	Browsing Logs	✓
API Tokens	Browsing API tokens	✓
	Creating an API token	✓
	Deleting API tokens	✓
Certificate Access Tags	Browsing certificate access tags	✓
	Creating a certificate access tag	✓
	Editing a certificate access tag	✓
	Deleting Certificate Access Tags	✓
Roles	Browsing roles	✓
	Creating a role	✓
	Editing a role	✓
	Deleting roles	✓
Settings	General	✓
	Identity Provider	✓
	Reports	✓
	License	✓
	Plugins	✓

Operator Role

This role for backward compatibility maintains the previous permissions of existing users. See below for the permissions granted by this role.

- [Find permissions](#)
- [Control permissions](#)
- [Automate permissions](#)
- [Report permissions](#)
- [Administer permissions](#)











 You can edit or delete this role after the upgrade.

Find permissions

Administrators with the Operator Role have no permission to use the [Find](#) menu.

Control permissions

Administrators with the Operator Role the following permissions on the menu options under [Control](#).

Menu option	Operation	Operator permissions
CA Gateways	Browsing CA Gateway instances	
	Adding a CA Gateway instance	
	Editing a CA Gateway instance	
	Deleting a CA Gateway instance	
Authorities	Browsing authorities	
	Adding authorities	
	Editing an authority	
	Deleting authorities	
Key Managers	Browsing key managers	
	Creating a key manager	
	Editing a key manager	Only own-created.
	Deleting key managers	Only own-created.

Menu option	Operation	Operator permissions
Custom Fields	Browsing custom fields	✗
	Creating a custom field	✗
	Editing a custom field	✗
	Deleting custom fields	✗
Public Enrollment Forms	Browsing public enrollment forms	✗
	Creating a public enrollment form	✗
	Editing a public enrollment form	✗
	Deleting public enrollment forms	✗
Requests For Approval	Browsing pending requests	✗
	Approving a pending certificate request	✗
	Rejecting a pending certificate request	✗
My Certificate Requests	Browsing my certificate requests	✗
	Making a certificate request	✗
Certificates	Browsing certificates	✗
	Creating a certificate	✗
	Automating certificate renewal	✗
	Manually renewing a certificate	✗
	Editing a single certificate	✗
	Editing certificates in bulk	✗

Menu option	Operation	Operator permissions
	Revoking a certificate	✗
	Releasing a certificate from hold	✗
	Exporting a certificate	✗
	Importing certificates	✗
	Archiving certificates	✗
Endpoints	Browsing Endpoints	✗
Certificate History	Browsing the certificate history	✗
	Restoring archived certificates	✗
Domains	Browsing domains	✓
	Registering a domain	✗
	Checking a domain status	✗
	Re-verifying a domain	✗

Automate permissions

Administrators with the Operator Role the following permissions on the menu options under [Automate](#).

Menu option	Operation	Operator permissions
Sources	Browsing sources	✗
	Creating a source	✗
	Editing a source	✗
	Deleting sources	✗
Destinations	Browsing destinations	Only own-created.

Menu option	Operation	Operator permissions
	Creating a destination	✓
	Editing a destination	Only own-created.
	Deleting destinations	Only own-created.
Rules and Actions	Browsing rules	✗
	Creating a rule	✗
	Editing a rule	✗
	Deleting rules and actions	✗

Report permissions

Administrators with the Operator Role the following permissions on the menu options under [Report](#).

Menu option	Operation	Operator permissions
Designer	Browsing reports	✓
	Creating a report	✓
	Editing a report	✓
	Designing a report	✓
	Updating a report design	✓
	Deleting reports	✓
Report Schedules	Browsing report schedules	Only own-created.
	Creating a report schedule	✓
	Editing a report schedule	Only own-created.
	Deleting report schedules	Only own-created.

Menu option	Operation	Operator permissions
History	Browsing generated reports	Only own-created.
	Deleting generated reports	Only own-created.
	Downloading generated reports	Only own-created.

Administer permissions

Administrators with the Operator Role the following permissions on the menu options under [Administer](#).

Menu option	Operation	Operator permissions
Administrators	Browsing administrators	✗
	Creating an administrator	✗
	Editing an administrator	✗
	Deleting administrators	✗
Address Book	Browsing the address book	✓
	Creating an address	✗
	Importing addresses	✗
	Editing an address	✗
	Deleting addresses	✗
Audit Log	Browsing Logs	✗
API Tokens	Browsing API tokens	Only own-created.
	Creating an API token	✓
	Deleting API tokens	Only own-created.
Certificate Access Tags	Browsing certificate access tags	✓

Menu option	Operation	Operator permissions
	Creating a certificate access tag	✓
	Editing a certificate access tag	✓
	Deleting Certificate Access Tags	✓
Roles	Browsing roles	✗
	Creating a role	✗
	Editing a role	✗
Settings	General	✗
	Identity Provider	✗
	Reports	✗
	License	✗
	Plugins	✗

renewal_daemon

This system role for automated certificate renewals cannot be assigned to administrators.

Creating a role

See below for creating a [Certificate Role](#) or a [Custom Role](#) in Certificate Manager.

To create a role

- Log in as an administrator with either:
 - The [global_admin](#) role to create [Certificate Roles](#) or [Custom Roles](#).
 - The [<ca>_admin](#) role to create [Certificate Roles](#).
- Go to **Administer > Roles**.
- Click **Create**.
- In the **Name** field, enter a unique name for the role.
- In the **Description** field, enter an optional description of the role purpose.
- In the **Role Type** list, select one of the following values.
 - [Certificate Role](#)
 - [Custom Role](#)

Certificate Role

Certificate roles are user-defined roles for covering certificate lifecycle management. When selecting this role type, configure the following settings.

- [Certificate Role Template](#)
- [Authority](#)
- [Profiles](#)
- [Certificate Access Tag](#)
- [Permissions](#)

Certificate Role Template

Select one of the following templates for creating the role.

Role type	Role permissions
Manager	Manage Certificates .
Requestor	Create certificate requests as explained in Making a certificate request .
Approver	Approve certificate requests as explained in Approving a pending certificate request , or manage public forms as explained in Creating a public enrollment form .

Authority


The certificate authority that issued, or will issue, the certificates. Select one of the Certificate Manager-managed [Authorities](#) for granting permissions to:

- Issue, edit, revoke, or unhold certificates issued by that certificate authority.
- Manage public forms for the end-users to request certificates from this certificate authority.
- Approve or create certificate requests for this certificate authority.

If this optional field is omitted, the role permissions will be limited to unmanaged certificates – that is, certificates issued by certificate authorities not managed by Certificate Manager.

Profiles

The certificate profiles the **Authority** will use for issuing new certificates. This setting does not affect existing certificates.

 The **All Profiles Enabled** default option grants role permissions on all the certificate profiles issued by the **Authority**.

Certificate Access Tag

The [Certificate Access Tag](#) assigned to the certificates.

Permissions

The permissions granted by the role on certificates:

- Issued by the **Authority** using the selected **Profiles**.
- Labeled with the **Certificate Access Tag**.

Custom Role

A custom role is a user-defined role covering access to:

- [Key Managers](#)
- [Destinations](#)
- [Sources](#)
- [Rules and Actions](#)

When selecting this role type, configure the following settings.

Authorization Tag

The name of a new authorization tag.

Permissions

The permissions granted by the role on the entities with the **Authorization tag**.

Editing a role

See below for how to edit an administrator role in Certificate Manager.

To edit a role

1. Log in as an administrator with:
 - The [global_admin](#) role, to edit the [Operator Role](#), a [Certificate Role](#), or a [Custom Role](#).
 - The [<ca>_admin](#) role, to edit a [Certificate Role](#).
2. Go to **Administer > Roles**.
3. Define role views.
 - Unfold the **Columns** list to select the properties you want to display as columns.
 - Click **Show Filter Options** to display a filtering form below each column name.
 - Select **Show Filter Options / Remove all filters** to remove all filters.
 - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
 - Click **Show Filter Options** to hide the filtering options and keep the filters.
 - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
 - Click **Reset layout** to remove all the column and filter customizations.
 - Click the refresh icon to rerun the query with the current filters.
4. In the main grid:
 - Select a role of the **Certificate Role** type to edit the settings described in [Certificate Role](#).
 - Select a role of the **Custom Role** type to edit the settings described in [Custom Role](#).
 - Select the **Operator Role** to edit the default settings described in [Operator Role](#).

Deleting roles

See below for how to delete administrator roles in Certificate Manager.

To delete Certificate Manager roles

1. Log in as an administrator with:
 - The [global_admin](#) role, to delete the [Operator Role](#), a [Certificate Role](#), or a [Custom Role](#).
 - The [<ca>_admin](#) role, to delete a [Certificate Role](#).
2. Go to **Administer > Roles**.
3. Select one or more roles in the main grid and click **Delete**.

Settings

The Settings section provides access to options generally set up as part of the initial system deployment but can be changed anytime to support the evolving business needs.

- [General](#)
- [Identity Provider](#)
- [Reports](#)
- [License](#)
- [Plugins](#)

General

Log in as an administrator with the [global_admin](#) role to configure the following general settings.

- [Enable Public Enrollment Forms](#)
- [Certificate Request Retention Period](#)


Enable Public Enrollment Forms

Enable or disable the [Public Enrollment Forms](#). Once disabled:

- External users can no longer access public enrollment forms.
- Certificate Manager Administrators can still define and manage public enrollment forms.

Certificate Request Retention Period

The number of days to retain certificate requests. Requests whose status has not changed during this period will be removed.

 The default retention period for certificate requests is 365 days.

Identity Provider

After deploying Certificate Manager, you can integrate Identity Providers (IdPs) already in use in the corporate environment.

To configure an identity provider

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Administer > Settings > IDENTITY PROVIDER**.
3. In the **Select Identity Provider** list, choose one of the mechanisms already described for the Cryptographic Security Platform Management Console.
 - [Entrust Identity as a Service \(IDaaS\)](#)
 - [Internal password](#)
 - [Lightweight Directory Access Protocol](#)
 - [OpenID Connect 1.0](#)
4. Configure the selected identity providers. For Certificate Manager, the OIDC claim email attribute is the user's unique username. Therefore, all users logging from an IdP must have unique email addresses.
5. Optionally, disable the [Internal password](#) authentication mechanism.
6. In **Administer > Administrators**, manage the new IdP-registered administrators.

Reports


Customize the corporate branding of the reports previously configured with the designer.

To customize the report branding

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Administer > Settings > REPORTS**.
3. Configure the following settings.
 - [Retention period field](#)
 - [Logo](#)
 - [Footer Text](#)
 - [Header Color](#)
4. Click **Save** to save the report settings.
5. Click **Preview Report** to generate a sample report with the selected branding.
6. In the **Report Name** dropdown list of the **Preview Report** dialog, select the name of the report design.
7. In the **Format** dropdown list of the **Preview Report** dialog, select the file format for the generated preview: CSV, PDF, Microsoft Excel, or Microsoft Word.
8. Click **Preview** to generate and download the report preview.

Retention period field

The number of days for which Certificate Manager will keep the generated reports.

 By default, Certificate Manager removes generated reports exceeding 365 days.

Logo

The corporate logo for the generated reports. Check the current logo in the **Current image** field (if any).

Footer Text

The footer text for the generated reports.

Header Color

The header color for the generated reports.


License

After a new Certificate Manager installation or an upgrade from 2.1.1, Certificate Manager only provides Administer options. To run the other options, you must import a license.

- [Importing a license](#)
- [Checking the imported license](#)

Importing a license

Import a license for the Certificate Manager application and the installed plugins.

 You can upload updated licenses for the same order number. Licenses with new order numbers require a new Certificate Manager installation.

To import a license

1. Log in as an administrator with the [global_admin](#) role.
2. Go to **Administer > Settings > LICENSE**.
3. Click **Select Files...** and select the license file for your Certificate Manager installation. When importing a zipped license, you must type the **Password** you received by email along with the license file.
4. Click **Save**. The application will display the license details described in the next section Checking the imported license.

Checking the imported license

To check the imported license, you can either:

- Go to **Administer > Settings > LICENSE**.
- Select **About** in the top-right **<username>** menu.


See below for a description of each license field.

Field	Application license	Plugin license
Order Number	The license order number.	The license order number.
Product License	The license name.	The license name.
Summary	The licensed capabilities.	The licensed capabilities.
License Validity	The license validity period.	The license validity period.
Quantity	The number of certificates Certificate Manager is allowed to manage. For non-capped licenses, the value of this field is "Unlimited".	The number of licensed plugins.

Plugins

Manage the installed plugins.

To manage an installed plugin

1. Log in as an administrator with the [global_admin](#) role.
2. Select a plugin.
3. Click **Edit**.
4. Manage the following settings.
 - [Name](#)
 - [Version](#)
 - [Active](#)
 - [Title](#)
 - [Description](#)
 - [Group](#)
 - [Plugin type](#)
5. In grid view, click the plus button  to display the global settings of a plugin (if any).

Name


The plugin identifier.

Version

The plugin version.

Active

Yes if the plugin is active, **No** otherwise.

 Activating a plugin requires installing the corresponding License, and you cannot deactivate a plugin in use.

Title

The name of the plugin.

Description

Additional information about the plugin.

Group

The internal identifier of the plugin.

Plugin type

The intended use of the plugin.

Plugin Type	Use
Destination	Integrate certificate publication destinations, as explained in Creating a destination .
Key Management	Integrate key managers, as explained in Creating a key manager .
Notification	Send notifications triggered by Rules and Actions , Report Schedules and certificate requests.
Source	Integrate certificate sources, as explained in Creating a source .

Menu options

Select the following options in the top-right menu.


- [Search for help on...](#)
- [Notifications](#)
- [User menu](#)

Search for help on...

Enter a search term to quickly find information across all UI pages, the user guide, and related content.

Notifications

Check a list of the received notifications (if any).

 Notifications on issued certificates include a download link.

User menu


Click your user name and select:

- **Help** to browse this guide in HTML format.
- **API Help** to browse the Certificate Manager API documentation.
- **Language** to change the interface language.
- **Profile Account** to display user details such as:
 - The number of managed [CA Gateways](#).
 - The number of managed [Authorities](#).
 - The total number of issued [Certificates](#), including details on the number of certificates expiring in 7 days and the number of scheduled renewals.
 - The time and date of the last login.
 - The granted [Roles](#).
 - The managed [Certificate Access Tags](#).
 - The number of managed [Discovery Agents](#).
 - The number of requested workflows.
- **Change Password** to change the user password.
- **Settings** to manage the Certificate Manager [Settings](#).
- **About** to check:
 - The time and date when the Certificate Manager API was last updated.
 - The Certificate Manager API current version.
 - The License details.
- **Logout** to terminate the user session.

Certificate Manager API

Certificate Manager provides an API for programmatic access to:

- Query certificates on their associated metadata (owner, description, and custom fields).
- Import new certificates into Certificate Manager.
- Update the metadata of custom fields.

 As explained in [API Tokens](#), the available API operations depend on the permissions of the API token holder.

Open the following URL in your browser to access the Swagger interactive documentation for the Certificate Manager API.


```
https://<cm>/api
```

Where `<cm>` is the URL or IP address of your Certificate Manager installation.

Certificate Manager error reference

When executed, Certificate Manager can print the following errors.

- [Certificate Manager authentication and authorization errors](#)
- [Certificate Manager administration errors](#)
- [Certificate Manager automation errors](#)
- [Certificate Manager control errors](#)
- [Certificate Manager certificate errors](#)

 See [Browsing logs with Grafana](#) for how to browse Certificate Manager logs.

Certificate Manager authentication and authorization errors

The application throws the following authentication and authorization errors.

Code	Message
ERR_1006	Failed to hash the password for user: <code><Username></code>
ERR_1010	<code>hasPermission</code> unexpectedly invoked for <code><Permission></code>
ERR_1011	The util command must have a <code>--cmd</code> argument.
ERR_1012	Unknown command <code><Command></code>
ERR_1013	<code>--username</code> , <code>--password</code> , and <code>--email</code> must be supplied to the <code>createUser</code> command.
ERR_1014	Unexpected crypto error:
ERR_1015	Error creating default cert expiry rule for initial user:
ERR_1016	<code>--username</code> and <code>--role</code> must be provided.
ERR_1017	Unexpected crypto exception:
ERR_1040	Unexpected parsing error while loading auth request:
ERR_1041	Unexpected parsing error while saving auth request:
ERR_1042	Unexpected parsing error while removing auth request:
ERR_1046	Could not find password auth provider entry.
ERR_1047	Failed to hash the password for user: <code><Username></code>
ERR_1048	Cannot update non-existent user. User must have existing id.

Code	Message
ERR_1049	Login denied. Tenant id not found for user <code><Username></code> .
ERR_1056	More than one LDAP auth provider registration found (<code><Number of registrations></code>). Unexpected behavior may result!
ERR_1057	More than one PASSWORD auth provider registration found (<code><Number of registrations></code>). Unexpected behavior may result!
ERR_1076	Unable to create keystore: <code><CA></code>
ERR_1077	Cryptography issue when creating user.
ERR_1078	Cryptographic error processing password.
ERR_1079	Unable to initialize SSLContext for LDAPS
ERR_1080	More that one LDAP auth provider registration present. Unexpected results may occur.
ERR_1081	LDAP authentication error.
ERR_1082	Unexpected exception during LDAP lookup.
ERR_1083	Error closing LDAP context.
ERR_1084	Could not find Active Directory user.
ERR_1085	Error creating the daemon user:
ERR_1086	Error creating the initial user:

Certificate Manager administration errors

The application throws the following administration errors.

Code	Message
ERR_1100	Internal error occurred
ERR_1101	Error parsing license : <Error message>
ERR_1102	Error parsing license: Epm client could not parse license
ERR_1103	Error parsing license : <Error message>
ERR_1104	Error parsing license: Epm client could not parse license
ERR_1105	Order Number of <Order number> uploaded license doesn't match the existing license <Customer contact reference>
ERR_1106	License revision <Revision> already uploaded.
ERR_1107	Uploaded license revision <Uploaded revision> is outdated. Current license revision : <Current revision> .
ERR_1108	Failed to create the license expiry schedule
ERR_1109	Failed to send email for license consumption
ERR_1110	Failed to send email for license expiry
ERR_1111	Failed to check the license expiry schedule
ERR_1112	Failed to delete existing license expiry schedule
ERR_1113	Failed to create the license expiry schedule
ERR_1114	Invalid plugin name: <Plugin name>
ERR_1115	Error executing plugin options for plugin: <Plugin name>
ERR_1116	Error loading plugin jar <JAR file name> . Plugin will not be loaded!

Code	Message
ERR_1117	Error loading plugin classloader.
ERR_1118	Plugin <code><Canonical name></code> is missing a language bundle. Plugin will not be loaded!
ERR_1119	Plugin <code><Canonical name></code> has invalid language bundle. No messages section found. Plugin will not be loaded!
ERR_1120	Plugin <code><Canonical name></code> has invalid language bundle. No languages found. Plugin will not be loaded!
ERR_1121	Plugin <code><Canonical name></code> has an invalid language bundle. Language <code><Key></code> is an invalid map. Plugin will not be loaded!
ERR_1122	Plugin <code><Canonical name></code> has an invalid language bundle. Language <code><Name></code> , key <code><Key></code> is invalid (<code><Value></code>). Plugin will not be loaded!
ERR_1123	Error initializing plugins! No <code><Plugin class name></code> plugins will be loaded until invalid plugin is removed!
ERR_1124	updatePlugin: Error converting global options to Json string from list
ERR_1125	validatePluginStateUpdate : cannot deactivate plugins that don't require license
ERR_1126	validatePluginStateUpdate : cannot deactivate plugin <code><Name></code> as its in use by destination : <code><Label></code>
ERR_1127	validatePluginStateUpdate : cannot deactivate plugin <code><Name></code> as its in use by source : <code><Label></code>
ERR_1128	addPlugin: Error converting global options to Json string from list
ERR_1129	Error converting global options to list from <code>Json byte[]</code>
ERR_1130	addPlugin: Error converting global options to list from <code>Json byte[]</code>

Code	Message
ERR_1131	Error fetching language bundle, Plugin <code><Plugin name></code> not found
ERR_1132	Failed to add an entry to the keystore: <code><TBU></code>
ERR_1133	Plugin update failed, plugin ID <code><Plugin ID></code>
ERR_1149	Failed importing multiple addresses.
ERR_1150	Failed importing single addresses.
ERR_1153	Failed to check the events retention schedule: <code><Error></code>
ERR_1154	Failed to create the events retention schedule: <code><Error></code>
ERR_1199	Unhandled exception caught

Certificate Manager automation errors

The application throws the following automation errors.

Code	Message
ERR_1207	Failed to mapping existing source plugin options.
ERR_1208	Failed to process existing source plugin options.
ERR_1209	Failed to migrate existing source plugin options.
ERR_1214	Failed to send email for report <code><Report name></code> , schedule id: <code><Schedule ID></code> . Error:
ERR_1215	Failed to generate missing report: <code><Report ID></code>
ERR_1216	Failed to generate missing schedule: <code><Schedule ID></code>
ERR_1217	Failed to return report: <code><Report ID></code> . Error: <code><Error></code>

Code	Message
ERR_1218	Error while retrieving report data:
ERR_1219	Error while generating report:
ERR_1220	User <code><Username></code> does not have permission to edit or delete report <code><Report name></code>
ERR_1221	Error while generating report: <code><Error></code>
ERR_1222	User <code><Username></code> does not have permission to access artifact <code><Artifact ID></code>
ERR_1223	User <code><Username></code> does not have permission to access execution <code><Execution ID></code>
ERR_1224	Failed to check the reports retention schedule: <code><Error></code>
ERR_1225	Failed to create the reports retention schedule: <code><Error></code>
ERR_1230	Field ' <code><Name></code> ' value ' <code><Value></code> ' cannot be parsed as <code><Type></code> . Field will be treated as a String.
ERR_1231	Unexpected exception while processing rule. RULE WILL BE SKIPPED!
ERR_1232	Expiry notification is dropped for certificate <code><Certificate name></code> . The address field <code><Address field></code> is empty.
ERR_1233	Expiry notification is dropped for certificate <code><Certificate name></code> . The address field <code><Address field></code> is not referring to a text custom field.
ERR_1234	Action plugins not currently supported. THIS ACTION WILL BE SKIPPED!
ERR_1235	Exception while executing rule. RULE WILL BE SKIPPED!
ERR_1236	Error running rules engine for certificate renewal rule.

Code	Message
ERR_1237	Execution of action failed.
ERR_1238	FAILED processing conditions. RULE WILL BE SKIPPED!
ERR_1239	I/O issue while parsing conditions. RULE WILL BE SKIPPED!
ERR_1240	Error running rules engine for event.
ERR_1241	Could not parse plugin config, ACTION WILL BE SKIPPED: <Plugin config>
ERR_1242	FAILED to create the expiration rules schedule! Expiry notifications will not be sent!
ERR_1243	Error while processing event rule conditions. RULE WILL BE SKIPPED!
ERR_1244	Only NOTIFICATION actions are supported! ACTION WILL BE SKIPPED!
ERR_1254	Unexpected IOException while formatting the certificate. Error:
ERR_1255	Unexpected IOException while formatting the certificate chain. Error:
ERR_1256	Unexpected IOException while formatting the certificate. Error:
ERR_1260	FAILED to create the key manager scan schedule! Key managers will not be scanned!
ERR_1261	Error encountered while scanning key manager.
ERR_1262	Error encountered while scanning source.
ERR_1271	User <User ID> does not have permission to view, edit or delete destination <Label>
ERR_1272	Error verifying destination config <Label>
ERR_1273	Error verifying destination config for plugin <Plugin name>

Code	Message
ERR_1274	Error while generating report.
ERR_1275	Failed to retrieve schedule runtimes for <code><Schedule name></code>
ERR_1276	Failed to parse schedule runtimes for <code><Schedule name></code>
ERR_1280	Failed processing conditions for renewal success. RULE WILL BE SKIPPED!
ERR_1281	I/O issue while parsing conditions for renewal success. RULE WILL BE SKIPPED!
ERR_1282	Failed processing conditions for renewal failure. RULE WILL BE SKIPPED!
ERR_1283	I/O issue while parsing conditions for renewal failure. RULE WILL BE SKIPPED!
ERR_1289	Expiry notification is dropped for certificate <code><Certificate name></code> . The address field <code><Address field></code> is empty.
ERR_1290	Error running rules engine for certificate renewal rule.
ERR_1291	Failed processing rule. RULE WILL BE SKIPPED!
ERR_1292	I/O issue while running rule. RULE WILL BE SKIPPED!
ERR_1293	Expiry notification is dropped for certificate <code><Certificate name></code> . The custom field <code><Custom field></code> is empty.
ERR_1294	Expiry notification is dropped for certificate <code><Certificate name></code> . The address field <code><Address field></code> is not referring to a text custom field.
ERR_1295	Expiry notification is dropped for certificate <code><Certificate name></code> . The address field <code><Address field></code> is empty.
ERR_1296	Error running rules engine for certificate renewal rule.
ERR_1299	Execution of rule action failed.

Certificate Manager control errors

The application throws the following control errors.

Code	Message
ERR_1302	Error getting authority capabilities from CAGW
ERR_1303	Failed to check the domain sync trigger
ERR_1304	Unable to add domain sync for authority
ERR_1305	Internal error contacting CAGW.
ERR_1306	Error while reading XML stream from upload.
ERR_1307	Unexpected exception while pushing certificate:
ERR_1308	HTTP Error while uploading certificate: <code><Error> : \n <Response body></code>
ERR_1309	Error while uploading certificate: <code><Error></code>
ERR_1310	Unable to parse properties for domain: <code><Domain name></code>
ERR_1311	User <code><User ID></code> doesn't have access to authority <code><Authority ID></code>
ERR_1312	Internal error contacting CAGW.
ERR_1313	Unable to get profiles for authority
ERR_1314	Unable to get the subject DN for authority
ERR_1315	Unable to get the Capabilities for authority
ERR_1316	Unexpected error contacting CAGW: <code><Error></code>
ERR_1330	User <code><User ID></code> does not have permission to view, edit or delete key manager <code><Key manager></code>

Code	Message
ERR_1331	Error verifying key manager config <code><Key manager label></code>
ERR_1332	saveOrUpdateKeyManager: Error converting plugin options to Json string from list
ERR_1333	Error converting plugin options to list from Json byte[]
ERR_1334	Error verifying key manager config for plugin <code><Plugin name></code>
ERR_1349	Failed to sync domains, Error from CAGW: <code><Error></code>
ERR_1350	Unexpected response received from CAGW
ERR_1351	Internal error contacting CAGW
ERR_1352	Unexpected response received from CAGW: <code><Error></code>
ERR_1353	Unexpected response received from CAGW: <code><Error></code>
ERR_1354	Unexpected response received from CAGW: <code><Error></code>
ERR_1355	Error configuring the SSL client connection to the CAGW APIs.
ERR_1356	Error configuring the SSL client connection to the CAGW APIs.
ERR_1357	Error configuring the SSL client connection to the CAGW APIs
ERR_1358	Error configuring the SSL client connection to the CAGW APIs.
ERR_1359	Error configuring the SSL client connection to the CAGW APIs.
ERR_1362	Error parsing authority certificate validity period: <code><Certificate validity period></code>
ERR_1363	Error parsing authority certificate validity period: <code><Certificate validity period></code>

Code	Message
ERR_1374	Error response from CAGW: <Error>
ERR_1375	Unable to parse properties for domain: <Domain name>
ERR_1376	Internal error contacting CAGW: <Error>
ERR_1377	Internal error contacting CAGW.
ERR_1378	Internal error contacting CAGW.
ERR_1379	Internal error contacting CAGW while responding to an authority request.
ERR_1380	Failed to create the authority domain sync schedule for authority <Authority ID>
ERR_1381	Failed to delete the authority domain sync schedule for authority <Authority ID>
ERR_1382	Certificate Authority <Authority ID> not found
ERR_1383	Unable to parse plugin options for authority <Authority ID> :
ERR_1384	Error response from CAGW while getting domain: <Domain name>
ERR_1385	Failed to get domain. Error from CAGW: <Error>
ERR_1386	Failed to submit domain, Error from CAGW: <Error>
ERR_1387	Unable to fetch whois record from server <Server name> . Error:
ERR_1388	Unable to close whois client connection with server <Server name> . Error:
ERR_1389	Unable to fetch whois record from default host. Error:
ERR_1390	Unable to close whois client connection with default server. Error:

Code	Message
ERR_1392	Error on DNS lookup : <Error>
ERR_1394	Failed to submit domain, Error from CAGW: <Error>
ERR_1397	Certificate Authority <Authority ID> not found
ERR_1398	Unable to parse plugin options for authority <Authority ID>
ERR_1399	Unable to import/update domain id <Domain ID> due to Json parsing error from authority <Authority ID>

Certificate Manager certificate errors

The application throws the following certificate errors.

Code	Message
ERR_1426	Renewal failed. Missing certificate id.
ERR_1427	Failed auto renewal for certificate <Certificate ID> .
ERR_1428	Automated renewal failed for certificate <Certificate ID> due to certificate processing error
ERR_1430	Automated renewal failed for certificate <Certificate ID> due to destination errors: <List of errors>
ERR_1431	Failed to find the renewal daemon user for auto renewal
ERR_1432	Failed to create the renewal schedule for cert <Certificate serial> : <Error>
ERR_1433	Failed to check the renewal schedule <Error>
ERR_1434	Failed to create the renewal schedule <Error>

Code	Message
ERR_1435	Adding definition for custom field with duplicate display order : <Label> of type <Type> at position <Display order>
ERR_1436	Deleting definition for custom field with Id : <Metadata ID> failed as it is in use by <Certificates using metadata> certificates
ERR_1437	Updating definition for custom field with duplicate display order : <Label> of type <Type> at position <Display order>
ERR_1438	Updating definition for custom field with Id : <Metadata ID> failed as it is in use by <Certificates using metadata> certificates
ERR_1439	Updating definition for custom field with duplicate display order : <Metadata values>
ERR_1440	Other certificate custom field definitions exists with same display order <List>
ERR_1441	Updating definition for custom field with Id : <Metadata ID> failed as one of its value <List> is in use by <Certificates> certificates
ERR_1442	Error parsing the value <Value> for custom field <Metadata ID>
ERR_1443	Unsupported Operator <Operator> for custom field Id: <Metadata ID>
ERR_1450	Could not unarchive certificate because entitlement limit reached.
ERR_1452	Error response from CAGW <Error>
ERR_1453	Error exporting a certificate: <Error>
ERR_1454	Failed to parse certificate <Certificate name> stored in DB. Error: <Error>
ERR_1455	Certificate Chain is not available for export

Code	Message
ERR_1456	Error while exporting certificate: <code><Error></code>
ERR_1457	Error saving chain to keystore for export of: <code><Certificate name></code>
ERR_1458	Error adding P12 to response stream
ERR_1459	Unable to parse response from CAGW to export certificate for : <code><Certificate name></code> . Error: <code><Error></code>
ERR_1460	Certificate can not be exported since the issuing Authority is not known
ERR_1461	Certificate Authority not found
ERR_1462	Error adding P12 to response stream
ERR_1463	Unexpected response received from CAGW when exporting a certificate
ERR_1464	Internal error contacting CAGW
ERR_1465	Failed to export certificate for <code><Certificate name></code> . Error from CAGW: <code><Error></code>
ERR_1466	Failed to export certificate for <code><Certificate name></code> with serial number <code><Certificate serial number></code> . Certificate key is not backed up.
ERR_1467	Unable to parse response from CAGW to export certificate for : <code><Certificate name></code> . Error: <code><Error></code>
ERR_1468	Export private key is not supported for export type <code><Type></code> You can uncheck \\\\"Include Private Key\\\\" and try again, however, your exported certificate will not have the private key
ERR_1469	Export certificate chain is not supported for export type <code><Type></code> You can uncheck \\\\"Include Certificate Chain\\\\" and try again, however, your exported certificate will not have certificate chain
ERR_1470	Public certificate must be requested for export type <code><Type></code>

Code	Message
ERR_1471	At least one of public certificate, certificate chain or private key must be requested for export type <code><Type></code>
ERR_1472	At least one of public certificate, certificate chain or private key must be requested for export type <code><Type></code>
ERR_1473	Unable to revoke the authority <code><Authority name></code>
ERR_1474	Unable to unhold the authority <code><Authority name></code>
ERR_1477	Error building certificate query with filter : <code><Filter></code> . Error <code><Error></code>
ERR_1478	Error fetching certificates with predicate : <code><Predicate></code> . Error <code><Error></code>
ERR_1479	Certificate Bulk Edit Error: 'certificatesFilter' missing from request body
ERR_1480	Certificate Bulk Edit Error: If 'clearOutAccessTags' is set, 'accessTags' must be empty.
ERR_1481	Certificate Bulk Edit Error: No updated values provided
ERR_1482	Certificate Bulk Edit Error building certificate query with filter : <code><Filter></code> , Error : <code><Error></code> .
ERR_1483	Certificate Bulk Edit Error building certificate query with filter : <code><Filter></code> , Error : <code><Error></code> .
ERR_1484	Certificate Bulk Edit Error updating certificates with filter : <code><Filter></code> , Error : <code><Error></code>
ERR_1486	Certificate unhold error : Could not find certificate with id: <code><Certificate ID></code> .
ERR_1487	Certificate unhold error : No Authority Id associated with this certificate: <code><Certificate ID></code> .

Code	Message
ERR_1488	Certificate unhold error : Cannot unhold certificate <Certificate ID> . Authority is not active : <Authority ID> .
ERR_1489	Certificate unhold error : Cannot unhold certificate <Certificate ID> . No external id found.
ERR_1490	Issue certificate error : Subject DN is required for CSR.
ERR_1491	Issue certificate error : CAGW failed to create certificate for authority <Authority ID>
ERR_1492	Issue certificate error : CAGW Failed to create certificate: <Key manager ID> .
ERR_1493	Issue certificate error : Subject DN is required for CSR.
ERR_1494	Issue certificate error : Subject DN is required for CSR.
ERR_1495	Issue certificate error : Subject DN is required for CSR.
ERR_1496	Issue certificate error : Subject DN is required for CSR.
ERR_1497	Failed to save certificate: <Error>
ERR_1498	Failed to upload certificate to the key manager <Key manager ID> . Error <Error>
ERR_1499	Certificate revoke error : No Authority Id associated with this certificate. <Certificate ID>
ERR_1500	Certificate revoke error : Cannot revoke certificate <Certificate ID> . Authority <Authority ID> is not active.
ERR_1501	Certificate revoke error : Cannot revoke certificate <Certificate ID> . No external id found.
ERR_1502	Failed to apply service-level filters on query <Filter>

Code	Message
ERR_1503	Failed to apply service-level filters on query <Filter>
ERR_1504	Failed to apply service-level filters on query <Filter>
ERR_1505	Could not find certificate with id <Certificate ID>
ERR_1506	Could not find certificate with id <Certificate ID>
ERR_1508	Failed to issue a certificate from authority <Authority name> . Error <Error>
ERR_1509	Failed to parse the X509 certificate <Certificate body> \n Message: <Error>
ERR_1510	Unable to find certificate <Certificate ID>
ERR_1511	Failed to process the certificate <Certificate import request body> \n Message: <Error>
ERR_1512	Failed to process the certificate <Certificate body> \n External ID: <Certificate External ID> \n Message: <Error>
ERR_1513	Failed to apply service-level filters on query <Filter>
ERR_1514	Failed to run the certificate count query: <Error>
ERR_1521	Error verifying source config <Source Label>
ERR_1522	Error verifying source config for plugin <Plugin name>
ERR_1523	addOrUpdateSource: Error converting plugin options to Json string from list
ERR_1524	Error scheduling source sync, sources will not be scanned!
ERR_1525	Error creating certificate from certificate request

Code	Message
ERR_1526	Failed to send new external certificate request notification to approver(s). Error: <Notification message>
ERR_1527	Failed to send external certificate request cancellation notification to requestor. Error: <Notification message>
ERR_1528	Failed to send certificate request approval notification to requestor. Error: <Notification message>
ERR_1529	Failed to send certificate request rejection notification to requestor. Error: <Notification message>
ERR_1530	Failed to send new certificate request notification to internal requestor. Error: <Notification message>
ERR_1531	Failed to send new internal certificate request notification to approver(s). Error: <Notification message>
ERR_1533	Failed to send new certificate request notification to external requestor. Error: <Notification message>
ERR_1534	CSR key algorithm <CSR key algorithm> does not match the required key algorithm <Allowed key algorithm>
ERR_1536	CSR key algorithm keysize <CSR key size> does not meet minimum public key size required: <Allowed key size>
ERR_1537	Invalid certificate signing request provided
ERR_1540	Failed to send new certificate request notification to external requestor. SMTP Notification Plugin not found
ERR_1541	Failed to send certificate request cancellation notification to external requestor. SMTP Notification Plugin not found
ERR_1542	Failed to send new external certificate request notification to approver(s). SMTP Notification Plugin not found

Code	Message
ERR_1543	Failed to send new certificate request notification to admin. SMTP Notification Plugin not found
ERR_1544	Failed to send new internal certificate request notification to approver(s). SMTP Notification Plugin not found
ERR_1545	Failed to send notification for certificate request cancellation. SMTP Notification Plugin not found
ERR_1546	Failed to send notification for certificate request approval. SMTP Notification Plugin not found
ERR_2010	Found invalid certificate with name <code><Certificate name></code> .
ERR_2011	Unexpected exception while processing certificate.
ERR_2012	Error processing certificate.
ERR_2013	Error creating certificate factory.
ERR_2015	Failed to parse certificate <code><Certificate name></code> stored in DB. Error: <code><Error message></code>

Migrating Certificate Manager database to an external host

Only Certificate Manager installations migrated from older versions support an internal database—that is, a database running on the same host as the application. See below for switching from an internal database to an external one.

- [Exporting the database contents](#)
- [Restoring the database contents](#)
- [Applying the database changes to Certificate Manager](#)



Run the steps below in the same version of Certificate Manager that will use the database.

Exporting the database contents

On any Cryptographic Security Platform installation node, open an SSH session and set the following environment variables.

Variable	Value
KUBECTL	kubectl
NAMESPACE	certhub
POSTGRES_DB	certhub
POSTGRES_PWD	The value of the Database User Password configuration parameter described in Configuring and deploying Certificate Manager .
POSTGRES_USER	The value of the Database User Name configuration parameter described in Configuring and deploying Certificate Manager .

Run the following commands

```
now=$(date +"%m_%d_%Y")
```

```
$KUBECTL exec deployment/postgres -n "$NAMESPACE" -- bash -c "export  
PGPASSWORD=$POSTGRES_PWD; pg_dump -d $POSTGRES_DB -U $POSTGRES_USER" > "db-backup-  
$now.sql"
```

Restoring the database contents

Perform the following steps on an external host to restore the database contents.

To restore the database contents on an external host

1. Install the PostgreSQL version described in [Database requirements](#).
2. Copy the `db-backup-<date>.sql` backup file generated when [Exporting the database contents](#).
3. Set the following environment variables to the values described in [Exporting the database contents](#).
 - POSTGRES_DB
 - POSTGRES_PWD
 - POSTGRES_USER
4. Run the following command.

```
export PGPASSWORD=$POSTGRES_PWD; psql -d $POSTGRES_DB -U $POSTGRES_USER -f db-  
backup-<date>.sql
```

Applying the database changes to Certificate Manager

Complete database migration by performing the following operations on Cryptographic Security Platform.

To apply the database changes to Certificate Manager

1. Log in to the Management Console.
2. Update the database configuration parameters described in [Configuring and deploying Certificate Manager](#) to match the new external database.
3. Redeploy Certificate Manager to make the changes effective.
4. Wait while the redeployment with the external database is complete.
5. Open an SSH session as an administrator.
6. Manually remove the PostgreSQL pod.

9 Managing Certificate Enrollment Gateway

See below for configuring, deploying, and administering the Certificate Enrollment Gateway solution.

- [Certificate Enrollment Gateway overview](#)
- [Preparing to deploy Certificate Enrollment Gateway](#)
- [Issuing TLS certificates for Certificate Enrollment Gateway](#)
- [Configuring and deploying Certificate Enrollment Gateway](#)
- [Enrollment URLs for Certificate Enrollment Gateway](#)
- [Integrating Certificate Enrollment Gateway](#)

See [Browsing logs with Grafana](#) for how to browse Certificate Enrollment Gateway logs.

Certificate Enrollment Gateway overview

Entrust Certificate Enrollment Gateway provides automated certificate enrollment and renewal for the following protocols:

- WSTEP
- ACMEv2
- Intune-SCEP
- SCEP
- MDMWS
- MDM-SCEP



Certificate Enrollment Gateway does not archive or back up private keys for data decryption.

In this architecture:

- Each enrollment endpoint is a user or device that requests a certificate issuance or renewal.
- The Certificate Enrollment Gateway service runs in CSP 1.0.0. This microservices-based cluster provides easy installation and uninstallation, centralized logging and reporting, and operational dashboards.



The Certificate Enrollment Gateway service supports an HTTP and HTTPS proxy for outbound connections.

- Each certificate Issuer is a Certificate Authority (CA) that issues certificates to the enrollment endpoints.

Preparing to deploy Certificate Enrollment Gateway

This section describes how to prepare for new deployments of Certificate Enrollment Gateway.

- [Deploying Entrust CA Gateway for an on-premises CA](#)
- [Configuring an on-premises Entrust Certificate Authority for Certificate Enrollment Gateway](#)

Deploying Entrust CA Gateway for an on-premises CA



For Entrust PKI as a Service deployments, CA Gateway is installed and managed by Entrust.

When deploying Certificate Enrollment Gateway with an on-premises CA, you must also deploy Entrust CA Gateway on-premises.

Entrust CA Gateway enables full certificate lifecycle management and operational management across all your Entrust-supported Certification Authorities (CAs). Each Entrust CA Gateway client can access one or several CAs. Certificate Enrollment Gateway will send certificate requests to Entrust CA Gateway. Entrust CA Gateway will forward the request to the appropriate Managed CA, and send the generated certificate back to Certificate Enrollment Gateway.

For detailed information about installing and configuring Entrust CA Gateway, see the Entrust CA Gateway documentation.

- [Configuring CSP CA Gateway for WSTEP enrollment](#)
- [Configuring CSP CA Gateway for SCEP and Intune-SCEP enrollment](#)
- [Configuring CSP CA Gateway for MDMWS P12 enrollment](#)
- [Configuring CSP CA Gateway for MDM-SCEP enrollment](#)
- [Configuring CSP CA Gateway for ACMEv2 enrollment](#)
- [Defining profiles in CSP CA Gateway for issuing RA certificates](#)
- [Generating a file containing the CA certificate chain for the CSP CA Gateway server certificate](#)
- [Issuing a client credential for Certificate Enrollment Gateway](#)

Configuring CSP CA Gateway for WSTEP enrollment

In CA Gateway, you must create profiles for each Managed CA that will issue certificates for WSTEP enrollment. Each profile must issue one of the WSTEP certificate types you added earlier to the Managed CA.

When adding these profiles to CA Gateway:

- The values for the **Certificate Type** and **Certificate Definition** settings must match the values specified in the Managed CA.
- The **LDAP entry creation mode** setting must be **false**.
- The value for **LDAP directory mode** must be **NO_OP**.
- The **Subject Builder Requirements** settings are supported when the **Subject Builder Configuration** settings are used.
- The **Subject Builder Configuration** settings supported when Certificate Enrollment Gateway has mapped a Windows certificate template to the Profile ID.
WSTEP requests to Certificate Enrollment Gateway will include Windows certificate template information. When configuring Certificate Enrollment Gateway, the WSTEP configuration setting **Certificate Templates** can map Windows certificate templates to Profile IDs in CA Gateway (see [WSTEP](#)).
 - If the certificate template is not mapped to a Profile ID, the **Subject Builder Configuration** settings are ignored.
 - If the certificate template is mapped to the Profile ID and the **Subject Builder Configuration** settings are configured:
 - The **Subject Builder Name** setting must be set to `com.entrust.adminservices.cagw.common.subjects.TemplateSubjectBuilder`.
 - For machines, the **Subject name** in the certificate template must be **Common name** or **DNS**. For information about configuring the **Subject name** in the Windows certificate template, see [Creating Windows certificate templates for the Entrust WSTEP Service](#).
 - For users, the **Subject name** in the certificate template must be **Common name**. For information about configuring the **Subject name** in the Windows certificate template, see [Creating Windows certificate templates for the Entrust WSTEP Service](#).
 - If the certificate template is mapped to the Profile ID and the **Subject Builder Configuration** settings are not configured:
 - For machines, the subject of the issued certificate will be either `CN=<Common Name>` or `CN=<DNS name>`.
 - For users, the subject of the issued certificate will be `CN=<Common Name>`.

Configuring CSP CA Gateway for SCEP and Intune-SCEP enrollment

Note

For SCEP and Intune-SCEP enrollment, you must also define profiles in CA Gateway for issuing RA certificates (see [Defining profiles in CSP CA Gateway for issuing RA certificates](#)).

In CA Gateway, you must create profiles for each Managed CA that will issue certificates for SCEP or Intune-SCEP enrollment. Each profile must issue one of the SCEP certificate types you added earlier to Security Manager.

When adding these profiles to CA Gateway:

- The **Subject Variable Requirements** settings are not supported.
- The **Subject Builder Configuration** settings are not supported.
- The values for the **Certificate Type** and **Certificate Definition** settings must match the values specified in the Managed CA.
- The **LDAP entry creation mode** setting must be **false**.
- The value for **User Role** must match a role that allows PKCS #12 export. You may have created a role that allows PKCS #12 export named **End User P12**.

Configuring CSP CA Gateway for MDMWS P12 enrollment

In CA Gateway, you must create profiles for each Managed CA that will issue certificate for MDM Web Service enrollment (PKCS #12 enrollment over the MDMWS protocol). Each profile must issue one of the MDMWS P12 certificate types you added earlier to the Managed CA.

When adding these profiles to CA Gateway:

- The **Subject Variable Requirements** settings are not supported.
- The **Subject Builder Configuration** settings are not supported.
- The values for the **Certificate Type** and **Certificate Definition** settings must match the values specified in the Managed CA.
- The **LDAP entry creation mode** setting must be **false**.
- The value for **User Role** must match a role that allows PKCS #12 export. You may have created a role that allows PKCS #12 export named **End User P12**.

Configuring CSP CA Gateway for MDM-SCEP enrollment

Note

For SCEP and Intune-SCEP enrollment, you must also define profiles in CA Gateway for issuing RA certificates (see [Defining profiles in CSP CA Gateway for issuing RA certificates](#)).

In CA Gateway, you must create profiles for each Managed CA that will issue certificates for MDM-SCEP enrollment. Each profile must issue one of the MDM-SCEP certificate types you added earlier to the Managed CA.

When adding these profiles to CA Gateway:

- The **Subject Variable Requirements** settings are not supported.
- The **Subject Builder Configuration** settings are not supported.
- The values for the **Certificate Type** and **Certificate Definition** settings must match the values specified in the Managed CA.
- The **LDAP entry creation mode** setting must be **false**.

Configuring CSP CA Gateway for ACMEv2 enrollment

In CA Gateway, you must create profiles for each Managed CA that will issue certificates for ACMEv2 enrollment. Each profile must issue one of the ACMEv2 certificate types you added earlier to the Managed CA.

When adding these profiles to CA Gateway:

- The **Subject Variable Requirements** settings are not supported.
- The **Subject Builder Configuration** settings are not supported.
- The values for the **Certificate Type** and **Certificate Definition** settings must match the values specified in the Managed CA.
- The **LDAP entry creation mode** setting must be **false**.

Defining profiles in CSP CA Gateway for issuing RA certificates

For all SCEP-related protocols (SCEP, MDM-SCEP, and Intune-SCEP), Certificate Enrollment Gateway uses RA certificates to sign and encrypt SCEP PKI messages. In Entrust CA Gateway, for each Managed CA that will issue certificates for all SCEP-related protocols, you must create a profile for issuing RA certificates.

All profiles used for RA certificates must allow for Dual Usage (both Digital Signature and Key Encipherment). It is recommended that you use a Dual Usage certificate type that you created earlier for a SCEP-related protocol. For example, for the SCEP and Intune-SCEP protocols, you can use the SCEP Signing and Encryption (ent_scep_sig_enc) certificate type you created earlier for the SCEP and Intune-SCEP protocols in [Adding certificate types to Entrust Certificate Authority for SCEP and Intune-SCEP enrollment](#).

When adding a profile to CA Gateway for issuing RA certificates:

- The **Subject Variable Requirements** settings are not supported.
- The **Subject Builder Configuration** settings are not supported.
- The values for the **Certificate Type** and **Certificate Definition** settings must match the values specified in the Managed CA.
- The **LDAP entry creation mode** setting must be **false**.

Generating a file containing the CA certificate chain for the CSP CA Gateway server certificate

Certificate Enrollment Gateway requires the CA certificate chain of Entrust CA Gateway's server certificate. When connecting to Entrust CA Gateway, Certificate Enrollment Gateway will use the CA certificate chain to validate Entrust CA Gateway's server certificate.

The CA certificate chain must be stored in one of the following files.

File	Description
CA Gateway Truststore	This file must be a PKCS #12 (P12) file. The file must contain at least one Trusted CA Certificate entry (TrustedCertEntry). You can re-use the CA Gateway Keystore if it contains the CA certificate chain.
CA Certificates File	The file must be a PEM-formatted file. The file must contain at least one PEM-formatted CA certificate. Each CA certificate must include any BEGIN CERTIFICATE and END CERTIFICATE lines if present.

- [Generating a CA Gateway Truststore](#)
- [Generating a CA Certificates file](#)

Generating a CA Gateway Truststore

See below to generate a CA Gateway Truststore file in P12 format using the Java keytool utility.

To generate a CA Gateway Truststore

1. Obtain the certificate chain for CA Gateway's server certificates, from the server certificate to the root CA certificate.
2. Log in to a computer that has Java installed.
3. For each certificate, enter the following command to generate the CA Gateway Truststore file and import certificates into the truststore:

```
keytool -import -alias <alias> -trustcacerts -file <cert-file> -keystore  
<truststore>
```

Where:

- `<alias>` is an alias for the certificate. Use a different alias for each certificate you will import.
- `<cert-file>` is the path and file name of the certificate.
- `<truststore>` is the path and file name of the CA Gateway Truststore file. For example, `cagwtruststore.p12`. The utility will create the file if it does not exist.

For example:

```
keytool -import -alias cagw-root -trustcacerts -file /tmp/root.cer -keystore /  
home/user/cagwtruststore.p12
```

4. When prompted, enter a password for the truststore.

Generating a CA Certificates file

See below to generate a CA Certificates file in PEM format.

To generate a CA Certificates file

1. Obtain the certificate chain for CA Gateway's server certificate, from the server certificate to the root CA certificate.
2. Open a text editor.
3. Create a new file.
4. Paste the contents of each CA certificate file into the new file, from the server certificate to the root CA certificate. Each CA certificate must include any BEGIN CERTIFICATE and END CERTIFICATE lines if present.
For example:

```
-----BEGIN CERTIFICATE-----  
<TLS server certificate in Base64 encoding>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Issuing CA certificate in Base64 encoding>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Root CA certificate in Base64 encoding>  
-----END CERTIFICATE-----
```

5. The text file should look similar to the following:

```
-----BEGIN CERTIFICATE-----
MIIDqQYJKoZIhvcNAQcCoIIDmjCCA5YCAQExADALBgkqhkiG9w0BBwGgggN...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDejCCAmKgAwIBAgIQ8e7ock59Y21Mtcy7rGJUDANBgkqhkiG9w0BAQs...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIQ0EgRW50cnkwHhcNMjMwMjA4MTUxNzEwWhcNMzMwMjA4MTU0NzEwWjAyM...
-----END CERTIFICATE-----
```

6. Save and close the file.

Issuing a client credential for Certificate Enrollment Gateway

i In Certificate Enrollment Gateway, the client credential is called the CA Gateway Keystore. The CA Gateway Keystore can contain multiple private keys (multiple PrivateKeyEntry entries) and certificates. You can specify the alias of the private key to use for the client credential when you configure Certificate Enrollment Gateway.

Certificate Enrollment Gateway requires a client credential issued from Entrust CA Gateway. Certificate Enrollment Gateway uses this client credential to access and authenticate to Entrust CA Gateway. The client credential must be a PKCS #12 (P12) file that contains a private key and client certificate issued by a Managed CA in Entrust CA Gateway.

To issue a client credential to Certificate Enrollment Gateway, you must configure Certificate Enrollment Gateway as a client in Entrust CA Gateway. In Entrust CA Gateway, you must assign the Certificate Enrollment Gateway client either the integrator or policy-override-tenant role.

For information about configuring clients in Entrust CA Gateway, see [Configuring and deploying CA Gateway](#).

Configuring an on-premises Entrust Certificate Authority for Certificate Enrollment Gateway

See below for how to configure an on-premises Entrust Certificate Authority for using with Certificate Enrollment Gateway.

- [Configuring an on-premises Entrust Certificate Authority for ACMEv2 enrollment](#)
- [Configuring an on-premises Entrust Certificate Authority for MDM-SCEP enrollment](#)
- [Configuring an on-premises Entrust Certificate Authority for MDMWS enrollment](#)
- [Configuring an on-premises Entrust Certificate Authority for SCEP or Intune-SCEP enrollment](#)
- [Configuring an on-premises Entrust Certificate Authority for WSTEP enrollment](#)

Configuring an on-premises Entrust Certificate Authority for ACMEv2 enrollment

See below to configure an on-premises Entrust Certificate Authority for using Certificate Enrollment Gateway with ACMEv2 enrollment,

- [Adding certificate types to Entrust Certificate Authority for ACMEv2 enrollment](#)
- [Mapping certificate definition policies to the ACMEv2 certificate types](#)

Adding certificate types to Entrust Certificate Authority for ACMEv2 enrollment

For ACMEv2 enrollment, you must add the following certificate types to Entrust Certificate Authority.

- ACME V2 TLS Client
- ACME V2 TLS Server
- ACME V2 TLS Client and Server

See below for the required steps.

To add ACMEv2 certificate types

1. Log into Entrust Certificate Authority Administration.
2. Export the certificate specifications to a file by selecting **File > Certificate Specifications > Export**.
3. Open the certificate specifications file in a text editor.
4. Add the following lines to the `[Certificate Types]` section.

```
; -----  
; Certificate types to be used with ACME  
; -----  
acme_tls_client=enterprise,ACME V2 TLS Client,ACME V2 TLS Client Certificate  
acme_tls_server=enterprise,ACME V2 TLS Server,ACME V2 TLS Server Certificate  
acme_tls_client_srv=enterprise,ACME V2 TLS Client and Server,ACME V2 TLS Client  
and Server Certificate
```

5. Add the following lines to the `[Extension Definitions]` section.

```
; -----  
; Certificate definitions to be used with ACME Public protocol in CEG  
; -----  
  
[acme_tls_client Certificate Definitions]  
1=Dual Usage  
  
[acme_tls_client Dual Usage Extensions]  
; KeyUsage = DigitalSignature + KeyEncipherment  
keyusage=2.5.29.15,n,m,BitString,101  
; TLS Client Authentication  
extkeyusage=2.5.29.37,n,o,SeqOfObjectIdentifier,1.3.6.1.5.5.7.3.2  
  
[acme_tls_client Advanced]  
noUserInDirectory=1  
  
[acme_tls_server Certificate Definitions]  
1=Dual Usage  
  
[acme_tls_server Dual Usage Extensions]  
; KeyUsage = DigitalSignature + KeyEncipherment  
keyusage=2.5.29.15,n,m,BitString,101  
; TLS Server Authentication  
extkeyusage=2.5.29.37,n,o,SeqOfObjectIdentifier,1.3.6.1.5.5.7.3.1  
  
[acme_tls_server Advanced]  
noUserInDirectory=1
```

```
[acme_tls_client_srv Certificate Definitions]
1=Dual Usage

[acme_tls_client_srv Dual Usage Extensions]
; KeyUsage = DigitalSignature + KeyEncipherment
keyusage=2.5.29.15,n,m,BitString,101
; TLS Server Authentication + TLS Client Authentication
extkeyusage=2.5.29.37,n,o,SeqOfObjectIdentifier,1.3.6.1.5.5.7.3.1 1.3.6.
_continue_=1.5.5.7.3.2

[acme_tls_client_srv Advanced]
noUserInDirectory=1

; --- END ACME Certificate Definitions -----
```

6. Save and close the file.
7. Import the certificate specifications back into Entrust Certificate Authority. In Entrust Certificate Authority Administration, select **File > Certificate Specifications > Import**.

Mapping certificate definition policies to the ACMEv2 certificate types

In Entrust Certificate Authority, map certificate definition policies to the certificate types created in [Adding certificate types to Entrust Certificate Authority for ACMEv2 enrollment](#).

- [Mapping to the ACME V2 TLS Client certificate type](#)
- [Mapping to the ACME V2 TLS Server certificate type](#)
- [Mapping to the ACME V2 TLS Client and Server certificate type](#)

Mapping to the ACME V2 TLS Client certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the ACME V2 TLS Client certificate type.

To map a certificate definition policy to the ACME V2 TLS Client certificate type

1. Log into Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > ACME V2 TLS Client > Dual Usage**.
3. In the **Certificate definition Policy** drop-down list, select **Dual Usage Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the ACME V2 TLS Server certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the ACME V2 TLS Server certificate type.

To map a certificate definition policy to the ACME V2 TLS Server certificate type

1. Log into Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > ACME V2 TLS Server > Verification_p10**.
3. In the **Certificate definition Policy** drop-down list, select **Dual Usage Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the ACME V2 TLS Client and Server certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the ACME V2 TLS Client and Server certificate type.

To map a certificate definition policy to the ACME V2 TLS Client and Server certificate type

1. Log into Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > ACME V2 TLS Client and Server > Dual Usage**.
3. In the **Certificate definition Policy** drop-down list, select **Dual Usage Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Configuring an on-premises Entrust Certificate Authority for MDM-SCEP enrollment

See below to configure an on-premises Entrust Certificate Authority for using Certificate Enrollment Gateway with MDM-SCEP enrollment.

- [Mapping certificate definition policies to the MDM-SCEP certificate types](#)
- [Adding certificate types to Entrust Certificate Authority for MDM-SCEP enrollment](#)
- [Configuring Entrust Certificate Authority to allow server-generated keys for MDM-SCEP enrollment](#)

Mapping certificate definition policies to the MDM-SCEP certificate types

Map the Entrust Certificate Authority certificate definition policies to the certificate definitions added in [Adding certificate types to Entrust Certificate Authority for MDM-SCEP enrollment](#).

- [Mapping to the MDM SCEP Encryption certificate type](#)
- [Mapping to the MDM SCEP Signing certificate type](#)
- [Mapping to the MDM SCEP Signing and Encryption certificate type](#)
- [Mapping to the MDM SCEP Signing and Nonrepudation certificate type](#)

Mapping to the MDM SCEP Encryption certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the MDM SCEP Encryption certificate type.

To map a certificate definition policy to the MDM SCEP Encryption certificate type

1. Log into Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > MDM SCEP Encryption > Encryption_p10**.
3. In the **Certificate definition Policy** drop-down list, select **Encryption_P10 Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the MDM SCEP Signing certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the MDM SCEP Signing certificate type.

To map a certificate definition policy to the MDM SCEP Signing certificate type

1. Log into Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > MDM SCEP Signing > Verification_p10**.
3. In the **Certificate definition Policy** drop-down list, select **Verification_p10 Policy**.

4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the MDM SCEP Signing and Encryption certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the MDM SCEP Signing and Encryption certificate type.

To map a certificate definition policy to the MDM SCEP Signing and Encryption certificate type

1. Log into Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > MDM SCEP Signing and Encryption > Dual Usage**.
3. In the **Certificate definition Policy** drop-down list, select **Dual Usage Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the MDM SCEP Signing and Nonrepudiation certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the MDM SCEP Signing and Nonrepudiation certificate type.

To map a certificate definition policy to the MDM SCEP Signing and Nonrepudiation certificate type

1. Log into Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > MDM SCEP Signing and Nonrepudiation > Nonrepudiation**.
3. In the **Certificate definition Policy** drop-down list, select **Nonrepudiation Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Adding certificate types to Entrust Certificate Authority for MDM-SCEP enrollment

For MDM-SCEP enrollment, you must add the following certificate types to Entrust Certificate Authority.

- signing
- encryption
- dual usage (signing and encryption)
- non-repudiation

See below for the required steps.

To add MDM-SCEP certificate types

1. Log into Entrust Certificate Authority Administration.
2. Export the certificate specifications to a file by selecting **File > Certificate Specifications > Export**.
3. Open the certificate specifications file in a text editor.
4. Add the following lines to the `[Certificate Types]` section.

```
; -----  
; Certificate types to be used with MDM for SCEP Enrollments  
; -----  
ent_mdm_scep_sig=enterprise,MDM-SCEP Signing,MDM-SCEP Signing Certificate  
ent_mdm_scep_enc=enterprise,MDM-SCEP Encryption,MDM-SCEP Encryption Certificate  
ent_mdm_scep_sig_enc=enterprise,MDM-SCEP Signing and Encryption,MDM-SCEP  
Signing and Encryption Certificate
```

```
ent_mdm_scep_nonrep=enterprise,MDM-SCEP Signing and Nonrepudiation,MDM-SCEP  
Signing and Nonrepudiation Certificate  
; -----
```

5. Add the following lines to the `[Extension Definitions]` section.

```
; -----  
; Certificate definitions to be used with MDM for SCEP Enrollments  
; -----  
[ent_mdm_scep_sig Certificate Definitions]  
1=Verification_p10  
  
[ent_mdm_scep_sig Verification_p10 Extensions]  
keyusage=2.5.29.15,n,m,BitString,1  
  
[ent_mdm_scep_sig Advanced]  
noUserInDirectory=1  
  
[ent_mdm_scep_enc Certificate Definitions]  
1=Encryption_p10  
  
[ent_mdm_scep_enc Encryption_p10 Extensions]  
keyusage=2.5.29.15,n,m,BitString,001  
  
[ent_mdm_scep_enc Advanced]  
noUserInDirectory=1  
  
[ent_mdm_scep_sig_enc Certificate Definitions]  
1=Dual Usage  
  
[ent_mdm_scep_sig_enc Dual Usage Extensions]  
keyusage=2.5.29.15,n,m,BitString,101  
  
[ent_mdm_scep_sig_enc Advanced]  
noUserInDirectory=1  
  
[ent_mdm_scep_nonrep Certificate Definitions]  
1=Nonrepudiation  
  
[ent_mdm_scep_nonrep Nonrepudiation Extensions]  
keyusage=2.5.29.15,n,m,BitString,11  
  
[ent_mdm_scep_nonrep Advanced]  
noUserInDirectory=1  
; -----
```

6. Save and close the file.
7. Import the certificate specifications back into Entrust Certificate Authority. In Entrust Certificate Authority Administration, select **File > Certificate Specifications > Import**.

Configuring Entrust Certificate Authority to allow server-generated keys for MDM-SCEP enrollment

For MDM-SCEP enrollment with Certificate Enrollment Gateway, Entrust Certificate Authority must allow server-generated verification and nonrepudiation keys.

To allow server-generated verification and nonrepudiation keys

1. Edit the `entmgr.ini` settings file.
2. Set the following contents.

```
[policy]
allowServerGenVerCert=true
allowServerGenNonRepudCert=true
```

3. Save the changes.

Configuring an on-premises Entrust Certificate Authority for MDMWS enrollment

See below for configuring an on-premises Entrust Certificate Authority to use with Certificate Enrollment Gateway and MDM Web Service (MDMWS) enrollment.

- [Mapping certificate definition policies to the MDMWS P12 certificate types](#)
- [Creating certificate definition policies for MDMWS P12 certificate types](#)
- [Adding certificate types to Entrust Certificate Authority for MDMWS P12 enrollment](#)
- [Creating a client policy and role for MDMWS P12 enrollments](#)
- [Configuring Entrust Certificate Authority to allow server-generated keys for MDMWS enrollment](#)

Mapping certificate definition policies to the MDMWS P12 certificate types

Map the certificate definition policies created in [Creating certificate definition policies for MDMWS P12 certificate types](#).

- [Mapping to the MDMWS P12 Encryption certificate type](#)
- [Mapping to the MDMWS P12 Signing certificate type](#)
- [Mapping to the MDMWS P12 Signing and Encryption certificate type](#)
- [Mapping to the MDMWS P12 Signing and Nonrepudiation certificate type](#)

Mapping to the MDMWS P12 Encryption certificate type

See below to map Entrust Certificate Authority certificate definition policies to the MDMWS P12 Encryption certificate type.

To map a certificate definition policy to the MDMWS P12 Encryption certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > MDM P12 Encryption > Encryption**.
3. In the **Certificate definition Policy** drop-down list, select **Encryption P12 Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the MDMWS P12 Signing certificate type

See below to map Entrust Certificate Authority certificate definition policies to the MDMWS P12 Signing certificate type.

To map a certificate definition policy to the MDMWS P12 Signing certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > MDM P12 Signing > Verification**.
3. In the **Certificate definition Policy** drop-down list, select **Verification P12 Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the MDMWS P12 Signing and Encryption certificate type

See below to map Entrust Certificate Authority certificate definition policies to the MDMWS P12 Signing and Encryption certificate type.

To map a certificate definition policy to the MDMWS P12 Signing and Encryption certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > MDM P12 Signing and Encryption > Dual Usage**.
3. In the **Certificate definition Policy** drop-down list, select **Dual Usage P12 Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the MDMWS P12 Signing and Nonrepudiation certificate type

See below to map Entrust Certificate Authority certificate definition policies to the MDMWS P12 Signing and Nonrepudiation certificate type.

To map a certificate definition policy to the MDMWS P12 Signing and Nonrepudiation certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > MDM P12 Signing and Nonrepudiation > Nonrepudiation**.
3. In the **Certificate definition Policy** drop-down list, select **Nonrepudiation P12 Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Creating certificate definition policies for MDMWS P12 certificate types

In Entrust Certificate Authority, create new certificate definition policies for the certificate types added in [Adding certificate types to Entrust Certificate Authority for MDMWS P12 enrollment](#).

These new certificate definitions will allow server-generated keys and private key backup. You will later map them in [Mapping certificate definition policies to the MDMWS P12 certificate types](#).

- [Creating a Dual Usage P12 certificate definition policy](#)
- [Creating an Encryption P12 certificate definition policy](#)
- [Creating a Verification P12 certificate definition policy](#)
- [Creating a Nonrepudiation P12 certificate definition policy](#)

Creating a Dual Usage P12 certificate definition policy

See below to create a Dual Usage P12 certificate definition policy in Entrust Certificate Authority.

To create a Dual Usage P12 certificate definition policy

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, select **Security Policy > User Policies > Dual Usage Policy**.
3. Select **User Policies > Selected User Policy > Copy**. The **Copy User Policy** dialog box appears.
4. In the **Label** field, enter `Dual Usage P12 Policy`.

5. In the **Common name** field, enter `Dual Usage P12 Policy`.
6. Under **Policy Attributes**:
 - Select **Back up private key**.
 - Deselect **Generate key at client**.
7. Click **Apply**.
8. If prompted, authorize the operation.

Creating an Encryption P12 certificate definition policy

See below to create an Encryption P12 certificate definition policy in Entrust Certificate Authority.

To create an Encryption P12 certificate definition policy

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, select **Security Policy > User Policies > Encryption Policy**.
3. Select **User Policies > Selected User Policy > Copy**. The **Copy User Policy** dialog box appears.
4. In the **Label** field, enter `Encryption P12 Policy`.
5. In the **Common name** field, enter `Encryption P12 Policy`.
6. Under **Policy Attributes**:
 - Select **Back up private key**.
 - Deselect **Generate key at client**.
7. Click **Apply**.
8. If prompted, authorize the operation.

Creating a Verification P12 certificate definition policy

See below to create a Verification P12 certificate definition policy in Entrust Certificate Authority.

To create a Verification P12 certificate definition policy

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, select **Security Policy > User Policies > Verification Policy**.
3. Select **User Policies > Selected User Policy > Copy**. The **Copy User Policy** dialog box appears.
4. In the **Label** field, enter `Verification P12 Policy`.
5. In the **Common name** field, enter `Verification P12 Policy`.
6. Under **Policy Attributes**:
 - Select **Back up private key**.
 - Deselect **Generate key at client**.
7. Click **Apply**.
8. If prompted, authorize the operation.

Creating a Nonrepudiation P12 certificate definition policy

See below to create a Nonrepudiation P12 certificate definition policy in Entrust Certificate Authority.

To create a Nonrepudiation P12 certificate definition policy

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, select **Security Policy > User Policies > Encryption Policy**.
3. Select **User Policies > Selected User Policy > Copy**. The **Copy User Policy** dialog box appears.
4. In the **Label** field, enter `Nonrepudiation P12 Policy`.
5. In the **Common name** field, enter `Nonrepudiation P12 Policy`.
6. Under **Policy Attributes**:
 - Select **Back up private key**.
 - Deselect **Generate key at client**.

7. Click **Apply**.
8. If prompted, authorize the operation.

Adding certificate types to Entrust Certificate Authority for MDMWS P12 enrollment

For MDMWS PKCS #12 (P12) enrollment, you must add the following certificate types to Entrust Certificate Authority CA.

- signing
- encryption
- dual usage (signing and encryption)
- non-repudiation

See below for the required steps.

To add MDMWS P12 certificate types

1. Log in to Entrust Certificate Authority Administration.
2. Export the certificate specifications to a file by selecting **File > Certificate Specifications > Export**.
3. Open the certificate specifications file in a text editor.
4. Add the following lines to the `[Certificate Types]` section.

```
; -----  
; Certificate types to be used with MDM for P12 Enrollments  
; -----  
ent_mdm_p12_sig=enterprise,MDM P12 Signing,MDM P12 Signing Certificate  
ent_mdm_p12_enc=enterprise,MDM P12 Encryption,MDM P12 Encryption Certificate  
ent_mdm_p12_sig_enc=enterprise,MDM P12 Signing and Encryption,MDM P12 Signing  
and Encryption Certificate  
ent_mdm_p12_nonrep=enterprise,MDM P12 Signing and Nonrepudiation,MDM P12  
Signing and Nonrepudiation Certificate  
; -----
```

5. Add the following lines to the `[Extension Definitions]` section.

```
; -----  
; Certificate definitions to be used with MDM for P12 Enrollments  
; -----  
[ent_mdm_p12_sig Certificate Definitions]  
1=Verification  
  
[ent_mdm_p12_sig Verification Extensions]  
keyusage=2.5.29.15,n,m,BitString,1  
  
[ent_mdm_p12_sig Advanced]  
noUserInDirectory=1  
  
[ent_mdm_p12_enc Certificate Definitions]  
1=Encryption  
  
[ent_mdm_p12_enc Encryption Extensions]  
keyusage=2.5.29.15,n,m,BitString,001
```

```
[ent_mdm_p12_enc Advanced]
noUserInDirectory=1

[ent_mdm_p12_sig_enc Certificate Definitions]
1=Dual Usage

[ent_mdm_p12_sig_enc Dual Usage Extensions]
keyusage=2.5.29.15,n,m,BitString,101

[ent_mdm_p12_sig_enc Advanced]
noUserInDirectory=1

[ent_mdm_p12_nonrep Certificate Definitions]
1=Nonrepudiation

[ent_mdm_p12_nonrep Nonrepudiation Extensions]
keyusage=2.5.29.15,n,m,BitString,11

[ent_mdm_p12_nonrep Advanced]
noUserInDirectory=1
;-----
```

6. Save and close the file.
7. Import the certificate specifications back into Entrust Certificate Authority. In Entrust Certificate Authority Administration, select **File > Certificate Specifications > Import**.

Creating a client policy and role for MDMWS P12 enrollments

In Entrust Certificate Authority, create a client policy and a role to allow PKCS #12 enrollment through the MDMWS protocol.

- [Creating a client policy for MDMWS P12 enrollment](#)
- [Creating a role for MDMWS P12 enrollment](#)

Creating a client policy for MDMWS P12 enrollment

See below to create an Entrust Certificate Authority client policy for MDMWS P12 enrollment.

To create a client policy for MDMWS P12 enrollment

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, select **Security Policy > User Policies > End User Policy**.
3. Select **User Policies > Selected User Policy > Copy**. The Copy User Policy dialog box appears.
4. In the **Label** field, enter `End User P12 Policy`.
5. In the **Common name** field, enter `End User P12 Policy`.
6. Under **Policy Attributes**:
 - Select **Allow PKCS#12 Export**.
 - Deselect **All exportable**.
7. Click **Apply**.
8. If prompted, authorize the operation.

Creating a role for MDMWS P12 enrollment

See below to create an Entrust Certificate Authority role allowing PKCS #12 export.

! In CA Gateway, the CA profile Certificate Enrollment Gateway will use for MDMWS enrollment must assign this role to end users. The XAP administrator profile used to manage the CA profile must also have permission to administer this role.

To create a role for MDMWS P12 enrollment

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, select **Security Policy > Roles > End User**.
3. Select **User Policies > Selected Role > Copy**. A copy of the role appears at the bottom of the list of roles in the tree view, and the new role's properties appear in the right pane.
4. In the **Unique name** field, enter **End User P12**.
5. In the **User Policy** drop-down list, select **End User P12 Policy**.
6. Click **Apply**.
7. If prompted, authorize the operation.

Configuring Entrust Certificate Authority to allow server-generated keys for MDMWS enrollment

For MDMWS enrollment with Certificate Enrollment Gateway, Entrust Certificate Authority must allow server-generated verification and nonrepudiation keys.

To allow server-generated verification and nonrepudiation keys in Entrust Certificate Authority

1. Edit the `entmgr.ini` configuration file.
2. Add the following settings.

```
[policy]
allowServerGenVerCert=true
allowServerGenNonRepudCert=true
```

3. Save the changes.

Configuring an on-premises Entrust Certificate Authority for SCEP or Intune-SCEP enrollment

See below to configure an on-premises Entrust Certificate Authority for using Certificate Enrollment Gateway with SCEP or Intune-SCEP enrollment.

- [Adding certificate types to Entrust Certificate Authority for SCEP and Intune-SCEP enrollment](#)
- [Mapping certificate definition policies to the SCEP certificate types](#)

Adding certificate types to Entrust Certificate Authority for SCEP and Intune-SCEP enrollment

For SCEP and Intune-SCEP enrollment, you must add the following certificate types to the Entrust Certificate Authority:

- signing
- encryption
- dual usage (signing and encryption)
- non-repudiation

See below to add these types.

To add SCEP certificate types to Entrust Certificate Authority

1. Log in to Entrust Certificate Authority Administration.
2. Export the certificate specifications to a file by selecting **File > Certificate Specifications > Export**.
3. Open the certificate specifications file in a text editor.

4. Add the following lines to the `[Certificate Types]` section.

```
; -----  
; Certificate types to be used with SCEP  
; -----  
ent_scep_sig=enterprise,SCEP Signing,SCEP Signing Certificate  
ent_scep_enc=enterprise,SCEP Encryption,SCEP Encryption Certificate  
ent_scep_sig_enc=enterprise,SCEP Signing and Encryption,SCEP Signing and  
Encryption Certificate  
ent_scep_sig_nonrep=enterprise,SCEP Signing and Nonrepudiation,SCEP Signing and  
Nonrepudiation Certificate  
; -----
```

5. Add the following lines to the `[Extension Definitions]` section.

```
; -----  
; Certificate definitions to be used with SCEP  
; -----  
[ent_scep_sig Certificate Definitions]  
1=Verification_p10  
  
[ent_scep_sig Verification_p10 Extensions]  
keyusage=2.5.29.15,n,m,BitString,1  
  
[ent_scep_sig Advanced]  
noUserInDirectory=1  
  
[ent_scep_enc Certificate Definitions]  
1=Encryption_p10  
  
[ent_scep_enc Encryption_p10 Extensions]  
keyusage=2.5.29.15,n,m,BitString,001  
  
[ent_scep_enc Advanced]  
noUserInDirectory=1  
  
[ent_scep_sig_enc Certificate Definitions]  
1=Dual Usage  
  
[ent_scep_sig_enc Dual Usage Extensions]  
keyusage=2.5.29.15,n,m,BitString,101  
  
[ent_scep_sig_enc Advanced]  
noUserInDirectory=1  
  
[ent_scep_sig_nonrep Certificate Definitions]  
1=Nonrepudiation  
  
[ent_scep_sig_nonrep Nonrepudiation Extensions]  
keyusage=2.5.29.15,n,m,BitString,11
```

```
[ent_scep_sig_nonrep Advanced]
noUserInDirectory=1
; -----
```

6. Save and close the file.
7. Import the certificate specifications back into Entrust Certificate Authority. In Entrust Certificate Authority Administration, select **File > Certificate Specifications > Import**.

Mapping certificate definition policies to the SCEP certificate types

Map Entrust Certificate Authority certificate definition policies to the certificate types added in [Adding certificate types to Entrust Certificate Authority for SCEP and Intune-SCEP enrollment](#).

- [Mapping to the SCEP Encryption certificate type](#)
- [Mapping to the SCEP Signing certificate type](#)
- [Mapping to the SCEP Signing and Encryption certificate type](#)
- [Mapping to the SCEP Signing and Nonrepudation certificate type](#)

Mapping to the SCEP Encryption certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the SCEP Encryption certificate type.

To map a certificate definition policy to the SCEP Encryption certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > SCEP Encryption > Encryption_p10**.
3. In the **Certificate definition Policy** drop-down list, select **Encryption_P10 policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the SCEP Signing certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the SCEP Signing certificate type.

To map a certificate definition policy to the SCEP Signing certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > SCEP Signing > Verification_p10**.
3. In the **Certificate definition Policy** drop-down list, select **Verification_p10 Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the SCEP Signing and Encryption certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the SCEP Signing and Encryption certificate type.

To map a certificate definition policy to the SCEP Signing and Encryption certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > SCEP Signing and Encryption > Dual Usage**.
3. In the **Certificate definition Policy** drop-down list, select **Dual Usage Policy**.
4. Click **Apply**.

5. If prompted, authorize the operation.

Mapping to the SCEP Signing and Nonrepudiation certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the SCEP Signing and Nonrepudiation certificate type.

To map a certificate definition policy to the SCEP Signing and Nonrepudiation certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > SCEP Signing and Nonrepudiation > Nonrepudiation**.
3. In the **Certificate definition Policy** drop-down list, select **Nonrepudiation Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Configuring an on-premises Entrust Certificate Authority for WSTEP enrollment

See below to configure an on-premises Entrust Certificate Authority for using Certificate Enrollment Gateway with WSTEP enrollment.

- [Mapping certificate definition policies to the WSTEP certificate types](#)
- [Adding certificate types to Entrust Certificate Authority for WSTEP enrollment](#)
- [Configuring certificates issued by Entrust Certificate Authority for WSTEP enrollment](#)

Mapping certificate definition policies to the WSTEP certificate types

Map the Entrust Certificate Authority certificate definition policies to the ones added in [Adding certificate types to Entrust Certificate Authority for WSTEP enrollment](#).

- [Mapping to the to the WSTEP Encryption certificate type](#)
- [Mapping to the to the WSTEP Signing certificate type](#)
- [Mapping to the WSTEP Signing and Encryption certificate type](#)
- [Mapping to the WSTEP Signing and Nonrepudiation certificate type](#)

Mapping to the to the WSTEP Encryption certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the WSTEP Encryption certificate type.

To map a certificate definition policy to the WSTEP Encryption certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > WSTEP Encryption (WSTEP Encryption Certificate) > Encryption_p10**.
3. In the **Certificate definition Policy** drop-down list, select **Encryption_P10 policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the to the WSTEP Signing certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the WSTEP Signing certificate type.

To map a certificate definition policy to the WSTEP Signing certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > WSTEP Signing (WSTEP Signing Certificate) > Verification_P10**.

3. In the **Certificate definition Policy** drop-down list, select **Verification_P10 policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the WSTEP Signing and Encryption certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the WSTEP Signing and Encryption certificate type.

To map a certificate definition policy to the WSTEP Signing and Encryption certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > WSTEP Signing and Encryption (WSTEP Signing and Encryption Certificate) > Dual Usage**.
3. In the **Certificate definition Policy** drop-down list, select **Dual Usage Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the WSTEP Signing and Nonrepudiation certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the WSTEP Signing and Nonrepudiation certificate type.

To map a certificate definition policy to the WSTEP Signing and Nonrepudiation certificate type

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > WSTEP Signing and Nonrepudiation (WSTEP Signing and Nonrepudiation Certificate) > Nonrepudiation**.
3. In the **Certificate definition Policy** drop-down list, select **Nonrepudiation Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Adding certificate types to Entrust Certificate Authority for WSTEP enrollment

For WSTEP enrollment, you must add the following certificate types to Entrust Certificate Authority.

- signing
- encryption
- dual usage (signing and encryption)
- non-repudiation

See below for the required steps.

To add WSTEP certificate types to Entrust Certificate Authority

1. Log in to Entrust Certificate Authority Administration.
2. Export the certificate specifications to a file by selecting **File > Certificate Specifications > Export**.
3. Open the certificate specifications file in a text editor.
4. Add the following lines to the `[Certificate Types]` section.

```
; -----  
; Certificate types to be used with WSTEP  
; -----  
ent_wstep_sig=enterprise,WSTEP Signing,WSTEP Signing Certificate  
ent_wstep_enc=enterprise,WSTEP Encryption,WSTEP Encryption Certificate
```

```
ent_wstep_sig_enc=enterprise,WSTEP Signing and Encryption,WSTEP Signing and  
Encryption Certificate  
ent_wstep_sig_nonrep=enterprise,WSTEP Signing and Nonrepudiation,WSTEP Signing  
and Nonrepudiation Certificate  
; -----
```

5. Add the following lines to the [\[Extension Definitions\]](#) section.

```
; -----  
; Certificate definitions to be used with WSTEP  
; -----  
  
[ent_wstep_sig Certificate Definitions]  
1=Verification  
  
[ent_wstep_sig Verification Extensions]  
keyusage=2.5.29.15,n,m,BitString,1  
  
[ent_wstep_sig Advanced]  
noUserInDirectory=1  
  
[ent_wstep_enc Certificate Definitions]  
1=Encryption  
  
[ent_wstep_enc Encryption Extensions]  
keyusage=2.5.29.15,n,m,BitString,001  
  
[ent_wstep_enc Advanced]  
noUserInDirectory=1  
  
[ent_wstep_sig_enc Certificate Definitions]  
1=Dual Usage  
  
[ent_wstep_sig_enc Dual Usage Extensions]  
keyusage=2.5.29.15,n,m,BitString,101  
  
[ent_wstep_sig_enc Advanced]  
noUserInDirectory=1  
  
[ent_wstep_sig_nonrep Certificate Definitions]  
1=Nonrepudiation  
  
[ent_wstep_sig_nonrep Nonrepudiation Extensions]  
keyusage=2.5.29.15,n,m,BitString,11  
  
[ent_wstep_sig_nonrep Advanced]  
noUserInDirectory=1
```

6. Save and close the file.
7. Import the certificate specifications back into Entrust Certificate Authority. In Entrust Certificate Authority Administration, select **File > Certificate Specifications > Import**.

Configuring certificates issued by Entrust Certificate Authority for WSTEP enrollment

When using secure LDAP (LDAPS) for WSTEP integration, all TLS certificates issued by Entrust Certificate Authority must include a valid HTTP CDP (CRL Distribution Point).

Issuing TLS certificates for Certificate Enrollment Gateway

Certificate Enrollment Gateway requires a TLS certificate to secure incoming connections over HTTPS. This TLS certificate must be issued and installed into CSP 1.0.0 before Certificate Enrollment Gateway can accept any enrollment requests over HTTPS.

You must issue the TLS certificate when deploying Certificate Enrollment Gateway for the first time. You must also renew the certificate before it expires so Certificate Enrollment Gateway can continue accepting enrollment requests.

- [Installing the Certificate Enrollment Gateway certificate chain into CSP 1.0.0](#)
- [Building a TLS certificate chain for the Certificate Enrollment Gateway certificate](#)
- [Issuing TLS certificates with an on-premises CA](#)
- [Issuing TLS certificates with Entrust PKI as a Service](#)
- [Creating a CSR for the Certificate Enrollment Gateway certificate](#)

Installing the Certificate Enrollment Gateway certificate chain into CSP 1.0.0

After building the TLS certificate chain for the Certificate Enrollment Gateway certificate, you can install the certificate into CSP 1.0.0. To install the certificate, CSP 1.0.0 requires the following:

- A single file containing the TLS certificate chain, from the TLS certificate to the root CA. You created this file earlier in [Building a TLS certificate chain for the Certificate Enrollment Gateway certificate](#).
- The private key for the certificate. The private key was generated when you created the CSR for the certificate.

Run the following command on the CSP 1.0.0 node where the Certificate Enrollment Gateway certificate chain is located

```
sudo clusterctl certificate --cert <cert> --key <key>
```

See below for each option.

Parameter	Description
<cert>	The path of a PEM-formatted file containing the entire TLS certificate chain.
<key>	The path of a PEM-formatted file containing the private key for TLS.

For example:

```
sudo clusterctl certificate --cert /home/sysadmin/ceg/corporate.example.com/tls.crt  
--key /home/sysadmin/ceg/corporate.example.com/tls.key
```

Building a TLS certificate chain for the Certificate Enrollment Gateway certificate

CSP 1.0.0 requires the full TLS certificate chain for the Certificate Enrollment Gateway certificate, from the TLS certificate up to the root CA. You must combine all certificates in the TLS certificate chain into one file as described in the following procedure.

To combine the Certificate Enrollment Gateway certificate and CA certificates into a single file

1. Create a new text file.
2. Copy the contents of the Certificate Enrollment Gateway certificate (including BEGIN CERTIFICATE and END CERTIFICATE lines) into the new text file.
3. At the end of the new text file, copy the contents of each CA certificate in the chain (including BEGIN CERTIFICATE and END CERTIFICATE lines), in order from the Issuing CA certificate to the Root CA certificate. For example:

```
-----BEGIN CERTIFICATE-----
<TLS server certificate in Base64 encoding>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Issuing CA certificate in Base64 encoding>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA certificate in Base64 encoding>
-----END CERTIFICATE-----
```

For Entrust PKI as a Service, the Issuing CA and Root CA are different CAs. For an on-premises CA, the Issuing CA may be the root CA. If the issuing CA is the root CA, the file would contain only the TLS certificate and the root CA.

4. The text file should look similar to the following:

```
-----BEGIN CERTIFICATE-----
MIIDqQYJKoZIhvcNAQcCoIIDmJCCA5YCAQExADALBgkqhkiG9w0BBwGggN...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDejCCAmKgAwIBAgIQQ8e7ock59Y21Mtcy7rGJUDANBgkqhkiG9w0BAQs...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIQ0EgRW50cnkwHhcNMjMwMjA4MTUxNzEwWmcNMzMwMjA4MTU0NzEwWjAyM...
-----END CERTIFICATE-----
```

5. Save the file. It is recommended that you save the file with a `.pem` or `.crt` extension. For example, `tlscertchain.pem`.

After building the TLS certificate chain, proceed to [Installing the Certificate Enrollment Gateway certificate chain into CSP 1.0.0](#).

Issuing TLS certificates with an on-premises CA

If you are using Certificate Enrollment Gateway with an on-premises CA, you can use native Linux tools to create a CSR (certificate signing request) for the Certificate Enrollment Gateway certificate, then use your existing CA tools to process the CSR and create the certificate.

- [Obtaining the CA certificate chain](#)
- [Processing the CSR with an on-premises CA](#)
- [Creating or recovering a user account in an on-premises CA](#)

Obtaining the CA certificate chain

CSP 1.0.0 requires the full TLS certificate chain for the Certificate Enrollment Gateway certificate, from the TLS certificate up to the root CA. Obtain all CA certificates in the CA certificate chain, from the issuing CA to the root CA. (In your environment, the issuing CA may be the root CA.) The CA certificates must be in PEM format.

After obtaining all CA certificates in the certificate chain, proceed to [Building a TLS certificate chain for the Certificate Enrollment Gateway certificate](#).

Processing the CSR with an on-premises CA

You can process the CSR using the Profile Creation Utility. The Profile Creation Utility is a command line utility that can create and manage Entrust profiles for an on-premises Entrust Certificate Authority. You can use the Profile Creation Utility to process Certificate Signing Requests (CSRs) and generate certificates. The Profile Creation Utility is available as a separate software download for Entrust CA Gateway.

- [Installing the Profile Creation Utility](#)
- [Processing the CSR](#)



When processing a CSR, the Profile Creation Utility will prompt you for the certificate definition required for the certificate. In Entrust Certificate Authority, that certificate definition for the user's certificate type must be assigned a certificate definition policy (user policy). If no certificate definition policy is assigned to the certificate definition you specify, an error will occur and the Profile Creation Utility will fail to process the CSR.

Installing the Profile Creation Utility

See below to download and install the Profile Creation Utility

To install the Profile Creation Utility

1. Install a Java Development Kit (JDK) and set the `JAVA_HOME` environment variable.
2. Log in to Entrust TrustedCare (<https://trustedcare.entrust.com>).
3. Go to **PKI > Authority > CA Gateway** and click the latest version of the product.
4. Under software downloads, download the Profile Creation Utility for your preferred operating system:
 - `cagw-profilecreationutility-linux64-version.zip` for Linux 64-bit.
 - `cagw-profilecreationutility-win64-version.zip` for Windows 64-bit.
5. Extract the file contents of the ZIP file to a location on the computer.

Processing the CSR


See below to process the CSR with the Process Creation Utility.

To process the CSR

1. Obtain the CSR file along with the reference number and authorization code associated with the Entrust Certificate Authority user account.
When you create a user in Entrust Certificate Authority or set a user for key recovery, Entrust Certificate Authority generates a reference number and authorization code. You need these activation codes to process the CSR.

2. To process the CSR, the Profile Creation Utility requires an Entrust desktop profile (EPF file). the role associated with the profile requires the following permissions:
 - Under the **Certificates** permission category: permissions to administer the certificate category and certificate type of the certificate being issued.
 - Under the **Groups** permission category: **View** and permission to administer the group associated with the Entrust Certificate Authority user being issued the certificate.
 - Under the **Roles** permission category: **View** and permission to administer the role associated with the Entrust Certificate Authority user being issued the certificate.
 - Under the **Searchbase** permission category: **View** and permission to administer the searchbase associated with the Entrust Certificate Authority user being issued the certificate.
 - Under the **Users** permission category: **View** and **Perform PKIX** requests. Obtain the Entrust desktop profile (EPF file) from a Entrust Certificate Authority administrator.
3. Navigate to the directory containing the Profile Creation Utility.
4. Run the following command:
 - On Windows, run `pcu.bat`.
 - On Linux, run `pcu`.
5. The Profile Creation Utility main menu appears:

```
Main Menu
1. Exit
2. Help
3. Create Entrust profile
4. Recover Entrust profile
5. Inspect Entrust profile (read only)
6. Inspect and update Entrust profile (read/write)
7. Create Server Login credentials
8. Create PKCS #12 file (Entrust Certificate Authority)
9. Recover PKCS #12 file (Entrust Certificate Authority)
10. Create PKCS #12 file (3rdParty)
11. Update PKCS #12 file (3rdParty)
12. Process PKCS #10 Certificate Signing Request (CSR)
13. Generate/Process Certificate Signing Request on HSM (3rdParty)
14. Change password
Select an operation [3]:
```

 To return to the main menu at any time, enter a period (.). For help about using the Profile Creating Utility, enter 2 in the main menu.

Enter 12 to process the CSR.

6. The following prompt appears:

```
Take settings from an existing entrust.ini file (y/n) [y]:
```

- To use Certificate Authority (CA) connection settings from an existing `entrust.ini` file, enter `y`.
 - To provide CA connection settings manually, enter `n`.
7. If you chose to use an existing `entrust.ini` file, you are prompted to enter the full path to the `entrust.ini` file:

Enter full path to entrust.ini file:

Enter the full path and file name of the `entrust.ini` file.

8. If you chose to enter CA connections setting manually, the following prompts appear:
 - a. You are prompted to provide the host name (or IP address) and port of the CA server:

Enter the CA hostname or IP address and port in the form name:port:

Enter the host name (or IPv4 address) and CMP port of the server hosting the CA in format of `<hostname>:<port>`. If you omit the port number, it defaults to 829.

- b. You are prompted to provide the host name (or IP address) and port of the directory server:

Enter the directory hostname or IP address and port in the form name:port:

Enter the host name (or IPv4 address) and LDAP port of the server hosting the directory in format of `<hostname>:<port>`. The name or address defaults to the same value that you entered for the CA address. If you omit the port number, it defaults to 389.

9. You are prompted for the full path to an administration profile:

Enter full path to administration profile:

Enter the full path and file name of an administration profile.

10. You are prompted to enter the profile password:

Enter profile password:

Enter the profile password.

11. You are asked if the CSR is authenticated:

Is the CSR authenticated? (y/n)? [n]:

Enter `n`. The CSR is not authenticated.

12. You are prompted for the full path to the CSR:

Enter full path to CSR:

Enter the full path and file name of the CSR.

13. You are prompted to enter the reference number for the CSR:

Enter reference number:

Enter the reference number you recorded earlier.

14. You are prompted to enter the authorization code for the CSR:

Enter authorization code:

Enter the authorization code you recorded earlier.

15. You are prompted to enter a file name for the certificate:

Enter certificate file to create:

Enter the full path and file name for the certificate file.

16. You are prompted to enter the certificate definition required for the certificate:

Enter certificate definition required [Verification]:

Enter the certificate definition required for the certificate, such as Verification or Dual Usage.

17. The Profile Creation Utility processes the certificate. If the operation is successful, Entrust Certificate Authority issues a certificate and the Profile Creation Utility writes the certificate to a file.

```
Requesting certificate from Security Manager...
Obtained new certificate with serial number 1340207625 from issuer
o=Example,c=US
Certificate written to c:\new_certificate.cer
```

18. After processing the CSR and obtaining the certificate, proceed to [Obtaining the CA certificate chain](#).

Creating or recovering a user account in an on-premises CA

To issue a certificate for Certificate Enrollment Gateway, a user account for the certificate must exist in your on-premises CA. You must create a user account to issue the initial Certificate Enrollment Gateway certificate. You must recover (reset) the user account to renew the Certificate Enrollment Gateway certificate.

To manually create or recover (reset) a user account, you can use an administration application such as:

- Entrust Certificate Authority Administration
- User Management Service (Entrust Administration Services)

When creating a new user account:

- It is recommended that you configure the user's name (using the directory naming attributes) to be the fully qualified domain name of the server hosting CSP 1.0.0. For example, `example.com`.
- Select a 1-key-pair certificate type with a Dual Usage certificate definition that includes an Extended Key Usage extension with server authentication and client authentication. The certificate definition should also be assigned a certificate definition policy. For example, the Enterprise Machine (ent_machine) certificate type.
- For the Subject Alternative Name (SubjectAltName) extension, add a DNS Name component for each DNS name that may be used by the CSP 1.0.0 cluster.

For information about creating or recovering user accounts, see the documentation for the client application.

Issuing TLS certificates with Entrust PKI as a Service

If you are using Certificate Enrollment Gateway with Entrust PKI as a Service, you can use native Linux tools to create a CSR (certificate signing request) for the Certificate Enrollment Gateway certificate, then process the CSR using Entrust PKI as a Service to create a certificate.

- [Downloading the CA certificate chain from Entrust PKI as a Service](#)
- [Processing the CSR with Entrust PKI as a Service](#)

Downloading the CA certificate chain from Entrust PKI as a Service

Cryptographic Security Platform 1.0.0 requires the full TLS certificate chain for the Certificate Enrollment Gateway certificate, from the TLS certificate up to the root CA. Download all CA certificates in the CA certificate chain from Entrust PKI as a Service, from the Issuing CA to the root CA.

To download CA certificates from Entrust PKI as a Service

1. Log in the Entrust Certificate Services interface.
2. Select **Administration > PKIaaS Management**.
A list of private CAs appear.
3. For each CA in the TLS certificate chain, from the Issuing CA to the Root CA:
 - a. Select the CA.
 - b. Click **Download certificate**.

Processing the CSR with Entrust PKI as a Service

After creating the certificate signing request (CSR) for the Certificate Enrollment Gateway certificate, you can submit the CSR to an Issuing CA in Entrust PKI as a Service. The Issuing CA will process the CSR and generate the certificate.

To submit the CSR to Entrust PKI as a Service and obtain the TLS certificate

1. Log in the Entrust Certificate Services interface.
2. Select **Create > PKIaaS**.
The Select **Certificate Authority** pane appears.
3. From the **Certificate Authority** drop-down list, select the CA you want to issue the TLS certificate.
4. From the **Certificate Profile** drop-down list, select the certificate profile you want to use for the TLS certificate. The certificate profile must include Digital Signature for TLS certificates.
5. Click **Next**.
The **Certificate Details** pane appears.
6. In the **Subject DN** field, enter a value for the certificate's subject DN. The value should be the DNS name of the server hosting CSP 1.0.0 – for example:

```
cn=example.com
```

7. For **Certificate Expiry**, provide an expiry date for TLS certificate. It is recommended that the TLS certificate be valid for 1 year or less.
8. Under **Subject Alternative Names**, add one or more DNS Name components to the Subject Alternative Name (subjectAltName) extension in the certificate. The subjectAltName extension must have a DNS Name component for each DNS name that may be used by the CSP 1.0.0 cluster.
To add a DNS Name component the Subject Alternative Name extension:
 - a. For **SAN type**, select **DNS Name**.
 - b. In the **Value** field, enter a DNS name that may be used by the server.
 - c. Click **Add** to add the DNS Name component to the Subject Alternative Name extension.
The component is added to the list of components in the Subject Alternative Name extension
 - d. To remove a component from the Subject Alternative Name extension, click **Remove** next to the extension that you want to remove.
9. Copy the contents of the CSR you generated earlier, and paste the contents into the **Certificate Signing Request (CSR)** text box.

10. Click **Submit**.
If the certificate is generated successfully, a success message appears.
11. Click **Download the newly created certificate** to download the TLS certificate.

Creating a CSR for the Certificate Enrollment Gateway certificate

Certificate Enrollment Gateway requires a TLS certificate to secure incoming connections over HTTPS. To create a key pair and CSR for this certificate, run the following command in any CSP 1.0.0 cluster node.

```
openssl req -nodes -newkey rsa:2048 -keyout <keyout> -out <csr> -subj "<subject>"
```

See below for each option.


Parameter	Description
<keyout>	The file path for the private key. You will need this file later to install the certificate in CSP 1.0.0.
<csr>	The file path for the CSR.
<subject>	The subject for the CSR.

For example:

```
openssl req -nodes -newkey rsa:2048 -keyout /home/sysadmin/ceg/private.key -out /home/sysadmin/ceg/csr.txt -subj "/CN=example.com"
```

Configuring and deploying Certificate Enrollment Gateway

See below for configuring and deploying Certificate Enrollment Gateway with the Management Console.

-  Repeat the following steps each time a configuration update is required. Do not forget to click **Deploy** to make the changes effective.

To configure and deploy Certificate Enrollment Gateway with the Management Console

1. Open the following URL in a Web browser.

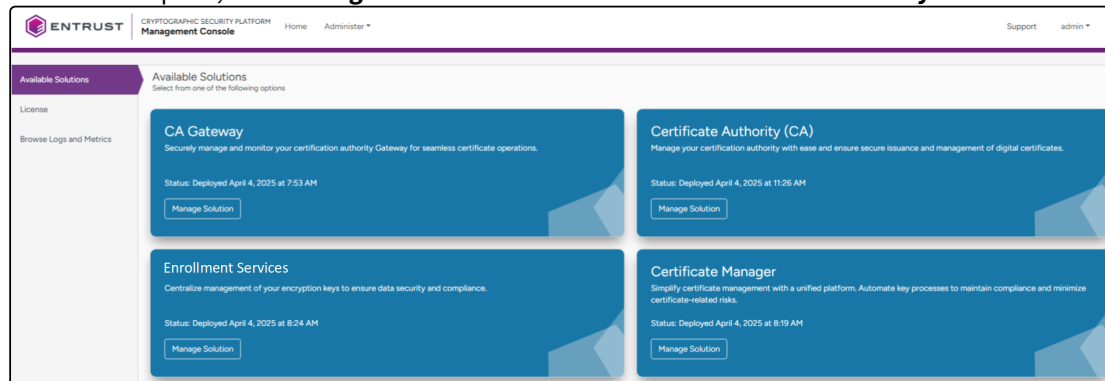
```
https://<machine>/management-console
```

Where **<machine>** is the IP address or domain name of the machine hosting Cryptographic Security Platform.

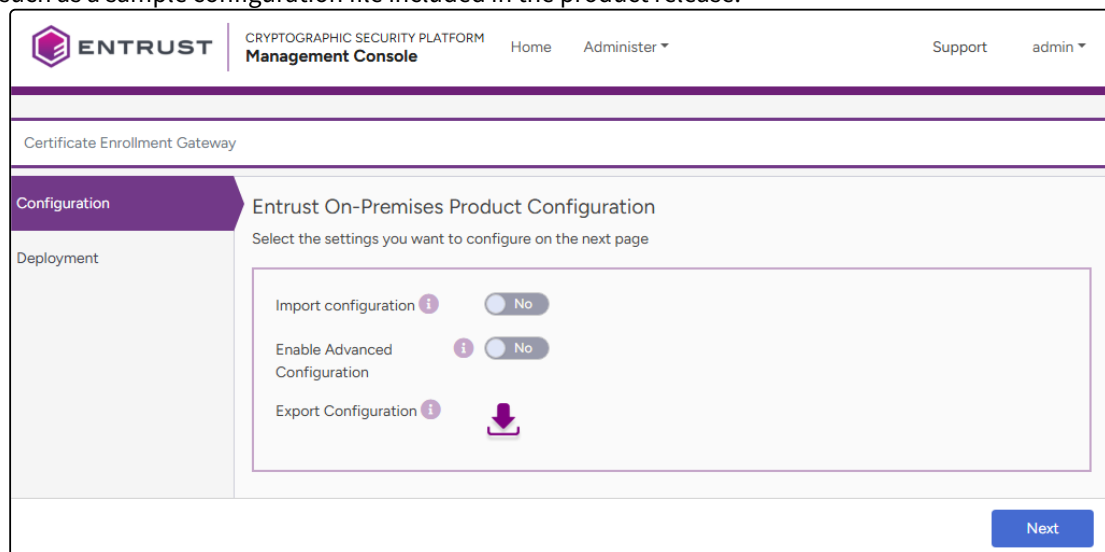
2. Log into the Management Console a user belonging to a role with Certificate Enrollment Gateway management permissions – for example, the initial **admin** administrator user.

-  See [Starting up the Management Console](#) for how to manage users and roles.

- In the content pane, click **Manage Solution** under **Certificate Enrollment Gateway**.



- Activate the **Import configuration** toggle switch if you want to import configuration settings from a file, such as a sample configuration file included in the product release.



- Click **Next**.
- Configure the solution settings described in the following sections.
 - WSTEP
 - SCEP
 - Intune
 - MDMWS
 - ACMEv2
 - CAGW
 - Tenants
- Click **Validate** to validate the configured settings.
- Correct any detected configuration error until the **Validate** option displays no warnings.
- Optionally, click the **Download** button to export the current configuration. You can later import this configuration using the already mentioned **Import configuration** toggle switch.
- Click **Submit** and wait while Cryptographic Security Platform uploads the configuration and any attached file, such as a P12 file with authentication credentials.
- Click **Deploy**.

WSTEP

Select the **WSTEP** tab of the **Configuration** page to configure WSTEP enrollment.

- [Active Directory Domains](#)
- [WSTEP CAGW Settings](#)
- [Enable WSTEP](#)

Active Directory Domains

Configure the following settings for each connection with Active Directory domains.

- [Authentication Type for LDAP and Global Catalog Connections](#)
- [Enable WSTEP Kerberos Authentication for WSTEP Enrollment](#)
- [Computer Name](#)
- [Domain Name](#)

Authentication Type for LDAP and Global Catalog Connections

This authentication method for LDAP and Global Catalog connections to Active Directory. Select:

- **Username/Password** for username and password authentication. This option requires configuring the [LDAP Connection Settings](#).
- **Kerberos (Required for Cross-Forest Enrollments)** for Kerberos authentication. This option requires configuring the [LDAP Connection Settings](#) and the [Kerberos LDAP Referrals](#).

Mandatory: Yes.

Kerberos LDAP Referrals

Configure the following settings when [Authentication Type for LDAP and Global Catalog Connections](#) is **Kerberos (Required for Cross-Forest Enrollments)**.

- [Principal](#)
- [Keytab File](#)
- [Kerberos Configuration File](#)
- [Maximum LDAP Referrals](#)

Principal

The Kerberos principal that the CEG Service will use to authenticate to each Active Directory forest for cross-forest WSTEP enrollment. You must use the same Kerberos principal to generate the keytab file used for Kerberos v5 LDAP referrals.

The value must be a string with the following syntax:

```
HTTP/<ceg-fqdn>
```

Where `<ceg-fqdn>` is the fully qualified domain name (FQDN) of the server hosting Certificate Enrollment Gateway. For example:

```
HTTP/cegserver1.example.com
```

Mandatory: Only when cross-forest trust must be supported for WSTEP enrollment with Kerberos authentication.

Keytab File

A keytab file for the domain controller. The keytab file is used to authenticate incoming WSTEP requests.

Mandatory: Only when cross-forest trust must be supported for WSTEP enrollment with Kerberos authentication.

Kerberos Configuration File

A Kerberos configuration file for Kerberos V5 LDAP Referrals.

Mandatory: Only when cross-forest trust must be supported for WSTEP enrollment with Kerberos authentication.

Maximum LDAP Referrals

The maximum number of Kerberos V5 LDAP Referrals to follow. The value must be an integer from 0 to 10.

Mandatory: Yes.

LDAP Connection Settings

Configure the LDAP connection to Active Directory.

- [Enable LDAPS](#)
- [CA Certificates File Format \(P12 or PEM\)](#)
- [WSTEP LDAPS Trusted CA Certificates File \(PEM\)](#)
- [WSTEP LDAPS Truststore File \(P12\)](#)
- [LDAPS Truststore Password](#)
- [LDAP Port](#)
- [Global Catalog Port](#)
- [LDAP Connect Timeout](#)
- [LDAP Read Timeout](#)
- [Username](#)
- [Password](#)

Enable LDAPS

Select **Yes** to use LDAPS (secure LDAP) for all connections to Active Directory; select **No** to use LDAP for connections to Active Directory.

Mandatory: No. This setting defaults to **No**.

CA Certificates File Format (P12 or PEM)

The format of the file containing the CA certificate chain for the Active Directory server certificate. Select;

- **P12** if the file is a P12 truststore.
- **PEM** if the file is a PEM-formatted file.

Mandatory: When **Enable LDAPS** is **Yes**.

WSTEP LDAPS Trusted CA Certificates File (PEM)

A PEM-formatted file that contains the CA certificate chain for Active Directory's server certificate.

Mandatory: When **CA Certificates File Format (P12 or PEM)** is **PEM**.

WSTEP LDAPS Truststore File (P12)

An LDAPS Truststore file (P12 file) that contains the CA certificate chain for Active Directory's server certificate.

Mandatory: When **CA Certificates File Format (P12 or PEM)** is **P12**.

LDAPS Truststore Password

The password of the LDAPS Truststore file for LDAPS authentication to Active Directory.

Mandatory: When **CA Certificates File Format (P12 or PEM)** is **P12**.

LDAP Port

The LDAP or LDAPS port to connect to Active Directory.

Mandatory: No. This setting defaults to port 389 (LDAP) or 636 (LDAPS).

Global Catalog Port

The port for connecting with the global catalog in Active Directory.

Mandatory: No. This setting defaults to port 3268 (LDAP) or 3269 (LDAPS).

LDAP Connect Timeout

The number of milliseconds Certificate Enrollment Gateway will wait for Active Directory to establish a connection before aborting the connection attempt.

Mandatory: No. This setting defaults to 30000 (30 seconds).

LDAP Read Timeout

The number of milliseconds Certificate Enrollment Gateway will wait for Active Directory to respond to an LDAP request before aborting the read attempt.

Mandatory: No. This setting defaults to 30000 (30 seconds).

Username

The username for WSTEP to connect with the Active Directory domain. It can be the username of any Active Directory Domain user.

This domain user account must be a service logon account without any special permissions. This service account will be used for read-only access with LDAP and Global Catalog.

Mandatory: When [Authentication Type for LDAP and Global Catalog Connections](#) is **Username/Password**.

Password

The password for WSTEP to connect to Active Directory.

Mandatory: When [Authentication Type for LDAP and Global Catalog Connections](#) is **Username/Password**.

Enable WSTEP Kerberos Authentication for WSTEP Enrollment

Select **Yes** to enable Kerberos authentication for WSTEP enrollment and configure the following settings.

- [Principal](#)
- [Keytab File](#)
- [Permit Deprecated Algorithms \(3DES and RC4\)](#)

Select **No** to disable Kerberos authentication for WSTEP enrollment.

Mandatory: No. This setting defaults to **No**.

Principal

The Kerberos principal that the CEG Service will use to authenticate to each Active Directory forest for cross-forest WSTEP enrollment. You must use the same Kerberos principal to generate the keytab file used for Kerberos v5 LDAP referrals.

The value must be a string with the following syntax:

HTTP/<ceg-fqdn>

Mandatory: When cross-forest trust must be supported for WSTEP enrollment with Kerberos authentication.

Keytab File

The name of the Kerberos keytab file for the domain controller. The keytab file is used to authenticate incoming WSTEP requests.

Mandatory: When cross-forest trust must be supported for WSTEP enrollment with Kerberos authentication.

Permit Deprecated Algorithms (3DES and RC4)

Check this box to permit the 3DES and RC4 deprecated Kerberos algorithms. Uncheck this box to reject these algorithms.

Mandatory: No. This box is unchecked by default.

Computer Name

The fully qualified domain name (FQDN) of the Active Directory domain controller. For example:

activedirectory.example.com

If this setting is configured, Certificate Enrollment Gateway will use this FQDN for LDAP and Global Catalog connections.

If this setting is not configured, Certificate Enrollment Gateway will use DNS to find the Active Directory domain controller from the domain name specified in the WSTEP request.

Mandatory: No.

Domain Name

The Active Directory domain name. The Active Directory domain name is the root domain naming context of the Active Directory. For example:

example.com

To retrieve the Active Directory domain name, run the following PowerShell command:

```
([ADSI]"LDAP://RootDSE").rootDomainNamingContext -replace '^DC=', '' -replace '.DC=', ''
```

You can specify multiple domain names by specifying multiple **Domain Name** settings. This setting contains child settings that configure the connection to the Active Directory domain.

Mandatory: Yes.

WSTEP CAGW Settings

Configure the following settings for each enrollment connection with CA Gateway.

- [CAGW CA ID](#)
- [Parent DN](#)

- [CAGW Profile ID for Digital Signature](#)
- [CAGW Profile ID for Key Encipherment](#)
- [CAGW Profile ID for Digital Signature and Key Encipherment](#)
- [CAGW Profile ID for Digital Signature and Nonrepudiation](#)
- [Certificate Templates](#)

Certificate Templates

The required mappings for each certificate template.

- For **Value**, enter the name of a Profile ID defined in CA Gateway for issuing the certificate.
- For **Value**, enter the name of a Profile ID defined in CA Gateway for issuing the certificate.

Note that:

- For machines, the **Subject name** in the certificate template must be **Common name** or **DNS name**.
- For users, the **Subject name** in the certificate template must be **Common name**.

See [Subject Name tab](#) for information on configuring the **Subject name** in the Windows certificate template.

Mandatory: No.

CAGW Profile ID for Digital Signature and Nonrepudiation

The unique ID defined in CA Gateway for the WSTEP signing and nonrepudiation certificate profile.

Mandatory: Yes.

CAGW Profile ID for Digital Signature and Key Encipherment

This unique ID defined in CA Gateway for the WSTEP signing and encryption certificate profiles.

Mandatory: Yes.

CAGW Profile ID for Key Encipherment

The unique ID defined in CA Gateway for the WSTEP encryption certificate profile.

Mandatory: Yes.

CAGW Profile ID for Digital Signature

The unique ID defined in CA Gateway for the WSTEP signing certificate profile.

Mandatory: Yes.

Parent DN

The parent DN (distinguished name) for certificates issued by the CEG WSTEP service. The selected value is appended to incoming Subject DNs.

CA Type	Parent DN
Entrust Certificate Authority	A known searchbase defined in Entrust Certificate Authority.
Entrust PKI as a Service	An absent parent DN, or a user-defined or custom parent DN.

Examples:

ou=Devices, o=My Company, c=US

cn=Users, ou=North America, o=My Company, c=GB

Mandatory: No.

CAGW CA ID

The CA identifier (CA ID) in CA Gateway of the CA for WSTEP enrollment.

Mandatory: Yes.

Enable WSTEP

Select **Yes** to enable the WSTEP protocol; **No** to disable the WSTEP protocol.

Mandatory: No. This setting defaults to **No**.

SCEP

Select the **SCEP** tab of the **Configuration** page to configure SCEP enrollment.

- [Enable SCEP](#)
- [SCEP Enrollment Service Configurations](#)

Enable SCEP

Select **Yes** to enable the SCEP protocol; **No** to disable the SCEP protocol.

Mandatory: No. This setting defaults to **No**.


SCEP Enrollment Service Configurations

Configure the following settings for each **SCEP Enrollment Service Configuration**.

- [CAGW CA ID](#)
- [SCEP Challenge Password](#)
- [Insecure SCEP \(Permit an empty challenge password\)](#)
- [Revoke Old Certificate on Renewal](#)

Revoke Old Certificate on Renewal

Check this box to revoke the old certificate with the "Superseded" reason after issuing the new certificate. Uncheck this box for the old certificate to be valid after the new certificate is issued.

 This setting only applies to requests sent through the SCEP Service. It does not apply to requests sent through the Intune-SCEP Service because Microsoft Intune validates these requests.

Mandatory: No. By default, this box is not checked.

Insecure SCEP (Permit an empty challenge password)

Check this box to allow an empty [SCEP Challenge Password](#); uncheck this box to make the challenge password mandatory.

✗ Deliberately configuring SCEP without a challenge password can be a security risk.

Mandatory: No. This box is unchecked by default.

SCEP Challenge Password

A challenge password for SCEP clients.

i This setting only applies to requests sent through the SCEP Service. It does not apply to requests sent through the Intune-SCEP Service because Microsoft Intune validates these requests.

Mandatory: When the [Insecure SCEP \(Permit an empty challenge password\)](#) box is not checked.

CAGW CA ID

The CA identifier (CA ID) of the CA for certificate enrollments, as defined in Entrust PKI as a Service or an on-premises CA Gateway.

Mandatory: Yes.

Intune

Select the **Intune** tab of the **Configuration** page to configure Intune-SCEP enrollment.

- [Intune-SCEP Enrollment Service Configurations](#)
- [Intune Revocation Cron Job](#)
- [Enable Intune-SCEP](#)

InTune-SCEP Enrollment Service Configurations

Configure the following settings for each **InTune-SCEP Enrollment Service Configuration**.

- [Override Default InTune Endpoints](#)
- [Azure Authentication Method](#)
- [Azure Tenant](#)
- [Azure Application ID](#)
- [CAGW CA ID](#)

Override Default InTune Endpoints

Select **Yes** to override some default setting values and work with the following non-default Intune endpoints.

Setting	Value
Override: Authentication Authority	The URL of the Microsoft authentication authority.
Override: Graph API Version	The version of the Microsoft Graph API.

Setting	Value
Override: Graph Resource URL	This URL of the Microsoft Graph Resource.
Override: InTune Application ID	The application ID of Microsoft Intune.
Override: InTune Resource URL	The URL of the Microsoft Intune Resource.

Select **No** to support only default Intune endpoints.

Mandatory: No. This setting defaults to **No**.

Azure Authentication Method

If the registered Azure application authenticates with certificate-based (P12) credentials, select **App P12** and configure the following settings.

Setting	Value
Registered Azure Application Credential Key Store File (P12)	The P12 file containing the Azure application credential.
Registered Azure Application Key Store Password	The password of the P12 credential

If the application authenticates with application keys (client secrets), select **App Secret** and configure the following setting.

Setting	Value
Registered Azure Application Key (Client Secret)	The application key (client secret) for connecting to the Intune instance.

Mandatory: Yes.

Azure Tenant


The tenant for connecting to the Intune instance. For example:

test.example.com

Mandatory: Yes.

Azure Application ID

The Application ID of the Registered Azure Application, as viewed from Azure.

 The selected Registered Azure Application must have the proper API permissions.

Mandatory: Yes.

CAGW CA ID

The CA identifier (CA ID) for certificate enrollments defined in Entrust PKI as a Service or an on-premises CA Gateway.

Mandatory: Yes.

InTune Revocation Cron Job

The schedule for Certificate Enrollment Gateway to check Microsoft Intune for revocations. The value must be a cron schedule expression in the following format:

```
<second> <minute> <hour> <day-of-month> <month> <day-of-week>
```

For example, to run the cron job every 15 minutes:

```
0 0/15 * * * ?
```

Mandatory: No. This setting defaults to a period of 15 minutes.

Enable InTune-SCEP

Select **Yes** to enable the Intune-SCEP protocol, **No** to disable the Intune-SCEP protocol.

Mandatory: No. This setting defaults to **No**.

MDMWS

Select the **MDMWS** tab of the **Configuration** page to configure MDMWS enrollment.

- [MDMWS Enrollment Service Configuration](#)
- [MDMWS Users](#)
- [MDMWS Expired Token Clean-up Cron Job](#)
- [MDM-SCEP Token Expire Lifetime](#)
- [Enable MDMWS](#)

MDMWS Enrollment Service Configuration

Configure one or more Digital ID Configurations for the MDM protocols.

- [Digital ID](#)
- [CAGW CA ID](#)
- [CAGW Profile ID](#)
- [Parent DN](#)
- [RDN Format](#)



An **MDMWS Digital ID Configuration** is a template Certificate Enrollment Gateway uses to issue digital IDs for a mobile device with an MDM protocol.

Digital ID

A unique name for the Digital ID Configuration. This name:

- Must be at least four characters long,
- Must contain only letters, numbers, underscores, spaces, and hyphens.

Mandatory: Yes.

CAGW CA ID

The CA identifier (CA ID) in CA Gateway of the CA for certificate enrollments.

Mandatory: Yes.

CAGW Profile ID

The profile identifier (Profile ID) in CA Gateway of the CA for certificate enrollments.

Mandatory: Yes.

Parent DN

The parent DN (distinguished name) for certificates issued by Certificate Enrollment Gateway.

- For an on-premises CA, the parent DN must be a known searchbase defined in the CA.
- For Entrust PKI as a Service, the parent DN must be an absent or custom parent DN.

Examples:

```
ou=Devices,o=My Company,c=US
```

```
cn=Users,ou=North America,o=My Company,c=GB
```

Certificate Enrollment Gateway will build the rest of the client's DN when enrolling the client.

Mandatory: No.

RDN Format

This setting specifies the relative distinguished name (RDN) format that Certificate Enrollment Gateway uses to find and create users.


Enclose variables with angled brackets (< and >). The incoming MDMWS request must have these variables defined. Examples:

```
cn=<firstname> <lastname>  
cn=<igusername> <iggroup> <devicetype>
```

Mandatory: Yes.

MDMWS Users

Configure a **Username** and **Password** for each user of the MDMWS protocol.

 The MDMWS protocol is protected with username and password authentication. Clients such as the Mobile Device Management (MDM) software must authenticate to Certificate Enrollment Gateway using valid username and password credentials.

MDMWS Expired Token Clean-up Cron Job

The frequency for removing expired MDM challenges from the internal database. The value must be a cron schedule expression in the following format:

```
<second> <minute> <hour> <day-of-month> <month> <day-of-week>
```

Mandatory: Yes.

MDM-SCEP Token Expire Lifetime

The lifetime of MDM challenges, in seconds. The minimum permitted value is 1 second.

Mandatory: Yes.

Enable MDMWS

Select **Yes** to enable the MDM Web Service (MDMWS) and MDM-SCEP protocols; **No** to disable them.

Mandatory: No. This setting defaults to **No**.

ACMEv2

Select the **ACMEv2** tab of the **Configuration** page to configure ACMEv2 enrollment.

- [ACMEv2 HTTP-01 Redirect on POST](#)
- [ACMEv2 HTTP-01 Retry Interval](#)
- [ACMEv2 HTTP-01 Retry Count](#)
- [ACMEv2 DNS-01 Query Timeout](#)
- [ACMEv2 DNS-01 Nameservers](#)
- [Delete Expired Authorizations Cron Job](#)
- [Delete Expired Order Cron Job](#)
- [ACMEv2 Order Expiry Interval](#)
- [Enable ACMEv2](#)

ACMEv2 HTTP-01 Redirect on POST


Whether to enable redirects when the client responds with the 302, 307, or 308 HTTP code. Select:

- **Yes** to enable redirects and follow redirects up to 50 hops.
- **No** to disable redirects, mark the challenge as failed, and flag the associated client order as invalid.

Mandatory: No. This setting defaults to **No**.

ACMEv2 HTTP-01 Retry Interval

The number of seconds to wait between HTTP-01 Validation attempts.

 HTTP-01 Validation attempts can fail when the HTTP-01 challenge server responds with the *503 Service Unavailable* HTTP code.

If set to 0, the ACMEv2 server will wait 1 second after the first connection failure and 2 seconds after each subsequent failure.

Mandatory: No. This defaults to 0.

ACMEv2 HTTP-01 Retry Count

The maximum number of times the CEG ACMEv2 Enrollment Service will retry HTTP-01 Validation before timing out.

i HTTP-01 Validation attempts can fail when the HTTP-01 challenge server responds with the *503 Service Unavailable* HTTP code.

This setting supports a value range from 0 to unlimited.

Mandatory: No. This setting defaults to 4.

ACMEv2 DNS-01 Query Timeout

The number of milliseconds to continue attempting DNS-01 Validation before timing out.

Mandatory: No. This value defaults to 10000 (10 seconds).

ACMEv2 DNS-01 Nameservers

The list of DNS nameservers for DNS-01 validation for ACMEv2. Use the following syntax to enter the IPv4 address and port (typically port 53) of each DNS nameserver.

<IP> : <PORT>

For example:

192.0.2.0:53

Mandatory: No. If this setting is absent, the ACMEv2 service will use the nameservers in the `resolv.conf` file.

Delete Expired Authorizations Cron Job

The schedule for Certificate Enrollment Gateway to remove expired ACMEv2 authorizations from the internal database. The value must be a cron schedule expression in the following format:

<second> <minute> <hour> <day-of-month> <month> <day-of-week>

For example, to run the cron job every 1 hour:

0 0 * * * *

Mandatory: No. If this setting is absent, Certificate Enrollment Gateway removes expired ACMEv2 authorizations every 1 hour.

Delete Expired Order Cron Job

The schedule for Certificate Enrollment Gateway to remove expired ACMEv2 orders from the internal database. The value must be a cron schedule expression in the following format:

<second> <minute> <hour> <day-of-month> <month> <day-of-week>

For example, to run the cron job every 1 hour:

0 0 * ? * *

Mandatory: No. If this setting is absent, Certificate Enrollment Gateway removes expired ACMEv2 orders every 1 hour.

ACMEv2 Order Expiry Interval

The period of time an ACMEv2 order can remain unprocessed by a client before the ACMEv2 server marks the order as "invalid". Enter a period in ISO-8601 duration format:

PnDTnHnMn.nS

Mandatory: No. This setting defaults to **p7D** (seven days).

Enable ACMEv2

Select **Yes** to enable the ACMEv2 protocol, **No** to disable the ACMEv2 protocol.

Mandatory: No.

CAGW

Select the **CAGW** tab of the **Configuration** page to configure the connection with an Entrust CA Gateway instance.

- [RA Certificate Profile IDs](#)
- [Trusted CA Certificates File Format](#)
- [CAGW Keystore Alias](#)
- [CAGW Keystore Password](#)
- [CAGW Keystore File \(P12\)](#)
- [CA Gateway URL](#)

RA Certificate Profile IDs

One or more **RA Certificate Profile ID** mappings to issue an RA certificate. Define the following values for each mapping.

- [Key Name](#)
- [Value](#)

 Certificate Enrollment Gateway uses RA certificates to sign and encrypt SCEP PKI messages.


Mandatory: Add at least one mapping.

Key Name

The **CA ID** defined in the CA Gateway instance for the CA that will generate the RA certificate.

Value

The name of a **Profile ID** defined in the CA Gateway instance to issue the RA certificate.

 The selected **Profile ID** must allow Dual Usage (both Digital Signature and Key Encipherment).

Trusted CA Certificates File Format

The format of the file containing the CA certificate chain for the CA Gateway client credential. Select one of the following values.

- [Re-use the CAGW Keystore File](#)
- [P12](#)
- [PEM](#)

Mandatory: Yes.

Re-use the CAGW Keystore File

Select this value to re-use the [CAGW Keystore File \(P12\)](#).

 The deployment will fail if the [CAGW Keystore File \(P12\)](#) does not contain at least a Trusted CA Certificate entry.

P12

Select this value to:

- Import a P12 truststore file in the **CAGW Truststore File (P12)** field
- Enter a P12 truststore password in the **CAGW Truststore Password** field.

PEM

Select this value to import a PEM-formatted file in the **CA Certificates File (PEM)** field.

CAGW Keystore Alias

The alias of the private key entry (`PrivateKeyEntry`) in the CA Gateway Keystore. Run the following command to list all alias names in the `<file>` keystore.

```
keytool -v -list -keystore <file>
```

Mandatory: When the CA Gateway Keystore contains more than one private key.

CAGW Keystore Password

The password of the PKCS #12 file selected in [CAGW Keystore File \(P12\)](#).

Mandatory: Yes.

CAGW Keystore File (P12)

A CA Gateway keystore file. This file must be a PKCS #12 file containing a private key and client certificate for Certificate Enrollment Gateway.

Specifically, to authenticate in the built-in CA Gateway service of the Certificate Authority solution, you must:

1. Create a user of the type described in [Creating Certificate Authority tenants](#).
2. Add this user as an administrator of each CA instance you want to manage, as explained in [Managing Certificate Authority instances](#). When completing the process:
 - Download the PKCS #12 credential file.
 - Copy the PKCS #12 password.
3. Select the downloaded PKCS #12 in the **CAGW Keystore File (P12)** field of the Certificate Enrollment Gateway configuration.
4. Paste the PKCS #12 password in the [CAGW Keystore Password](#) field of the Certificate Enrollment Gateway configuration.

Mandatory: Yes.

CA Gateway URL

The URL of CA Gateway. This URL:

- Must not contain the API version – for example, it must not contain `/api/v1`.
- Must not end with a trailing slash `/`.

For example:

```
https://cagw.example.com/cagw
```

Mandatory: Yes.

Tenants

Select the **Tenants** tab of the **Configuration** page to configure the following settings.

- [CEG Web Admin Password](#)
- [CEG Web Admin Username](#)
- [CEG Tenant Unique ID](#)

CEG Web Admin Password

The password to log in to the CEG Web Admin interface.




The CEG Web Admin interface is for troubleshooting or modifying the log levels under Entrust Customer Support's guidance.

Mandatory: For security reasons, it is recommended to change the `changeme` initial password.

CEG Web Admin Username

The username to log in to the CEG Web Admin interface.

 The CEG Web Admin interface is for troubleshooting or modifying the log levels under Entrust Customer Support's guidance.

Mandatory: For security reasons, it is recommended to change the `WebAdmin` initial username.

CEG Tenant Unique ID

A unique tenant identifier for the CEG Service. The selected identifier does not need to match any value defined in CA Gateway.

This value will be present in incoming enrollment request URLs. The value is case-sensitive and can include only the following characters:

- Dashes (-)
- Underscores (_)
- Tildes (~)
- Uppercase letters (A to Z)
- Lowercase letters (a to z)
- Numbers (0 to 9)

 Certificate Enrollment Gateway supports only one tenant.

Mandatory: Yes.

Enrollment URLs for Certificate Enrollment Gateway

When deploying or redeploying Certificate Enrollment Gateway, CSP 1.0.0 will display a list of local test commands and enrollment URLs for Certificate Enrollment Gateway.

- [ACMEv2 enrollment URL](#)
- [Intune-SCEP enrollment URL](#)
- [MDM-SCEP enrollment URL](#)
- [MDMWS enrollment URL](#)
- [SCEP enrollment URL](#)
- [WSTEP enrollment URL](#)

ACMEv2 enrollment URL

ACMEv2 clients must use the following URL to communicate with Certificate Enrollment Gateway:

```
https://<CEG-server>/acme/<tenant-ID>/<CA-ID>/<profile-ID>/directory
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the ACMEv2 endpoint.
- `<profile-ID>` is the profile ID defined in CA Gateway that defines the certificate type issued to the ACMEv2 client. For Entrust PKI as a Service, the profile ID is one of the following


- `privatessl-tls-client-server`
- `privatessl-tls-server`
- `privatessl-tls-client`.

For example:

```
https://cegserver.example.com/acme/tenant1/example_ca1/privatessl_tls_client/
directory
```

Intune-SCEP enrollment URL

Microsoft Intune must be configured to use one of the following URLs to communicate with Certificate Enrollment Gateway:

-  The following Intune-SCEP enrollment URL requires the trailing forward slash (/). To support macOS (Apple) devices, the URL must start with `http` instead of `https`.

```
http://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/intune/
https://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/intune/
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the SCEP client.
- `<profile-ID>` is the profile ID defined in CA Gateway that defines the certificate type issued to the SCEP client. For Entrust PKI as a Service, the profile ID is one of the following:
 - `intune-digital-signature-key-encipherment`
 - `intune-digital-signature`
 - `intune-key-encipherment`
 - `intune-non-repudiation`

For example:

```
http://cegserver.example.com/scep/tenant1/example_ca1/intune-digital-signature-key-
encipherment/intune/
https://cegserver.example.com/scep/tenant1/example_ca1/intune-digital-signature-key-
encipherment/intune/
```

MDM-SCEP enrollment URL

MDM-SCEP clients must use one of the following URLs to communicate with Certificate Enrollment Gateway:

-  To support macOS (Apple) devices, the URL must start with `http` instead of `https`.


```
http://<CEG-server>/scep/<tenant-ID>/<digitalid-config>/mdm
https://<CEG-server>/scep/<tenant-ID>/<digitalid-config>/mdm
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<digitalid-config>` is a digital ID configuration defined in the CEG Service.

For example:

```
http://cegserver.example.com/scep/tenant1/digitalid-config1/mdm
https://cegserver.example.com/scep/tenant1/digitalid-config1/mdm
```

MDMWS enrollment URL

Mobile Device Management products must use the following URL to communicate with Certificate Enrollment Gateway:

```
https://<CEG-server>/mdm/services/<tenant-ID>
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.

For example:

```
https://cegserver.example.com/mdm/services/tenant1
```

SCEP enrollment URL

SCEP clients must use one of the following URLs to communicate with Certificate Enrollment Gateway:

i The following SCEP enrollment URL requires the trailing forward slash (/). To support macOS (Apple) devices, the URL must start with `http` instead of `https`.

```
http://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/
https://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.

- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the SCEP client.
- `<profile-ID>` is the profile ID defined in CA Gateway that defines the certificate type issued to the SCEP client. For Entrust PKI as a Service, the profile ID is one of the following:
 - scep-digital-signature-key-encipherment
 - scep-digital-signature
 - scep-key-encipherment
 - scep-non-repudiation

For example:

```
http://cegserver.example.com/scep/tenant1/example_ca1/scep-digital-signature/  
https://cegserver.example.com/scep/tenant1/example_ca1/scep-digital-signature/
```

Some SCEP clients will append an additional parameter to all SCEP URLs. For these clients, you must append `nop/` to the SCEP URL. For example:

```
http://cegserver.example.com/scep/tenant1/example_ca1/scep-digital-signature/nop/  
https://cegserver.example.com/scep/tenant1/example_ca1/scep-digital-signature/nop/
```

WSTEP enrollment URL

For WSTEP enrollment, the enrollment service in Active Directory must use the following URL to communicate with Certificate Enrollment Gateway:

```
https://<CEG-server>:443/wstep/<auth>/services/<tenant-ID>/<CA-ID>
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<auth>` is the authentication method, either `usertoken` for user name and password authentication or `kerberos` for Kerberos (Windows integrated) authentication.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the Windows endpoint.

For example, when authenticating with a user name and password:

```
https://cegserver1.example.com:443/wstep/usertoken/services/tenant1/example-ca1
```

For example, when authenticating with Kerberos:

```
https://cegserver1.example.com:443/wstep/kerberos/services/tenant1/example-ca1
```

Integrating Certificate Enrollment Gateway

See below for the main integration use cases of the Certificate Enrollment Gateway solution.

- [Integrating WSTEP clients with Certificate Enrollment Gateway](#)
- [Integrating MDM and MDM-SCEP clients with Certificate Enrollment Gateway](#)
- [Integrating SCEP clients with Certificate Enrollment Gateway](#)
- [Integrating Microsoft Intune with Certificate Enrollment Gateway](#)
- [Integrating ACMEv2 clients with Certificate Enrollment Gateway](#)

Integrating WSTEP clients with Certificate Enrollment Gateway

The enrollment endpoints of the CEG Service can be:

- An end-user or machine in a Windows domain.
- A user or machine connected to a Windows domain.

This section describes how to integrate these endpoints with Certificate Enrollment Gateway using WS-Trust X.509v3 Token Enrollment Extensions (WSTEP). Certificate Enrollment Gateway does not use NTLM authentication.

Configuring the TLS certificate of the Windows endpoints

On the server hosting the Certificate Enrollment Policy Web Service, the TLS certificate installed on Microsoft IIS is irrelevant to Certificate Enrollment Gateway. Instead, what matters is that the issuing certificate chain is trusted by all devices on the domain, along with any non-domain WSTEP client.

- If you are integrating Certificate Enrollment Gateway with an existing Windows domain, this domain already has trusted TLS certificates, and you can skip this section.
- If you are integrating a new Windows domain, follow the steps below to install the TLS certificate chain.

This section contains the following topics:

- [Obtaining the CA certificates](#)
- [Installing the CA certificates in the Active Directory domain](#)

Obtaining the CA certificates

If you used TLS Bootstrapping feature when you deployed the CEG Service, the CA certificate chain will be a `certcerts.p7b` file, located in the directory where you exported the Certificate Enrollment Gateway configuration.

For CAs hosted by Entrust PKI as a Service, you should have obtained the CA certificates from the Entrust Certificate Services portal.

Copy this file from the CEG Service host to your machine.

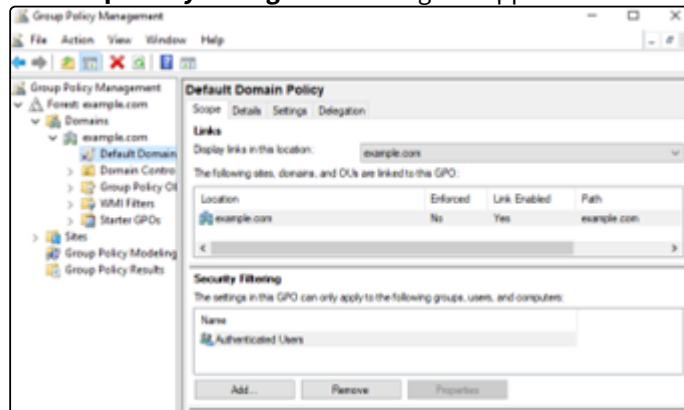
Installing the CA certificates in the Active Directory domain

In the Active Directory Domain Controller, install all certificates in the CA certificate chain as trusted root certificates.

To install the CA certificates in the Active Directory Domain Controller

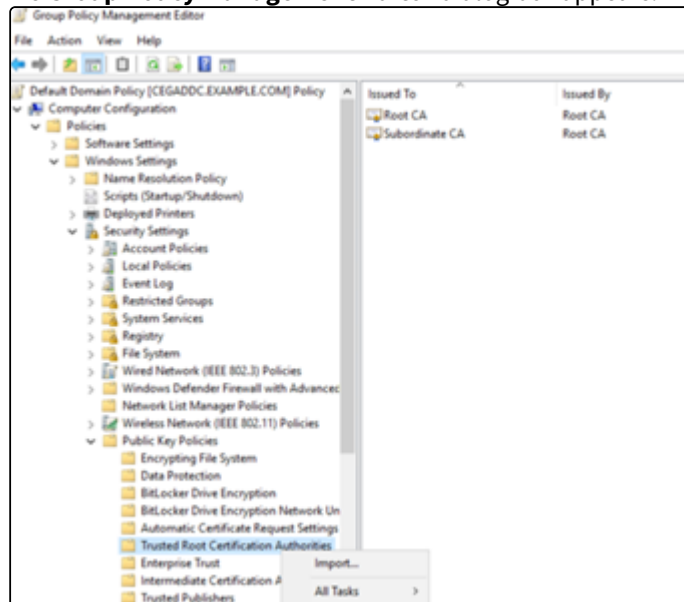
1. Log in to the server hosting Active Directory.
2. Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.

The **Group Policy Management** dialog box appears.



3. In the tree view, expand the Domain Controller you will modify.
4. Right-click **Default Domain Policy > Edit**.

The **Group Policy Management Editor** dialog box appears.



5. In the tree view, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities**.
6. Right-click **Trusted Root Certification Authorities > Import**.
7. Select the Entrust Certificate Authority certificates or the CA certificates file you obtained earlier in [Obtaining the CA certificates](#).

Configuring enrollment endpoints

You must configure all Windows Policies domain and non-domain endpoints for which the Certificate Enrollment Gateway will issue certificates.

- [Configuring Windows Domain Endpoints](#)
- [Configuring non-domain endpoints](#)

Configuring Windows Domain Endpoints

You must configure all Windows domain endpoints—domain controllers and computers in a Windows domain—that will be issued certificates by Certificate Enrollment Gateway.

i For WSTEP enrollment, some machines also need TLS certificates. You will be configuring the TLS certificates later, starting in Configuring the TLS certificate of the Windows endpoints.

- [Enabling certificate auto-enrollment for users](#)
- [Enabling certificate auto-enrollment for computers and domain controllers](#)
- [Configuring the Certificate Enrollment Policy Web Service for Windows users](#)
- [Configuring the Certificate Enrollment Policy Web Service for Windows domain endpoints](#)
- [Importing the CA certificate into Windows domain endpoints](#)
- [Obtaining the URL of the Certificate Enrollment Policy Web Service](#)

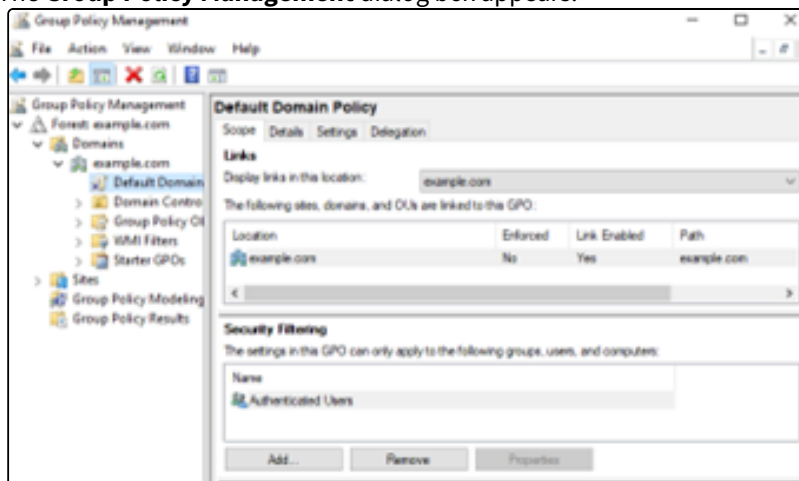
Enabling certificate auto-enrollment for users

In the Windows Domain, enable the certificate auto-enrollment for users.

To enable the certificate auto-enrollment for users

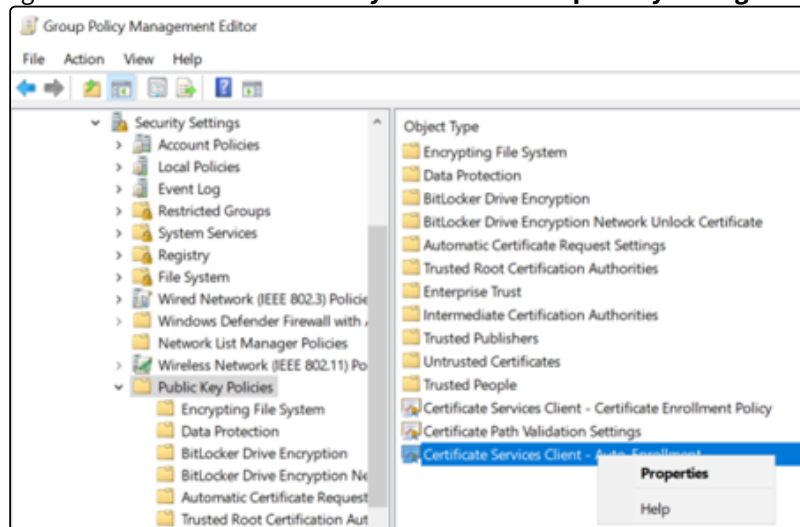
1. Log in to the server hosting Active Directory.
2. Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.

The **Group Policy Management** dialog box appears.

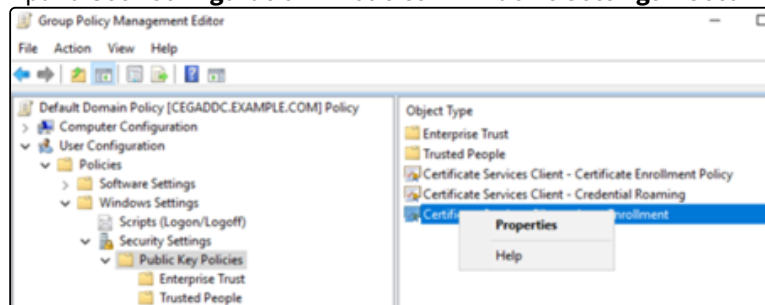


3. In the tree view, expand the Domain Controller you will modify.

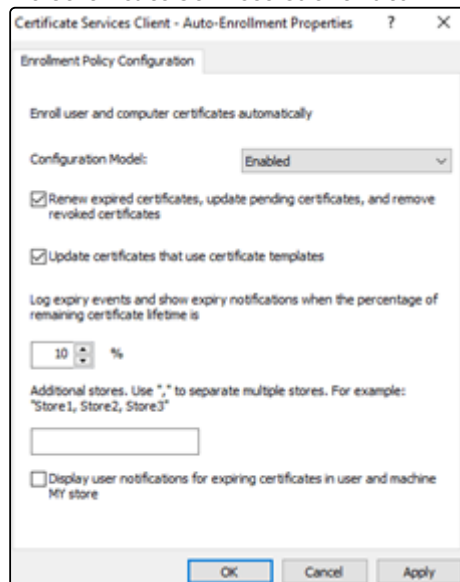
4. Right-click **Default Domain Policy > Edit**. The **Group Policy Management Editor** dialog box appears.



5. Expand **User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.



6. In the content pane, right-click **Certificate Services Client Auto Enrollment > Properties**. The **Certificate Services Client Auto Enrollment Properties** dialog box appears.



7. In the **Configuration Model** drop-down list, select **Enabled**.
8. Select **Renew expired certificates, update pending certificates, and remove revoked certificates**.
9. Select **Update certificates that use certificate templates**.
10. Click **OK**.

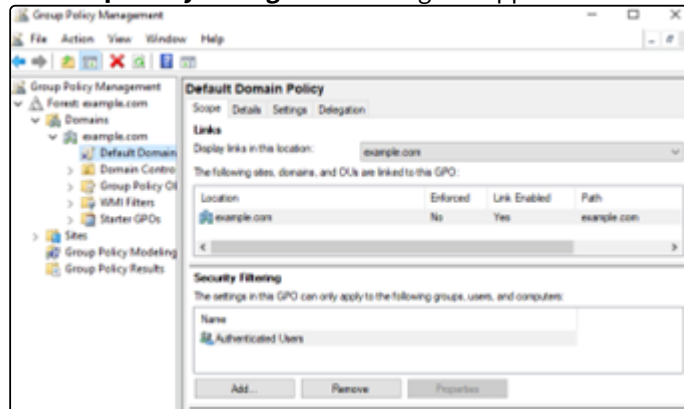
Enabling certificate auto-enrollment for computers and domain controllers

In the Windows domain, enable the certificate auto-enrollment for computers and domain controllers.

To enable certificate auto-enrollment for computers and domain controllers

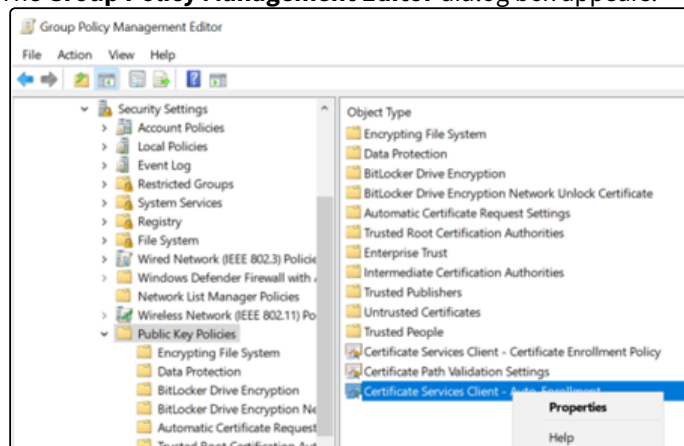
1. Log in to the server hosting Active Directory.
2. Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.

The **Group Policy Management** dialog box appears.



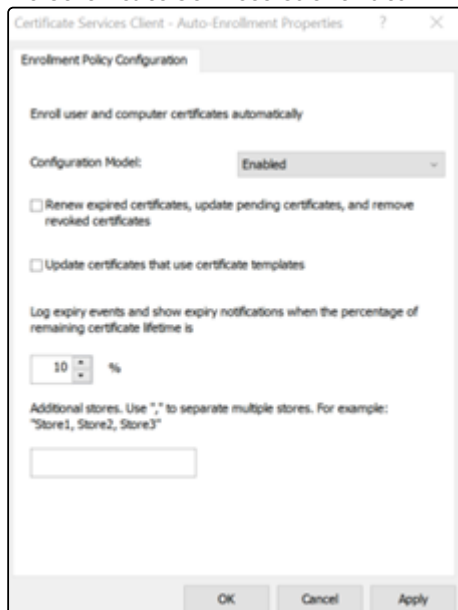
3. In the tree view, expand the Domain Controller you will modify.
4. Right-click **Default Domain Policy > Edit**.

The **Group Policy Management Editor** dialog box appears.



5. Expand to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.

- In the content pane, right-click **Certificate Services Client Auto Enrollment > Properties**. The **Certificate Services Client Auto Enrollment Properties** dialog box appears.



- In the **Configuration Model** drop-down list, select **Enabled**.
- Select **Renew expired certificates, update pending certificates, and remove revoked certificates**.
- Select **Update certificates that use certificate templates**.
- Click **OK**.

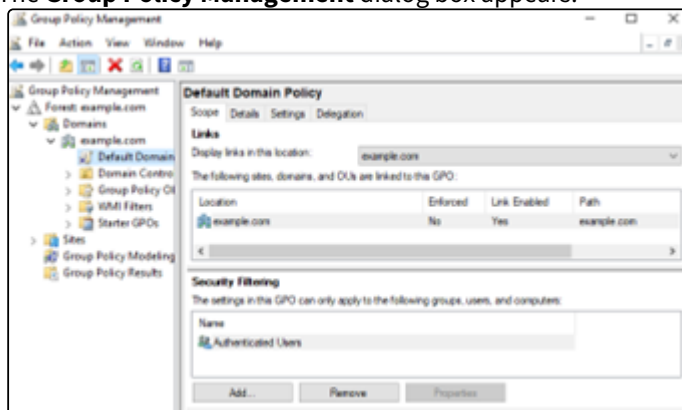
Configuring the Certificate Enrollment Policy Web Service for Windows users

To work with Certificate Enrollment Gateway, Windows domain endpoints need the Certificate Enrollment Policy Web Service URL. Complete the following procedure to add the Certificate Enrollment Policy Web Service URL to Windows domain endpoints.

To configure the Certificate Enrollment Policy Web Service for Windows users

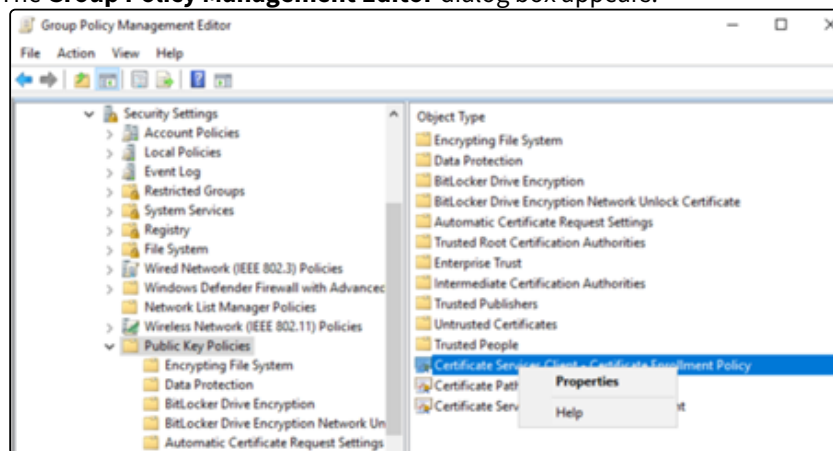
- Log in to the server hosting Active Directory.
- Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.

The **Group Policy Management** dialog box appears.

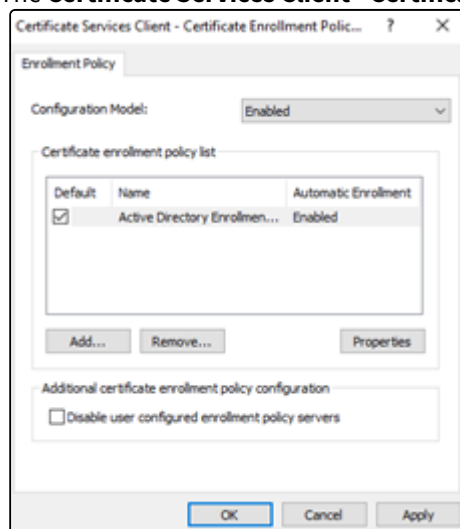


- In the tree view, expand the Domain Controller you will modify.

4. Right-click **Default Domain Policy > Edit** .
The **Group Policy Management Editor** dialog box appears.

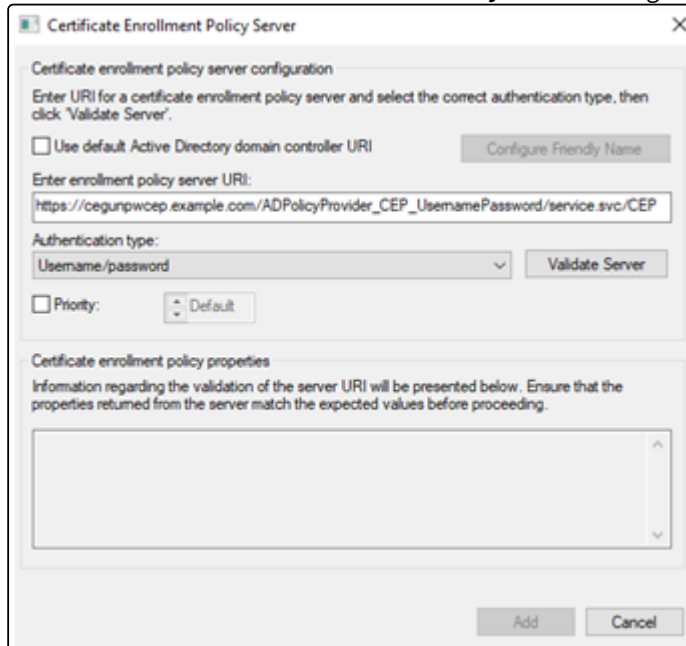


5. In the tree view, expand **User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
6. In the content pane, right-click **Certificate Services Client - Certificate Enrollment Policy > Properties**.
The **Certificate Services Client - Certificate Enrollment Policy Properties** dialog box appears.



7. In the **Configuration Model** drop-down list, select **Enabled**.
8. If you are not installing WSTEP along with an existing Microsoft CA, select **Active Directory Enrollment** in the **Certificate enrollment policy list** pane, and then click **Remove**.

9. Click **Add**. The **Certificate Enrollment Policy Server** dialog box appears.



Certificate Enrollment Policy Server

Certificate enrollment policy server configuration

Enter URI for a certificate enrollment policy server and select the correct authentication type, then click "Validate Server".

☐ Use default Active Directory domain controller URI Configure Friendly Name

Enter enrollment policy server URI:

Authentication type:
 Validate Server

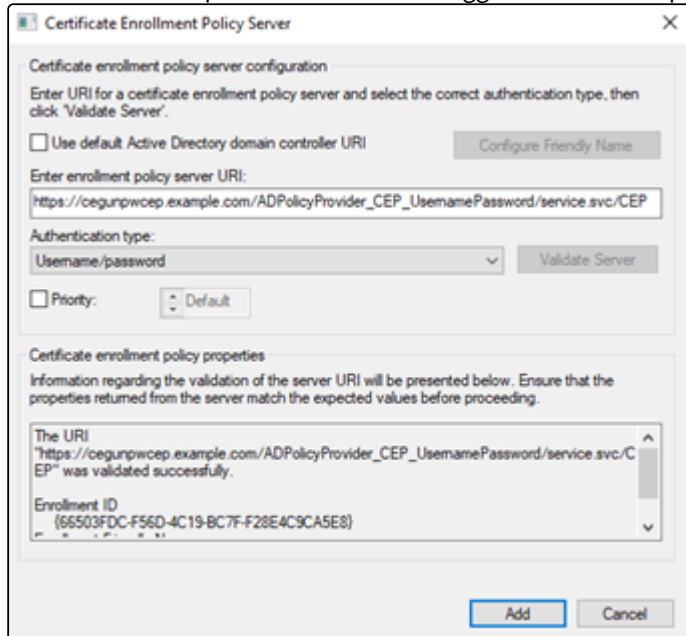
☐ Priority: Default

Certificate enrollment policy properties

Information regarding the validation of the server URI will be presented below. Ensure that the properties returned from the server match the expected values before proceeding.

Add Cancel

10. In the **Enter enrollment policy server URI** field, enter the Certificate Enrollment Policy Web Service URL that you obtained earlier.
11. In the **Authentication type** drop-down list, select the same authentication mode that you configured earlier in [Selecting the authentication mode of the CEP Web Service using the Windows graphical interface](#).
12. Click **Validate Server**. If the selected authentication type is **Username/password**, you will be prompted for the username and password of the user logged in to the computer.



Certificate Enrollment Policy Server

Certificate enrollment policy server configuration

Enter URI for a certificate enrollment policy server and select the correct authentication type, then click "Validate Server".

☐ Use default Active Directory domain controller URI Configure Friendly Name

Enter enrollment policy server URI:

Authentication type:
 Validate Server

☐ Priority: Default

Certificate enrollment policy properties

Information regarding the validation of the server URI will be presented below. Ensure that the properties returned from the server match the expected values before proceeding.

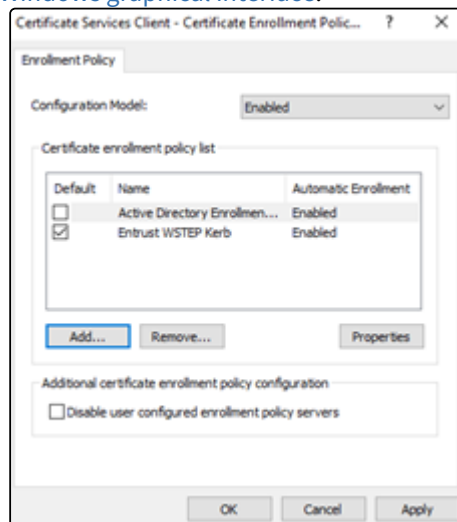
The URI
 "https://cegunpwcep.example.com/ADPolicyProvider_CEP_UsernamePassword/service.svc/CEP" was validated successfully.

Enrollment ID
 (66503FDC-F56D-4C19-BC7F-F28E4C9CA5E8)

Add Cancel

13. Click **Add**.
 The **Certificate enrollment policy list** pane should display the friendly name of the Certificate Enrollment Policy Web Service that you specified earlier in [Assigning a friendly name to the CEP Web Service using the](#)

Windows graphical interface.



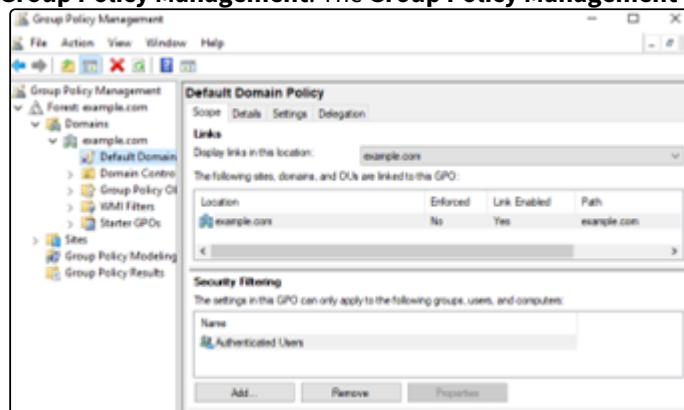
14. In the **Certificate enrollment policy list** pane, select the checkbox for the Certificate Enrollment Policy Web Service you just added to make it the default Certificate Enrollment Policy.
15. Click **OK**.

Configuring the Certificate Enrollment Policy Web Service for Windows domain endpoints

To work with Certificate Enrollment Gateway, Windows domain endpoints need the Certificate Enrollment Policy Web Service URL. Complete the following procedure to add the Certificate Enrollment Policy Web Service URL for Windows domain endpoints.

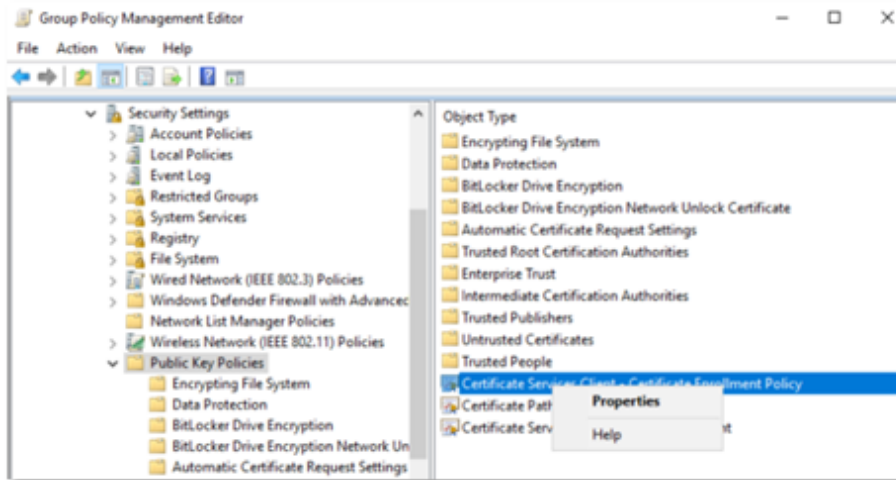
To configure the Certificate Enrollment Policy Web Service for Windows domain endpoints

1. Log in to the server hosting Active Directory.
2. Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**. The **Group Policy Management** dialog box appears.

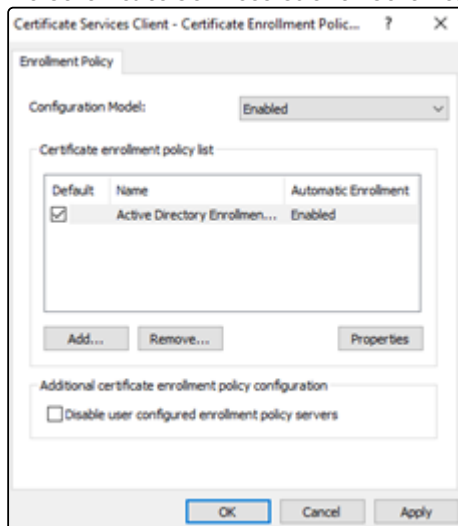


3. In the tree view, expand the Domain Controller you will modify.

4. Right-click **Default Domain Policy > Edit**. The **Group Policy Management Editor** dialog box appears.



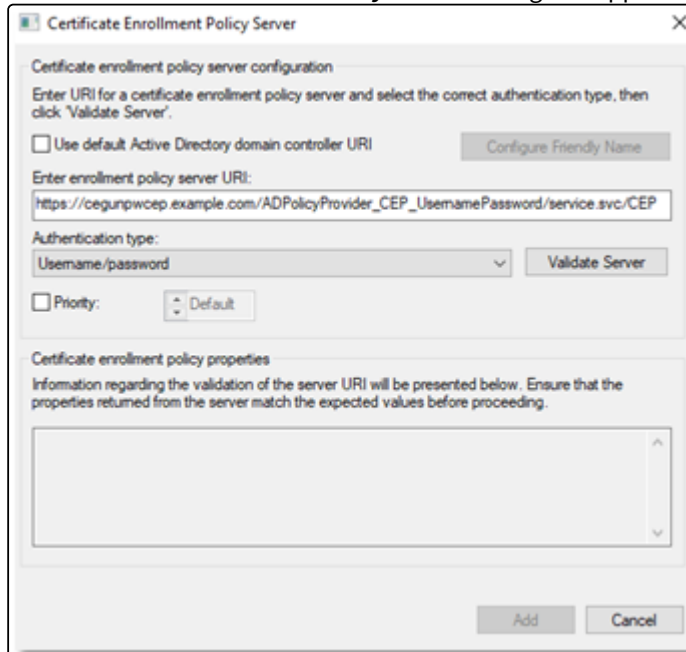
5. In the tree view, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
6. In the content pane, right-click **Certificate Services Client - Certificate Enrollment Policy > Properties**. The **Certificate Services Client - Certificate Enrollment Policy Properties** dialog box appears.



7. In the **Configuration Model** drop-down list, select **Enabled**.
8. If you are not installing WSTEP along with an existing Microsoft CA, select **Active Directory Enrollment** in the **Certificate enrollment policy list** pane, and then click **Remove**.

9. Click **Add**.

The **Certificate Enrollment Policy Server** dialog box appears.



Certificate Enrollment Policy Server

Certificate enrollment policy server configuration

Enter URI for a certificate enrollment policy server and select the correct authentication type, then click 'Validate Server'.

☐ Use default Active Directory domain controller URI Configure Friendly Name

Enter enrollment policy server URI:

Authentication type:
 Validate Server

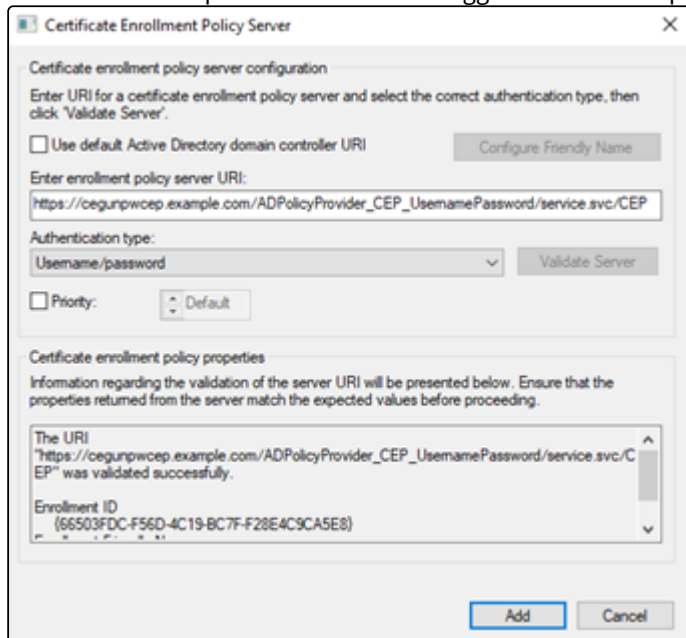
☐ Priority: Default

Certificate enrollment policy properties

Information regarding the validation of the server URI will be presented below. Ensure that the properties returned from the server match the expected values before proceeding.

Add Cancel

10. In the **Enter enrollment policy server URI** field, enter the Certificate Enrollment Policy Web Service URL that you obtained earlier.
11. In the **Authentication type** drop-down list, select the same authentication mode that you configured earlier in [Selecting the authentication mode of the CEP Web Service using the Windows graphical interface](#).
12. Click **Validate Server**. If the selected authentication type is **Username/password**, you will be prompted for the username and password of the user logged in to the computer.



Certificate Enrollment Policy Server

Certificate enrollment policy server configuration

Enter URI for a certificate enrollment policy server and select the correct authentication type, then click 'Validate Server'.

☐ Use default Active Directory domain controller URI Configure Friendly Name

Enter enrollment policy server URI:

Authentication type:
 Validate Server

☐ Priority: Default

Certificate enrollment policy properties

Information regarding the validation of the server URI will be presented below. Ensure that the properties returned from the server match the expected values before proceeding.

The URI
 "https://cegunpwcep.example.com/ADPolicyProvider_CEP_UsernamePassword/service.svc/CEP" was validated successfully.

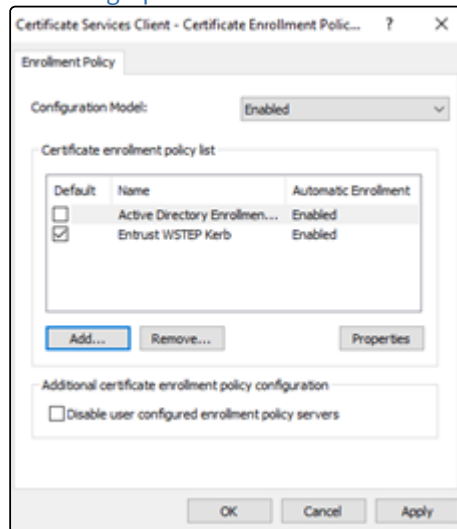
Enrollment ID
 {66503FDC-F56D-4C19-BC7F-F28E4C9CA5E8}

Add Cancel

13. Click **Add**.

The **Certificate enrollment policy list** pane should display the friendly name of the Certificate Enrollment Policy Web Service that you specified earlier in [Assigning a friendly name to the CEP Web Service using the](#)

Windows graphical interface.



14. In the **Certificate enrollment policy list** pane, select the checkbox for the Certificate Enrollment Policy Web Service you just added to make it the default Certificate Enrollment Policy.
15. Click **OK**.

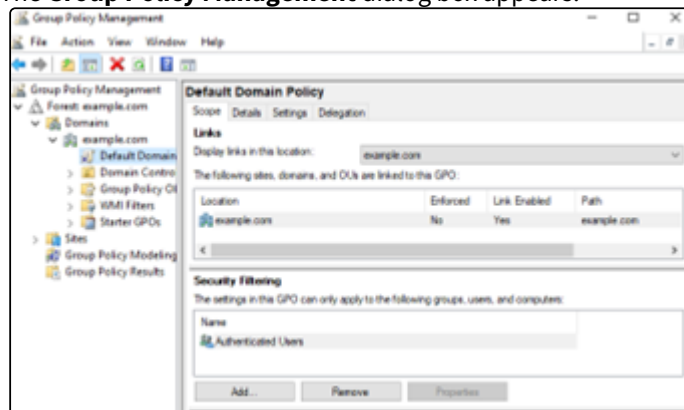
Importing the CA certificate into Windows domain endpoints

In each Windows domain enrollment endpoint, import the root certificate of the CA that will issue certificates for the enrollment service.

To import the CA certificate

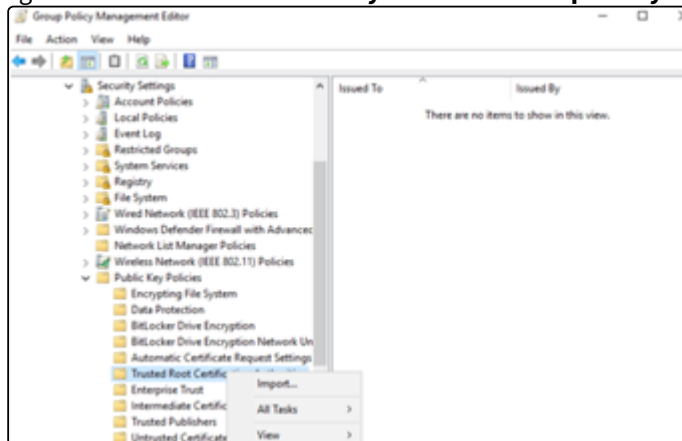
1. Log in to the server hosting Active Directory.
2. Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.

The **Group Policy Management** dialog box appears.

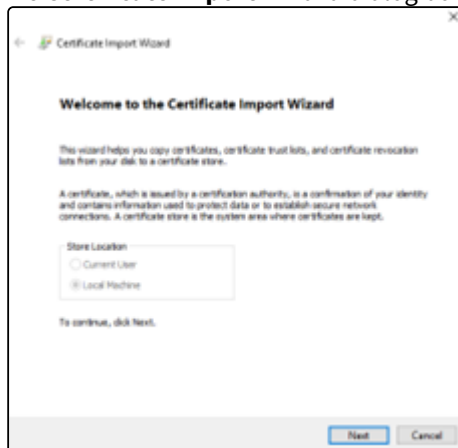


3. In the tree view, expand the Domain Controller you will modify.

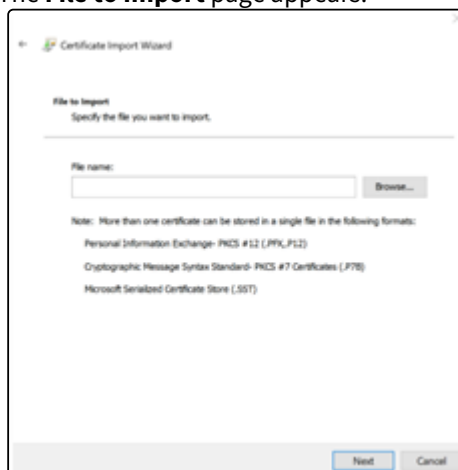
- Right-click **Default Domain Policy > Edit**. The **Group Policy Management Editor** dialog box appears.



- In the tree view, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
- Right-click **Trusted Root Certification Authorities** and select **Import**. The **Certificate Import Wizard** dialog box appears.



- Click **Next**. The **File to Import** page appears.



- Click **Browse** and select the root certificate of the CA that will issue certificates for the enrollment service.

9. Click **Next**.
The **Certificate Store** page appears.
10. The **Certificate Store** field is automatically set to **Trusted Root Certification Authorities**. Click **Next**.
The **Completing the Certificate Import Wizard** page appears.
11. Click **Finish**.

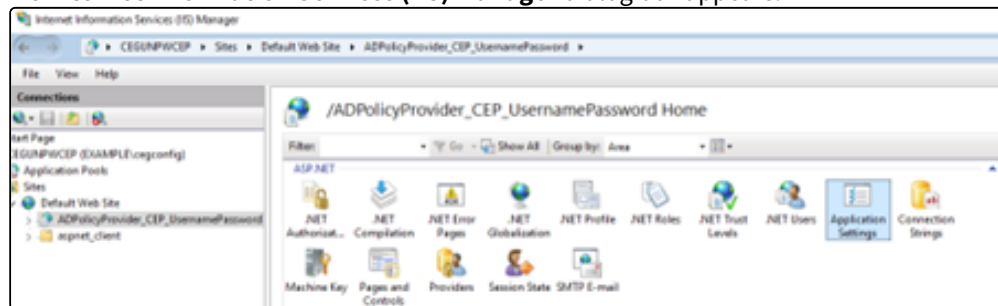
Obtaining the URL of the Certificate Enrollment Policy Web Service

To work with Certificate Enrollment Gateway, Windows domain endpoints need the Certificate Enrollment Policy Web Service URL. To obtain the URL, complete the following procedure.

To obtain the URL of the Certificate Enrollment Policy Web Service

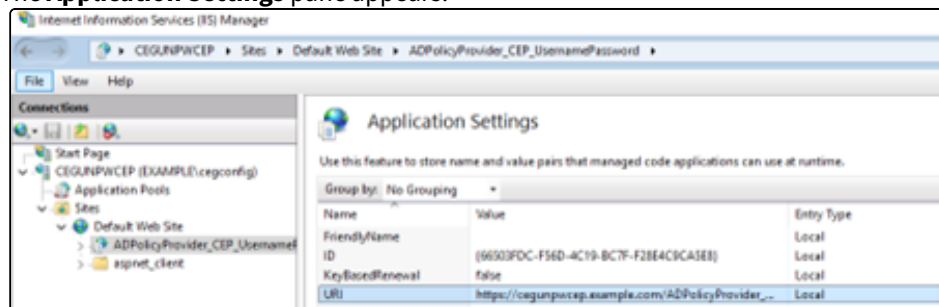
1. Log in to the server hosting the Certificate Enrollment Policy Web Service.
2. Open IIS Manager. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** dialog box appears.

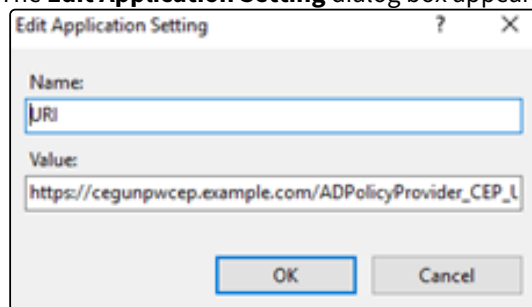


3. In the **Connections** pane, expand **Sites > Default Web site**.
4. Select the name of the Certificate Enrollment Policy Web Service application.
 - If you configured user name and password authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider_CEP_UsernamePassword**.
 - If you configured Kerberos (Windows integrated) authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider_CEP_Kerberos**.
5. In the Features pane, double-click **Application Settings**.

The **Application Settings** pane appears.



6. In the **Application Settings** pane, right-click **URI** > **Edit**.
The **Edit Application Setting** dialog box appears.



7. Copy the URL from the **Value** field.

Configuring non-domain endpoints

Enrollment endpoints outside the Windows domain require the manual configuration described in this section.

- [Configuring the enrollment policy in non-domain endpoints](#)
- [Importing the root CA certificate into non-domain endpoints](#)

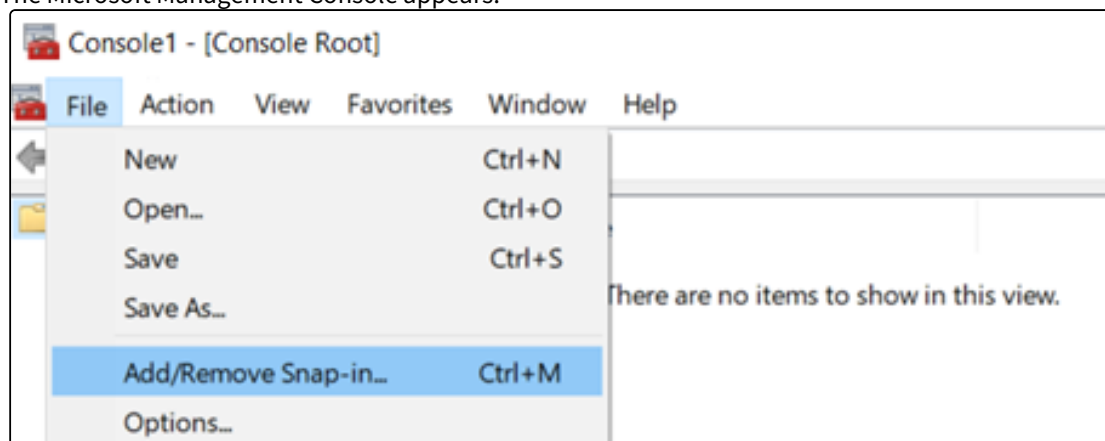
Configuring the enrollment policy in non-domain endpoints

In the enrollment endpoints outside the Windows Domain, add the enrollment policy as described in the following procedure.

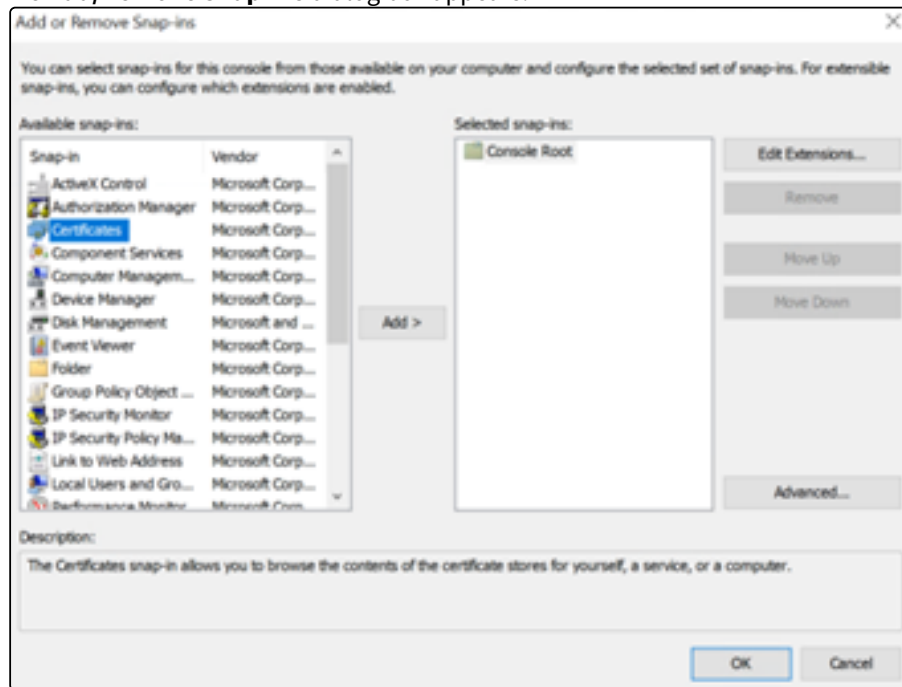
To configure the enrollment policy in non-domain endpoints

1. Log in to the non-domain endpoint.
2. Run `mmc.exe`.

The Microsoft Management Console appears.

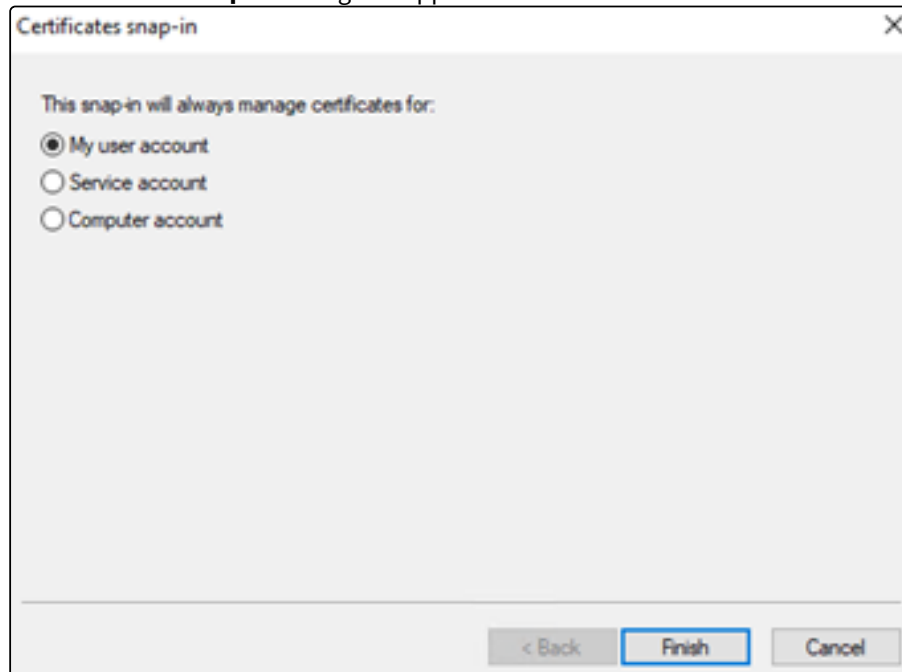


3. Select **File > Add/Remove Snap-in**.
The **Add/Remove Snap-ins** dialog box appears.



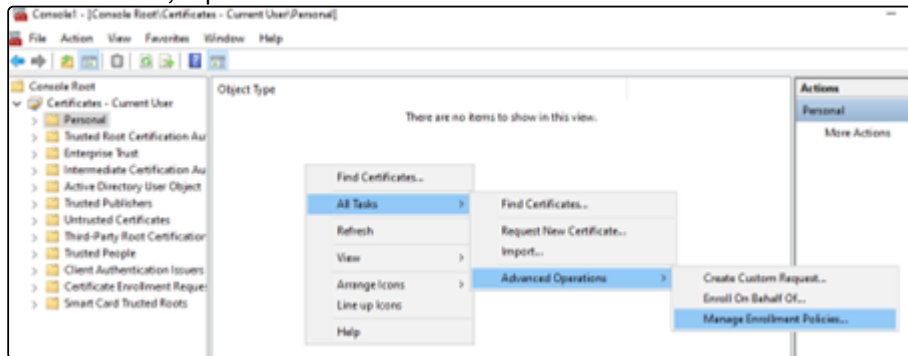
4. In the **Available snap-ins** list, select **Certificates**.
5. Click **Add**.

The **Certificates snap-in** dialog box appears.

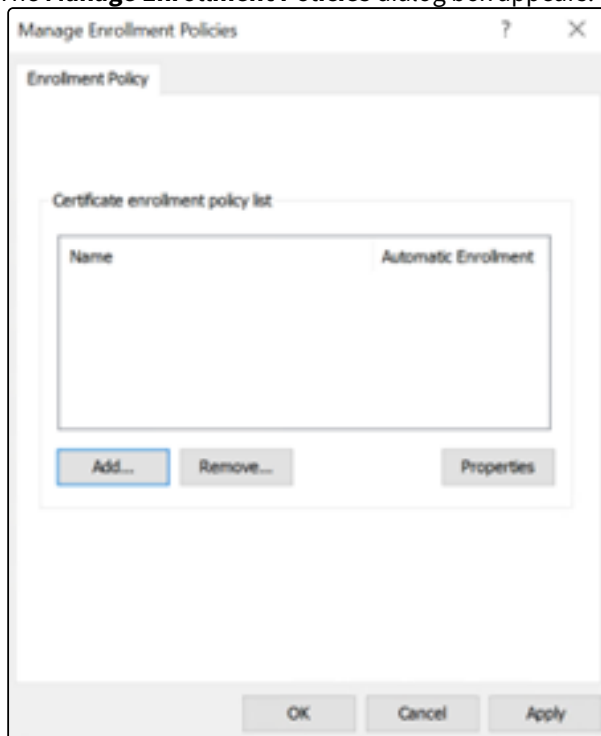


6. Select **My user account**.
7. Click **Finish** to close the **Certificates snap-in** dialog box.
8. Click **OK** to close the **Add or Remove Snap-ins** dialog box.

9. In the tree view, expand **Console Root > Certificates – Current User > Personal**.

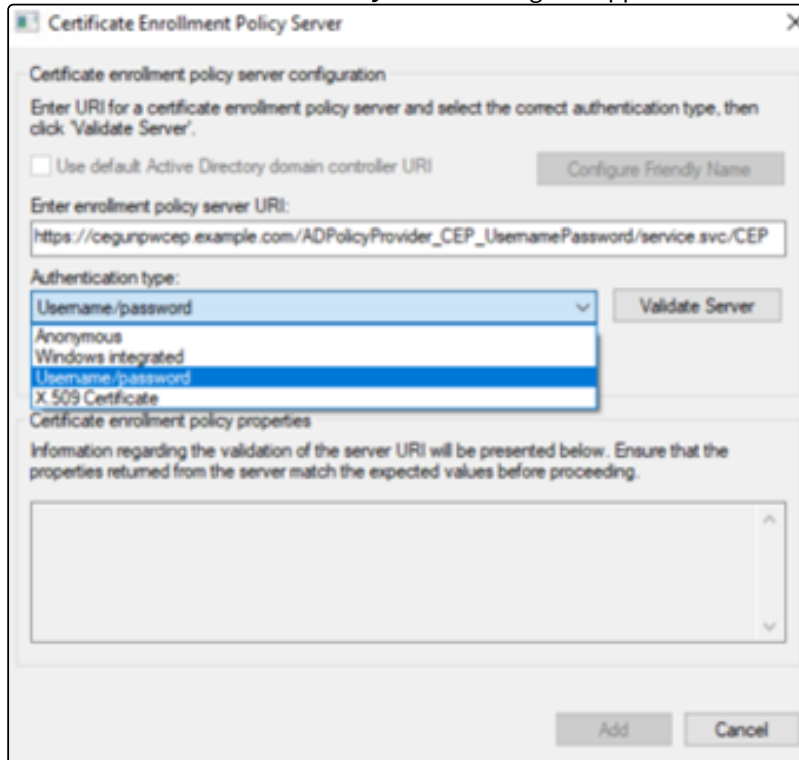


10. Right-click **Personal > All Tasks > Advanced Operations > Manage Enrollment Policies**. The **Manage Enrollment Policies** dialog box appears.



11. Click **Add**.

The **Certificate Enrollment Policy Server** dialog box appears.



The dialog box is titled "Certificate Enrollment Policy Server". It contains the following elements:

- A section titled "Certificate enrollment policy server configuration" with instructions: "Enter URI for a certificate enrollment policy server and select the correct authentication type, then click 'Validate Server'."
- A checkbox labeled "Use default Active Directory domain controller URI" (unchecked) and a disabled "Configure Friendly Name" button.
- A text field labeled "Enter enrollment policy server URI:" containing the text "https://cegumwcep.example.com/ADPolicyProvider_CEP_UsernamePassword/service.svc/CEP".
- A dropdown menu labeled "Authentication type:" with the following options: "Username/password" (selected), "Anonymous", "Windows integrated", "Username/password" (highlighted), and "X.509 Certificate".
- A "Validate Server" button.
- A section titled "Certificate enrollment policy properties" with instructions: "Information regarding the validation of the server URI will be presented below. Ensure that the properties returned from the server match the expected values before proceeding."
- A large empty text area for properties.
- "Add" and "Cancel" buttons at the bottom.

12. In the **Enter enrollment policy server URI** field, enter the URL of the Certificate Enrollment Policy Web Service that you obtained earlier in [Configuring Windows Domain Endpoints](#).
13. In the **Authentication Type** drop-down list, select **Username/Password**.
14. Click **Validate Server**.
15. When prompted, authenticate with your Windows user name and password.
16. Click **Add** to add the URL and close the **Certificate Enrollment Policy Server** dialog box.
17. Click **OK**.

Importing the root CA certificate into non-domain endpoints

In the enrollment endpoints outside the Windows Domain, import the certificate of the CA that will issue certificates for the enrollment service.

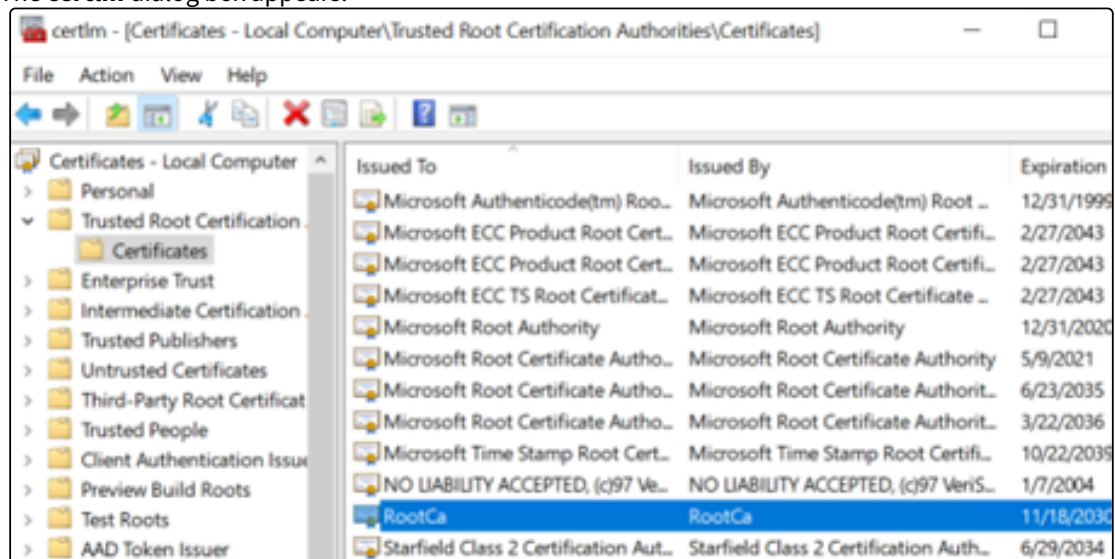
To import the root CA certificate in non-domain endpoints

1. Log in to the non-domain endpoint.
2. Open a Command Prompt window. Select **Start > Windows System > Command Prompt**.
3. Enter the following command.

```
certutil -addstore Root <cert_path>
```

Where `<cert_path>` is the full path and file name of the CA certificate file.

- Open the Certificate Manager snap-in. Select **Start > Run**, then enter `certlm.msc`.
The **certlm** dialog box appears.



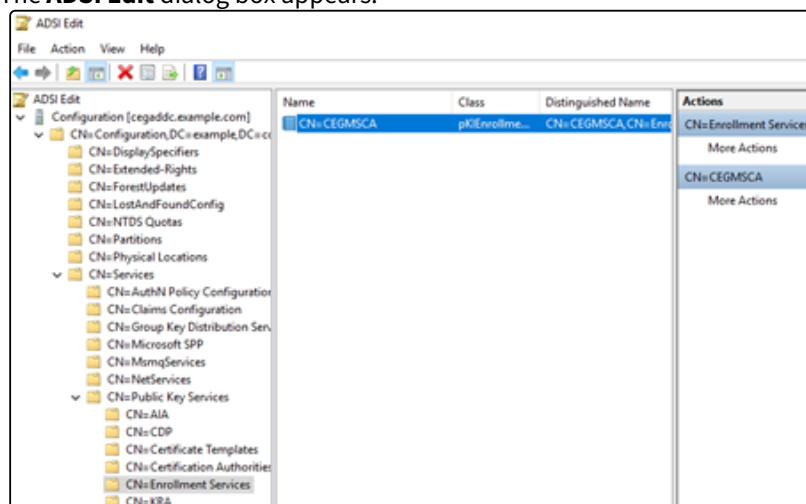
- In the tree view, expand **Certificates – Local Computer > Trusted Root Certification Authorities > Certificates**.
- In the content pane, verify that the root CA certificate you imported appears in the list of trusted root CA certificates.

Adding certificate templates to the enrollment service

Previously, you created certificate templates for the Entrust WSTEP Service (see [Creating Windows certificate templates for the Entrust WSTEP Service](#)). You must add all the certificate templates you created to the enrollment service.

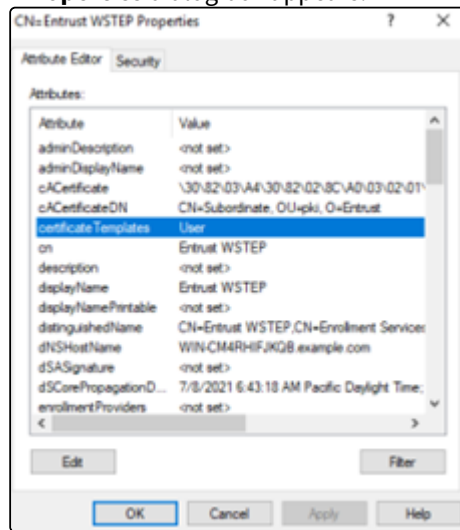
To add certificate templates to the enrollment service

- Log in to the server hosting Active Directory.
- Open ADSI Edit. Select **Start > Windows Administrative Tools > ADSI Edit**.
The **ADSI Edit** dialog box appears.



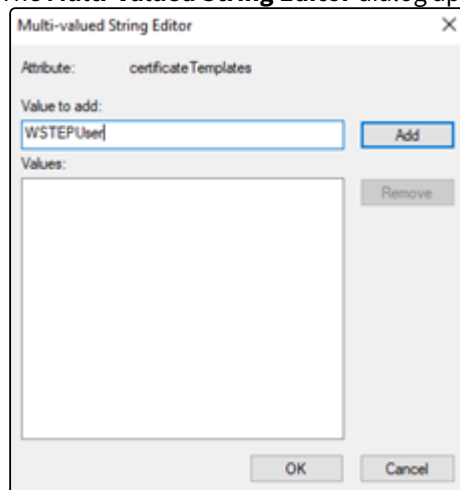
- In the tree view, expand **ADSI Edit > Configuration > CN=Configuration,<suffix> > CN=Services > CN=Public Key Services > CN=Certificate Enrollment Gateway**.

4. Double-click the Active Directory CA enrollment service.
A **Properties** dialog box appears.



5. Click the **Attribute Editor** tab.
6. Under **Attributes**, select **certificateTemplates**.
7. Click **Edit**.

The **Multi-valued String Editor** dialog appears.



8. In the **Value to add** field, paste the name of the certificate template. You must add at least the template with the WSTEPUser name.

i The template name is the value of the template's common name (CN) value. You can get all certificate template names at **ADSI Edit > Configuration > CN=Configuration,<suffix> > CN=Services > CN=Public Key Services > CN=Certificate Templates**.

9. Click **Add**.
10. If required, add additional templates to the list.
11. Click **OK**.

Removing an enrollment service from Active Directory using a PowerShell script

Entrust provides an `InstallEnrollmentService.ps1` PowerShell script that allows you to create, edit, and remove enrollment services in Active Directory. The script also allows you to remove enrollment services from Active Directory.

You should remove an enrollment service only when you will no longer use that enrollment service with Certificate Enrollment Gateway.

To run the script, you must use a Windows user account with Domain Admin and Enterprise Admin permissions.

To update the enrollment URLs for an enrollment service using the `InstallEnrollmentService.ps1` script

1. Open an elevated PowerShell window. Select **Start > Windows PowerShell**, then right-click **Windows PowerShell > Run as administrator**.
2. Navigate to the directory where you extracted the PowerShell scripts.
3. Enter the following command to run the `InstallEnrollmentService.ps1` script:

```
.\InstallEnrollmentService.ps1
```

The script validates the pre-requisites and installs any missing Windows packages or features. For example:

i The PowerShell script was tested on specific versions of PowerShell. When validating the prerequisites, the PowerShell version may be listed as Unverified, an "Unverified" version of PowerShell indicates that the script was not tested on that version of PowerShell. You can still use the script on an "Unverified" version of PowerShell.

```
Validating pre-requisites:
Script-Mode: Windows
Script Version: 1.5.1.19
  - Member of Domain:           Verified
  - Domain Admins privileges:   Verified
  - Enterprise Admins privileges: Verified
  - Windows Version:           Verified (Microsoft Windows NT 10.0.17763.0)
  - PowerShell Version:        Verified (5.1.17763.2931)

-----
Validating ldifde is installed.

ldifde.exe is installed.

Validating Windows Feature RSAT-ADCS-Mgmt is installed
Installing RSAT-ADCS-Mgmt
```

4. The script prompts you to select a management option:

```
Entrust Enrollment Service PowerShell
```

```
Using this PowerShell script, Enrollments servers can be created, removed
and Edited.
```

```
Please select from the following options to continue :  
[N] New Service [E] Edit Service [Q] Quit [?] Help (default is "N"):
```

Enter **E** to edit an existing enrollment service.

5. If more than one enrollment service is defined in Active Directory, the script displays the list of enrollment services and asks you to select one of the enrollment services:

```
Select from the following List of defined Certificate Enrollment Gateway :
```

```
Index Enrollment Service Name  
-----
```

```
1      CEG WSTEP  
2      Entrust WSTEP
```

```
Please select the Index to select an Enrollment Service. 0 to quit.:
```

Enter the number associated with the enrollment service you want to edit. If only one enrollment service exists, that service is automatically selected by the script.

6. The script displays the currently-selected enrollment service, and prompts you to choose from a list of options:

```
Currently Selected Enrollment Service : Entrust WSTEP
```

```
Choose from the following Options:
```

```
[E] Edit [R] Remove [P] Previous [?] Help (default is "E"):
```

Enter **R** to remove the selected enrollment service.

7. The script asks you to confirm the operation:

```
Removing Enrollment Service : CEG WSTEP
```

```
Are you sure you want to delete this Enrollment Service(y/n)?:
```

- To confirm that you want to delete the enrollment service, enter **y**. The script deletes the enrollment service from Active Directory.
- To cancel the operation and return to the previous menu, enter **n**.

8. To exit the script after removing the enrollment service:

- a. Keep entering **P** to return to a previous menu until you return to the main menu:

```
Entrust Enrollment Service PowerShell
```

```
Using this PowerShell script, Enrollments servers can be created, removed  
and Edited.
```

```
Please select from the following options to continue :
```



```
[N] New Service [E] Edit Service [Q] Quit [?] Help (default is "N"):
```

b. Enter `Q` to exit the script.

Editing an enrollment service in Active Directory using Windows tools

This section describes how to edit an enrollment service in Active Directory using native Windows tools.

- [Building the Enrollment URL](#)
- [Changing the enrollment URL of the enrollment service using ADSI Edit](#)
- [Adding the enrollment URL to the enrollment service using the certutil utility](#)

Building the Enrollment URL

To build the Enrollment Service URL, use the following syntax:

```
https://<CEG-server>:443/wstep/<auth>/services/<tenant-ID>/<CA-ID>
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<auth>` is the authentication method, either `usertoken` for user name and password authentication or `kerberos` for Kerberos (Windows integrated) authentication.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the Windows endpoint.

For example, when authenticating with a user name and password:

```
https://cegserver1.example.com:443/wstep/usertoken/services/tenant1/example-ca1
```

For example, when authenticating with Kerberos:

```
https://cegserver1.example.com:443/wstep/kerberos/services/tenant1/example-ca1
```

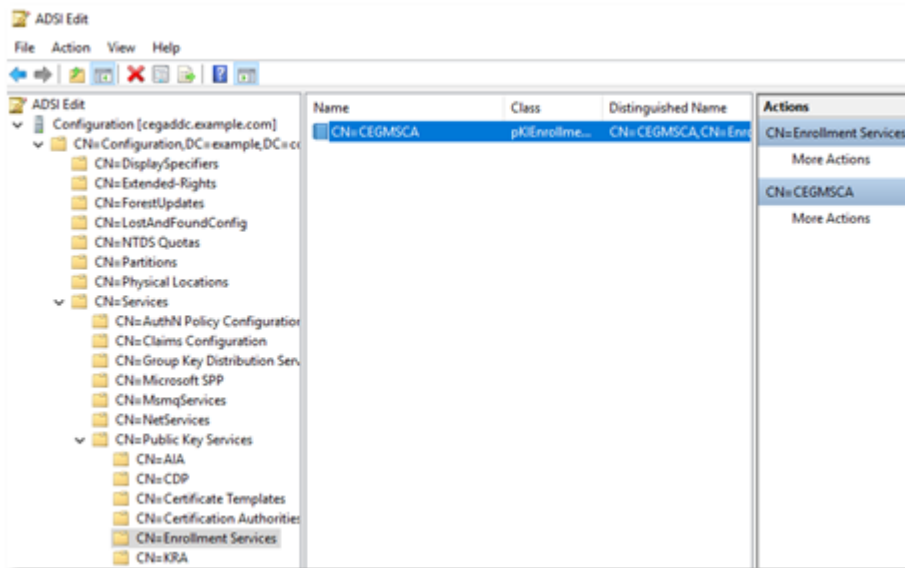
Changing the enrollment URL of the enrollment service using ADSI Edit

To add the enrollment service URL to Active Directory using ADSI Edit, complete the following procedure.

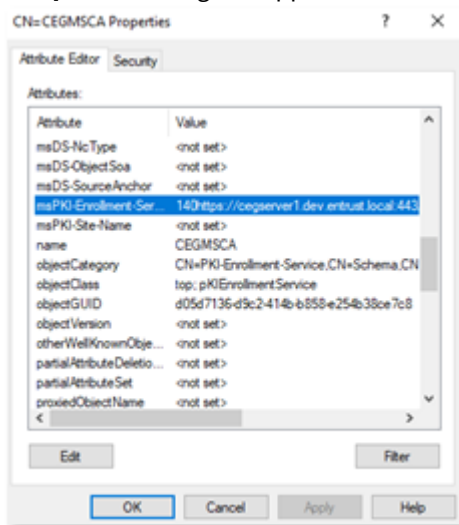
To add the enrollment service URL to Active Directory using ADSI Edit

1. Log in to the server hosting Active Directory.

- Open ADSI Edit. Select **Start > Windows Administrative Tools > ADSI Edit**. The **ADSI Edit** dialog box appears.



- In the tree view, expand **ADSI Edit > Configuration > CN=Configuration,<suffix> > CN=Services > CN=Public Key Services > CN=Certificate Enrollment Gateway**.
- Double-click the Active Directory CA enrollment service. A **Properties** dialog box appears.



- Click the **Attribute Editor** tab.
- Under **Attributes**, select **msPKI-Enrollment-Servers**. The URL in this field is preceded by three integers, where:
 - The first integer is the Priority of the service URL.
 - The second integer is the authentication method: 2 for Kerberos authentication, 4 for username and password authentication.
 - The third integer is 0 for certificate enrollment and renewal or 1 for certificate renewal only.
- Click **Edit**.
- Replace the current URL with the URL you built earlier in [Building the Enrollment URL](#).

❌ Do not overwrite the preceding integers when replacing the URL. The integers are required.

9. Click **OK**.

Adding the enrollment URL to the enrollment service using the certutil utility

On the Active Directory server, open a Command Prompt window and run the following command to add the Enrollment Service URL with the `certutil` utility.

```
certutil -config "<name>" -enrollmentserverURL <url> <auth> [<priority>]
```

Where:

- `<name>` is the name of the enrollment service.
- `<url>` is the URL described in [Building the Enrollment URL](#).
- `<auth>` is the identifier of the authentication mode: `kerberos` for Kerberos authentication, or `usertoken` for user name and password authentication.
- `<priority>` is the server priority. If you omit this parameter, the value defaults to 1.

For example, when authenticating with a user name and password:

```
certutil -config "CEGMSCA" -enrollmentserverURL https://cegserver1.example.com:443/wstep/usertoken/services/tenant1/example-ca1 username
```

For example, when authenticating with Kerberos:

```
certutil -config "CEGMSCA" -enrollmentserverURL https://cegserver1.example.com:443/wstep/kerberos/services/tenant1/example-ca1 kerberos
```

To check the added URL, run `certutil` without arguments. For example:

```
PS C:\Windows\system32> certutil
Entry 0:
  Name: "CEGMSCA"
  Organizational Unit: ""
  Organization: ""
  Locality: ""
  State: ""
  Country/region: ""
  Config: "cegmsca.example.com\CEGMSCA"
  Exchange Certificate: ""
  Signature Certificate: ""
  Description: ""
  Server: "cegmsca.example.com"
  Authority: "CEGMSCA"
  Sanitized Name: "CEGMSCA"
  Short Name: "CEGMSCA"
  Sanitized Short Name: "CEGMSCA"
```

```
Flags:                                "1"
Web Enrollment Servers:
1
4
0
https://cegserver1.example.com:443/wstep/usertoken/services/tenant1/example-ca1
0

1
2
0
https://cegserver1.example.com:443/wstep/kerberos/services/tenant1/example-ca1
0
CertUtil: -dump command completed successfully.
```

Editing an enrollment service in Active Directory using a PowerShell script

Entrust provides an `InstallEnrollmentService.ps1` PowerShell script that allows you to create, edit, and remove enrollment services in Active Directory. When editing an enrollment service in Active Directory, you can:

- Update the enrollment URLs assigned to the enrollment service.
- Update security groups (access groups) assigned to the enrollment service.

To run the script, you must use a Windows user account with Domain Admin and Enterprise Admin permissions.

- [Updating the enrollment URLs for an enrollment service using a PowerShell script](#)
- [Updating the security groups for an enrollment service using a PowerShell script](#)

Updating the enrollment URLs for an enrollment service using a PowerShell script

Entrust provides an `InstallEnrollmentService.ps1` PowerShell script that allows you to create, edit, and remove enrollment services in Active Directory. When editing an enrollment service in Active Directory, you can update the enrollment URLs assigned to the enrollment service. When updating the enrollment URLs assigned to an enrollment service, you can:

- List all the enrollment URLs that are assigned to the enrollment service.
- Add an enrollment URL to the enrollment service.
- Remove one or all enrollment URLs from the enrollment service.

To run the script, you must use a Windows user account with Domain Admin and Enterprise Admin permissions.

To update the enrollment URLs for an enrollment service using the `InstallEnrollmentService.ps1` script

1. Open an elevated PowerShell window. Select **Start > Windows PowerShell**, then right-click **Windows PowerShell > Run as administrator**.
2. Navigate to the directory where you extracted the PowerShell scripts.
3. Enter the following command to run the `InstallEnrollmentService.ps1` script:

```
.\InstallEnrollmentService.ps1
```

The script validates the prerequisites and installs any missing Windows packages or features. For example:

i The PowerShell script was tested on specific versions of PowerShell. When validating the prerequisites, the PowerShell version may be listed as Unverified, an "Unverified" version of PowerShell indicates that the script was not tested on that version of PowerShell. You can still use the script on an "Unverified" version of PowerShell.

```
Validating pre-requisites:
Script-Mode: Windows
Script Version: 1.5.1.19
  - Member of Domain:          Verified
  - Domain Admins privileges:  Verified
  - Enterprise Admins privileges: Verified
  - Windows Version:          Verified (Microsoft Windows NT
10.0.17763.0)
  - PowerShell Version:       Verified (5.1.17763.2931)

-----

Validating ldifde is installed.

ldifde.exe is installed.

Validating Windows Feature RSAT-ADCS-Mgmt is installed
Installing RSAT-ADCS-Mgmt
```

4. The script prompts you to select a management option:

```
Entrust Enrollment Service PowerShell

Using this PowerShell script, Enrollments servers can be created, removed
and Edited.

Please select from the following options to continue :
[N] New Service [E] Edit Service [Q] Quit [?] Help (default is "N"):
```

Enter **E** to edit an existing enrollment service.

5. If more than one enrollment service is defined in Active Directory, the script displays the list of enrollment services and asks you to select one of the enrollment services:

```
Select from the following List of defined Certificate Enrollment Gateway :

Index Enrollment Service Name
-----
1      CEG WSTEP
2      Entrust WSTEP

Please select the Index to select an Enrollment Service. 0 to quit.:
```

Enter the number associated with the enrollment service you want to edit. If only one enrollment service exists, that service is automatically selected by the script.

6. The script displays the currently-selected enrollment service, and prompts you to choose from a list of options:

```
Currently Selected Enrollment Service : Entrust WSTEP

Choose from the following Options:
[E] Edit  [R] Remove  [P] Previous  [?] Help (default is "E"):
```

Enter **E** to edit the selected service.

7. The script prompts you to select an edit option:

```
Updating Enrollment Service : Entrust WSTEP

Menu to select between:
Updating the Enrollment Service URL(s)
Updating the Security Groups for the Enrollment Service.

Choose from the following Options:
[U] Update URL(s)  [S] Update Security Group(s)  [P] Previous  [?] Help
(default is "U"):
```

Enter **U** to update the enrollment URLs.

8. The script asks you to select an update option:

```
Editing the URL(s) for Enrollment Service : Entrust WSTEP

Choose from the following Options:
[A] Add URL  [D] Delete URL  [L] List URL  [P] Previous  [?] Help (default is
"L"):
```

- To list all enrollment URLs for the enrollment service, enter **L**.
- To delete an enrollment URL from the enrollment service, enter **D**.
- To add an enrollment URL to the enrollment service, enter **A**.

9. If you chose to list the enrollment URLs for the enrollment service, the script displays information about each enrollment URL for the enrollment service. For example:

```
Enrollment Service Name : Entrust WSTEP

Priority      : 1
Auth Type    : UserName
Renewal Only : 0
URL          : https://cegserver1.example.com:443/wstep/usertoken/services/
tenant1/example-ca1
```

For each URL, the script displays the following information:

- **Priority** displays the priority of the enrollment server. If multiple enrollment servers are defined, then the priority determines which enrollment server is preferred.

- **Auth Type** displays the authentication type, either **UserName** for user name and password authentication, or **Kerberos** for Kerberos authentication (integrated Windows authentication).
- **Renewal Only** indicates if the enrollment URL is for certificate renewal only.
0 indicates that the enrollment URL is for both certificate enrollment and renewal.
1 indicates that the enrollment URL is for certificate renewal only.
- **URL** displays the enrollment URL.

10. If you chose to delete an enrollment URL from the enrollment service:

- a. The script displays a list of enrollment URLs and asks you to select which URL to remove:

```
Selected Enrollment Service Name : Entrust WSTEP
```

```
Retrieving URL(s) from AD.
```

```
Index    URL
```

```
-----
```

```
1        https://cegserver1.example.com:443/wstep/usertoken/services/tenant1/example-ca1
```

```
Select the URL to remove. -1 to remove all, 0 to quit.:
```

- To remove a specific enrollment URL, enter the number associated with the URL in the list.
- To remove all enrollment URLs, enter -1.
- To go back without removing any enrollment URLs, enter 0.

- b. The script asks you to confirm the removal of the URL or URLs. For example:

```
https://cegserver1.example.com:443/wstep/usertoken/services/tenant1/example-ca1 is slated to be removed  
Continue with removal of URL (y/n)?:
```

- To confirm that you want remove the URL, enter **y**.
- To cancel the removal, enter **n**.

11. If you chose to add an enrollment URL to the enrollment service, the script asks if you want to configure an enrollment URL for user name and password authentication:

```
Configure UserName Enrollment URL ? (y/n):
```

- To configure an enrollment URL for user name and password authentication, enter **y**.
- To skip configuring an enrollment URL for user name and password authentication, enter **n**.

12. If you chose to add an enrollment URL for user name and password authentication:

- a. The script prompts you to enter an enrollment URL:

```
Please enter the Enrollment Server URL :
```

Enter the enrollment URL using the following format:

```
https://<CEG-server>:443/wstep/usertoken/services/<tenant-ID>/<CA-ID>
```

Where:

- **<CEG-server>** is the hostname or IP address of the Certificate Enrollment Gateway server.

- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the Windows endpoint.

For example:

```
https://cegserver1.example.com:443/wstep/usertoken/services/tenant1/
example-ca1
```

- b. The script prompts you to specify the priority of the enrollment server:

The URI for the enrollment server which has the lowest priority number as defined in the enrollment policy. If two enrollment servers have the same priority then

- a. The URI with the following authentication type is preferred in order:
Kerberos, Anonymous, Username/Password cached in the vault or Client Auth Certificate cached in the vault, Username/Password or Client Auth Certificate.
- b. If all properties are equal then a URI is randomly selected.

Please enter the Priority of this Enrollment URL [Default : 1]:

If multiple enrollment servers are defined, then the priority determines which enrollment server is preferred. Enter the priority for the enrollment server.

- c. The script asks if the URL will be used for certificate renewal only:

Will this URL be used for Renewal ONLY ? (y/n):

- If the enrollment URL is for certificate renewal only, enter `y`.
- If the enrollment URL is for certificate enrollment and renewal, enter `n`.

- d. The script displays information about the enrollment URL and asks if you want to continue:

```
Enrollment Service : Entrust WSTEP
Authentication Type : UserName
Enrollment URL      : https://cegserver1.example.com:443/wstep/usertoken/
services/tenant1/example-ca1
Priority             : 1
Modifiers            :
Continue with above settings? (y/n):
```

- To continue and add the enrollment URL, enter `y`.
- To go back and re-enter information about the enrollment URL, enter `n`.

13. If you chose to add an enrollment URL to the enrollment service, the script asks if you want to configure an enrollment URL for Kerberos (Windows integrated) authentication:

Configure Kerberos Enrollment URL ? (y/n):

- To configure an enrollment URL for Kerberos authentication, enter **y**.
- To skip configuring an enrollment URL for Kerberos authentication, enter **n**.

14. If you chose to add an enrollment URL for Kerberos authentication:

a. The script prompts you to enter an enrollment URL:

Please enter the Enrollment Server URL :

Enter the enrollment URL using the following format:

```
https://<CEG-server>:443/wstep/kerberos/services/<tenant-ID>/<CA-ID>
```

Where:

- **<CEG-server>** is the hostname or IP address of the Certificate Enrollment Gateway server.
- **<tenant-ID>** is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- **<CA-ID>** is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the Windows endpoint.

For example:

```
https://cegserver1.example.com:443/wstep/kerberos/services/tenant1/  
example-ca1
```

b. The script prompts you to specify the priority of the enrollment server:

The URI for the enrollment server which has the lowest priority number as defined in the enrollment policy. If two enrollment servers have the same priority then

- a. The URI with the following authentication type is preferred in order:
Kerberos, Anonymous, Username/Password cached in the vault or Client Auth Certificate cached in the vault, Username/Password or Client Auth Certificate.
- b. If all properties are equal then a URI is randomly selected.

Please enter the Priority of this Enrollment URL [Default : 1]:

If multiple enrollment servers are defined, then the priority determines which enrollment server is preferred. Enter the priority for the enrollment server.

c. The script asks if the URL will be used for certificate renewal only:

Will this URL be used for Renewal ONLY ? (y/n):

- If the enrollment URL is for certificate renewal only, enter **y**.
- If the enrollment URL is for certificate enrollment and renewal, enter **n**.

- d. The script displays information about the enrollment URL and asks if you want to continue:

```
Enrollment Service : Entrust WSTEP
Authentication Type : Kerberos
Enrollment URL      : https://cegserver1.example.com:443/wstep/kerberos/
services/tenant1/example-ca1
Priority             : 1
Modifiers            :
Continue with above settings? (y/n):
```

- To continue and add the enrollment URL, enter **y**.
- To go back and re-enter information about the enrollment URL, enter **n**.

15. To exit the script after updating the enrollment URLs:

- a. Keep entering **P** to return to a previous menu until you return to the main menu:

```
Entrust Enrollment Service PowerShell

Using this PowerShell script, Enrollments servers can be created, removed
and Edited.

Please select from the following options to continue :
[N] New Service [E] Edit Service [Q] Quit [?] Help (default is "N"):
```

- b. Enter **Q** to exit the script.

Updating the security groups for an enrollment service using a PowerShell script

Entrust provides an `InstallEnrollmentService.ps1` PowerShell script that allows you to create, edit, and remove enrollment services in Active Directory. When editing an enrollment service in Active Directory, you can update the security groups (access groups) assigned to the enrollment service. When updating the security groups assigned to an enrollment service, you can:

- List all the security groups that are assigned to the enrollment service.
- Add a security group to the enrollment service.
- Remove a security group from to the enrollment service.

To run the script, you must use a Windows user account with Domain Admin and Enterprise Admin permissions.

To update the security groups for an enrollment service using the `InstallEnrollmentService.ps1` script

1. Open an elevated PowerShell window. Select **Start > Windows PowerShell**, then right-click **Windows PowerShell > Run as administrator**.
2. Navigate to the directory where you extracted the PowerShell scripts.
3. Enter the following command to run the `InstallEnrollmentService.ps1` script:

```
.\InstallEnrollmentService.ps1
```

The script validates the pre-requisites and installs any missing Windows packages or features. For example:

i The PowerShell script was tested on specific versions of PowerShell. When validating the prerequisites, the PowerShell version may be listed as Unverified, an "Unverified" version of PowerShell indicates that the script was not tested on that version of PowerShell. You can still use the script on an "Unverified" version of PowerShell.

```
Validating pre-requisites:
Script-Mode: Windows
Script Version: 1.5.1.19
  - Member of Domain:          Verified
  - Domain Admins privileges:  Verified
  - Enterprise Admins privileges: Verified
  - Windows Version:          Verified (Microsoft Windows NT
10.0.17763.0)
  - PowerShell Version:       Verified (5.1.17763.2931)

-----

Validating ldifde is installed.

ldifde.exe is installed.

Validating Windows Feature RSAT-ADCS-Mgmt is installed
Installing RSAT-ADCS-Mgmt
```

4. The script prompts you to select a management option:

```
Entrust Enrollment Service PowerShell

Using this PowerShell script, Enrollments servers can be created, removed
and Edited.

Please select from the following options to continue :
[N] New Service  [E] Edit Service  [Q] Quit  [?] Help (default is "N"):
```

Enter **E** to edit an existing enrollment service.

5. If more than one enrollment service is defined in Active Directory, the script displays the list of enrollment services and asks you to select one of the enrollment services:

```
Select from the following List of defined Certificate Enrollment Gateway :

Index Enrollment Service Name
-----
1      CEG WSTEP
2      Entrust WSTEP

Please select the Index to select an Enrollment Service. 0 to quit.:
```

Enter the number associated with the enrollment service you want to edit. If only one enrollment service exists, that service is automatically selected by the script.

6. The script displays the currently-selected enrollment service, and prompts you to choose from a list of options:

```
Currently Selected Enrollment Service : Entrust WSTEP

Choose from the following Options:
[E] Edit [R] Remove [P] Previous [?] Help (default is "E"):
```

Enter **E** to edit the selected service.

7. The script prompts you to select an edit option:

```
Updating Enrollment Service : Entrust WSTEP

Menu to select between:
Updating the Enrollment Service URL(s)
Updating the Security Groups for the Enrollment Service.

Choose from the following Options:
[U] Update URL(s) [S] Update Security Group(s) [P] Previous [?] Help
(default is "U"):
```

Enter **S** to update the security groups.

8. The script asks you to select an update option:

```
Updating Security Groups for Enrollment Service: Entrust WSTEP

Choose from the following Options:
[A] Add Security Group(s) [R] Remove Security Group(s) [L] List Security
Group(s) [P] Previous [?] Help
(default is "L"):
```

- To list all security groups for the enrollment service, enter **L**.
- To remove a security group from the enrollment service, enter **D**.
- To add a security group to the enrollment service, enter **A**.

9. If you chose to list the security groups for the enrollment service, the script displays a list of security groups assigned to the enrollment service. For example:

Index	SecurityGroup	Permission
-----	-----	-----
1	NT AUTHORITY\Authenticated Users	Allow
2	NT AUTHORITY\SYSTEM	Allow
3	EXAMPLE-AD\Domain Admins	Allow
4	EXAMPLE-AD\Entrust WSTEP Access	Allow
5	EXAMPLE-AD\Enterprise Admins	Allow
6	EXAMPLE-AD\Domain Admins	Allow

10. If you chose to remove a security group from the enrollment service:

- a. The script displays a list of security groups assigned to the enrollment service and asks you to select which security group to remove:

Index	SecurityGroup	Permission
1	NT AUTHORITY\Authenticated Users	Allow
2	NT AUTHORITY\SYSTEM	Allow
3	EXAMPLE-AD\Domain Admins	Allow
4	EXAMPLE-AD\Entrust WSTEP Access	Allow
5	EXAMPLE-AD\Enterprise Admins	Allow
6	EXAMPLE-AD\Domain Admins	Allow

Select the index of the Security Group to be removed. 0 to quit. :

Enter the index number associated with the security group you want to remove from the enrollment service.

- b. The script asks you to confirm the removal of security group. For example:

Removing Security Group : EXAMPLE-AD\Domain Admins
Are you sure you want to remove the Security Group (y/n)?:

- To confirm that you want remove the security group from the enrollment service, enter **y**.
- To cancel the removal, enter **n**.

11. If you chose to add a security group to the enrollment service:

- a. The script displays information about how to enter the name of the security group, then asks you to enter the security group you want to add to the enrollment service:

The Security group must exist before this script can add to the Enrollment Service.

Enrollment service to be modified : Entrust WSTEP

For a Security Group, the following options are supported :

- 1) domain\group
- 2) domain.com\group
- 3) group@domain
- 4) group@domain.com

Security Groups must be:

- 1) GroupCategory must be Security
- 2) objectClass must be type group

Enter security Group. 0 to quit.:

Enter the name of the security group you want to add to the enrollment service, or enter 0 to go back without adding a security group.

The security group must already exist in Active Directory. In Active Directory, the GroupCategory of the group must be **Security**, and the objectClass of the group must be **group**.

You must enter the name of the group using one of the following formats:

- <domain>\<group>
- <fqdn>\<group>
- <group>@<domain>
- <group>@<fqdn>

Where:

- <domain> is the Active Directory domain where the security group is located.
- <fqdn> is the fully-qualified domain name of the Active Directory forest where the security group is located.
- <group> is the name of the security group.

Examples:

```
EXAMPLE\Example Group
EXAMPLE.COM\Example Group
Example Group@EXAMPLE
Example Group@EXAMPLE.COM
```

- b. The script adds the security group to the enrollment service. For example:

```
Adding the Access group : EXAMPLE-AD\Domain Users to the Enrollment
Service : Entrust WSTEP
Access Group EXAMPLE-AD\Domain Users added to Enrollment Service : Entrust
WSTEP
```

12. To exit the script after updating the security groups assigned to the enrollment service:

- a. Keep entering **P** to return to a previous menu until you return to the main menu:

```
Entrust Enrollment Service PowerShell

Using this PowerShell script, Enrollments servers can be created, removed
and Edited.

Please select from the following options to continue :
[N] New Service [E] Edit Service [Q] Quit [?] Help (default is "N"):
```

- b. Enter **Q** to exit the script.

Creating an enrollment service in Active Directory using a PowerShell script

You must create an enrollment service for each CA that will issue certificates to the WSTEP endpoints. Entrust provides an [InstallEnrollmentService.ps1](#) PowerShell script that allows you to create, edit, and remove enrollment services in Active Directory.

To run the script, you must use a Windows user account with Domain Admin and Enterprise Admin permissions.

An enrollment service requires a DER-encoded CA certificate from the issuing CA. The script will prompt you to provide the CA certificate when creating an enrollment service.

To created an enrollment service with the InstallEnrollmentService.ps1 script

1. Log in to a Windows server that is joined to the Active Directory domain. It is recommended that you run the PowerShell script on a different server than the domain controller.

2. From Entrust TrustedCare, download the PowerShell scripts for Certificate Enrollment Gateway.
3. Extract the PowerShell scripts to a directory on the server.
4. PowerShell scripts downloaded from the Internet may be blocked from running. To unblock a PowerShell script:
 - a. Right-click the PowerShell script > **Properties**.
A **Properties** dialog box appears.
 - b. Under the **General** tab, click **Unblock**.
5. Open an elevated PowerShell window. Select **Start > Windows PowerShell**, then right-click **Windows PowerShell > Run as administrator**.
6. Navigate to the directory where you extracted the PowerShell scripts.
7. Enter the following command to run the `InstallEnrollmentService.ps1` script:

```
.\InstallEnrollmentService.ps1
```

The script validates the pre-requisites and installs any missing Windows packages or features. For example:

i The PowerShell script was tested on specific versions of PowerShell. When validating the prerequisites, the PowerShell version may be listed as Unverified, an "Unverified" version of PowerShell indicates that the script was not tested on that version of PowerShell. You can still use the script on an "Unverified" version of PowerShell.

```
Validating pre-requisites:
Script-Mode: Windows
Script Version: 1.5.1.19
  - Member of Domain:           Verified
  - Domain Admins privileges:   Verified
  - Enterprise Admins privileges: Verified
  - Windows Version:           Verified (Microsoft Windows NT 10.0.17763.0)
  - PowerShell Version:        Verified (5.1.17763.2931)

-----
Validating ldifde is installed.

ldifde.exe is installed.

Validating Windows Feature RSAT-ADCS-Mgmt is installed
Installing RSAT-ADCS-Mgmt
```

8. The script prompts you to select a management option:

```
Entrust Enrollment Service PowerShell

Using this PowerShell script, Enrollments servers can be created, removed
and Edited.

Please select from the following options to continue :
[N] New Service  [E] Edit Service  [Q] Quit  [?] Help (default is "N"):
```

Enter **N** to create a new enrollment service.

9. The script prompts you to provide the distinguished name (DN) of the configuration context.

```
Configuration Context DN
Format : DC=Example,DC=com
Configuration Context For Enrollment Service [Default: DC=example,DC=com]:
```

Enter the DN of the configuration context for Active Directory. The default value is the configuration context of the Active Directory forest.

10. The script prompts you to provide the host name for the enrollment service:

```
Hostname for Enrollment Service
Enrollment Service Hostname [Default: mmwin2019-2.example-ad.local]:
```

Enter the fully qualified domain name (FQDN) for the enrollment service. The default host name is the FQDN of the local server.

11. The script prompts you to provide a name for the enrollment service.

```
Enrollment Service Name is required to continue configuration
Enrollment Service Name [Default: Entrust WSTEP]:
```

Enter a name for the enrollment service. When entering a name:

- The name must be unique in the Active Directory forest.
- The name must start with an alphanumeric character.
- The name must contain only alphanumeric characters, spaces, hyphens, and underscores.

12. The script prompts you to provide the CA certificate from the issuing Certificate Authority (CA).

```
A der formatted certificate is required from the issuing CA.
Please use the full pathname and filename.
Example : C:\Users\admin\Downloads\cacert.der
Provide the full path and filename for the issuing CA certificate to proceed:
```

Enter the full path and file name of the certificate file. The CA certificate must be DER-encoded.

13. The script parses the file contents, displays the certificate settings, then asks if you want to use the certificate. For example:

```
Parsing Issuing CA cert for Subject DN.
Issuing CA Subject DN           : CN=Subordinate, OU=pki, O=Entrust
Issuing CA Certificate Effective Date : 5/25/2021 2:52:36 PM
Issuing CA Certificate Expiry Date   : 5/23/2031 2:52:36 PM
Use this CA Certificate? (y/n): y
```

- To use the selected CA certificate and continue, enter **y**.
- To go back and provide a different CA certificate, enter **n**.

14. The script prompts you to select the initial Certificate Template to be associated with the enrollment service:

```
Please select the initial Certificate Template to be associated
with the Enrollment Service.
```


The 'Template Name' cannot contain any spaces.
Certificate Template [Default: User]:

Enter the name of an existing Certificate Template to use as the initial Certificate Template for the enrollment service. The name cannot contain spaces.

15. The script asks if you want to continue with the selected Certificate Template.

Continue with User ? (y/n):

- To continue with the selected initial Certificate Template for the enrollment service, enter **y**.
- To go back and change the initial Certificate Template for the enrollment service, enter **n**.

16. The script displays the information you provided for the enrollment service and asks if you want to continue. For example:

```
Configuration Context DN      : DC=example,DC=com
Forest                       : example.com
Local hostname as DNS Hostname : cegaddc.example.com
Enrollment Service Name     : Entrust WSTEP
Issuing CA Der formatted Certificate : C:\EntrustPSScripts\ca.cer
Issuing CA                   : CN=Subordinate, OU=pki, O=Entrust
Certificate Template         : User
```

Continue with the above settings? (y/n):

- To continue with the settings and add the enrollment service to Active Directory, enter **y**.
- To go back and change all the settings for the enrollment service, enter **n**.

17. The script prompts you to provide the name of a new access group:

An Access group will be created for the Enrollment Service

By default, Active Directory provides the following domain groups for users, computers, and domain controllers: Domain Users, Domain Computers, and Domain Controllers. Creating a custom domain group for your Entrust WSTEP clients ensures that only members of the custom domain group (your Windows-native clients) can request certificates.

Configuring Access Group for example.com

Access Group Name [Default: Entrust WSTEP Access]:

By default, Active Directory provides the following domain groups for users, computers, and domain controllers: Domain Users, Domain Computers, and Domain Controllers. Creating a custom access group for your Windows-native clients ensures that only members of the custom access group (your Windows-native clients) can request certificates through the enrollment service.

Enter a name for the new access group (by default, Entrust WSTEP Access).

18. The script asks if you want to continue adding the new access group:

Continue adding Access Group : Entrust WSTEP Access ? (y/n):

- To add the access group to the forest and continue, enter **y**.
The script waits 20 seconds to allow the group to propagate in Active Directory.

```
Pausing for 20 seconds to allow for the group to propagate
19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Resuming
```

```
Adding the Access group : Entrust WSTEP Access to the Enrollment Service :
Entrust WSTEP
Access Group example.com\Entrust WSTEP Access added to Enrollment
Service : Entrust WSTEP
```

- To go back and enter and enter a new access group name, enter **n**.
19. If the current domain is a top-level domain with subdomains, the script will ask if you want to set up an access group for enabling the enrollment service in one of the subdomains.
- To add the access group to the subdomain, enter **y**.
 - To go back and enter and enter a new access group name, enter **n**.
20. The script asks if you want to configure enrollment server URLs using the script:

Continue script to configure Enrollment Server URL(s) (y/n):

- To continue and configure enrollment server URLs using the script, enter **y**.
The script displays a list of enrollment servers for the configured enrollment service. By default, the list should be NULL (no enrollment servers for the enrollment service). For example:

```
Enrollment Service Name : Entrust WSTEP
```

```
NULL set of Enrollment servers.
```

- To exit the script and configure the enrollment server URLs using the **certutil** utility later, enter **n**.
21. If you chose to configure enrollment server URLs using the script, the script asks if you want to configure an enrollment URL for user name and password authentication:

Configure UserName Enrollment URL ? (y/n):

- To configure an enrollment URL for user name and password authentication, enter **y**.
 - To skip configuring an enrollment URL for user name and password authentication, enter **n**.
22. If you chose to configure an enrollment URL for user name and password authentication:
- a. The script prompts you to enter an enrollment URL:

```
Please enter the Enrollment Server URL :
```

Enter the enrollment URL using the following format:

```
https://<CEG-server>:443/wstep/usertoken/services/<tenant-ID>/<CA-ID>
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the Windows endpoint.

For example:

```
https://cegserver1.example.com:443/wstep/usertoken/services/tenant1/example-ca1
```

- b. The script prompts you to specify the priority of the enrollment server:

The URI for the enrollment server which has the lowest priority number as defined in the enrollment policy. If two enrollment servers have the same priority then

- a. The URI with the following authentication type is preferred in order:
Kerberos, Anonymous, Username/Password cached in the vault or Client Auth Certificate cached in the vault, Username/Password or Client Auth Certificate.
- b. If all properties are equal then a URI is randomly selected.

Please enter the Priority of this Enrollment URL [Default : 1]:

If multiple enrollment servers are defined, then the priority determines which enrollment server is preferred. Enter the priority for the enrollment server.

- c. The script asks if the URL will be used for certificate renewal only:

```
Will this URL be used for Renewal ONLY ? (y/n):
```

- If the enrollment URL is for certificate renewal only, enter `y`.
- If the enrollment URL is for certificate enrollment and renewal, enter `n`.

23. If you chose to configure enrollment server URLs using the script, the script asks if you want to configure an enrollment URL for Kerberos (Windows integrated) authentication:

```
Configure Kerberos Enrollment URL ? (y/n):
```

- To configure an enrollment URL for Kerberos authentication, enter `y`.
- To skip configuring an enrollment URL for Kerberos authentication, enter `n`.

24. If you chose to configure an enrollment URL for Kerberos authentication:

- a. The script prompts you to enter an enrollment URL:

Please enter the Enrollment Server URL :

Enter the enrollment URL using the following format:

```
https://<CEG-server>:443/wstep/kerberos/services/<tenant-ID>/<CA-ID>
```

Where:

- **<CEG-server>** is the hostname or IP address of the Certificate Enrollment Gateway server.
- **<tenant-ID>** is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- **<CA-ID>** is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the Windows endpoint.

For example:

```
https://cegserver1.example.com:443/wstep/kerberos/services/tenant1/example-ca1
```

- b. The script prompts you to specify the priority of the enrollment server:

The URI for the enrollment server which has the lowest priority number as defined in the enrollment policy. If two enrollment servers have the same priority then

- a. The URI with the following authentication type is preferred in order:
Kerberos, Anonymous, Username/Password cached in the vault or Client Auth Certificate cached in the vault, Username/Password or Client Auth Certificate.
- b. If all properties are equal then a URI is randomly selected.

Please enter the Priority of this Enrollment URL [Default : 1]:

If multiple enrollment servers are defined, then the priority determines which enrollment server is preferred. Enter the priority for the enrollment server.

- c. The script asks if the URL will be used for certificate renewal only:

Will this URL be used for Renewal ONLY ? (y/n):

- If the enrollment URL is for certificate renewal only, enter **y**.
- If the enrollment URL is for certificate enrollment and renewal, enter **n**.

25. The main menu reappears:

Entrust Enrollment Service PowerShell

Using **this** PowerShell script, Enrollments servers can be created, removed and Edited.

Please select from the following options to **continue** :
[N] New Service [E] Edit Service [Q] Quit [?] Help (**default** is "N"):

To exit the script, enter **Q**.

Adjusting the polling interval of the Certificate Enrollment Policy Web Service (Optional)

By default, enrollment endpoints will poll the server hosting the Certificate Enrollment Policy Web Service every 8 hours. If you want to increase or decrease how often enrollment endpoints poll the Certificate Enrollment Policy Web Service, complete the following procedure.

To adjust the polling interval of the Certificate Enrollment Policy Web Service using PowerShell

1. Log in to the server hosting the Certificate Enrollment Policy Web Service.
2. Open an elevated PowerShell window. Select **Start > Windows PowerShell**, then right-click **Windows PowerShell > Run as administrator**.
3. Set the **\$PSPath** variable for the authentication type:
 - For user name and password authentication, enter the following command:

```
$PSPath = "MACHINE/WEBROOT/APPHOST/Default Web Site/  
ADPolicyProvider_CEP_UsernamePassword"
```

- For Kerberos authentication, enter the following command:

```
$PSPath = "MACHINE/WEBROOT/APPHOST/Default Web Site/  
ADPolicyProvider_CEP_Kerberos"
```

4. Enter the following command to add the configuration option **nextUpdateHours**:

```
Add-WebConfigurationProperty -pspath "$PSPath" -filter "appSettings" -name "."  
-value @{key="nextUpdateHours"}
```

The configuration option **nextUpdateHours** controls how often, in hours, enrollment endpoints will poll the Certificate Enrollment Policy Web Service.

5. Enter the following command to set the value of **nextUpdateHours** to 1 hour (the minimum interval supported).

```
Set-WebConfigurationProperty -pspath "$PSPath" -filter "appSettings/  
add[@key='nextUpdateHours']" -name "value" -value "1"
```

6. Enter the following command to add the configuration option **RetryIntervalMs**:

```
Add-WebConfigurationProperty -pspath "$PSPath" -filter "appSettings" -name "."  
-value @{key="RetryIntervalMs"}
```

The configuration option **RetryIntervalMs** controls how frequently, in milliseconds, Certificate Enrollment Policy Web Service refreshes templates and Certificate Authority (CA) information.

7. Enter the following command to set the value of **RetryIntervalMs** to 300,000 milliseconds (5 minutes):

```
Set-WebConfigurationProperty -pspath "$PSPath" -filter "appSettings/  
add[@key='RetryIntervalMs']" -name "value" -value "300000"
```

Avoid setting the value too small (values less than 1000) to avoid overhead on Microsoft IIS and Active Directory servers.

8. Enter the following command to restart Microsoft IIS and apply the changes:

```
iisreset
```

Installing and configuring the Certificate Enrollment Policy Web Service

The Certificate Enrollment Policy Web Service allows enrollment clients to retrieve certificate enrollment policies from a Certificate Authority (CA) when the clients are not permitted to access the Domain Controller. After receiving policy information from the Certificate Enrollment Policy Web Service, enrollment clients can then request a certificate from a certificate enrollment service.

In the Windows domain, install and configure the Certificate Enrollment Policy Web Service to forward WSTEP requests to Certificate Enrollment Gateway.

- It is recommended that you programmatically install and configure the service as explained in [Installing and configuring the CEP Web Service using a PowerShell script](#).
- However, you can also perform these operations manually, as explained in [Installing and configuring the CEP Web Service using the Windows graphical interface](#).

Installing and configuring the CEP Web Service using a PowerShell script

It is recommended that you install and configure the Certificate Enrollment Policy Web Service using the

`InstallConfigCEP.ps1` PowerShell script provided by Entrust. This script requires the TLS certificate previously obtained in [Issuing TLS certificates for the Certificate Enrollment Policy Web Service](#).

To install and configure the Certificate Enrollment Policy Web Service using a PowerShell script

1. Install a supported version of Microsoft Windows Server (if not already installed), and join it to the Windows domain.
2. From Entrust TrustedCare, download the PowerShell scripts for Certificate Enrollment Gateway.
3. Extract the PowerShell scripts to a directory on the server.
4. PowerShell scripts downloaded from the Internet may be blocked from running. To unblock a PowerShell script:
 - a. Right-click the PowerShell script > **Properties**.
A **Properties** dialog box appears.
 - b. Under the **General** tab, click **Unblock**.
5. Open an elevated PowerShell window. Select **Start > Windows PowerShell**, then right-click **Windows PowerShell > Run as administrator**.
6. Navigate to the directory where you extracted the PowerShell scripts.
7. Enter the following command to run the

`InstallConfigCEP.ps1`
script:

```
.\InstallConfigCEP.ps1
```

The script validates the pre-requisites, and then installs any required Windows packages or features. For example:

- i** The PowerShell script was tested on specific versions of PowerShell. When validating the prerequisites, the PowerShell version may be listed as Unverified, an "Unverified" version of PowerShell indicates that the script was not tested on that version of PowerShell. You can still use the script on an "Unverified" version of PowerShell.

```
Validating pre-requisites:
Script-Mode: Windows
Script Version: 1.5.1.19
  - Member of Domain:           Verified
  - Domain Admins privileges:   Verified
  - Enterprise Admins privileges: Verified
  - Windows Version:           Verified (Microsoft Windows NT 10.0.17763.0)
  - PowerShell Version:        Verified (5.1.17763.2931)

-----

Installing ADCS-Enroll-Web-Pol
ADCS-Enroll-Web-Pol installed

Checking for Web-Mgmt-Console
Installing Web-Mgmt-Console

Checking for Web-Mgmt-Compat
Installing Web-Mgmt-Compat
```

8. The script prompts you to select the authentication type:

```
CEP Authentication Setting
Choices :

Name      Value
----      -
UserName  4
Kerberos  2

Select Authentication Type [Default: 2]:
```

- To select user name and password authentication, enter 4.
User name and password authentication is the only authentication mode supported by non-domain enrollment endpoints.
- To select Kerberos (Windows integrated) authentication, enter 2.

9. The Certificate Enrollment Policy Web Service requires a certificate. The script prompts you to select a certificate option:

```
A CEP webserver certificate has not been selected.

Choose from the following Options:
```

```
[S] Select Existing Cert  [N] Supply New Certificate  [C] Continue with  
selected Certificate  [E] Exit  [?] Help  
(default is "S"):
```

- To select an existing certificate, enter **S**.
- To supply a new certificate, enter **N**.

10. If you chose to select an existing certificate:

- The script will search the server for existing TLS Web certificates.
The script will first search for a certificate assigned to the Default Web Site in Microsoft IIS. If no certificate is assigned to the Default Web Site, the script will then search the certificate store of the local computer for valid (not expired) certificates with the following:
 - a subject name with the fully qualified domain name (FQDN) of the host
 - a private key
 - an extended key usage of Server Authentication
- If the script finds a valid certificate, it asks if you want to use the certificate. For example:

```
Searching for Existing Certificate(s)
```

```
A certificate was found.
```

```
Subject       : CN=ceusername.example.com  
Issuer        : CN=ceusername.example.com  
KeyUsage      : DataEncipherment, KeyEncipherment  
EKU List      : Server Authentication (1.3.6.1.5.5.7.3.1)  
DNS SAN       : ceusername.example.com  
Serial Number : 37F2440E97A3AE8046AA54BD7227FAFC  
Thumbprint    : 50C09642942060AE1A58C5C3006F2455B57326BC  
Not After     : 09/05/2023 20:00:00  
PolicyId      :
```

```
Continue with above Certificate? (y/n):
```

- To continue with the certificate found by the script, enter **y**.
 - To go back and provide a different certificate, enter **n**.
- If the script finds multiple valid certificates, it will prompt you to select a certificate. For example:

```
Searching for Existing Certificate(s)
```

```
More than one certificate with FQDN ceusername.example.com has been  
found.
```

```
Certificate Index : 1
```

```
-----
```

```
Subject       : CN=ceusername.example.com  
Issuer        : CN=ceusername.example.com  
KeyUsage      : DataEncipherment, KeyEncipherment  
EKU List      : Server Authentication (1.3.6.1.5.5.7.3.1)  
DNS SAN       : ceusername.example.com  
Serial Number : 1862326CAB4507B1411EA7624F6DDDBA  
Thumbprint    : EEC5FF53EA64B1B56B8731A7E73C058257A4DC0E
```



```
Not After      : 09/06/2023 20:00:00
PolicyId       :
```

```
Certificate Index : 2
```

```
-----
Subject        : CN=ceusername.example.com
Issuer          : CN=ceusername.example.com
KeyUsage        : DataEncipherment, KeyEncipherment
EKU List        : Server Authentication (1.3.6.1.5.5.7.3.1)
DNS SAN         : ceusername.example.com
Serial Number   : 37F2440E97A3AE8046AA54BD7227FAFC
Thumbprint      : 50C09642942060AE1A58C5C3006F2455B57326BC
Not After       : 09/05/2023 20:00:00
PolicyId        :
```

Please select the Index to select a Certificate. 0 to **return** to previous menu.:

- To select one of the existing certificates, enter the index number associated with the certificate.
- To go back and provide a different certificate, enter 0.

11. If you chose to supply a certificate:

- a. The script prompts you to provide the certificate:

```
Please enter full path to certificate file including the filename :
```

Enter the full path and file name of the certificate, in PFX or P12 format.

- b. When prompted, enter the password of the certificate file.
- c. If the supplied certificate has a subject that does not match the fully qualified domain name (FQDN) of the host, the script displays a warning and asks if you want to continue with the certificate. For example:

```
The supplied certificate has a subject that does not match the FQDN of
this host.
```

```
Host FQDN : ceusername.example.com
```

```
Supplied certificate details:
```

```
-----
Subject        : CN=CEP Web Service, CN=CA Entry, O=Example, C=US
Issuer          : CN=CA Entry, O=Example, C=US
KeyUsage        : KeyEncipherment, DigitalSignature
EKU List        : Server Authentication (1.3.6.1.5.5.7.3.1) Client
Authentication  (1.3.6.1.5.5.7.3.2)
DNS SAN         : ceusername.example.com
Serial Number   : 6AFEE3C47A569F95A9C5622D679B42C1
Thumbprint      : 2E6601A98E2ADB4EBE5DF6D8C3A514CD7660BAD
Not After       : 09/06/2025 13:55:27
```

PolicyId :

Continue with above Certificate? (y/n):

- To continue with the certificate, enter **y**.
- To go back and provide a different certificate, enter **n**.

12. After providing a certificate, the script displays information about the certificate, and prompts you to select a certificate option:

Selected Webserver Certificate **for** CEP:

Subject : CN=ceusername.example.com
Issuer : CN=ceusername.example.com
KeyUsage : DataEncipherment, KeyEncipherment
EKU List : Server Authentication (1.3.6.1.5.5.7.3.1)
DNS SAN : ceusername.example.com
Serial Number : 1862326CAB4507B1411EA7624F6DDDBA
Thumbprint : EEC5FF53EA64B1B56B8731A7E73C058257A4DC0E
Not After : 09/06/2023 20:00:00
PolicyId :

Choose from the following Options:

[S] Select Existing Cert [N] Supply New Certificate [C] Continue with
selected Certificate [E] Exit [?] Help
(**default** is "S"):

- To go back and select a different existing certificate, enter **S**.
- To go back and supply and different certificate, enter **N**.
- To continue with the selected certificate, enter **C**.

13. After providing a certificate, the script prompts you to provide a Windows user to configure the Certificate Enrollment Policy. The user must have Domain Admin and Enterprise Admin permissions.

Configuring CEP Service

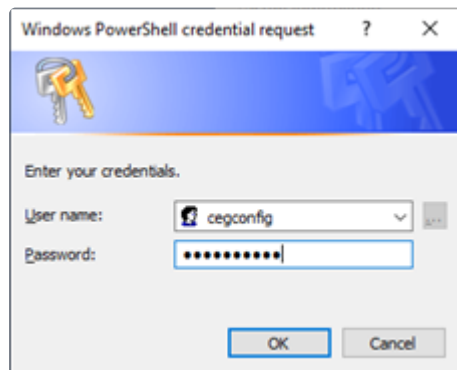
Please enter the user information to be able to configure CEP

The user must have Domain Admin and Enterprise Admin rights

cmdlet Get-Credential at command pipeline position 1

Supply values for the following parameters:

Credential



Enter the user name and password credentials of the Windows user.

14. The script installs the Certificate Enrollment Policy Web Service, then prompts you to provide a friendly name for the service:

```
Installing AdcsEnrollmentPolicyWebService
Authentication : UserName
SSLThumbprint  : DE45D685512D0F58A4CA7A60A485D8FD03723276
Install Complete
Please enter the 'Friendly Name' for the CEP Service :
```

Enter a friendly name for the Certificate Enrollment Policy Web Service. The friendly name must be unique for the domain. The friendly name will appear in some interfaces. For example: `WSTEP UserName CEP`.

15. To properly function with an existing Microsoft CA, the Certificate Enrollment Policy Web Service requires a UUID (Universally Unique Identifier). The script asks whether you want to generate a UUID or supply an external UUID.

```
All instances of the CEP Service must use the same UUID.
You must generate the UUID for the first instance, then supply the UUID for all
subsequent instances.
Generate or supply a UUID for the CEP Service?
Generate a UUID          1
Supply a UUID            2

Enter Selection ( 1 | 2 ) :
```

- If you are installing the initial instance of the Certificate Enrollment Policy Web Service and you want the script to generate the UUID, enter 1. For example:

```
Generating Unique UUID
UUID 6e42b254-0302-4428-9bc5-c34d11c3b4b6
WARNING: Use the same UUID on all the CEP instances for Entrust WSTEP.
Selected UUID : 6e42b254-0302-4428-9bc5-c34d11c3b4b6
```

Record the generated UUID. All instances of the Certificate Enrollment Policy Web Service must use the same UUID for Entrust WSTEP enrollment.

- If you are installing subsequent instances of the Certificate Enrollment Policy Web Service and you want to supply the UUID generated in the first instance, enter 2. For example:

```
Enter a unique valid UUID : 1435d47b-a043-4b39-9420-0ff067344e4e
Selected UUID : 1435d47b-a043-4b39-9420-0ff067344e4e
```

When using Kerberos authentication, you can obtain the UUID of the installed Certificate Enrollment Policy Web Service by entering the following PowerShell command:

```
(Get-WebConfigurationProperty -pspath "MACHINE/WEBROOT/APPHOST/Default Web
Site/ADPolicyProvider_CEP_Kerberos" -filter "appSettings/add[@key='ID']"
-name "value").value
```

When using user name and password authentication, you can obtain the UUID of the installed Certificate Enrollment Policy Web Service by entering the following PowerShell command.

```
(Get-WebConfigurationProperty -pspath "MACHINE/WEBROOT/APPHOST/Default Web
Site/ADPolicyProvider_CEP_UsernamePassword" -filter "appSettings/
add[@key='ID']" -name "value").value
```

16. The script asks if you want to continue with the provided UUID:

```
Continue with above UUID? (y/n):
```

- To continue with the provided UUID, enter **y**.
- To go back and change the UUID, enter **n**.

17. The script asks if you want to restart Microsoft IIS:

```
Recommended: Restart IIS
Restart IIS now ? (y/n):
```

It is recommended that you restart Microsoft IIS to ensure the changes are applied.

- To have the script restart Microsoft IIS, enter **y**.
- To not restart Microsoft IIS, enter **n**.

It is recommended that you manually restart Microsoft IIS to ensure that the changes are applied.

Installing and configuring the CEP Web Service using the Windows graphical interface

To install and configure the Certificate Enrollment Policy Web Service, it is recommended that you run a PowerShell script as explained in [Installing and configuring the CEP Web Service using a PowerShell script](#). However, you can also use the Windows graphical interface, as explained in the following sections.

- [Assigning a unique Enrollment Policy Identifier](#)
- [Assigning a friendly name to the CEP Web Service using the Windows graphical interface](#)
- [Selecting the authentication mode of the CEP Web Service using the Windows graphical interface](#)
- [Installing the CEP Web Service using the Windows graphical interface](#)

Assigning a unique Enrollment Policy Identifier

For Entrust WSTEP to work alongside an existing Microsoft CA, you must change the Enrollment Policy ID to something unique. You can perform this operation using either PowerShell or the Windows graphical interface.

- [Assigning a unique Enrollment Policy Identifier with PowerShell](#)

- [Assigning a unique Enrollment Policy Identifier with the Windows graphical interface](#)

Assigning a unique Enrollment Policy Identifier with PowerShell

See below for assigning a policy identifier with the Windows PowerShell command-line shell

To assign a unique Enrollment Policy Identifier using PowerShell

1. Log in to the server hosting the Certificate Enrollment Policy Web Service.
2. Open an elevated PowerShell window. Select **Start > Windows PowerShell**, then right-click **Windows PowerShell > Run as administrator**.
3. Generate a unique identifier with the following command.

```
[guid]::NewGuid()
```

For example:

```
PS C:\> [guid]::NewGuid()
Guid
----
1c84d0f5-0eb4-4189-9e8d-a02b5d4079bd
```

4. Set the new identifier. For example:

```
Set-WebConfigurationProperty -pspath "MACHINE/WEBROOT/APPHOST/Default Web Site/ADPolicyProvider_CEP_UsernamePassword" -filter "appSettings/add[@key='ID']" -name "value" -value "1c84d0f5-0eb4-4189-9e8d-a02b5d4079bd"
```

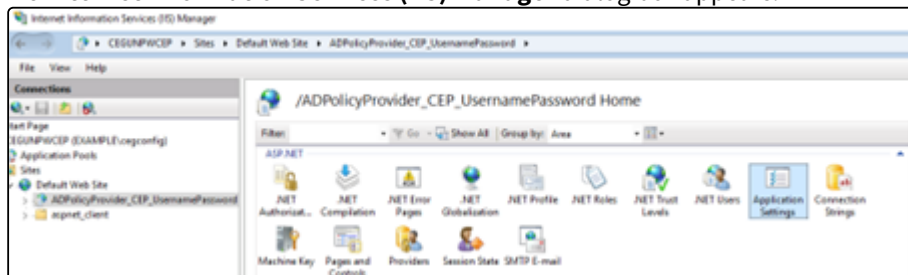
Assigning a unique Enrollment Policy Identifier with the Windows graphical interface

See below for assigning a policy identifier with the Windows graphical interface tools.

To assign a unique Enrollment Policy Identifier using the Windows graphical interface

1. Log in to the server hosting the Certificate Enrollment Policy Web Service.
2. Open IIS Manager. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** dialog box appears.

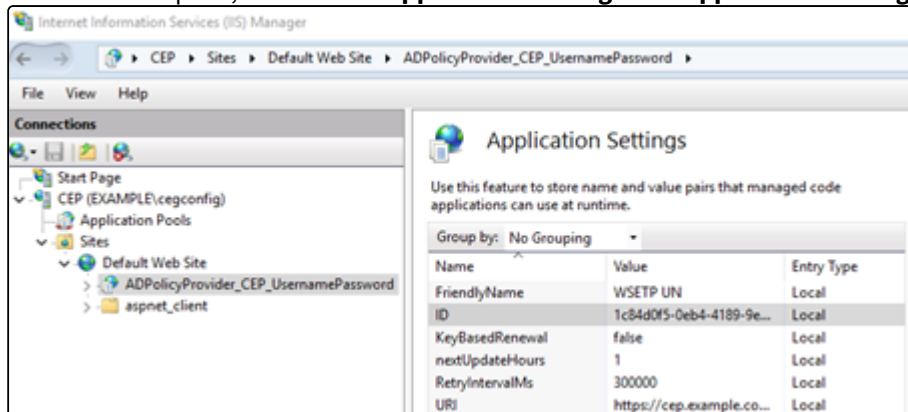


3. In the **Connections** pane, expand **Sites > Default Web Site**.
4. Select the name of the Certificate Enrollment Policy Web Service application.
 - If you configured user name and password authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider_CEP_UsernamePassword**.
 - If you configured Kerberos (Windows integrated) authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider_CEP_Kerberos**.

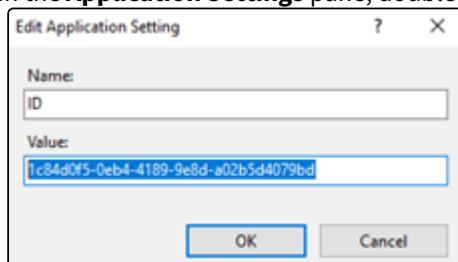
- If **Application Settings** is not available in the **Features** pane, run the following PowerShell command to install IIS Compatibility:

```
PS C:\>Add-WindowsFeature -Name Web-Mgmt-Compat
```

- In the **Features** pane, double-click **Application Settings**. The **Application Settings** pane appears.



- In the **Application Settings** pane, double-click on ID. The **Edit Application Setting** dialog box appears.



- In the **Value** field of the **Edit Application Setting** dialog box, enter a unique identifier.
- Click **OK**.
- Restart IIS.
- If you already added the Certificate Enrollment Policy to the group policy, remove the group policy's service and add it again to use the new identifier.

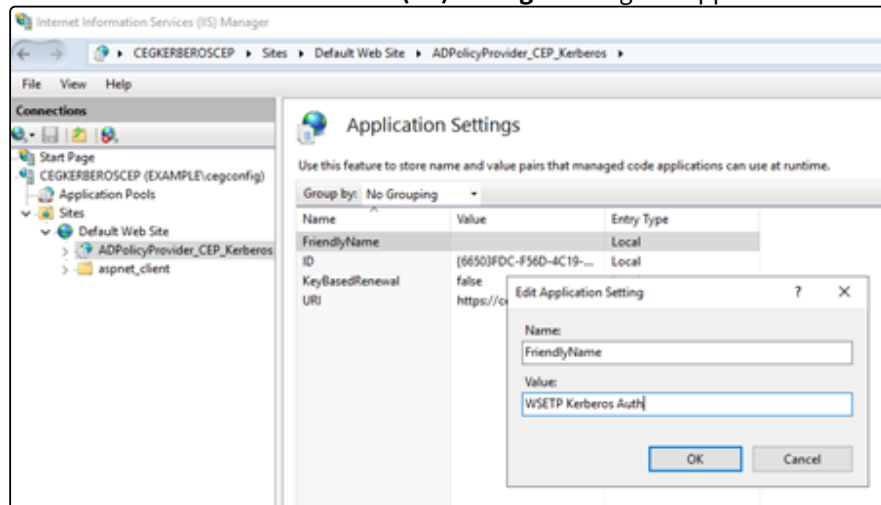
Assigning a friendly name to the CEP Web Service using the Windows graphical interface

Set a friendly name for each one of the configured Certificate Enrollment Policy Web Service instances. This friendly name will appear in some interfaces.

To set a friendly name for a CEP Web Service using the Windows graphical interface


- Log in to the server where you installed the Certificate Enrollment Policy Web Service.
- Open IIS Manager. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** dialog box appears.



3. In the **Connections** pane, expand **Sites > Default Web Site**.
4. Select the name of the Certificate Enrollment Policy Web Service application.
 - If you configured user name and password authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider_CEP_UsernamePassword**.
 - If you configured Kerberos (Windows integrated) authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider_CEP_Kerberos**.
5. In the content pane, double-click **Application Settings**.
An **Application Settings** pane appears.
6. In the **Application Settings** pane, double-click **FriendlyName**.
An **Edit Application Setting** dialog box appears.
7. In the **Value** field, enter a unique and friendly name for the service.
8. Click **OK**.

Selecting the authentication mode of the CEP Web Service using the Windows graphical interface

 The Certificate Enrollment Policy Web Service requires a TLS certificate in Microsoft IIS. You will set the TLS certificate later, as explained in [Configuring the TLS certificate of the Windows endpoints](#).

After installing the Windows Certificate Enrollment Policy Web Service as documented in [Installing the CEP Web Service using the Windows graphical interface](#), you must select the authentication mode supported for the Certificate Enrollment Policy Web Service endpoints.

The Certificate Enrollment Gateway supports both Windows integrated authentication (Kerberos) and password authentication. Client certificate authentication is currently not supported.

If you support non-domain enrollment endpoints, you must configure the Certificate Enrollment Policy Web Service for username and password authentication.

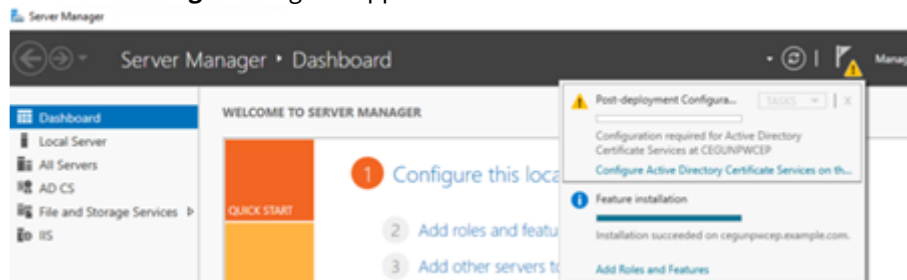
When authenticating with username and password, the CEP Service supports the following username formats.

- username
- domain\username
- username@domain
- domainfqdn\username
- username@domainfqdn

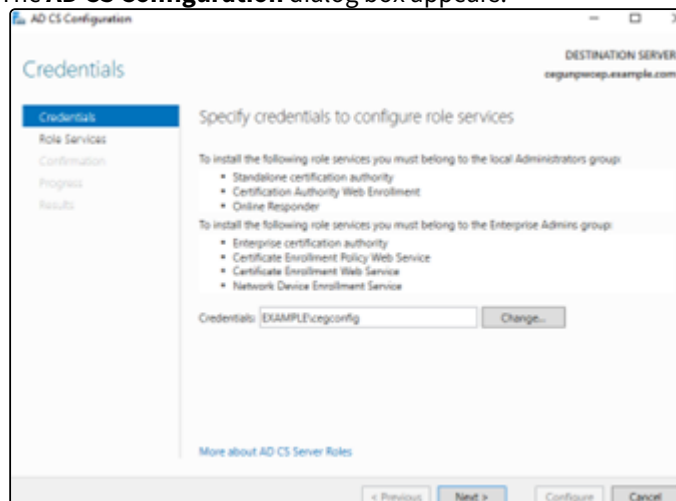
WSTEP will use the supplied domain information to validate the user. If the domain is not supplied, WSTEP will attempt to use the domain information in the SOAP request. If the SOAP request domain information does not exist, WSTEP will use the configured domain from the Certificate Enrollment Gateway configuring.

To select the authentication mode for the CEP Web Service using the Windows graphical interface

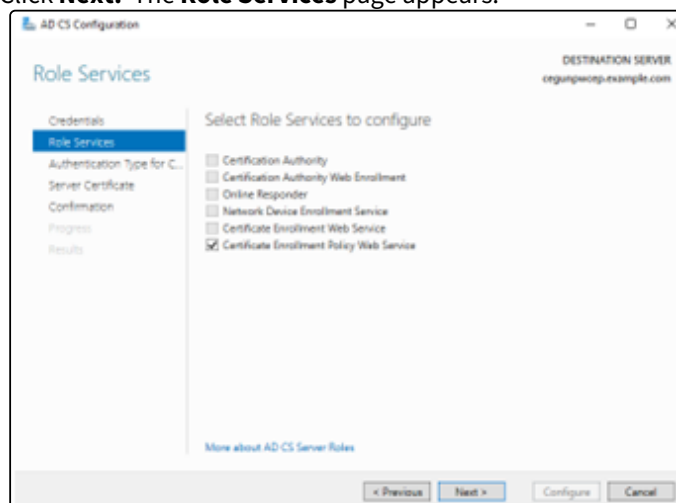
1. Log in to the server where you installed the Certificate Enrollment Policy Web Service.
2. Open Server Manager. Select **Start > Server Manager**.
The **Server Manager** dialog box appears.



3. Select **Notifications > Configure Active Directory Certificate Services** on the destination server.
The **AD CS Configuration** dialog box appears.

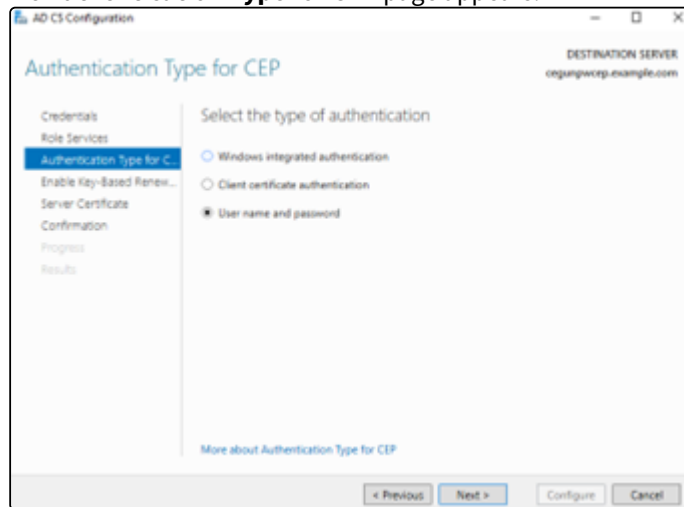


4. Enter or select the administrator credentials you will use to configure role services.
5. Click **Next**. The **Role Services** page appears.




6. Select **Certificate Enrollment Policy Web Service**.
7. Click **Next**.

The **Authentication Type for CEP** page appears.



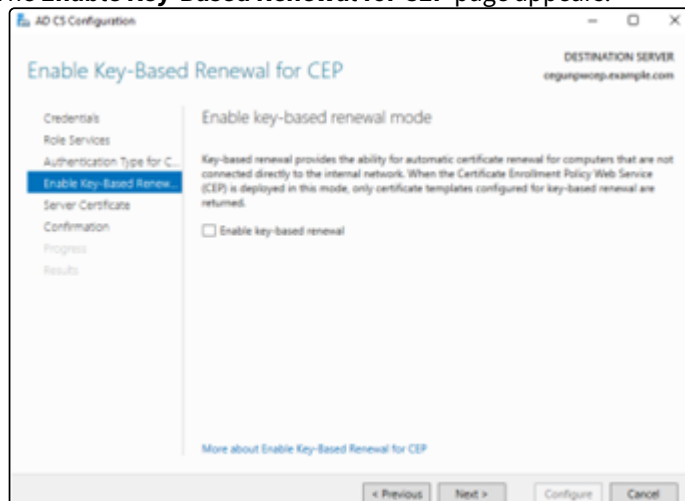
8. Select an authentication method supported by Certificate Enrollment Gateway.

 Client certificate authentication is currently not supported by Certificate Enrollment Gateway.

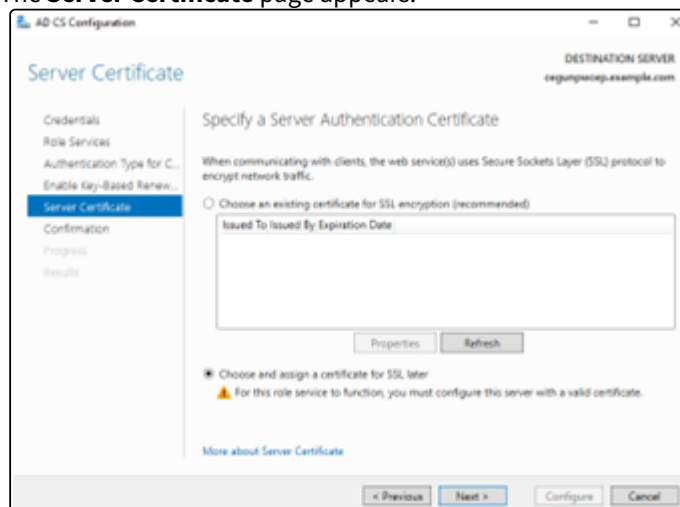
If you support non-domain enrollment endpoints, you must select **User name and password** as the authentication method.

9. Click **Next**.

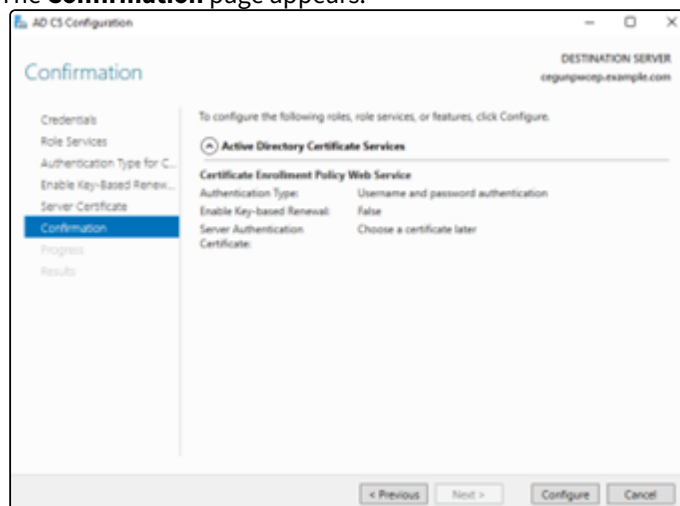
The **Enable Key-Based Renewal for CEP** page appears.



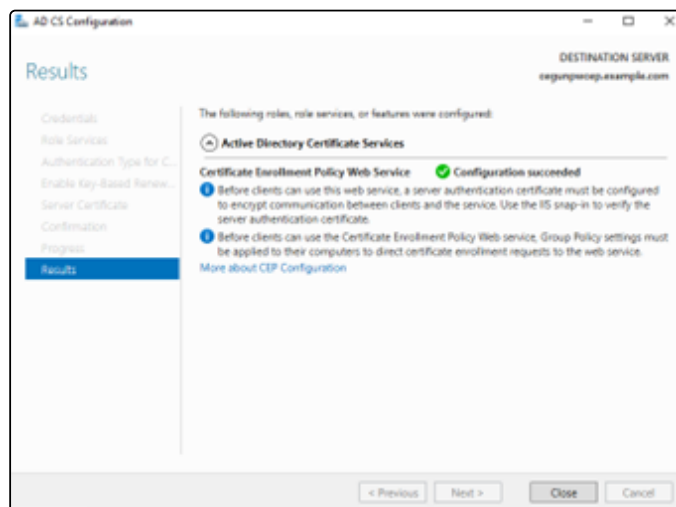
10. Do not select any options. Click **Next**.
The **Server Certificate** page appears.



11. Select **Choose and assign a certificate for SSL later**.
12. Click **Next**.
The **Confirmation** page appears.



13. Click **Configure**.
After the authentication mode is configured, the **Results** page appears.



14. Click **Close**.

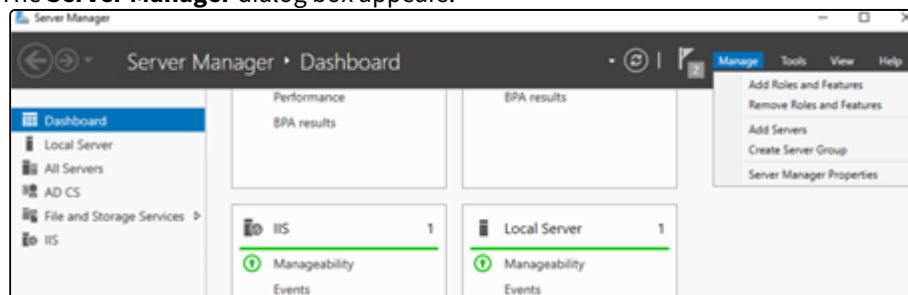
Installing the CEP Web Service using the Windows graphical interface

On a Windows server, install the Certificate Enrollment Policy Web Service.

i The Windows server hosting the Certificate Enrollment Policy Web Service can be the Active Directory server or any other server in the domain. However, it is recommended that you install and configure the Certificate Enrollment Policy Web Service on a different server than Active Directory.

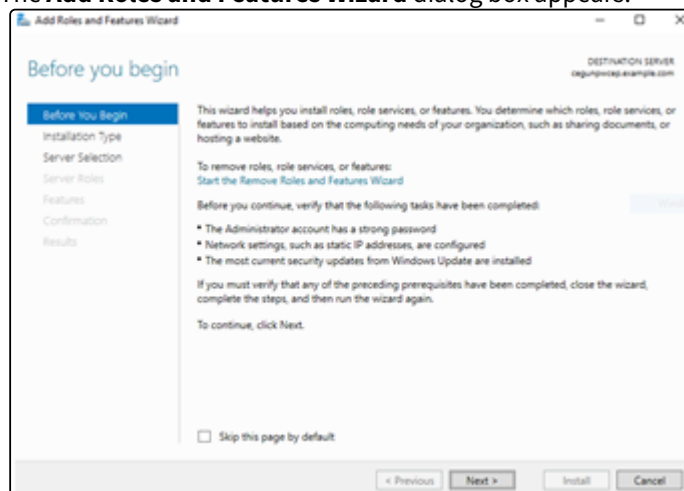
To install the CEP Web Service using the Windows graphical interface

1. Log in to a Windows server hosting Microsoft IIS as a user with Domain Administrator and Enterprise Administrator permissions.
2. Open Server Manager. Select **Start > Server Manager**. The **Server Manager** dialog box appears.



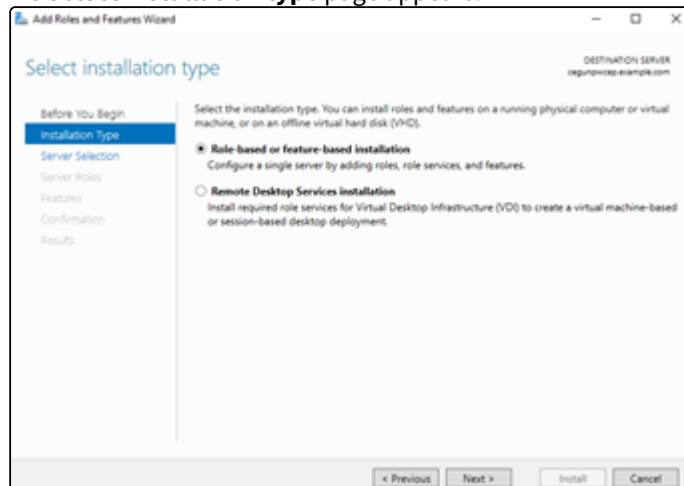
3. Select **Manage > Add Roles and Features**.

The **Add Roles and Features Wizard** dialog box appears.



4. If the **Before you Begin** page appears, click **Next**.

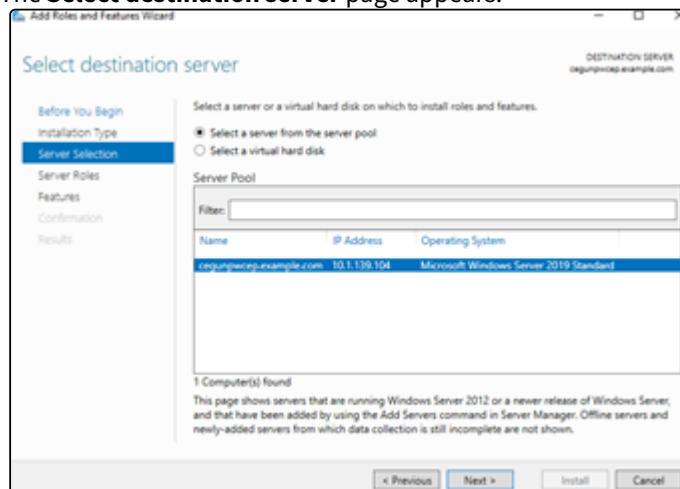
The **Select installation type** page appears.



5. Select **Role-based or feature-based installation**.

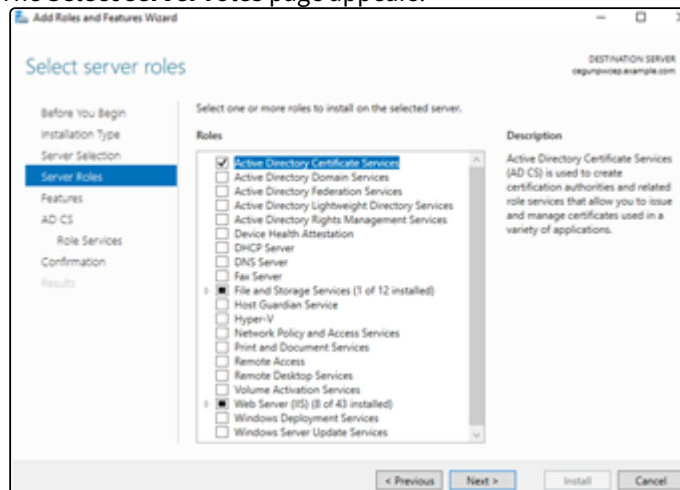
6. Click **Next**.

The **Select destination server** page appears.



7. Click **Select a server from the pool**.
8. In the **Server Pool** list, select the server.
9. Click **Next**.

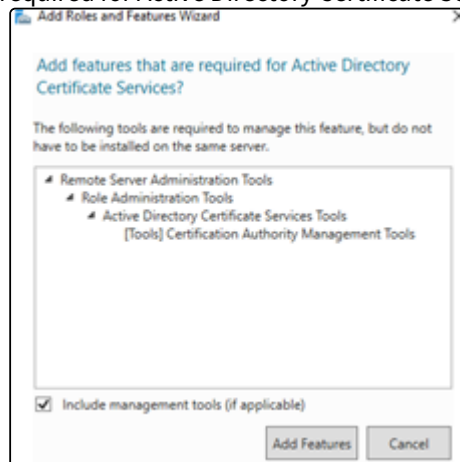
The **Select server roles** page appears.



10. Select **Active Directory Certificate Services**.

Another **Add Roles and Features Wizard** dialog box may appear, informing you that some features are

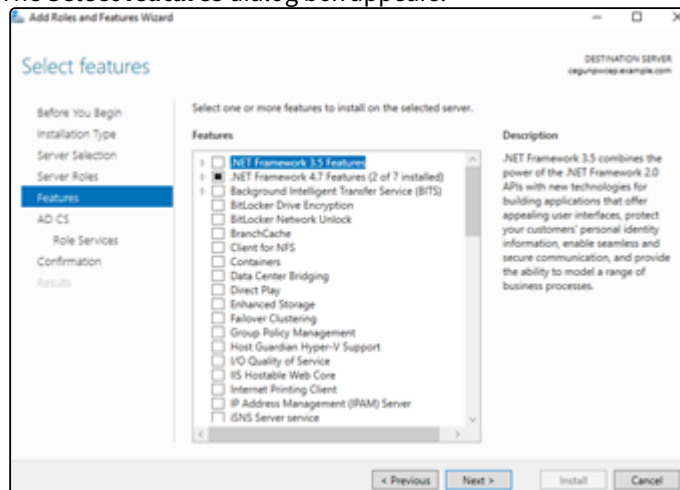
required for Active Directory Certificate Services.



11. Click **Add Features** to add these required features and close the dialog box.

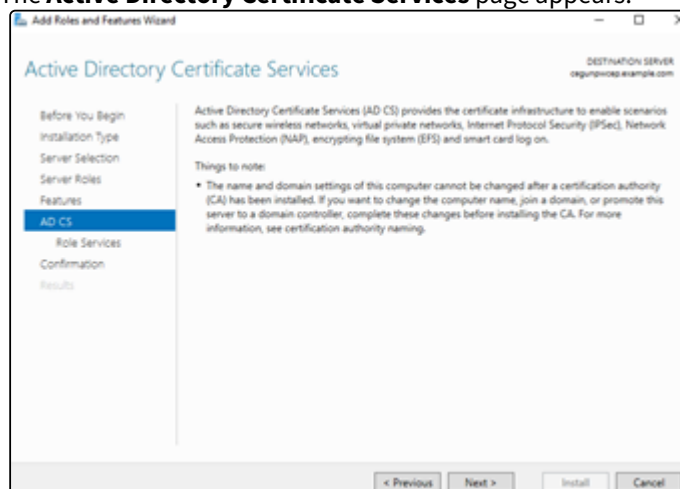
12. Click **Next**.

The **Select features** dialog box appears.



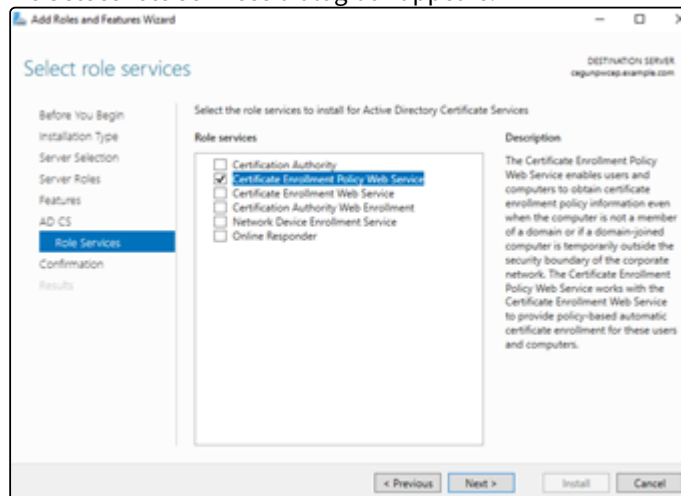
13. Click **Next**.

The **Active Directory Certificate Services** page appears.



14. Click **Next**.

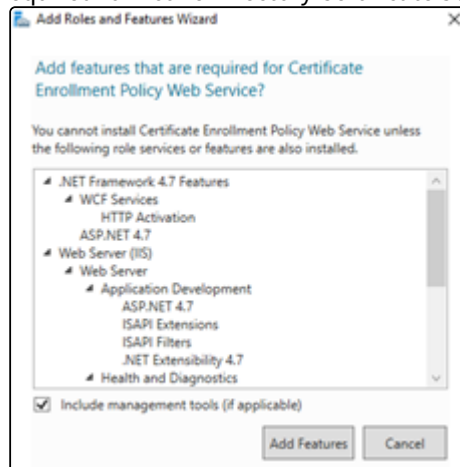
The **Select role services** dialog box appears.



15. If you are on a different server than Active Directory, deselect **Certificate Authority**.

16. Select Certificate Enrollment Policy Web Service.

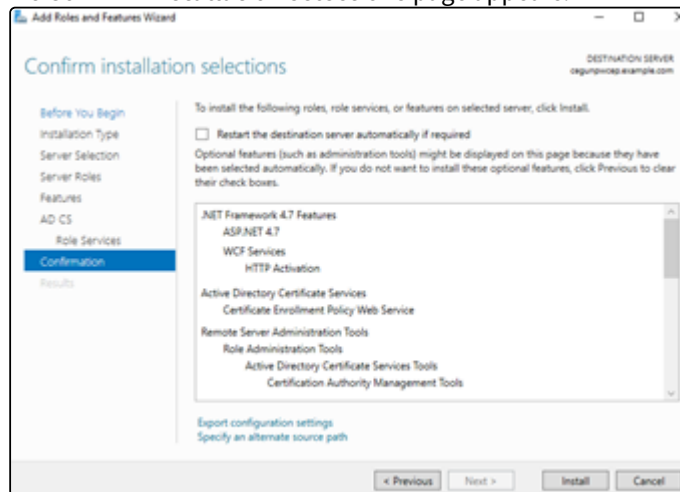
Another **Add Roles and Features Wizard** dialog box may appear, informing you that some features are required for Active Directory Certificate Services.



17. Click **Add Features** to add these required features and close the dialog box.

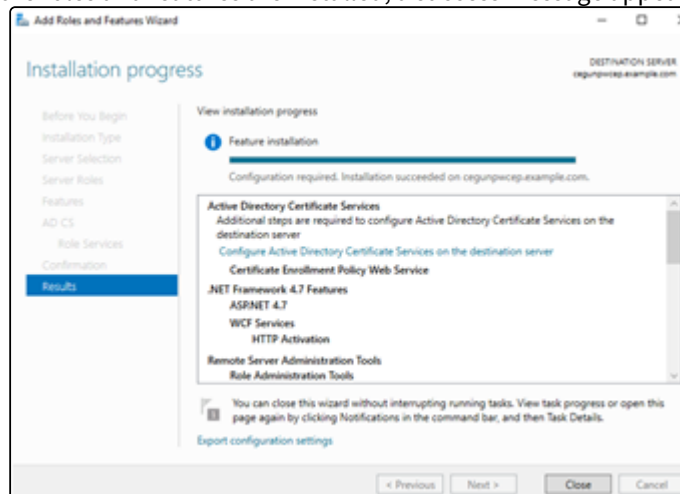
18. Click **Next**.

The **Confirm installation selections** page appears.



19. Click **Install**.

The **Installation Progress** page appears. A progress indicator displays the progress of the installation. After the roles and features are installed, a success message appears.



20. Click **Close**.

Issuing TLS certificates for the Certificate Enrollment Policy Web Service

The Certificate Enrollment Policy Web Service is installed as an application in Microsoft Internet Information Services (IIS). Microsoft IIS requires a TLS certificate so that the Certificate Enrollment Policy Web Service can accept WSTEP enrollment requests over HTTPS.

The following topics describe how to issue a TLS certificate for Microsoft IIS.

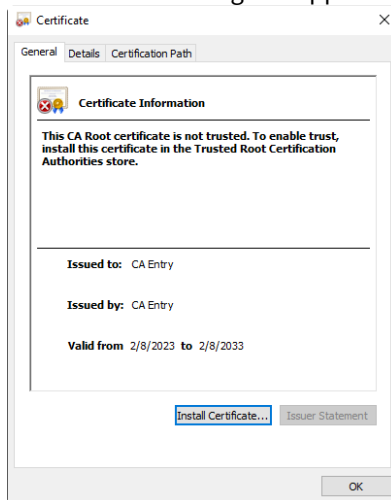
- [Installing the CA certificate chain for the Web server certificate](#)
- [Updating Microsoft IIS to use the Web server certificate](#)
- [Installing the Web server certificate into Microsoft IIS](#)
- [Issuing the Web server certificate with Entrust PKI as a Service](#)
- [Issuing the Web server certificate with an on-premises CA](#)
- [Creating a CSR for the Web server certificate](#)

Installing the CA certificate chain for the Web server certificate

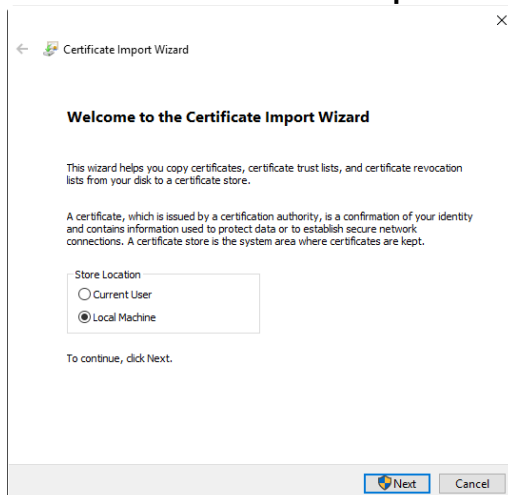
For Microsoft IIS to trust the Web server certificate, you must install the CA certificate chain for the Web server certificate into the server hosting Microsoft IIS. You must install the entire CA certificate chain, from the root CA to the issuing CA (the CA that issued the Web server certificate). For an on-premises CA, the root CA may be the issuing CA.

To install a CA certificate into the Web server

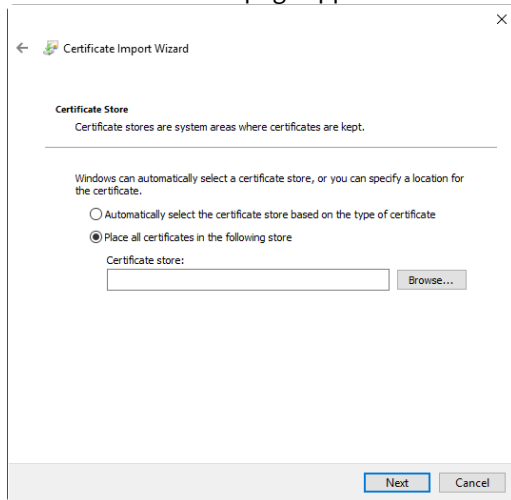
1. For an on-premises CA, obtain all CA certificates in the CA certificate chain using your on-premises CA tools. See the documentation for your on-premises CA for instructions.
2. For Entrust PKI as a Service, download all CA certificates in the certificate chain:
 - a. Log in the Entrust Certificate Services interface.
 - b. Select **Administration > PKIaaS Management**.
A list of private CAs appear.
 - c. For each CA in the TLS certificate chain (from the Issuing CA to the Root CA), select the CA and then click **Download certificate**.
3. Double-click the CA certificate file.
The **Certificate** dialog box appears.



4. Click **Install Certificate**.
The Certificate Import Wizard appears.
5. The **Welcome to the Certificate Import Wizard** page appears.

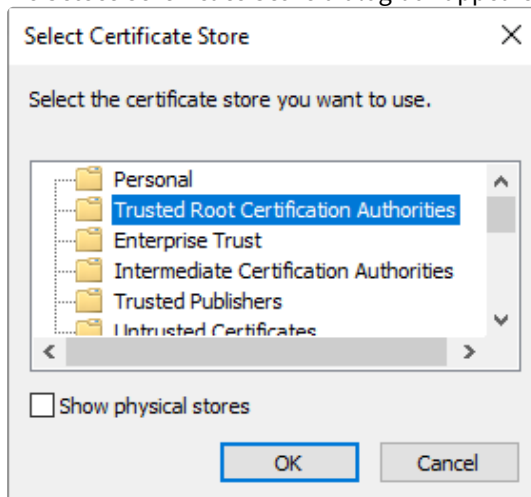


- a. For **Store Location**, select **Local Machine**.
 - b. Click **Next**.
6. The **Certificate Store** page appears.



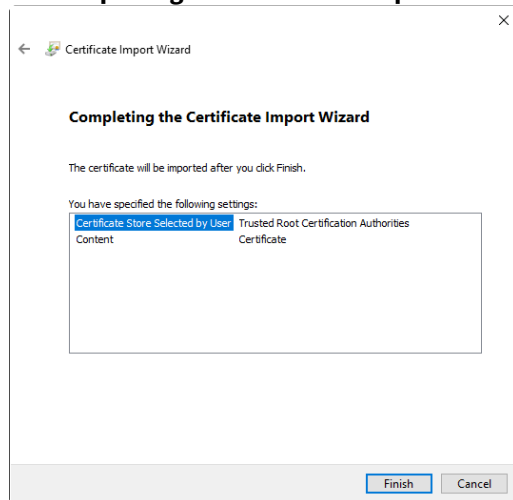
- a. Select **Place all certificates in the following store**.
- b. Click **Browse**.

The **Select Certificate Store** dialog box appears.



- c. If the CA certificate is a root CA certificate, select **Trusted Root Certification Authorities**.
- d. If the CA certificate is a subordinate (intermediate) CA certificate, select **Intermediate Certification Authorities**.
- e. Click **OK**.
- f. Click **Next**.

- The **Completing the Certificate Import Wizard** page appears.



- Click **OK**.

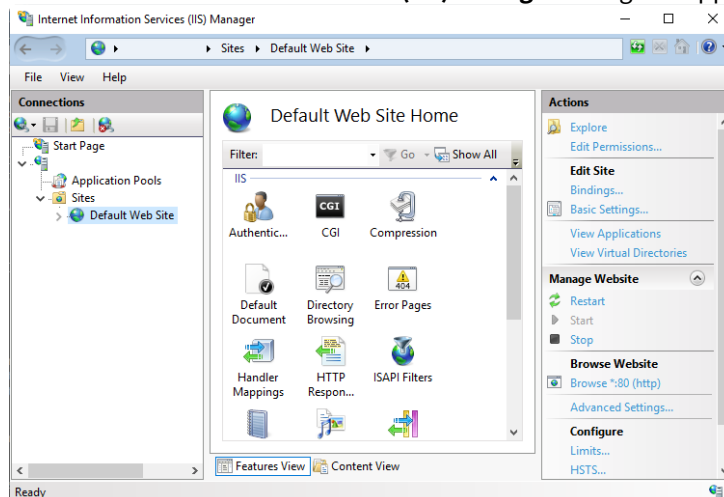
Updating Microsoft IIS to use the Web server certificate

After installing the Web server certificate into Microsoft IIS, you must update the HTTPS site binding for the Web server in Microsoft IIS to use the TLS certificate.

To add an initial HTTPS site binding in Microsoft IIS to use the Web server certificate

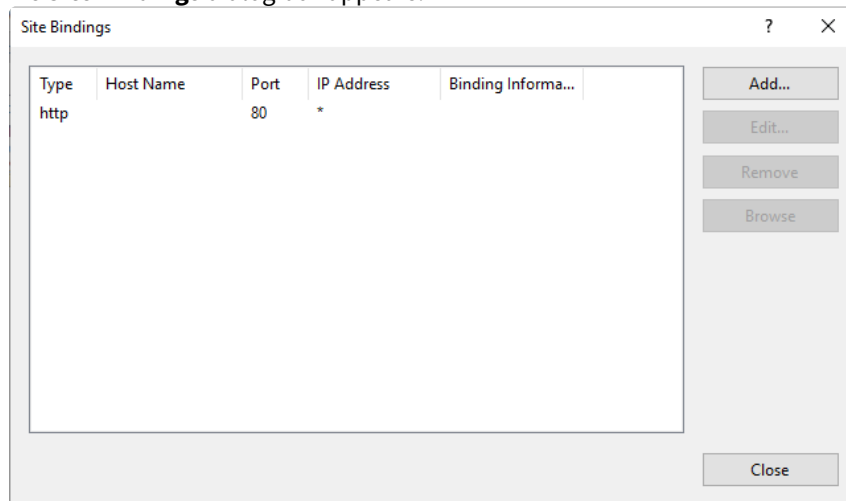
- Open IIS Manager. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** dialog box appears.

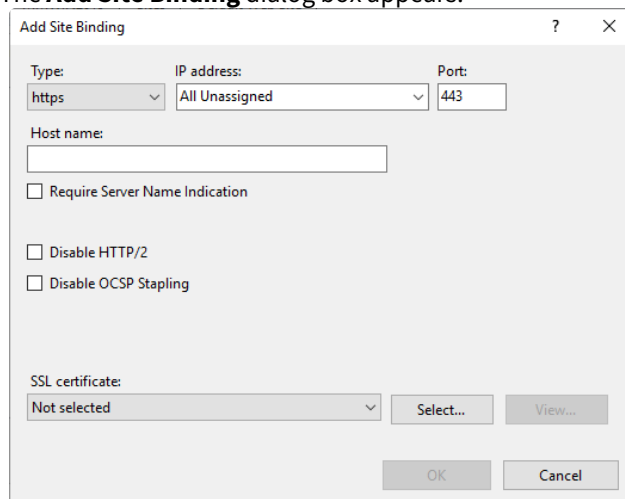


- In the **Connections** pane, select **Sites > Default Web Site**.
The Certificate Enrollment Policy Web Service will be installed as an application under the default Web site.

- In the **Actions** pane, click **Bindings**.
The **Site Bindings** dialog box appears.



- Click **Add**.
The **Add Site Binding** dialog box appears.

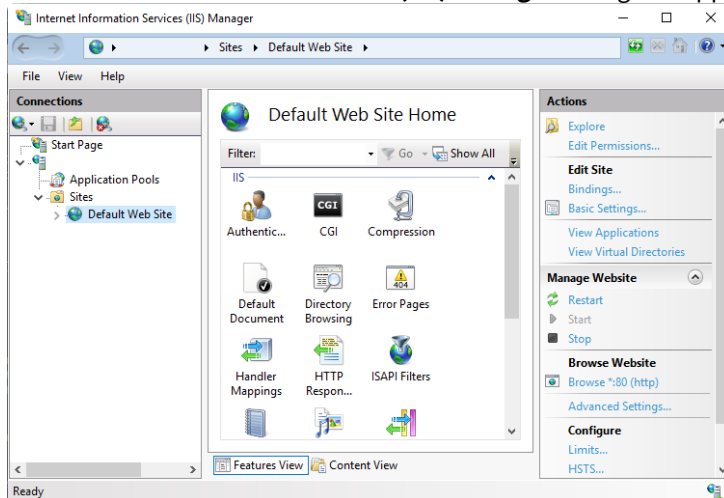


- In the **Type** drop-down list, select **https**.
- Keep **IP address** as **All Unassigned**.
- For **Port**, keep the default 443.
- From the **SSL certificate** drop-down list, select the Web server certificate you installed into Microsoft IIS earlier.
- Click **OK**.
The HTTPS binding is added to the list of site bindings.

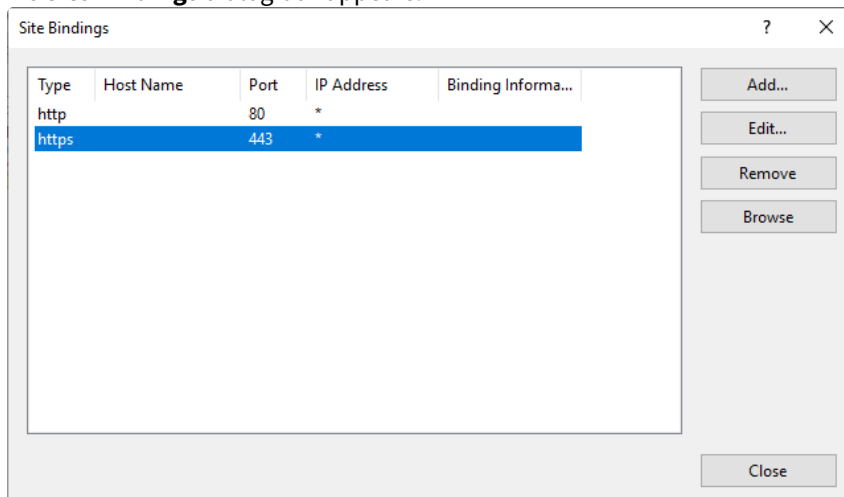
To update an existing HTTPS site binding in Microsoft IIS to use the Web server certificate

- Open IIS Manager. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** dialog box appears.



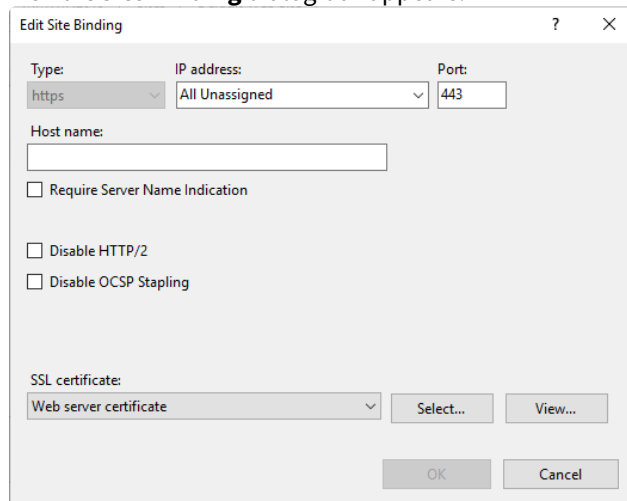
- In the **Connections** pane, select **Sites > Default Web Site**.
If the Certificate Enrollment Policy Web Service is installed, it appears as an application under the default Web site.
- In the **Actions** pane, click **Bindings**.
The **Site Bindings** dialog box appears.



- Select the **https** binding for port **443**.

5. Click **Edit**.

The **Edit Site Binding** dialog box appears.



6. From the **SSL certificate** drop-down list, select the Web server certificate you installed into Microsoft IIS earlier.
7. Click **OK**.

Installing the Web server certificate into Microsoft IIS

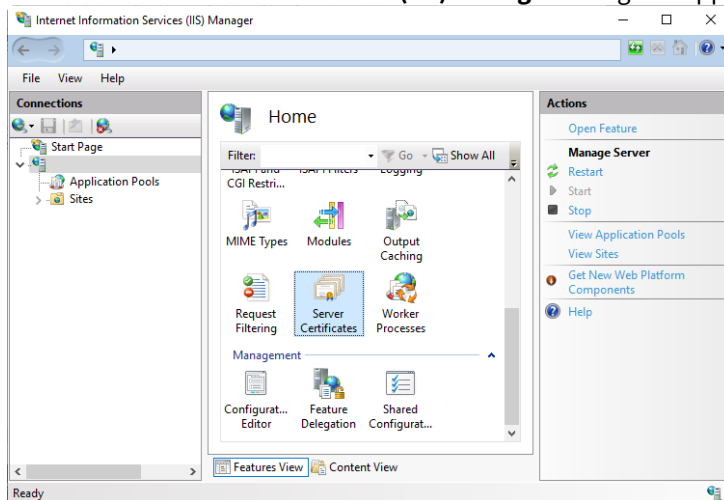
After obtaining the Web server certificate, you must install the certificate into Microsoft IIS. After processing the CSR with Entrust PKI as a Service or an on-premises CA, complete the certificate request in Microsoft IIS to install the certificate.

i If you will use the Entrust-provided PowerShell scripts to install and configure the Certificate Enrollment Policy Web Service, keep the certificate file after installing the certificate into Microsoft IIS. The PowerShell script will prompt you to select an existing certificate or supply a new certificate for the Certificate Enrollment Policy Web Service. If the PowerShell script cannot find the certificate you install into Microsoft IIS, you must supply the certificate.

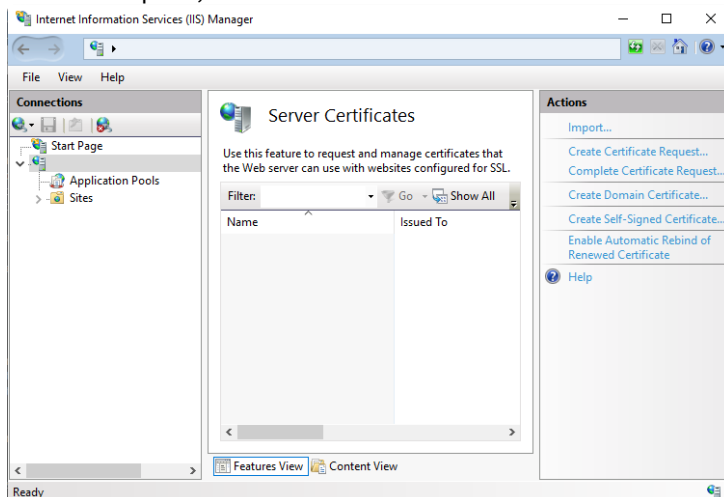
To complete a certificate request in Microsoft IIS

1. Open the Internet Information Services (IIS) Manager. Select **Start > Windows Administrative Applications > Internet Information Services (IIS) Manager**.

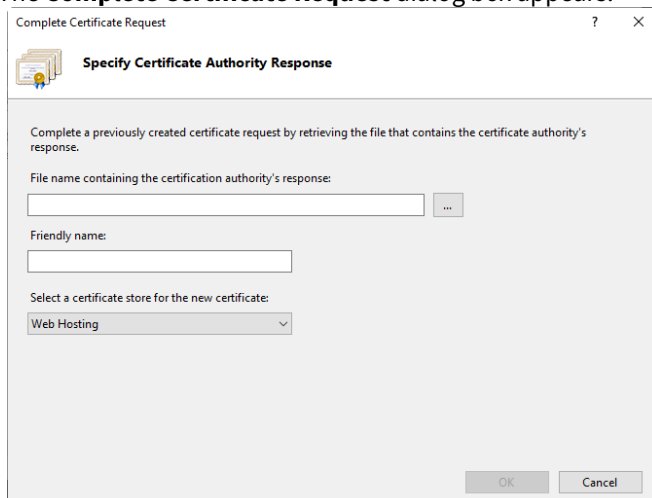
The **Internet Information Services (IIS) Manager** dialog box appears.



2. Under **Connections**, select the host name of the server.
3. In the **Home** pane, double-click **Server Certificates**.



4. In the **Actions** pane, click **Complete Certificate Request**.
The **Complete Certificate Request** dialog box appears.



5. In the **File name containing the certification authority response** field, enter the full path and file name of the Web server certificate, or click the Browse button to select the certificate.
6. In the **Friendly name** field, enter a friendly name for the certificate. This friendly name will be used to identify the certificate in the IIS Manager interface.
7. From the **Select a certificate store for the new certificate** drop-down list, select **Web Hosting**.
8. Click **OK**.
In the **Server Certificates** pane, the certificate appears in the list of server certificates. The certificate is listed by its friendly name.

Issuing the Web server certificate with Entrust PKI as a Service

After creating the certificate signing request (CSR) for the Certificate Enrollment Gateway certificate, you can submit the CSR to an Issuing CA in Entrust PKI as a Service. The Issuing CA will process the CSR and generate the certificate.

To submit the CSR to Entrust PKI as a Service and obtain the TLS certificate

1. Log in the Entrust Certificate Services interface.
2. Select **Create > PKIaaS**.
The Select **Certificate Authority** pane appears.
3. From the **Certificate Authority** drop-down list, select the CA you want to issue the TLS certificate.
4. From the **Certificate Profile** drop-down list, select the certificate profile you want to use for the TLS certificate. The certificate profile must include Digital Signature for TLS certificates.
5. Click **Next**.
The **Certificate Details** pane appears.
6. In the **Subject DN** field, enter a value for the certificate's subject DN. The value should be the DNS name of the server hosting Microsoft IIS. For example, `cn=example.com`.
7. For **Certificate Expiry**, provide an expiry date for TLS certificate. It is recommended that the TLS certificate be valid for 1 year or less.
8. Under **Subject Alternative Names**, add one or more DNS Name components to the Subject Alternative Name (subjectAltName) extension in the certificate. The subjectAltName extension must have a DNS Name component for each DNS name that may be used by the server hosting Microsoft IIS.
To add a DNS Name component the Subject Alternative Name extension:
 - a. For **SAN type**, select **DNS Name**.
 - b. In the **Value** field, enter a DNS name that may be used by the server hosting Microsoft IIS.
 - c. Click **Add** to add the DNS Name component to the Subject Alternative Name extension.
The component is added to the list of components in the Subject Alternative Name extension
 - d. To remove a component from the Subject Alternative Name extension, click **Remove** next to the extension that you want to remove.
9. Copy the contents of the CSR you generated earlier, and paste the contents into the **Certificate Signing Request (CSR)** text box.
10. Click **Submit**.
If the certificate is generated successfully, a success message appears.
11. Click **Download the newly created certificate** to download the TLS certificate.

After processing the CSR, proceed to [Installing the Web server certificate into Microsoft IIS](#).

Issuing the Web server certificate with an on-premises CA

If you are using Certificate Enrollment Gateway with an on-premises CA, you can use your existing CA tools to process the CSR and create the certificate.

- [Creating or recovering a user account for the Web server certificate](#)
- [Processing the CSR for the Web server certificate](#)

Creating or recovering a user account for the Web server certificate

To issue a certificate for the Web server, a user account for the certificate must exist in your on-premises CA. You must create a user account to issue the initial Web server certificate. You must recover (reset) the user account to renew the Web server certificate.

To manually create or recover (reset) a user account, you can use an administration application such as:

- The Entrust Certificate Authority administration portal
- The User Management Service (Entrust Administration Services)

When creating a new user account:

- It is recommended that you configure the user's name (using the directory naming attributes) to be the fully qualified domain name of the Web server. For example, `example.com`.
- Select a 1-key-pair certificate type with a Dual Usage certificate definition that includes an Extended Key Usage extension with server authentication and client authentication. The certificate definition should also be assigned a certificate definition policy. For example, the Enterprise Machine (ent_machine) certificate type.
- For the Subject Alternative Name (SubjectAltName) extension, add a DNS Name component for each DNS name that may be used by the Web server.

For information about creating or recovering user accounts, see the documentation for the client application.

Processing the CSR for the Web server certificate

You can process the CSR for the Web server certificate using the Profile Creation Utility. The Profile Creation Utility is a command line utility that can create and manage Entrust profiles for an on-premises Entrust Certificate Authority. You can use the Profile Creation Utility to process Certificate Signing Requests (CSRs) and generate certificates. The Profile Creation Utility is available as a separate software download for Entrust CA Gateway.

- [Installing the Profile Creation Utility](#)
- [Processing the CSR](#)

i When processing a CSR, the Profile Creation Utility will prompt you for the certificate definition required for the certificate. In Entrust Certificate Authority, that certificate definition for the user's certificate type must be assigned a certificate definition policy (user policy). If no certificate definition policy is assigned to the certificate definition you specify, an error will occur and the Profile Creation Utility will fail to process the CSR.

Installing the Profile Creation Utility

See below to download and install the Profile Creation Utility.

To install the Profile Creation Utility

1. Install a Java Development Kit (JDK) and set the `JAVA_HOME` environment variable.
2. Log in to Entrust TrustedCare (<https://trustedcare.entrust.com>).
3. Go to **PKI > Authority > CA Gateway** and click the latest version of the product.
4. Under software downloads, download the Profile Creation Utility for your preferred operating system:
 - `cagw-profilecreationutility-linux64-version.zip` for Linux 64-bit.
 - `cagw-profilecreationutility-win64-version.zip` for Windows 64-bit.
5. Extract the file contents of the ZIP file to a location on the computer.


Processing the CSR

See below to process the CSR using the Process Creation Utility.

To process the CSR using the Process Creation Utility

1. Obtain the CSR file along with the reference number and authorization code associated with the Entrust Certificate Authority user account.
When you create a user in Entrust Certificate Authority or set a user for key recovery, Entrust Certificate Authority generates a reference number and authorization code. You need these activation codes to process the CSR.
2. To process the CSR, the Profile Creation Utility requires an Entrust desktop profile (EPF file). The role associated with the profile requires the following permissions:
 - Under the **Certificates** permission category: permissions to administer the certificate category and certificate type of the certificate being issued.
 - Under the **Groups** permission category: **View** and permission to administer the group associated with the Entrust Certificate Authority user being issued the certificate.
 - Under the **Roles** permission category: **View** and permission to administer the role associated with the Entrust Certificate Authority user being issued the certificate.
 - Under the **Searchbase** permission category: **View** and permission to administer the searchbase associated with the Entrust Certificate Authority user being issued the certificate.
 - Under the **Users** permission category: **View** and **Perform PKIX** requests. Obtain the Entrust desktop profile (EPF file) from an Entrust Certificate Authority administrator.
3. Navigate to the directory containing the Profile Creation Utility.
4. Run the following command:
 - On Windows, run `pcu.bat`.
 - On Linux, run `pcu`.
5. The Profile Creation Utility main menu appears:

```
Main Menu
1. Exit
2. Help
3. Create Entrust profile
4. Recover Entrust profile
5. Inspect Entrust profile (read only)
6. Inspect and update Entrust profile (read/write)
7. Create Server Login credentials
8. Create PKCS #12 file (Entrust Certificate Authority)
9. Recover PKCS #12 file (Entrust Certificate Authority)
10. Create PKCS #12 file (3rdParty)
11. Update PKCS #12 file (3rdParty)
12. Process PKCS #10 Certificate Signing Request (CSR)
13. Generate/Process Certificate Signing Request on HSM (3rdParty)
14. Change password
Select an operation [3]:
```

 To return to the main menu at any time, enter a period (.). For help about using the Profile Creating Utility, enter 2 in the main menu.

Enter 12 to process the CSR.

6. The following prompt appears:

Take settings from an existing entrust.ini file (y/n) [y]:

- To use Certificate Authority (CA) connection settings from an existing `entrust.ini` file, enter `y`.
- To provide CA connection settings manually, enter `n`.

7. If you chose to use an existing `entrust.ini` file, you are prompted to enter the full path to the `entrust.ini` file:

Enter full path to entrust.ini file:

Enter the full path and file name of the `entrust.ini` file.

8. If you chose to enter CA connections setting manually, the following prompts appear:
- a. You are prompted to provide the host name (or IP address) and port of the CA server:

Enter the CA hostname or IP address and port in the form name:port:

Enter the host name (or IPv4 address) and CMP port of the server hosting the CA in format of `<hostname>:<port>`. If you omit the port number, it defaults to 829.

- b. You are prompted to provide the host name (or IP address) and port of the directory server:

Enter the directory hostname or IP address and port in the form name:port:

Enter the host name (or IPv4 address) and LDAP port of the server hosting the directory in format of `<hostname>:<port>`. The name or address defaults to the same value that you entered for the CA address. If you omit the port number, it defaults to 389.

9. You are prompted for the full path to an administration profile:

Enter full path to administration profile:

Enter the full path and file name of an administration profile.

10. You are prompted to enter the profile password:

Enter profile password:

Enter the profile password.

11. You are asked if the CSR is authenticated:

Is the CSR authenticated? (y/n)? [n]:

Enter `n`. The CSR is not authenticated.

12. You are prompted for the full path to the CSR:

Enter full path to CSR:

Enter the full path and file name of the CSR.

13. You are prompted to enter the reference number for the CSR:

Enter reference number:

Enter the reference number you recorded earlier.

14. You are prompted to enter the authorization code for the CSR:

Enter authorization code:

Enter the authorization code you recorded earlier.

15. You are prompted to enter a file name for the certificate:

Enter certificate file to create:

Enter the full path and file name for the certificate file.

16. You are prompted to enter the certificate definition required for the certificate:

Enter certificate definition required [Verification]:

Enter the certificate definition required for the certificate, such as Verification or Dual Usage.

17. The Profile Creation Utility processes the certificate. If the operation is successful, Entrust Certificate Authority issues a certificate and the Profile Creation Utility writes the certificate to a file.

```
Requesting certificate fromEntrust Certificate Authority...
Obtained new certificate with serial number 1340207625 from issuer
o=Example,c=US
Certificate written to c:\new_certificate.cer
```

18. After processing the CSR and obtaining the certificate, proceed to [Installing the Web server certificate into Microsoft IIS](#).

Creating a CSR for the Web server certificate

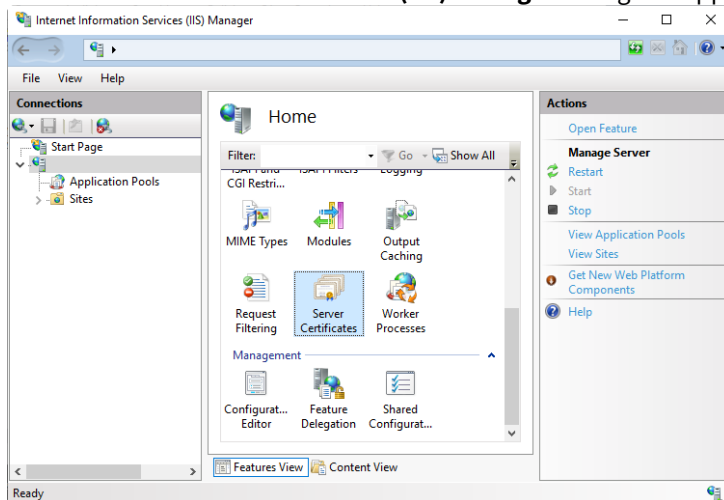
The Certificate Enrollment Policy Web Service is installed as an application in Microsoft Internet Information Services (IIS). Microsoft IIS requires a TLS certificate so that the Certificate Enrollment Policy Web Service can accept WSTEP enrollment requests over HTTPS.

The following procedure describes how to create a certificate signing request (CSR) in Microsoft IIS for a certificate. A CSR contains information that the issuing CA will use to create the certificate. Entrust PKI as a Service or an on-premises CA can process the CSR and issue the certificate.

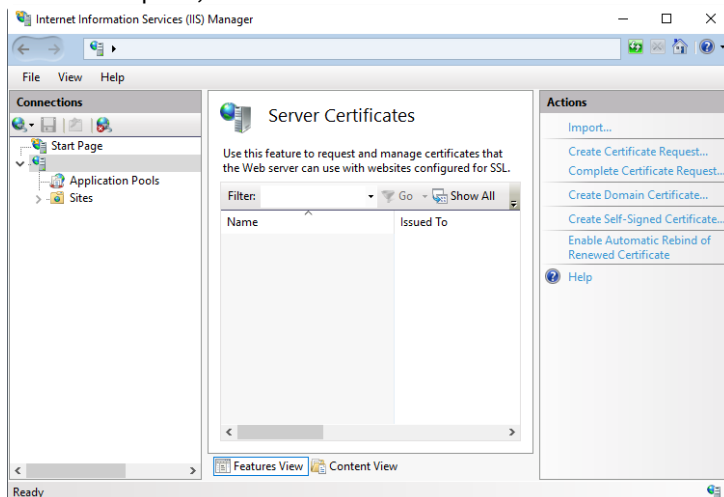
To create a CSR for Microsoft IIS

1. Open the Internet Information Services (IIS) Manager. Select **Start > Windows Administrative Applications > Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** dialog box appears.

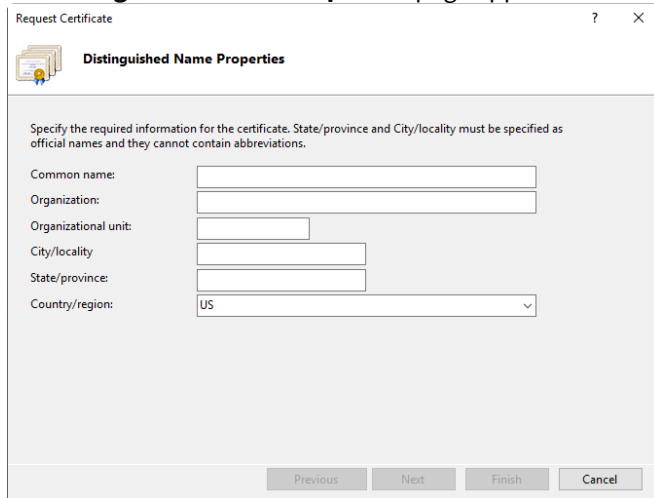


2. Under **Connections**, select the host name of the server.
3. In the **Home** pane, double-click **Server Certificates**.



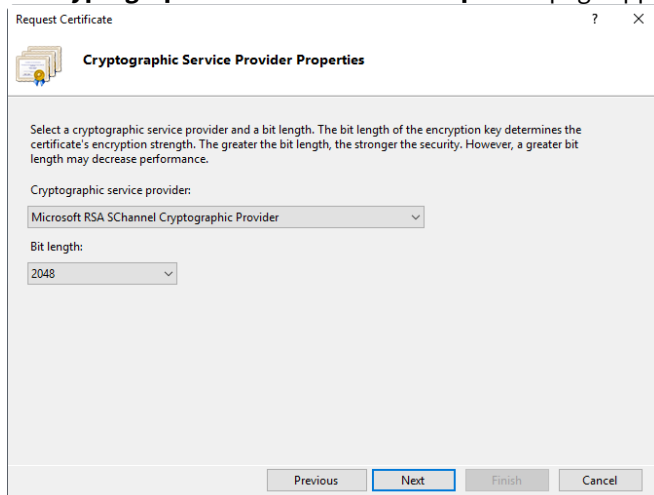
4. In the **Actions** pane, click **Create Certificate Request**.
The **Request Certificate** wizard appears.

5. The **Distinguished Name Properties** page appears.



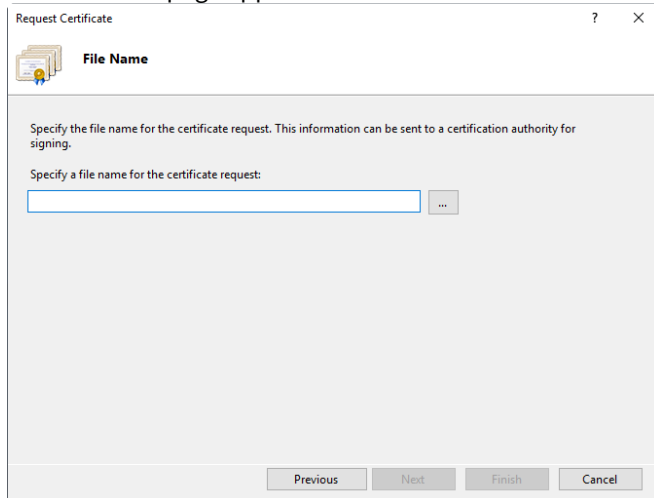
- In the provided fields, enter information that will be included in the CSR. Note that the issuing CA (either a CA in Entrust PKI as a Service, or an on-premises Entrust CA) will ignore this information.
- Click **Next**.

6. The **Cryptographic Service Provider Properties** page appears.



- From the **Cryptographic service provider** drop-down list, select a cryptographic service provider. It is recommended that you select **Microsoft RSA SChannel Cryptographic Provider**.
- In the **Bit length** list, select a bit length. It is recommended that you select 2048 as the bit length.
- Click **Next** to continue.

7. The **File Name** page appears.



- a. In the text field, enter a path and file name for the file that will contain the Web server certificate request.
 - b. Click **Finish**.
8. The CSR is saved in the file you specified in the previous step.

Preparing to install the Certificate Enrollment Policy Web Service

The Certificate Enrollment Policy Web Service will authenticate and forward WSTEP enrollment requests to Certificate Enrollment Gateway. The following topics describe how to prepare a server for the Certificate Enrollment Policy Web Service.

- [Installing Microsoft Internet Information Services](#)
- [Installing a server for the Certificate Enrollment Policy Web Service](#)

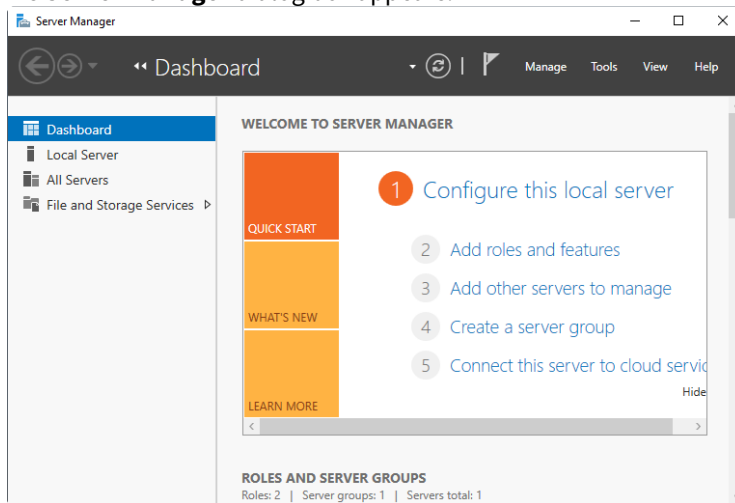
Installing Microsoft Internet Information Services

Microsoft Internet Information Services (IIS) is a Web server. The Certificate Enrollment Policy Web Service will be installed as an application in Microsoft IIS. The following procedure describes how to install Microsoft IIS.

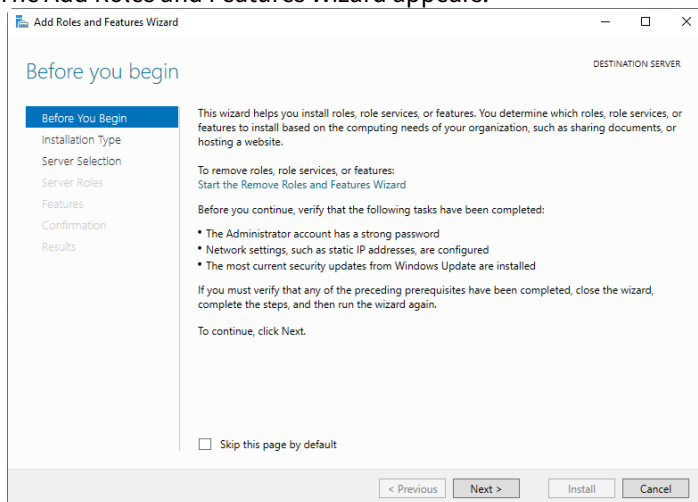
To install Microsoft Internet Information Services

1. Log in to the server that will host the Certificate Enrollment Policy Web Service.

2. Open Server Manager. Select **Start > Server Manager**.
The **Server Manager** dialog box appears.

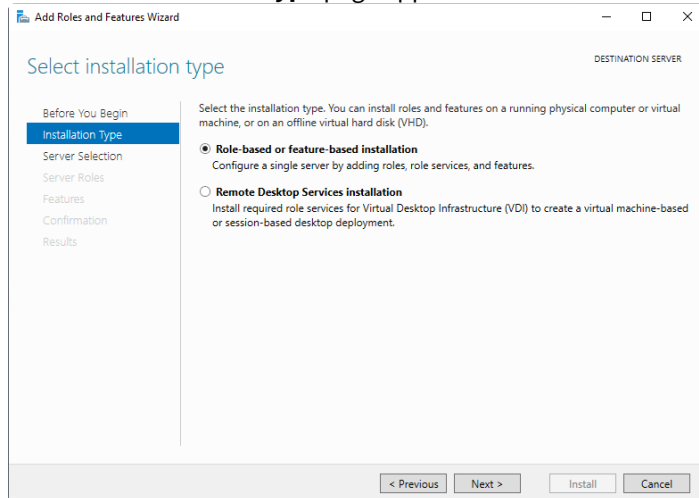


3. In the top navigation bar, select **Manage > Add Roles and Features**.
The **Add Roles and Features Wizard** appears.



4. Click **Next**.

The **Select installation type** page appears.

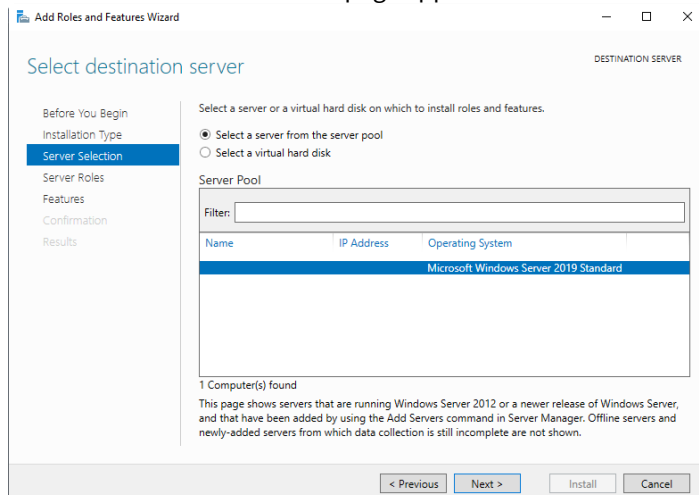


The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Select installation type'. On the left, there is a navigation pane with 'Before You Begin', 'Installation Type' (selected), 'Server Selection', 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the text: 'Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD)'. There are two radio button options: 'Role-based or feature-based installation' (selected) and 'Remote Desktop Services installation'. Below the first option is the text: 'Configure a single server by adding roles, role services, and features.' Below the second option is the text: 'Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

5. Click **Role-based or feature-based installation**. By default, this option is already selected.

6. Click **Next**.

The **Select destination server** page appears.



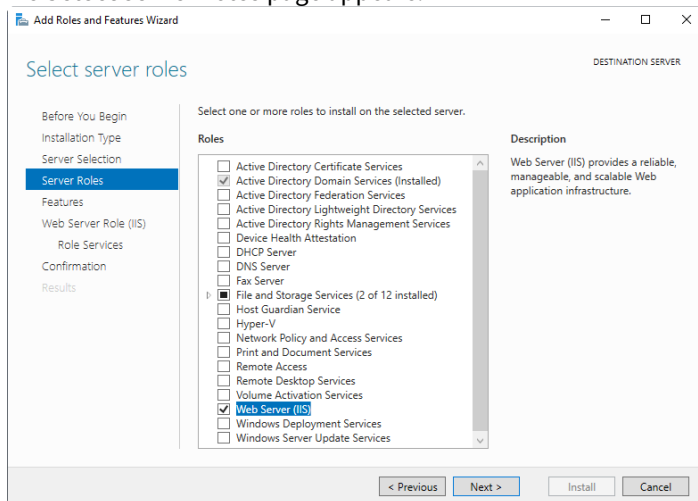
The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. On the left, there is a navigation pane with 'Before You Begin', 'Installation Type', 'Server Selection' (selected), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the text: 'Select a server or a virtual hard disk on which to install roles and features.' There are two radio button options: 'Select a server from the server pool' (selected) and 'Select a virtual hard disk'. Below the first option is a section titled 'Server Pool' with a 'Filter:' text box and a table. The table has three columns: 'Name', 'IP Address', and 'Operating System'. The first row of the table is 'Microsoft Windows Server 2019 Standard'. Below the table, it says '1 Computer(s) found'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

7. Click **Select a server from the server pool**. By default, this option should already be selected.

8. In the **Server Pool** list, select your server. By default, the server should already be selected.

9. Click **Next**.

The **Select server roles** page appears.

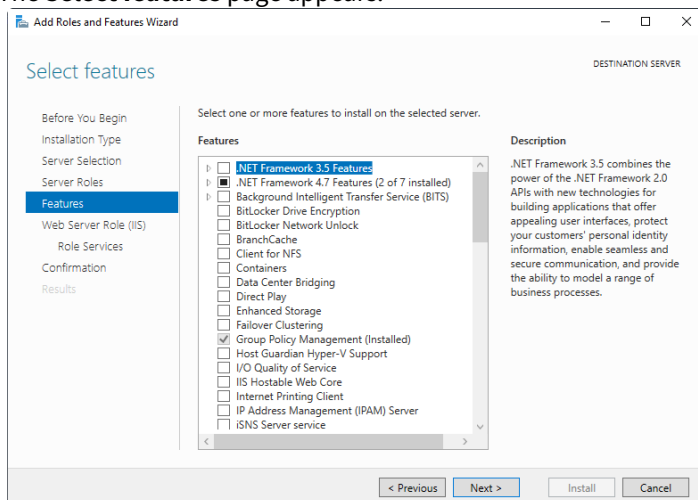


10. Select **Web Server (IIS)**.

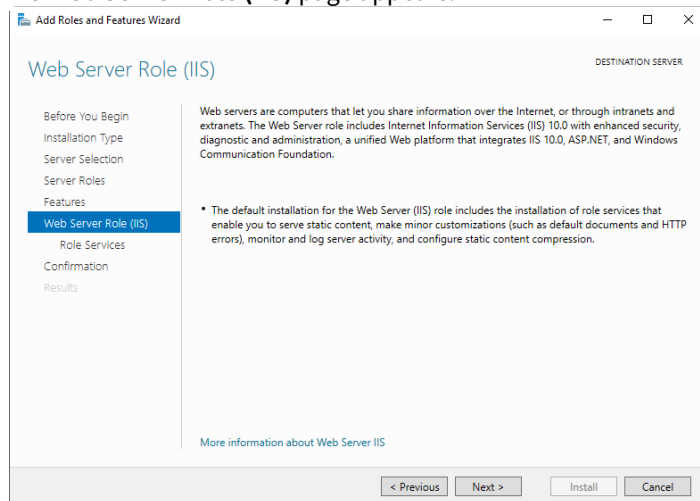
11. A dialog box may appear, informing you that some features are required for Microsoft IIS. Click **Add Features** to add these required features and close the dialog box.

12. Click **Next**.

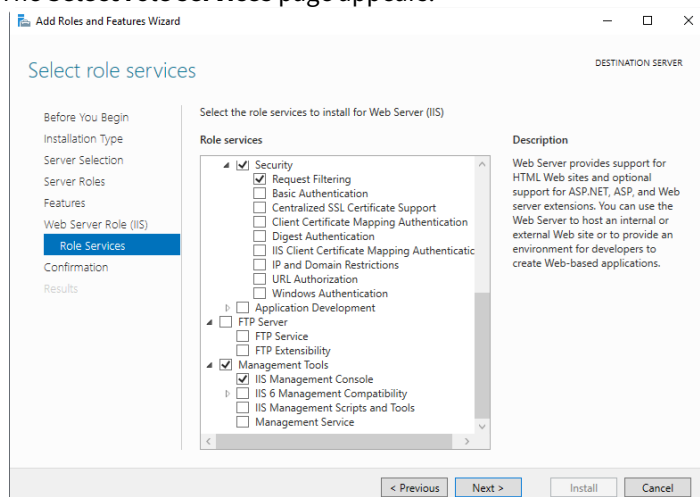
The **Select features** page appears.



13. You do not need to add any features on this page. Click **Next**.
The **Web Server Role (IIS)** page appears.



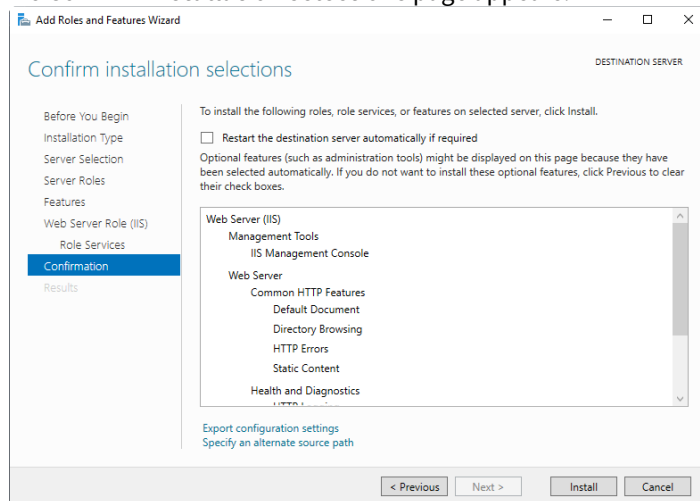
14. Click **Next**.
The **Select role services** page appears.



15. Under **Management Tools**, verify that **IIS Management Console** is selected.

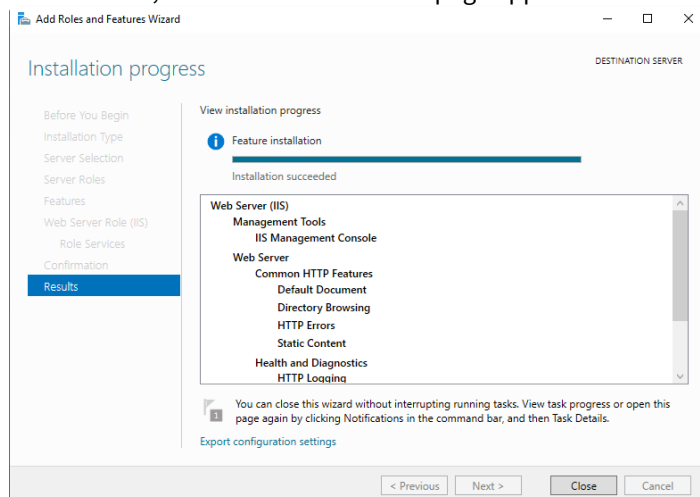
16. Click **Next**.

The **Confirm installation selections** page appears.



17. Click **Install**.

18. The **Installation Progress** page appears. A progress indicator displays the progress of the installation. After IIS is installed, the **Installation results** page appears.



19. Click **Close**.

Installing a server for the Certificate Enrollment Policy Web Service

The Windows server that will host the Certificate Enrollment Policy Web Service can be the domain controller or any other server in the domain. However, it is recommended that you install and configure the Certificate Enrollment Policy Web Service on a different server than the domain controller.

Install a supported version of Microsoft Windows Server (if not already installed), and join it to the Windows domain. Recommended system requirements for the Windows server:

- Windows Server 2016 or later
- Minimum 4 GB of RAM
- Minimum 2 CPU
- Minimum 40 GB free hard disk space

Configuring Active Directory for secure LDAP (Optional)

For WSTEP enrollment, Certificate Enrollment Gateway supports secure LDAP (LDAPS) connections with Active Directory. LDAPS connections with Active Directory is optional. The following topics describe how to configure Active Directory for secure LDAP.

- [Verifying LDAPS in Active Directory](#)
- [Installing the Active Directory server certificate](#)
- [Issuing the Active Directory server certificate with an on-premises CA](#)
- [Issuing the Active Directory server certificate with Entrust PKI as a Service](#)
- [Installing the CA certificate chain for the Active Directory certificate](#)
- [Creating a CSR for an Active Directory server certificate](#)

Verifying LDAPS in Active Directory

After installing the server certificate into Active Directory, test that LDAPS was enabled.

To verify LDAPS in Active Directory

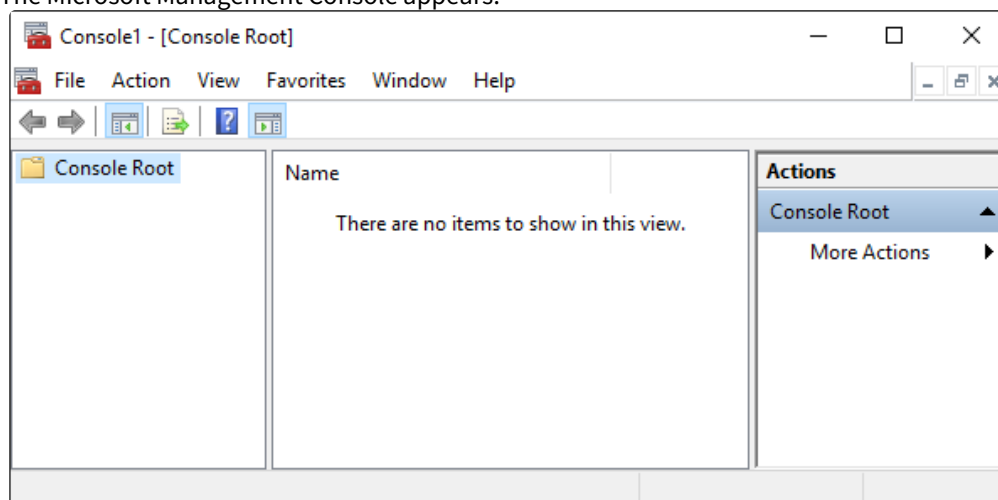
1. Start the Active Directory Administration Tool (`Ldp.exe`):
 - a. Select **Start > Windows System > Run**.
 - b. Enter `ldp.exe`.
2. Select **Connection > Connect**.
The **Connect** dialog box appears.
3. In the **Server** field, enter the domain controller to which you want to connect.
4. In the **Port** field, enter 636.
5. Click **OK**.

Installing the Active Directory server certificate

After obtaining the Active Directory server certificate, you must install the certificate into Active Directory. After processing the CSR with Entrust PKI as a Service or an on-premises CA, complete the certificate request to install the certificate into Active Directory. When the certificate is installed, LDAPS is automatically enabled in Active Directory.

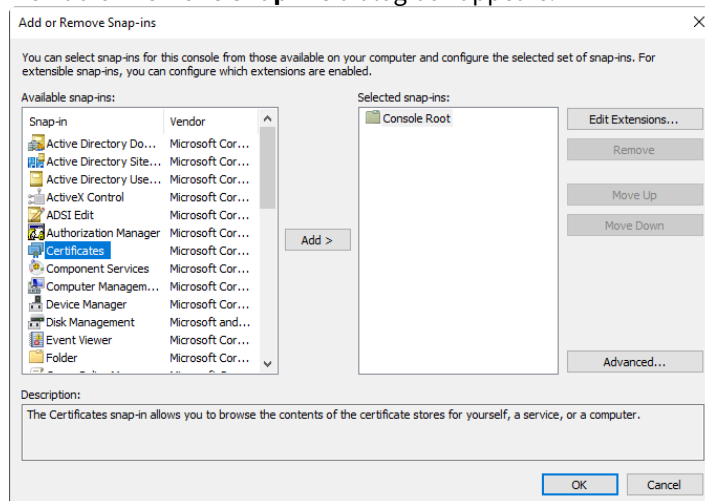
To complete a certificate request and install the Active Directory server certificate

1. Log into Active Directory as a member of the Domain Admins group.
2. Run `mmc.exe` (Select **Start > Windows System > Run**, then enter `mmc.exe`).
The Microsoft Management Console appears.



3. Select **File > Add/Remove Snap-in**.

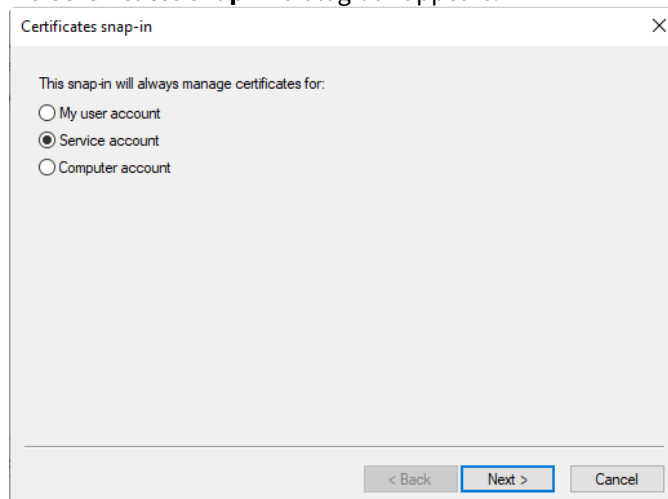
The **Add or Remove Snap-ins** dialog box appears.



4. In the **Available snap-ins** list, select **Certificates**.

5. Click **Add**.

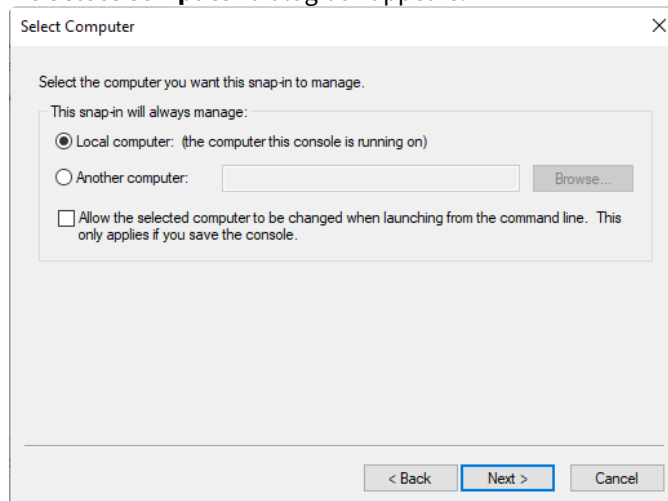
The **Certificates snap-in** dialog box appears.



6. Select **Service account**.

- Click **Next**.

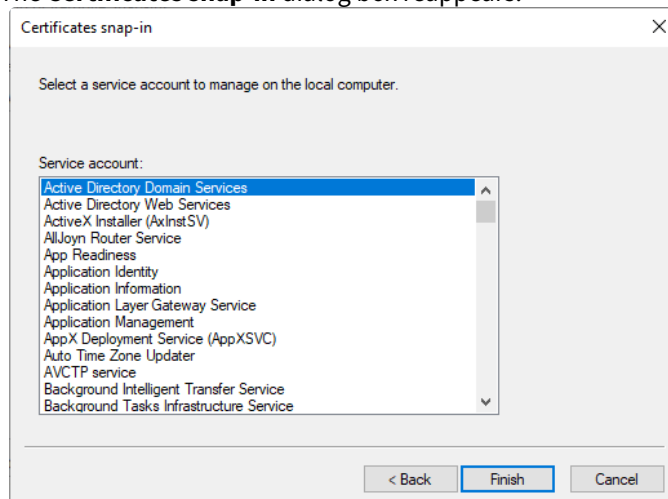
The **Select Computer** dialog box appears.



- Select **Local computer**.

- Click **Next**.

The **Certificates snap-in** dialog box reappears.



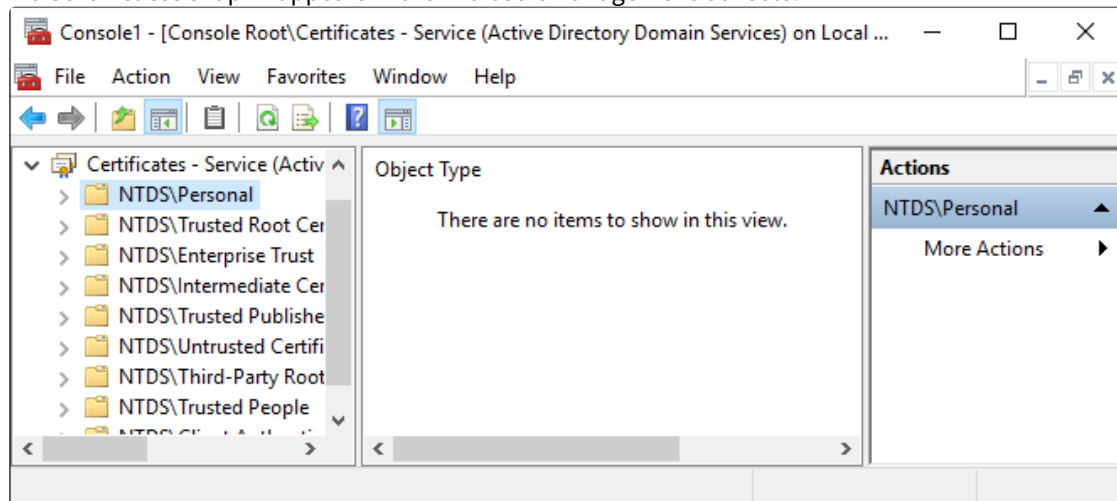
- Select **Active Directory Domain Services**.

- Click **Finish**.

The **Certificates** snap-in is added to the list of Selected snap-ins.

12. Click **OK**.

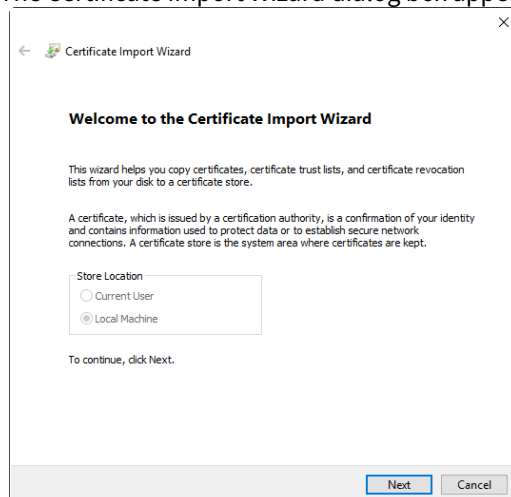
The **Certificates** snap-in appears in the Microsoft Management Console.



13. In the tree view, select **Certificates > NTDS\Personal**.

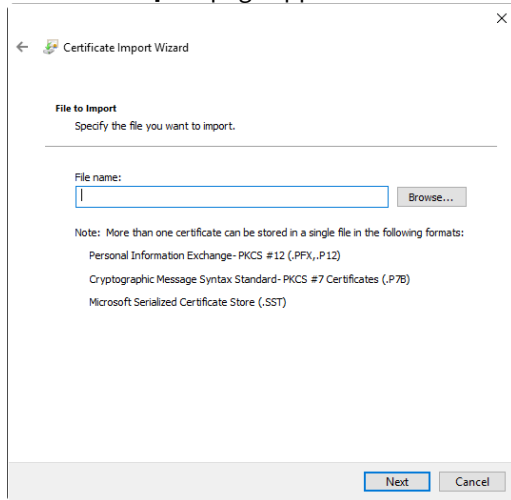
14. Select **Action > All Tasks > Import**.

The Certificate Import Wizard dialog box appears.



15. Click **Next**.

The **File to Import** page appears.

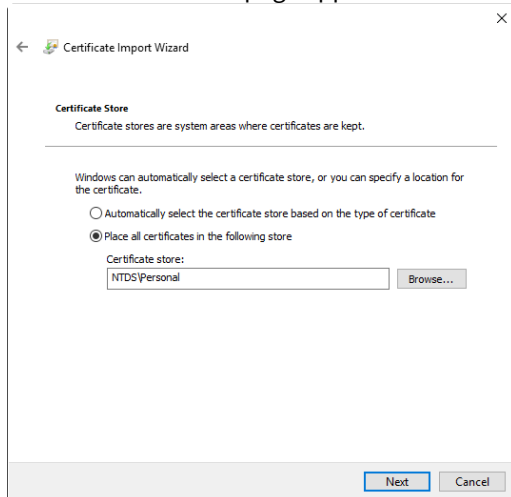


The screenshot shows the 'File to Import' step of the Certificate Import Wizard. The window title is 'Certificate Import Wizard'. It has a back arrow and a close button (X). The main heading is 'File to Import' with the instruction 'Specify the file you want to import.' Below this is a 'File name:' label followed by a text input field and a 'Browse...' button. A note states: 'Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange - PKCS #12 (.PFX, .P12), Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B), Microsoft Serialized Certificate Store (.SST)'. At the bottom are 'Next' and 'Cancel' buttons.

16. Click **Browse** and then select the Active Directory server certificate.

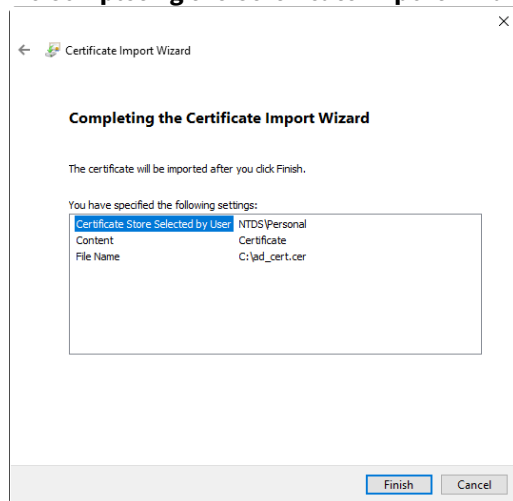
17. Click **Next**.

The **Certificate Store** page appears.



The screenshot shows the 'Certificate Store' step of the Certificate Import Wizard. The window title is 'Certificate Import Wizard'. It has a back arrow and a close button (X). The main heading is 'Certificate Store' with the instruction 'Certificate stores are system areas where certificates are kept.' Below this is a note: 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio button options: 'Automatically select the certificate store based on the type of certificate' (unselected) and 'Place all certificates in the following store' (selected). Below the selected option is a 'Certificate store:' label followed by a text input field containing 'NTDS\Personal' and a 'Browse...' button. At the bottom are 'Next' and 'Cancel' buttons.

18. The NTDS\Personal certificate store is already selected. Click **Next**. The **Completing the Certificate Import Wizard** page appears.



19. Click **Finish**.

Issuing the Active Directory server certificate with an on-premises CA

If you are using Certificate Enrollment Gateway with an on-premises CA, you can use your existing CA tools to process the CSR and create the certificate.

- [Creating or recovering a user account for the Active Directory server certificate](#)
- [Processing the CSR for the Active Directory server certificate](#)

Creating or recovering a user account for the Active Directory server certificate

To issue a certificate for Active Directory, a user account for the certificate must exist in your on-premises CA. You must create a user account to issue the initial Active Directory server certificate. You must recover (reset) the user account to renew the Web server certificate.

To manually create or recover (reset) a user account, you can use an administration application such as:

- The Entrust Certificate Authority administration portal
- The User Management Service (Entrust Administration Services)

When creating a new user account:

- It is recommended that you configure the user's name (using the directory naming attributes) to be the fully qualified domain name of the domain controller. For example, `activedirectory.example.com`.
- Select a 1-key-pair certificate type with a Dual Usage certificate definition that includes an Extended Key Usage extension with server authentication and client authentication, and a DomainController extension (OID 1.3.6.1.4.1.311.20.2). The certificate definition should also be assigned a certificate definition policy. For example, the Enterprise Domain Controller (ent_ad_dc) certificate type.
- For the Subject Alternative Name (SubjectAltName) extension, add a DNS Name component for each DNS name that may be used by Active Directory.

For information about creating or recovering user accounts, see the documentation for the client application.

Processing the CSR for the Active Directory server certificate

You can process the CSR for the Active Directory server certificate using the Profile Creation Utility. The Profile Creation Utility is a command line utility that can create and manage Entrust profiles for an on-premises Entrust Certificate Authority. You can use the Profile Creation Utility to process Certificate Signing Requests (CSRs) and

generate certificates. The Profile Creation Utility is available as a separate software download for Entrust CA Gateway.

- [Installing the Profile Creation Utility](#)
- [Processing the CSR with the Process Creation Utility](#)

i When processing a CSR, the Profile Creation Utility will prompt you for the certificate definition required for the certificate. In Entrust Certificate Authority, that certificate definition for the user's certificate type must be assigned a certificate definition policy (user policy). If no certificate definition policy is assigned to the certificate definition you specify, an error will occur and the Profile Creation Utility will fail to process the CSR.

Installing the Profile Creation Utility

See below for downloading and installing the Profile Creation Utility.

To download and install the Profile Creation Utility

1. Install a Java Development Kit (JDK) and set the `JAVA_HOME` environment variable.
2. Log in to Entrust TrustedCare (<https://trustedcare.entrust.com>).
3. Go to **PKI > Authority > CA Gateway** and click the latest version of the product.
4. Under software downloads, download the Profile Creation Utility for your preferred operating system:
 - `cagw-profilecreationutility-linux64-version.zip` for Linux 64-bit.
 - `cagw-profilecreationutility-win64-version.zip` for Windows 64-bit.
5. Extract the file contents of the ZIP file to a location on the computer.

Processing the CSR with the Process Creation Utility


See below for processing the CSR for the Active Directory server certificate with the Process Creation Utility,

To process the CSR using the Process Creation Utility

1. Obtain the CSR file along with the reference number and authorization code associated with the Entrust Certificate Authority user account.
When you create a user in Entrust Certificate Authority or set a user for key recovery, Entrust Certificate Authority generates a reference number and authorization code. You need these activation codes to process the CSR.
2. To process the CSR, the Profile Creation Utility requires an Entrust desktop profile (EPF file). the role associated with the profile requires the following permissions:
 - Under the **Certificates** permission category: permissions to administer the certificate category and certificate type of the certificate being issued.
 - Under the **Groups** permission category: **View** and permission to administer the group associated with the Entrust Certificate Authority user being issued the certificate.
 - Under the **Roles** permission category: **View** and permission to administer the role associated with the Entrust Certificate Authority user being issued the certificate.
 - Under the **Searchbase** permission category: **View** and permission to administer the searchbase associated with the Entrust Certificate Authority user being issued the certificate.
 - Under the **Users** permission category: **View** and **Perform PKIX** requests. Obtain the Entrust desktop profile (EPF file) from a Entrust Certificate Authority administrator.
3. Navigate to the directory containing the Profile Creation Utility.
4. Run the following command:
 - On Windows, run `pcu.bat`.
 - On Linux, run `pcu`.

5. The Profile Creation Utility main menu appears:

```
Main Menu
1. Exit
2. Help
3. Create Entrust profile
4. Recover Entrust profile
5. Inspect Entrust profile (read only)
6. Inspect and update Entrust profile (read/write)
7. Create Server Login credentials
8. Create PKCS #12 file (Entrust Certificate Authority)
9. Recover PKCS #12 file (Entrust Certificate Authority)
10. Create PKCS #12 file (3rdParty)
11. Update PKCS #12 file (3rdParty)
12. Process PKCS #10 Certificate Signing Request (CSR)
13. Generate/Process Certificate Signing Request on HSM (3rdParty)
14. Change password
Select an operation [3]:
```

 To return to the main menu at any time, enter a period (.). For help about using the Profile Creating Utility, enter 2 in the main menu.

Enter 12 to process the CSR.

6. The following prompt appears:

```
Take settings from an existing entrust.ini file (y/n) [y]:
```

- To use Certificate Authority (CA) connection settings from an existing `entrust.ini` file, enter `y`.
- To provide CA connection settings manually, enter `n`.

7. If you chose to use an existing `entrust.ini` file, you are prompted to enter the full path to the `entrust.ini` file:

```
Enter full path to entrust.ini file:
```

Enter the full path and file name of the `entrust.ini` file.

8. If you chose to enter CA connections setting manually, the following prompts appear:

- a. You are prompted to provide the host name (or IP address) and port of the CA server:

```
Enter the CA hostname or IP address and port in the form name:port:
```

Enter the host name (or IPv4 address) and CMP port of the server hosting the CA in format of `<hostname>:<port>`. If you omit the port number, it defaults to 829.

- b. You are prompted to provide the host name (or IP address) and port of the directory server:

```
Enter the directory hostname or IP address and port in the form name:port:
```

Enter the host name (or IPv4 address) and LDAP port of the server hosting the directory in format of `<hostname>:<port>`. The name or address defaults to the same value that you entered for the CA address. If you omit the port number, it defaults to 389.

9. You are prompted for the full path to an administration profile:

Enter full path to administration profile:

Enter the full path and file name of an administration profile.

10. You are prompted to enter the profile password:

Enter profile password:

Enter the profile password.

11. You are asked if the CSR is authenticated:

Is the CSR authenticated? (y/n)? [n]:

Enter `n`. The CSR is not authenticated.

12. You are prompted for the full path to the CSR:

Enter full path to CSR:

Enter the full path and file name of the CSR.

13. You are prompted to enter the reference number for the CSR:

Enter reference number:

Enter the reference number you recorded earlier.

14. You are prompted to enter the authorization code for the CSR:

Enter authorization code:

Enter the authorization code you recorded earlier.

15. You are prompted to enter a file name for the certificate:

Enter certificate file to create:

Enter the full path and file name for the certificate file.

16. You are prompted to enter the certificate definition required for the certificate:

Enter certificate definition required [Verification]:

Enter the certificate definition required for the certificate, such as Verification or Dual Usage.

17. The Profile Creation Utility processes the certificate. If the operation is successful, Entrust Certificate Authority issues a certificate and the Profile Creation Utility writes the certificate to a file.

```
Requesting certificate from Security Manager...
Obtained new certificate with serial number 1340207625 from issuer
o=Example,c=US
Certificate written to c:\new_certificate.cer
```

After processing the CSR and obtaining the certificate, proceed to [Installing the Active Directory server certificate](#).

Issuing the Active Directory server certificate with Entrust PKI as a Service

After creating the certificate signing request (CSR) for the Certificate Enrollment Gateway certificate, you can submit the CSR to an Issuing CA in Entrust PKI as a Service. The Issuing CA will process the CSR and generate the certificate.

To submit the CSR to Entrust PKI as a Service and obtain the TLS certificate

1. Log in the Entrust Certificate Services interface.
2. Select **Create > PKIaaS**.
The Select **Certificate Authority** pane appears.
3. From the **Certificate Authority** drop-down list, select the CA you want to issue the TLS certificate.
4. From the **Certificate Profile** drop-down list, select the certificate profile you want to use for the TLS certificate. The certificate profile must include Digital Signature for TLS certificates.
5. Click **Next**.
The **Certificate Details** pane appears.
6. In the **Subject DN** field, enter a value for the certificate's subject DN. The value should be the DNS name of the domain controller. For example, `cn=activedirectory.example.com`.
7. For **Certificate Expiry**, provide an expiry date for TLS certificate. It is recommended that the TLS certificate be valid for 1 year or less.
8. Under **Subject Alternative Names**, add one or more DNS Name components to the Subject Alternative Name (subjectAltName) extension in the certificate. The subjectAltName extension must have a DNS Name component for each DNS name that may be used by the domain controller.
To add a DNS Name component the Subject Alternative Name extension:
 - a. For **SAN type**, select **DNS Name**.
 - b. In the **Value** field, enter a DNS name that may be used by the domain controller.
 - c. Click **Add** to add the DNS Name component to the Subject Alternative Name extension.
The component is added to the list of components in the Subject Alternative Name extension
 - d. To remove a component from the Subject Alternative Name extension, click **Remove** next to the extension that you want to remove.
9. Copy the contents of the CSR you generated earlier, and paste the contents into the **Certificate Signing Request (CSR)** text box.
10. Click **Submit**.
If the certificate is generated successfully, a success message appears.
11. Click **Download the newly created certificate** to download the TLS certificate.

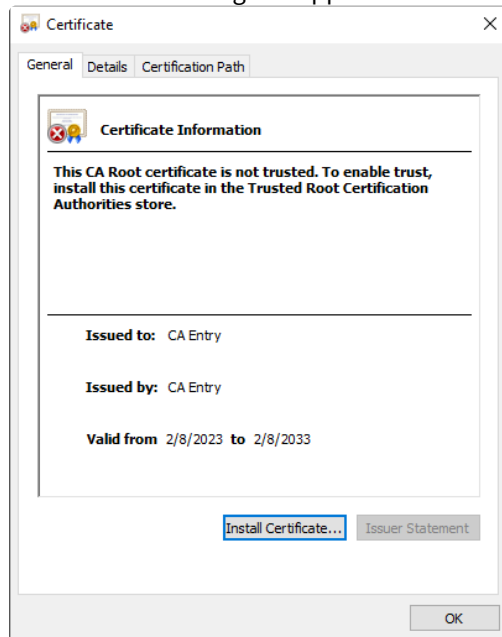
After processing the CSR, proceed to [Installing the Active Directory server certificate](#).

Installing the CA certificate chain for the Active Directory certificate

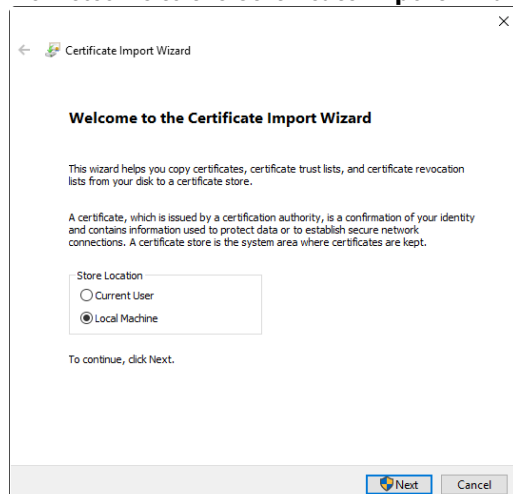
For Active Directory to trust the server certificate, you must install the CA certificate chain for the certificate into the server hosting Active Directory. You must install the entire CA certificate chain, from the root CA to the issuing CA (the CA that issued the server certificate). For an on-premises CA, the root CA may be the issuing CA. You must install the CA certificate chain into Active Directory before you install the server certificate.

To install a CA certificate into Active Directory

1. For an on-premises CA, obtain all CA certificates in the CA certificate chain using your on-premises CA tools. See the documentation for your on-premises CA for instructions.
2. For Entrust PKI as a Service, download all CA certificates in the certificate chain:
 - a. Log in the Entrust Certificate Services interface.
 - b. Select **Administration > PKIaaS Management**.
A list of private CAs appear.
 - c. For each CA in the TLS certificate chain (from the Issuing CA to the Root CA), select the CA and then click **Download certificate**.
3. Double-click the CA certificate file.
The **Certificate** dialog box appears.

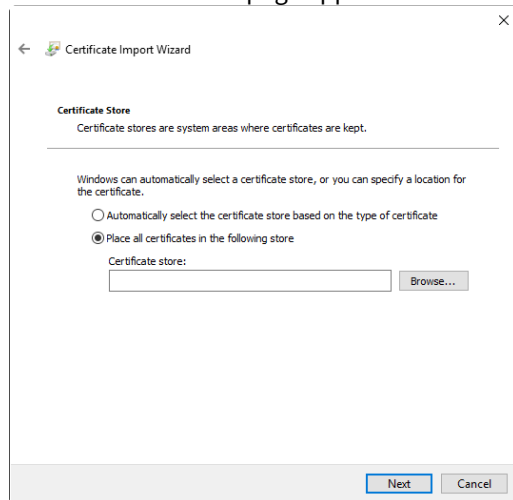


4. Click **Install Certificate**.
The Certificate Import Wizard appears.
5. The **Welcome to the Certificate Import Wizard** page appears.



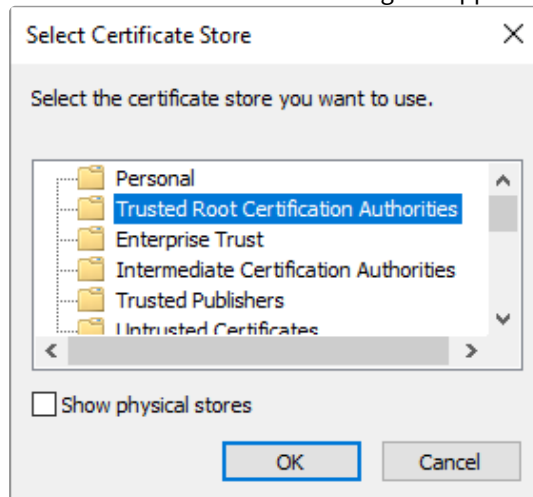
- a. For **Store Location**, select **Local Machine**.
- b. Click **Next**.

6. The **Certificate Store** page appears.



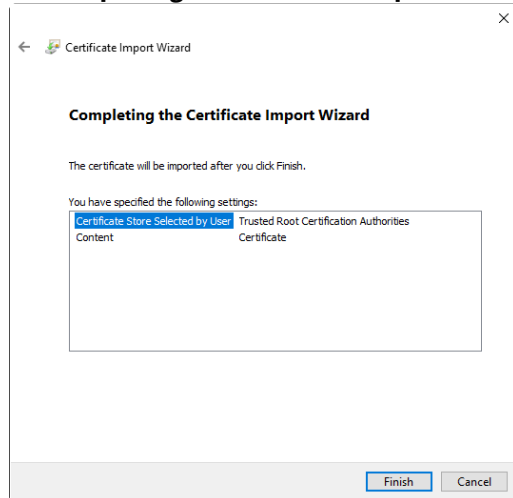
- a. Select **Place all certificates in the following store.**
- b. Click **Browse.**

The **Select Certificate Store** dialog box appears.



- c. If the CA certificate is a root CA certificate, select **Trusted Root Certification Authorities.**
- d. If the CA certificate is a subordinate (intermediate) CA certificate, select **Intermediate Certification Authorities.**
- e. Click **OK.**
- f. Click **Next.**

- The **Completing the Certificate Import Wizard** page appears.



- Click **OK**.

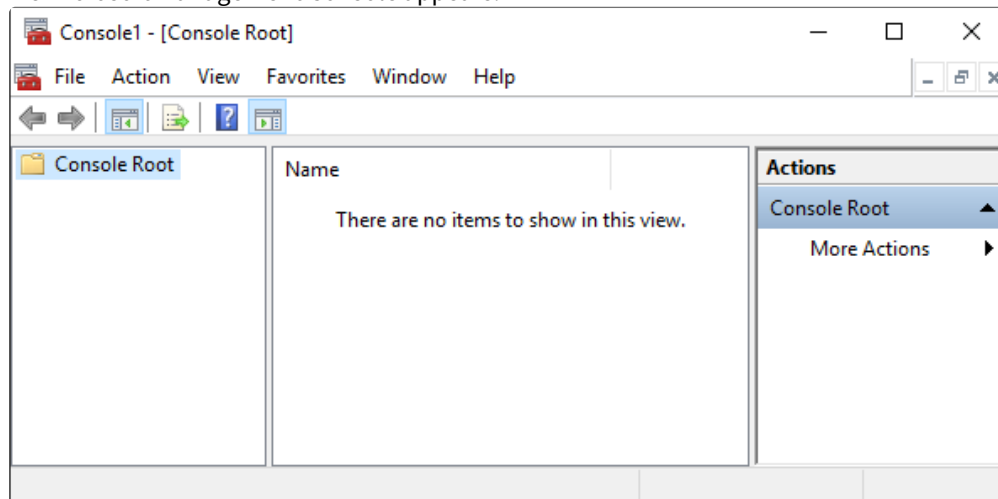
Creating a CSR for an Active Directory server certificate

Active Directory requires a server certificate to secure communications to the directory over LDAPS. The following procedure describes how to create a certificate signing request (CSR) for an Active Directory server certificate. A CSR contains information that the issuing CA will use to create the certificate. Entrust PKI as a Service or an on-premises CA can process the CSR and issue the certificate.

To create a CSR for an Active Directory server certificate

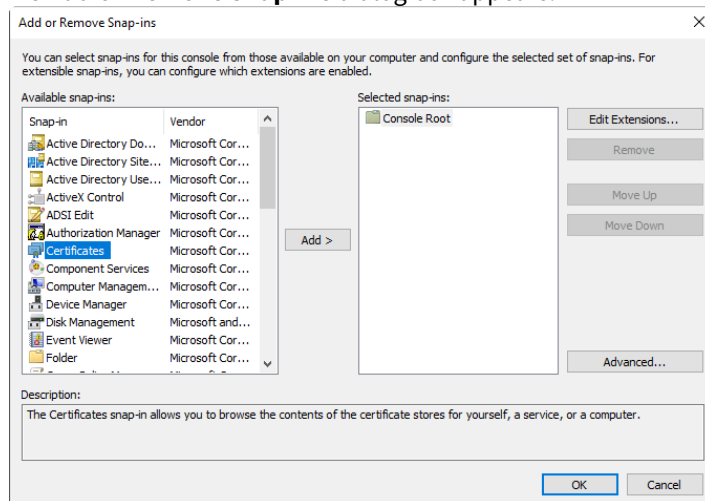
- Log into Active Directory as a member of the Domain Admins group.
- Run `mmc.exe` (Select **Start > Windows System > Run**, then enter `mmc.exe`).

The Microsoft Management Console appears.



3. Select **File > Add/Remove Snap-in**.

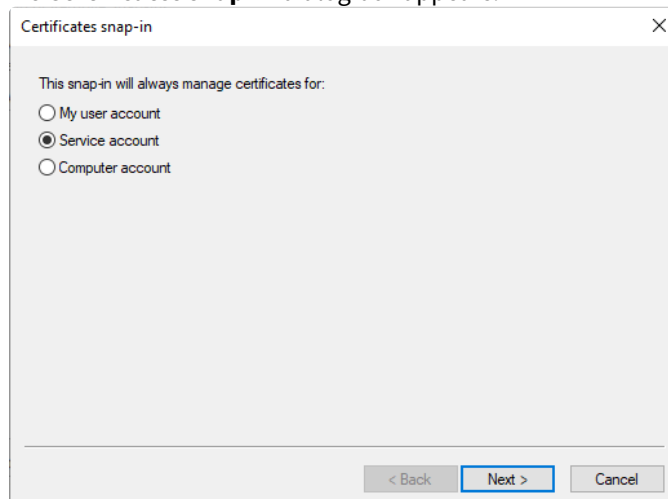
The **Add or Remove Snap-ins** dialog box appears.



4. In the **Available snap-ins** list, select **Certificates**.

5. Click **Add**.

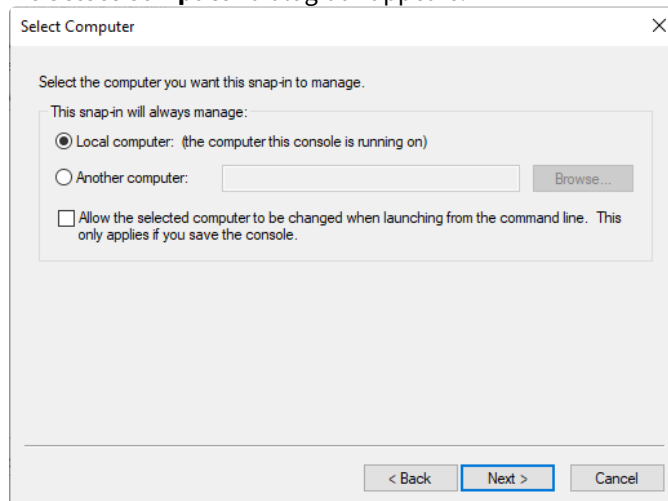
The **Certificates snap-in** dialog box appears.



6. Select **Service account**.

7. Click **Next**.

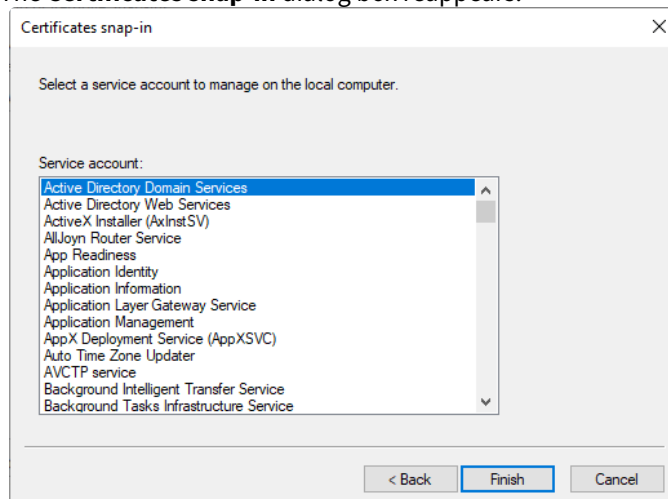
The **Select Computer** dialog box appears.



8. Select **Local computer**.

9. Click **Next**.

The **Certificates snap-in** dialog box reappears.



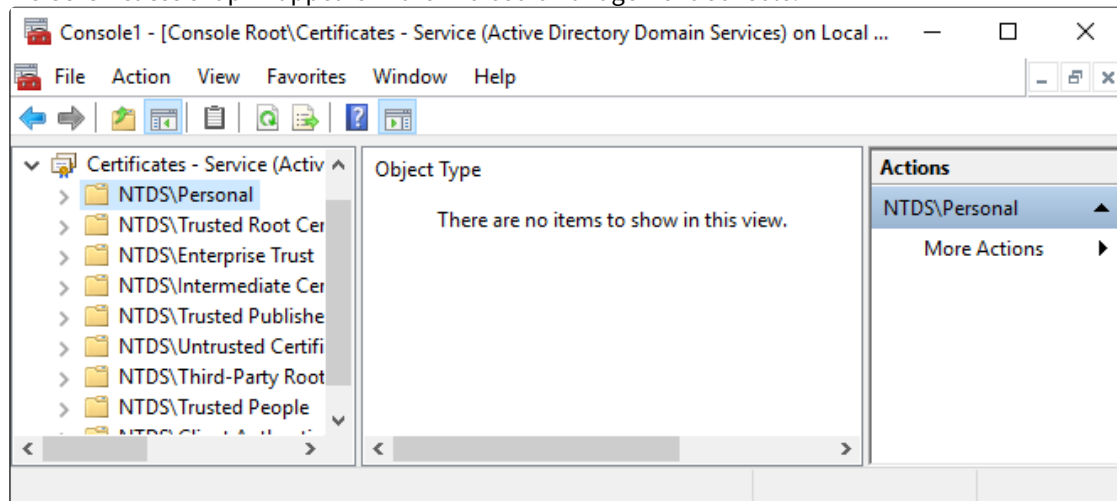
10. Select **Active Directory Domain Services**.

11. Click **Finish**.

The **Certificates** snap-in is added to the list of Selected snap-ins.

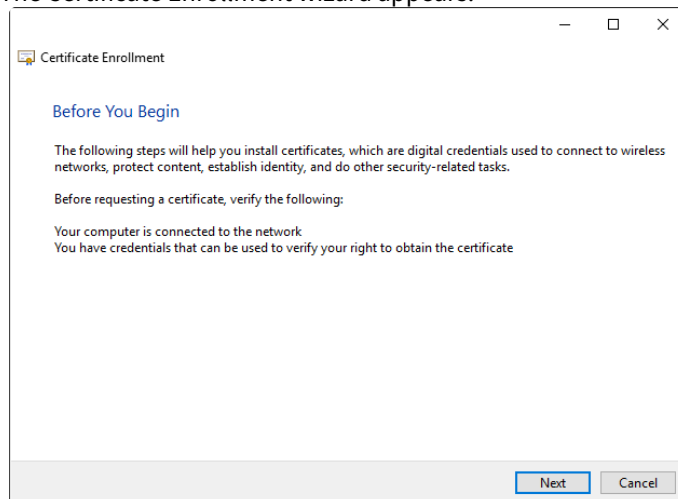
12. Click **OK**.

The **Certificates** snap-in appears in the Microsoft Management Console.



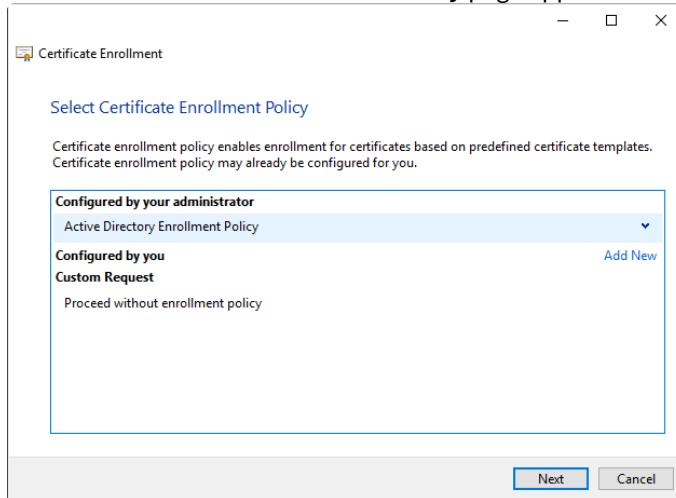
13. In the tree view, select **Certificates > NTDS\Personal**.
14. Select **Action > All Tasks > Advanced Operations > Create Custom Request**.

The Certificate Enrollment wizard appears.



15. Click **Next**.

The **Select Certificate Enrollment Policy** page appears.

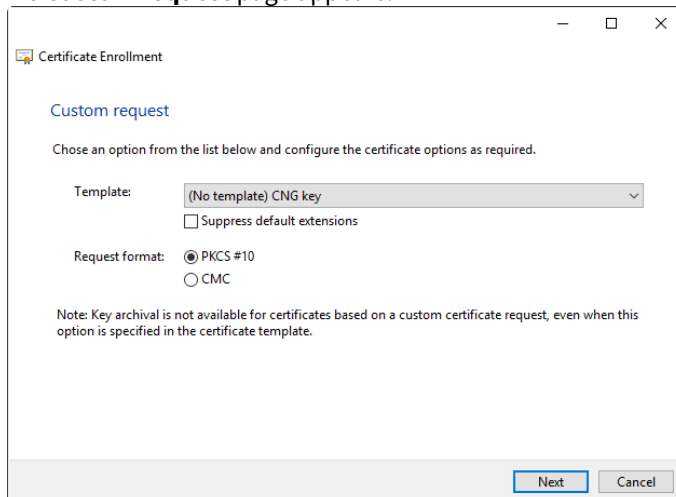


The dialog box is titled "Certificate Enrollment". It has a subtitle "Select Certificate Enrollment Policy". Below the subtitle, it says "Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you." There are two sections: "Configured by your administrator" and "Configured by you". Under "Configured by your administrator", there is a dropdown menu showing "Active Directory Enrollment Policy". Under "Configured by you", there is a section titled "Custom Request" with the text "Proceed without enrollment policy". There is an "Add New" link next to the "Custom Request" section. At the bottom, there are "Next" and "Cancel" buttons.

16. Under **Configured by your administrator**, select **Active Directory Enrollment Policy**.

17. Click **Next**.

The **Custom request** page appears.



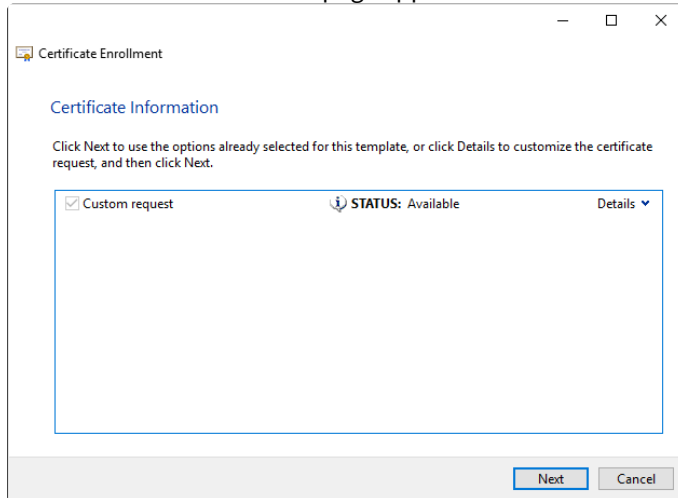
The dialog box is titled "Certificate Enrollment". It has a subtitle "Custom request". Below the subtitle, it says "Choose an option from the list below and configure the certificate options as required." There are two sections: "Template:" and "Request format:". Under "Template:", there is a dropdown menu showing "(No template) CNG key" and a checkbox labeled "Suppress default extensions". Under "Request format:", there are two radio buttons: "PKCS #10" (selected) and "CMC". At the bottom, there is a note: "Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template." At the bottom right, there are "Next" and "Cancel" buttons.

18. In the **Template** drop-down list, select **(No template) CNG key**.

19. For **Request format**, select **PKCS #10**.

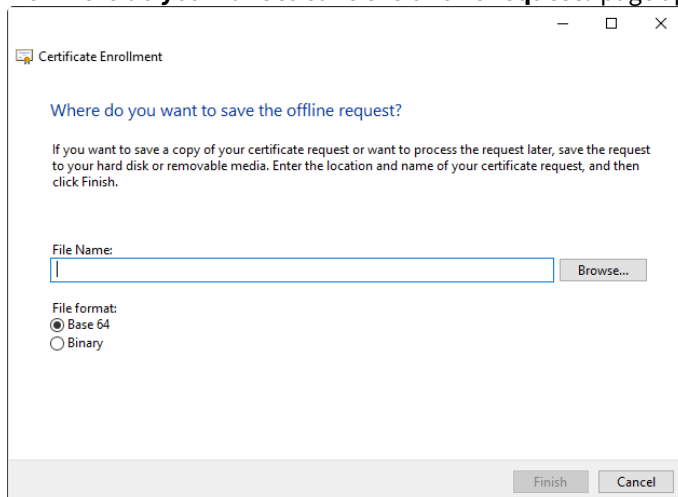
20. Click **Next**.

The **Certificate Information** page appears.

A screenshot of the 'Certificate Enrollment' window, specifically the 'Certificate Information' tab. The window title is 'Certificate Enrollment'. Below the title bar, there's a sub-header 'Certificate Information'. A message states: 'Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.' Below this, there's a section with a checkbox labeled 'Custom request' which is checked. To its right, it says 'STATUS: Available' with a small icon, and further right is a 'Details' dropdown menu. At the bottom of the window, there are 'Next' and 'Cancel' buttons.

21. Click **Next**.

The **Where do you want to save the offline request?** page appears.

A screenshot of the 'Certificate Enrollment' window, specifically the 'Where do you want to save the offline request?' tab. The window title is 'Certificate Enrollment'. Below the title bar, there's a sub-header 'Where do you want to save the offline request?'. A message states: 'If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.' Below this, there's a 'File Name:' label followed by a text input field and a 'Browse...' button. Underneath, there's a 'File format:' section with two radio buttons: 'Base 64' (which is selected) and 'Binary'. At the bottom of the window, there are 'Finish' and 'Cancel' buttons.

22. In the **File Name** field, enter the path and file name for the CSR, or click **Browse** to select a location.
23. For **File format**, select **Base 64**.
24. Click **OK**.

Creating Windows certificate templates for the Entrust WSTEP Service

The Entrust WSTEP Service is a component of Certificate Enrollment Gateway. The Entrust WSTEP Service is Certificate Enrollment Gateway's implementation of the WSTEP protocol.

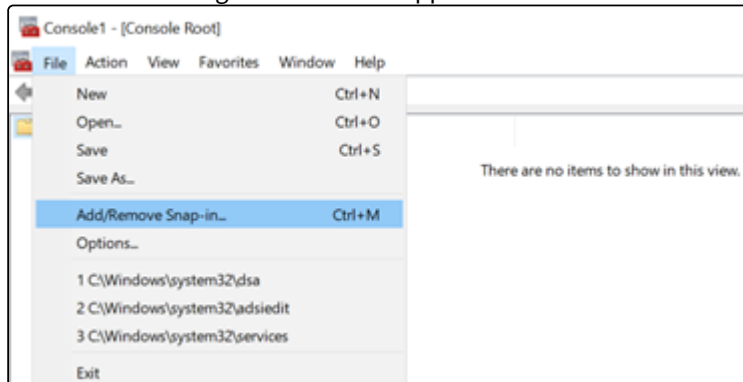
The Entrust WSTEP Service will use Windows certificate templates when enrolling users, computers, or domain controllers with your Windows-native endpoints. Create as many new certificate templates as you require. For example, users may require certificates with two key pairs (such as Encryption and Verification) or one key pair (such as Signature or Encryption).

To create a Windows certificate template for WSTEP

1. Log into Active Directory as a member of the Domain Admins group.

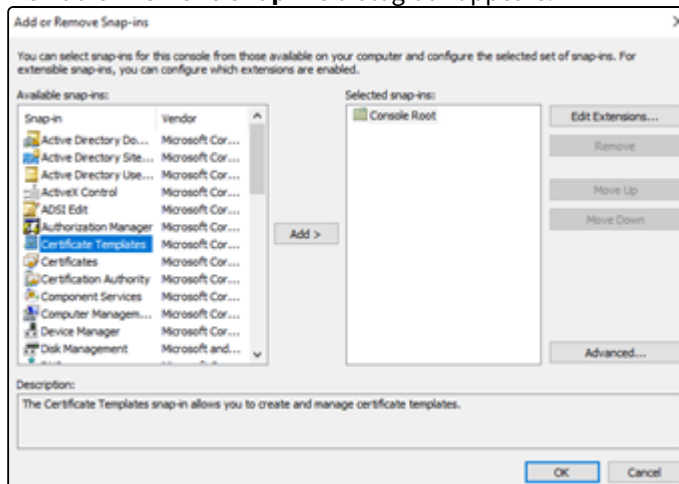
- Run `mmc.exe` (Select **Start > Windows System > Run**, then enter `mmc.exe`).

The Microsoft Management Console appears.




- Select **File > Add/Remove Snap-in**.

The **Add or Remove Snap-ins** dialog box appears.



- In the **Available snap-ins** list, select **Certificate Templates**.
- Click **Add**.
- In the tree view, select the **Certificate Templates** snap-in.
- Select the certificate you want to duplicate for the enrollment service. Supported templates:
 - Computer
 - Domain Controller
 - Kerberos Authentication
 - User
 - User Signature Only

8. Duplicate the template by selecting **Action > Duplicate Template**. A **Properties of New Template** dialog box appears.



The dialog box titled "Properties of New Template" has a close button (X) in the top right corner. It features several tabs: "Subject Name", "Server", "Issuance Requirements", "Superseded Templates", "Extensions", "Security", "Compatibility", "General", "Request Handling", "Cryptography", and "Key Attestation". The "Compatibility" tab is currently selected. Inside this tab, there is a text box stating: "The template options available are based on the earliest operating system versions set in Compatibility Settings." Below this, there is a checked checkbox labeled "Show resulting changes". Underneath, there is a section titled "Compatibility Settings" containing two dropdown menus: "Certification Authority" (set to "Windows Server 2012 R2") and "Certificate recipient" (set to "Windows 8.1 / Windows Server 2012 R2"). At the bottom, there is a disclaimer: "These settings may not prevent earlier operating systems from using this template." and four buttons: "OK", "Cancel", "Apply", and "Help".

9. Under each tab, configure template options as described in the following sections.

✗ Start configuring the template options from the **Compatibility** tab. Otherwise, the **Provider Category** option in the **Cryptography** tab will be locked to **Legacy Cryptographic Service Provider**.

- [Extensions tab](#)
- [Issuance Requirements tab](#)
- [Subject Name tab](#)
- [Key Attestation tab](#)
- [Cryptography tab](#)
- [Request Handling tab](#)
- [Security tab](#)
- [General tab](#)
- [Compatibility tab](#)

Extensions tab

All options under the **Extensions** tab are supported.

See the following table for the **Key Usage** combinations supported by each **Purpose** in the **Request Handling** tab.

Purpose	Supported Key Usage Combinations
Encryption	Key Encipherment
Signature	Digital Signature Digital Signature+Non-repudiation

Purpose	Supported Key Usage Combinations
Signature and Encryption	Digital Signature+Key Encipherment
Signature and smartcard logon.	Digital Signature

Issuance Requirements tab

Options under the **Issuance Requirements** tab are not supported.

Option	Supported
CA certificate manager approval	No. All certificate requests are processed automatically without any approval.
Require the following for reenrollment	No

Subject Name tab

Under the **Subject Name** tab, set the supported options.

Option	Supported	Value
Supply in request	Yes	The Subject Alternative Name RegisteredID is not supported. The Subject name types Title and Initials are not supported.
Use subject information from existing certificates for autoenrollment renewal requests	Yes	
Build from Active Directory information	Yes	

Option	Supported	Value
Subject name format	Yes	<p>For User certificate templates, the following formats are supported:</p> <ul style="list-style-type: none"> • Common name. • Fully distinguished name. This value is not supported when Certificate Enrollment Gateway has mapped the Windows certificate template to a Profile ID in CA Gateway. <p>For Computer or Domain Controller certificate templates, the following formats are supported:</p> <ul style="list-style-type: none"> • Common name. • DNS. • Fully distinguished name. This value is not supported when Certificate Enrollment Gateway has mapped the Windows certificate template to a Profile ID in CA Gateway.
Include e-mail name in subject name	No	
E-mail name	Yes	
DNS name	Yes	
User principal name (UPN)	Yes	
Service principal name (SPN)	Yes	

Key Attestation tab

Options under the **Key Attestation** tab are not supported.

Cryptography tab

Under the **Cryptography** tab, set the supported options.

Option	Supported	Value
Provider Category	Yes	
Algorithm name	Yes	

Option	Supported	Value
Minimum key size	Yes	2048
Requests can use any provider available on the subject's computer	Yes	
Requests must use one of the following providers	Yes	
Request hash	Yes	
Use alternate signature format	No	

Request Handling tab

Under the **Request Handling** tab, set the supported options.

Option	Supported	Value
Purpose	Yes	Encryption, Signature, Signature and encryption, and Signature and smartcard logon
Delete revoked or expired certificates (do not archive)	Yes	
Include symmetric algorithms allowed by the subject	Yes	SMIME settings
Archive subject's encryption private key	No	
Authorize additional service accounts to access the private key	No	
Allow private key to be exported	Yes	
Renew with the same key	Yes	
For automatic renewal of smart card certificates, use the existing key if a new key cannot be created	Yes	

Option	Supported	Value
Enroll subject without requiring any user input	Yes	
Prompt the user during enrollment	No	
Prompt the user during enrollment and require user input when the private key is used	No	

Security tab

Under the **Security** tab, set the following options.

Option	Value
Groups or usernames	Select the group that will use the new certificate template. For example, select the Domain Users group to use a copy of the User certificate template. If the group is not listed, click Add to add the group to the list.
Permissions for Authenticated Users	Set the following Allow permissions for the selected group: Read, Enroll, Autoenroll.

General tab


Under the **General** tab, configure the supported options.

Option	Supported	Value
Template display name	Yes	The display name for the new certificate template.
Template name	Yes	The name of the new template. The default value of this field is the value set in the Template display name field but without spaces. We recommend using this value. The name must contain only alphanumeric characters (a-z, A-Z, 0-9).
Validity Period	Yes	Any value allowed by the validity policy of the issuing CA.

Option	Supported	Value
Renewal Period	Yes	Controlled by the client.
Publish certificate in Active Directory	No	

Compatibility tab

Under the **Compatibility** tab, select the compatibility settings based on the earliest versions of the operating systems running in your environment.

Option	Minimum version
Certification Authority	Server 2012 R2 <div>  If you install a Windows Server 2016 CA, read the following Microsoft troubleshooting guide: Cannot select Windows Server 2016 CA-compatible certificate templates from Windows Server 2016 or later-based CAs or CEP servers. </div>
Certificate recipient	Windows 8.1 / Server 2012 R2. Earlier versions of Windows may not recognize template options introduced in later versions of the Windows certificate templates.

Adding the Windows Certificate Templates to Active Directory

The Entrust WSTEP Service is the Certificate Enrollment Gateway's implementation of the WSTEP protocol. The Entrust WSTEP Service will use Windows certificate templates when enrolling users, computers, or domain controllers with your Windows-native endpoints.

If you already have a Microsoft CA installed in Active Directory, the Certificate Templates feature is already enabled, and you can skip this section. Otherwise, you must add the Certificate Templates feature using either Windows PowerShell or the Windows graphical interface.

- [Adding the certificate templates feature using PowerShell](#)
- [Adding the certificate templates feature using the Windows graphical interface](#)

Adding the certificate templates feature using PowerShell

To add Certificate Templates using Windows PowerShell, complete the following procedure.

1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
2. Open an elevated PowerShell window. Select **Start > Windows PowerShell, then right-click Windows PowerShell > Run as administrator.**
3. Run the following command.

Add-WindowsFeature RSAT-ADCS-Mgmt

4. Launch the Certificate Templates snap-in.

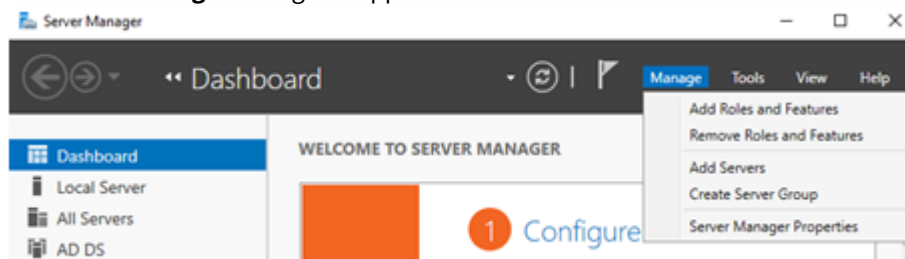
C:\Windows\System32\certtmpl.msc

5. Answer **Yes** when prompted to install the templates into Active Directory.

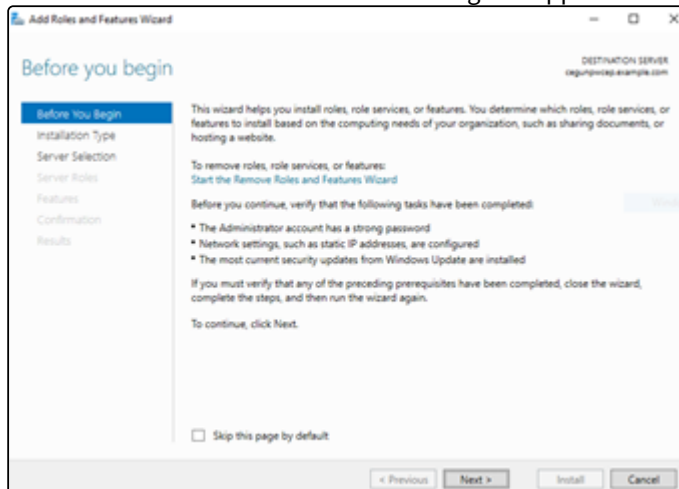
Adding the certificate templates feature using the Windows graphical interface

To add Certificate Templates using the Windows graphical interface, complete the following procedure.

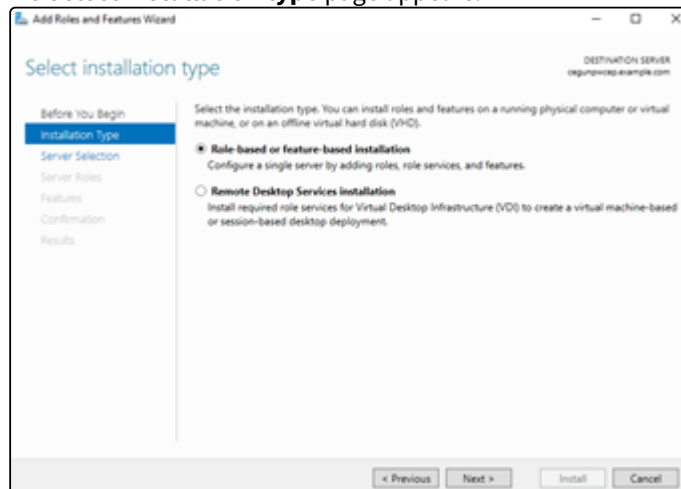
1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
2. Open Server Manager. Select **Start > Server Manager**.
The **Server Manager** dialog box appears.



3. Select **Manage > Add Roles and Features**.
The **Add Roles and Features Wizard** dialog box appears.

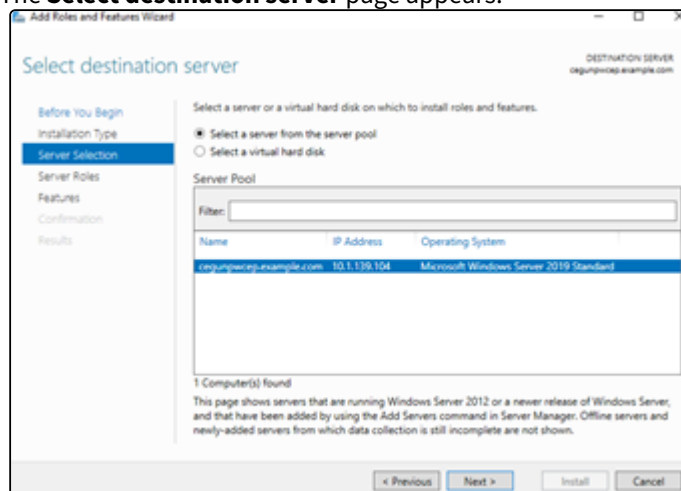


4. If the **Before you Begin** page appears, click **Next**.
The **Select installation type** page appears.



5. Select **Role-based or feature-based installation**.
6. Click **Next**.

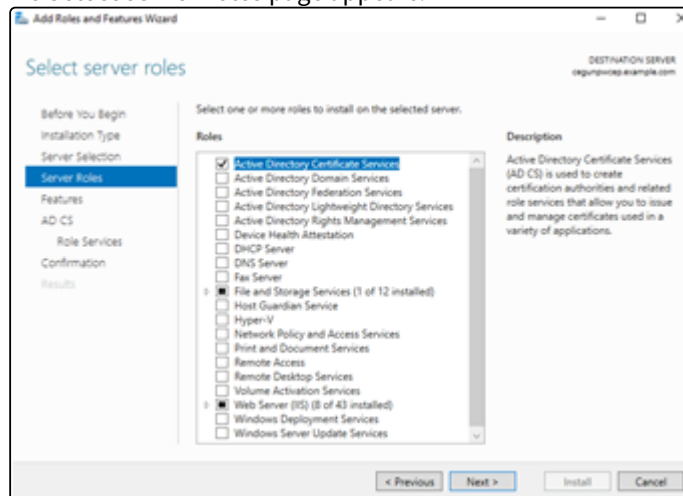
The **Select destination server** page appears.



7. Click **Select a server from the pool**.
8. In the **Server Pool** list, select the server.

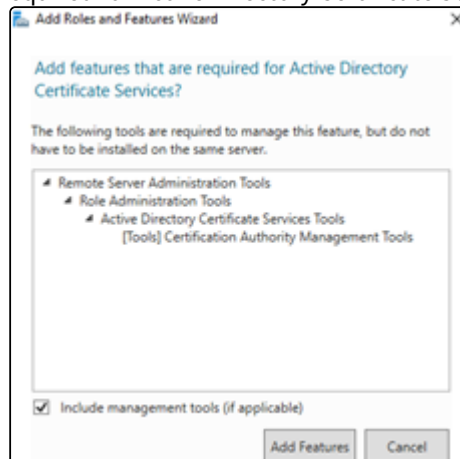
9. Click **Next**.

The **Select server roles** page appears.

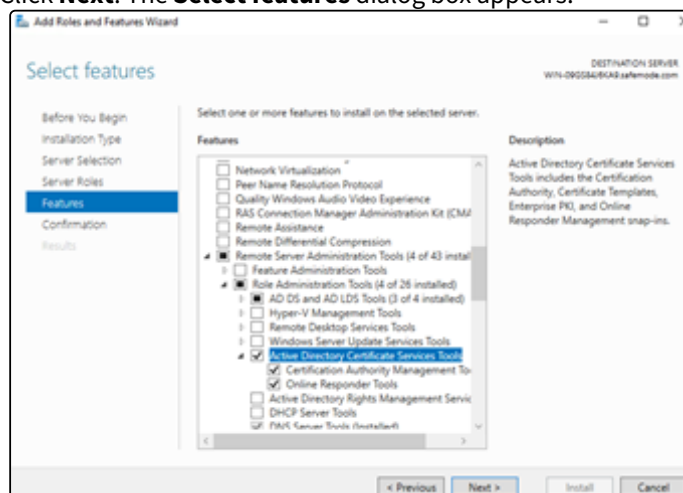


10. Select **Active Directory Certificate Services**.

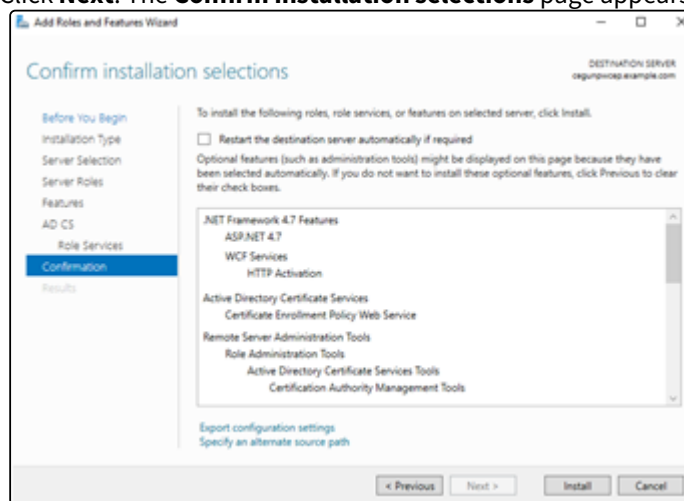
Another **Add Roles and Features Wizard** dialog box may appear, informing you that some features are required for Active Directory Certificate Services.



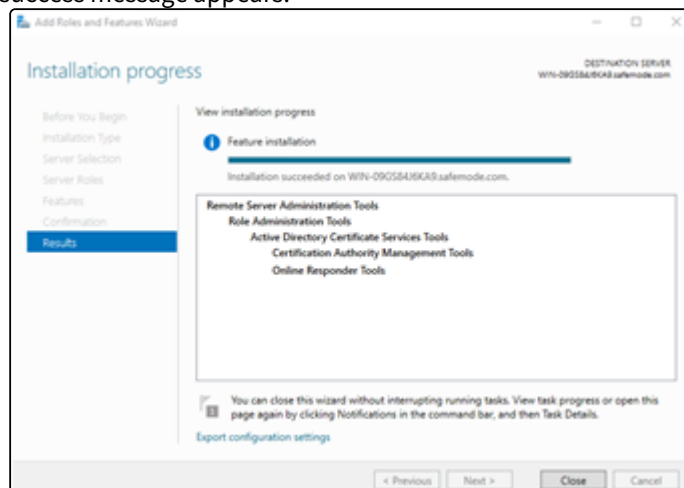
11. Click **Add Features** to add these required features and close the dialog box.
12. Click **Next**. The **Select features** dialog box appears.



13. Expand **Remote Server Administration Tools > Role Administration Tools**, then select **Active Directory Certificate Services Tools**.
14. Click **Next**. The **Confirm installation selections** page appears.

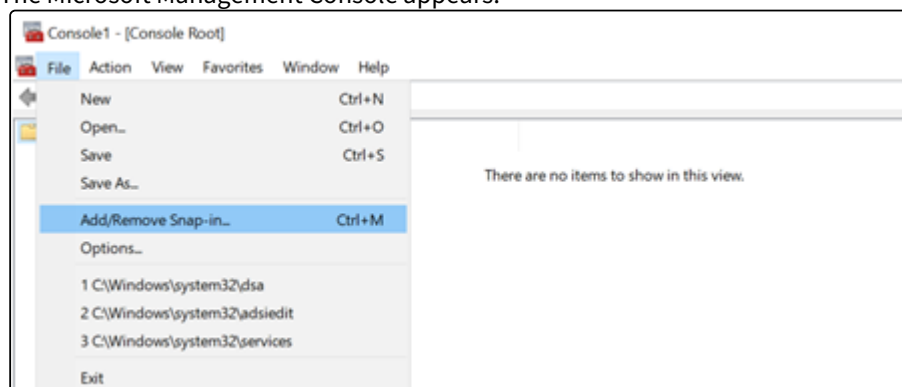


15. Click **Install**. The **Installation Progress** page appears.
A progress indicator displays the progress of the installation. After the roles and features are installed, a success message appears.

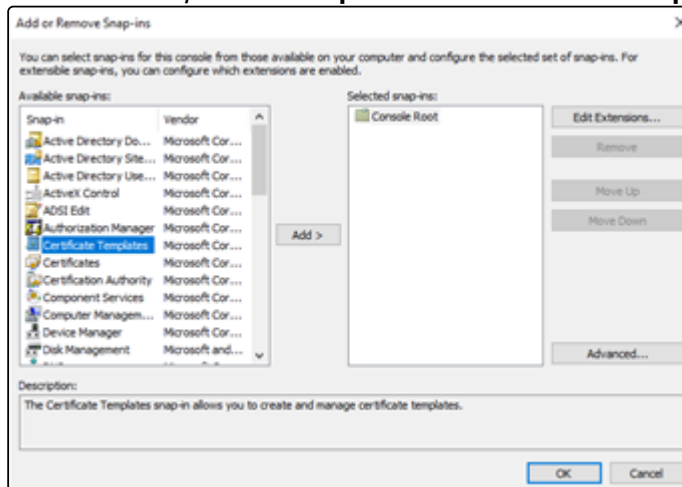


16. Click **Close**.
17. Run `mmc.exe`.

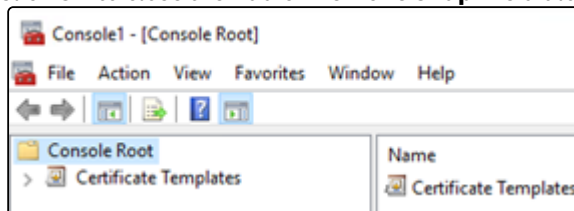
The Microsoft Management Console appears.



18. Select **File > Add/Remove Snap-in**. The **Add or Remove Snap-ins** dialog box appears.



19. In the **Available snap-ins** list, select **Certificate Templates**.
 20. Click **Add**.
 21. Click **OK** to close the **Add or Remove Snap-ins** dialog and return to the Microsoft Management Console.



22. Select **Certificate Templates**.
 A dialog will appear, prompting to install the certificate templates.
 23. Click **Yes** to install the templates.

Creating Kerberos files for Certificate Enrollment Gateway

If you will use Kerberos authentication for WSTEP enrollment, you must create one or more Kerberos files for Certificate Enrollment Gateway. When configuring Certificate Enrollment Gateway, you must provide these files when editing Certificate Enrollment Gateway settings.

- [Creating a Kerberos configuration file for cross-forest WSTEP enrollment](#)
- [Creating a Kerberos keytab file for WSTEP enrollment](#)

Creating a Kerberos configuration file for cross-forest WSTEP enrollment

To support Kerberos authentication with WSTEP enrollment in a cross-forest deployment, Certificate Enrollment Gateway requires a Kerberos configuration file. Certificate Enrollment Gateway uses the Kerberos configuration file for authenticating Kerberos V5 LDAP Referrals across forests in Active Directory.

The Kerberos configuration file (typically `krb5.conf`) file must contain the following information:

- A `[libdefaults]` section with a default realm.
 If Kerberos authentication uses 3DES or RC4 algorithms, the section must also contain the setting `allow_weak_crypto = true`.
- A `[realms]` section with the top-level domain of each forest defined as a realm.

The following example is a `krb5.conf` file with two cross-forests.

```
[libdefaults]
    default_realm = EXAMPLE.COM
    renew_lifetime = 3600
    ticket_lifetime = 3600
    allow_weak_crypto = true

[realms]
    EXAMPLE.COM = {
        kdc = hostname1.example.com
        kdc = hostname2.example.com
        kdc = example.com
        admin_server = hostname1.example.com
        master_kdc = hostname1.example.com
        default_domain = EXAMPLE.COM
    }
    EXAMPLE.ORG = {
        kdc = hostname1.example.org
        admin_server = hostname1.example.org
        master_kdc = hostname1.example.org
        default_domain = EXAMPLE.ORG
    }
```

For more information about creating a `krb5.conf` file, see https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html.

Creating a Kerberos keytab file for WSTEP enrollment

To support Kerberos authentication with WSTEP enrollment, Certificate Enrollment Gateway requires a Kerberos keytab file. A keytab file contains pairs of Kerberos principals and encrypted keys derived from the Kerberos password. Certificate Enrollment Gateway will use the keytab file to authenticate to various remote systems using Kerberos without entering a password.

Log in to the Active Directory domain controller as a user with Domain Admin and Enterprise Admin permissions, and run the following command in PowerShell.

```
ktpass /out <keytab_path> /mapuser <user> /princ <principal> /pass <password> /ptype
KRB5_NT_PRINCIPAL /crypto <algorithm>
```

See below for a description of each parameter.

- `<keytab_path>`
- `<user>`
- `<principal>`
- `<password>`
- `<algorithm>`

For example:

```
ktpass /out "C:\Users\cegconfig\Documents\kerberos.keytab" /mapuser kerberos@example.
com /princ HTTP/cegserver1.example.com@EXAMPLE.COM /pass EXAMPLE_password1234 /ptype
KRB5_NT_PRINCIPAL /crypto All
```

<keytab_path>

The full path and file name of the keytab file that the command will generate. For example:

```
C:\Users\cegconfig\Documents\kerberos.keytab
```

You will transfer this keytab file to the server hosting Certificate Enrollment Gateway.

<user>

The Kerberos Service Account, using the following format:

```
<logon>@<domain>
```

Where:

- <logon> is the Windows logon name of the Kerberos Service Account, in lowercase letters.
- <domain> is the domain name of the Kerberos Service Account, in lowercase characters.

For example:

```
kerberos@example.com
```

<principal>

The principal name of the Kerberos Service Account. The principal must be in the form:

```
HTTP/<ceg-fqdn>@<DOMAIN>
```

Where:

- <ceg-fqdn> is the fully qualified domain name of the server hosting Certificate Enrollment Gateway.
- <DOMAIN> is the domain name of the Kerberos Service Account, in uppercase characters.

For example:

```
HTTP/cegserver1.example.com@EXAMPLE.COM
```

This parameter is case-sensitive.

<password>


The password of the Kerberos Service Account.

<algorithm>

The keys that are generated in the keytab file. Permitted values:

- DES-CBC-CRC
- DES-CBC-MD5
- RC4-HMAC-NT
- AES256-SHA1

- AES128-SHA1
- All

 DES and RC4 algorithms are deprecated. You should specify an AES algorithm or All to allow all algorithms.

Configuring the Windows domain for WSTEP enrollment

This section describes how to configure the Windows domain for WSTEP enrollment with Entrust Certificate Enrollment Gateway.

Certificate Enrollment Gateway supports read-only domain controllers for WSTEP enrollment. A read-only domain controller (RODC) is a server that hosts an Active Directory database's read-only partitions and responds to security authentication requests. Certificate Enrollment Gateway can accept WSTEP enrollment requests and authenticate the request using an RODC.

Any configuration changes to a domain controller that are documented in this guide must be performed on the writeable domain controller.

- [Adding referrals for cross-forest deployments](#)
- [Configuring the Group Policy for cross-forest deployments](#)
- [Creating a Kerberos Service Account for Kerberos authentication](#)
- [Creating a service logon account for read-only access to Active Directory](#)
- [Active Directory role requirements for running the Entrust-provided PowerShell scripts](#)
- [Active Directory schema requirements](#)

Adding referrals for cross-forest deployments

WSTEP enrollment can use Kerberos authentication to authenticate Windows endpoints. For cross-forest deployments, Windows endpoints are located using Kerberos V5 LDAP referrals. The domain controller (Active Directory Domain Services), maintains referral data in its Configuration container, in crossRef objects. For more information about referrals, see the Microsoft documentation.

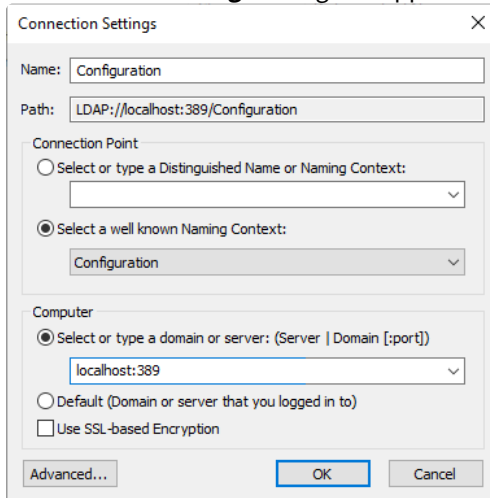
For cross-forest deployments with WSTEP enrollment, you must manually add a crossRef object into the domain controller for each cross-forest domain that you must support.

To add a cross-forest referral in a domain controller for cross-forest deployments

1. Open ADSI Edit. Select **Start > Windows Administrative Tools > ADSI Edit**.
2. Connect to the Configuration context.

- a. Select **Action > Connect to**.

A **Connection Settings** dialog box appears.



The **Connection Settings** dialog box is shown. It has the following fields and options:

- Name:** Configuration
- Path:** LDAP://localhost:389/Configuration
- Connection Point:**
 - ☐ Select or type a Distinguished Name or Naming Context:
 - ☒ Select a well known Naming Context: Configuration
- Computer:**
 - ☒ Select or type a domain or server: (Server | Domain [:port]) localhost:389
 - ☐ Default (Domain or server that you logged in to)
 - ☐ Use SSL-based Encryption
- Buttons: Advanced..., OK, Cancel

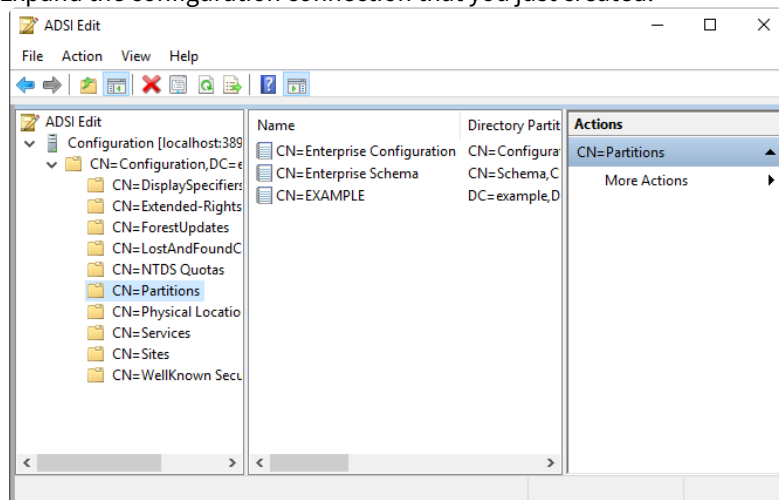
- b. In the **Name** field, enter a unique name for the connection.

- c. Under **Connection Point**, click **Select a well known Naming Context**, and then select **Configuration**.

- d. Under **Computer**, click **Select or type a domain or server**, and then enter the server and port of the domain controller, using the form `<server>: <port>`. If you are on the server hosting the domain controller, you can enter `localhost` for `<server>`.

- e. Click **OK**.

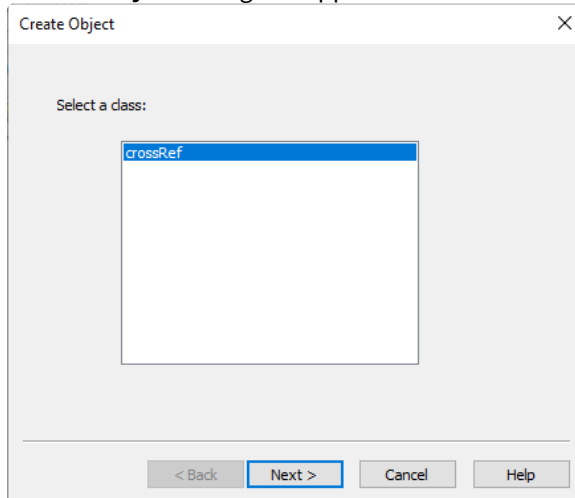
3. Expand the configuration connection that you just created.



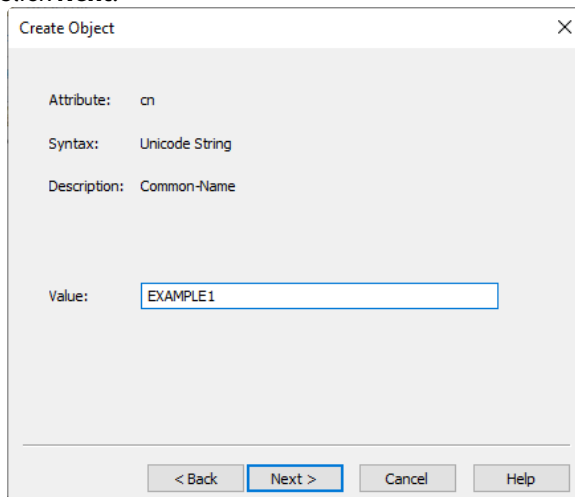
4. Expand **CN=Configuration,<suffix>** > **CN=Partitions**.

Where **<suffix>** is the suffix (distinguished name) of the domain controller.

5. Select **CN=Partitions**, and then select **Action > New > Object**.
A **Create Object** dialog box appears.

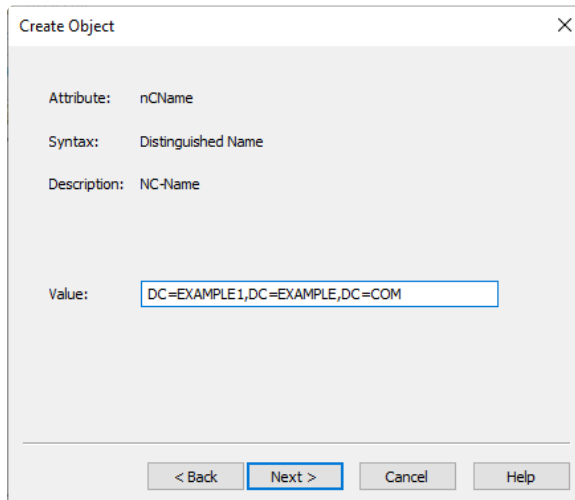
A screenshot of the 'Create Object' dialog box. The title bar says 'Create Object' with a close button. Inside, it says 'Select a class:' above a list box. The list box contains 'crossRef' and is currently empty. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

6. Select **crossRef**.
7. Click **Next**.

A screenshot of the 'Create Object' dialog box after clicking 'Next'. The title bar says 'Create Object' with a close button. Inside, it shows the following information: 'Attribute: cn', 'Syntax: Unicode String', and 'Description: Common-Name'. Below this is a 'Value:' label followed by a text box containing 'EXAMPLE1'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

8. In the **Value** field, enter the NetBIOS name of a cross-forest domain.

9. Click **Next**.



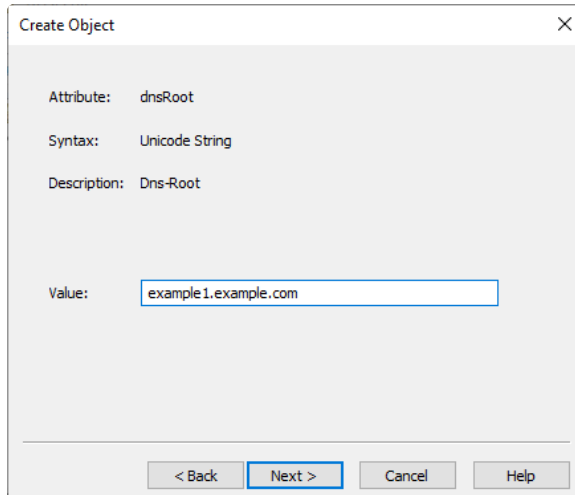
The 'Create Object' dialog box shows the following details:

- Attribute: nCName
- Syntax: Distinguished Name
- Description: NC-Name
- Value: DC=EXAMPLE1,DC=EXAMPLE,DC=COM

At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

10. In the **Value** field, enter the distinguished name of the cross-forest domain.

11. Click **Next**.



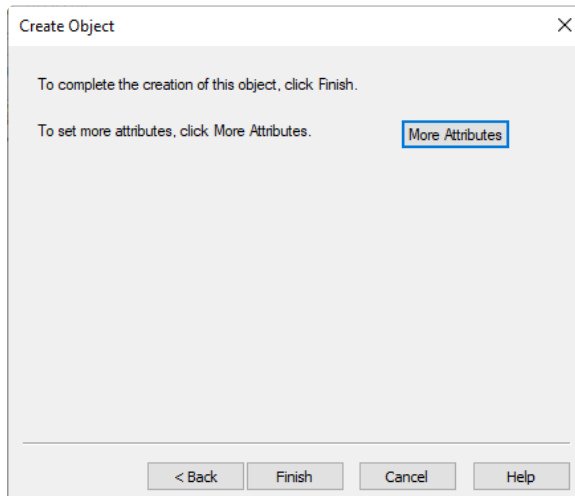
The 'Create Object' dialog box shows the following details:

- Attribute: dnsRoot
- Syntax: Unicode String
- Description: Dns-Root
- Value: example1.example.com

At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

12. In the **Value** field, enter the DNS name of the cross-forest domain.

13. Click **Next**.



The 'Create Object' dialog box shows the following text:

- To complete the creation of this object, click Finish.
- To set more attributes, click More Attributes.

At the bottom, there are four buttons: '< Back', 'Finish', 'Cancel', and 'Help'. The 'More Attributes' button is highlighted with a blue border.

14. Click **Finish**.
A crossRef object is added for the cross-forest domain.
15. Repeat this procedure for each cross-forest domain the domain controller must support for cross-forest referrals.

Configuring the Group Policy for cross-forest deployments

WSTEP enrollment can use Kerberos authentication to authenticate Windows endpoints. Kerberos authentication uses service principal names to associate a service instance with a service sign-in account. A service principal name is a unique identifier of a service instance. With Kerberos authentication, a service principal name allows a client application to request service authentication for an account, even if the client does not have the account name.

A service principal name (SPN) is a string that consists of either two or three parts, with each part separated by a forward slash. An example of a two-part SPN:

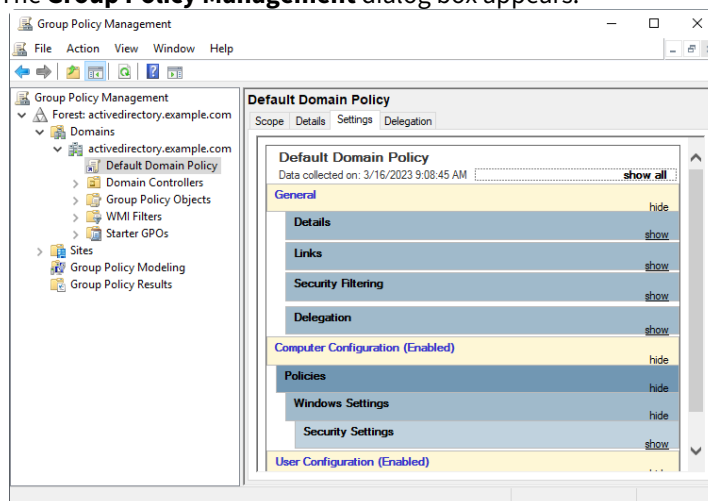
HTTP/server.example.com@EXAMPLE.COM

For cross-forest deployments, both the Key Distribution Center (KDC) and the Kerberos client must search a list of trusted forests when attempting to resolve a two-part SPN if the SPN cannot be found in the local forest. The list of trusted forests that the KDC and Kerberos clients can search is controlled by Group Policy settings in the domain controller. Cross-forest WSTEP enrollment can fail if the KDC or Kerberos client cannot resolve the two-part SPN. The list of trusted forests must be the same for both the KDC and Kerberos clients.

i To ensure consistent behavior, the Global Policy settings must be supported and set identically on all domain controllers in the domain.

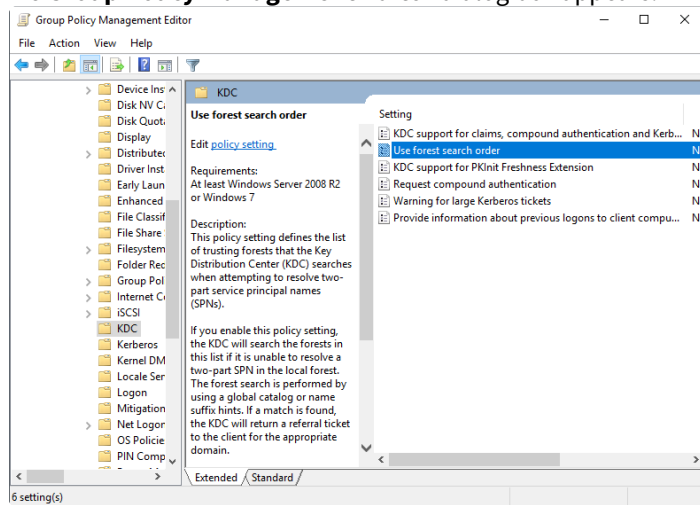
To configure the Group Policy for cross-forest deployments

1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
2. Select **Start > Windows Administrative Tools > Group Policy Management**.
The **Group Policy Management** dialog box appears.

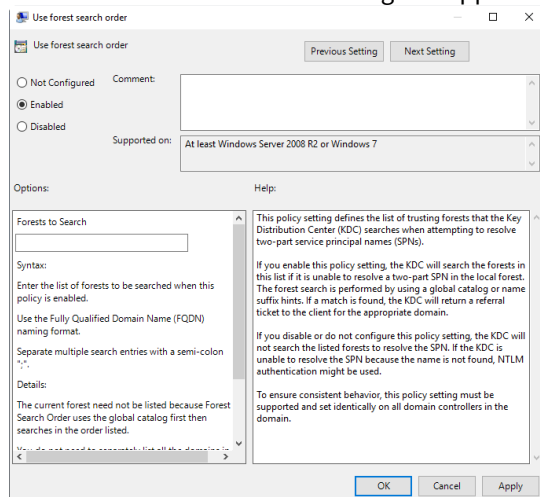


3. In the tree view, select **Group Policy Management > Forest: <forest> > Domains > <domain> > Default Domain Policy**.
Where **<forest>** is the FQDN (fully qualified domain name) of the forest, and **<domain>** is the FQDN of the domain.

4. Select **Action > Edit** to edit the default domain policy for the domain.
The **Group Policy Management Editor** dialog box appears.



5. Expand **Computer Configuration > Policies > Administrative Templates > System > KDC**.
6. In the **Settings** pane, select **Use Forest Search Order**.
7. Select **Action > Edit** to edit the **Use Forest Search Order** setting.
The **Use forest search order** dialog box appears.

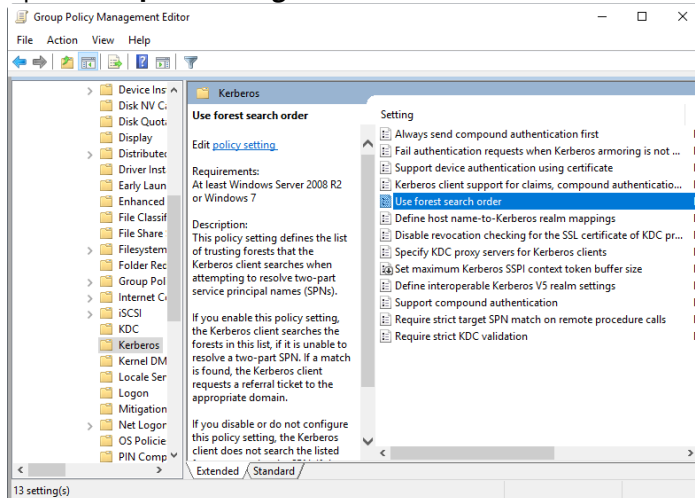


8. Select **Enabled**.
9. In the **Options** pane, in the **Forests to Search** field, enter the list of trusted forests that the Key Distribution Center (KDC) will search when attempting to resolve a two-part SPN that does not exist in the local forest. Separate each forest with a semicolon. For example:

example.com;example.net;example.org

10. Click **OK**.

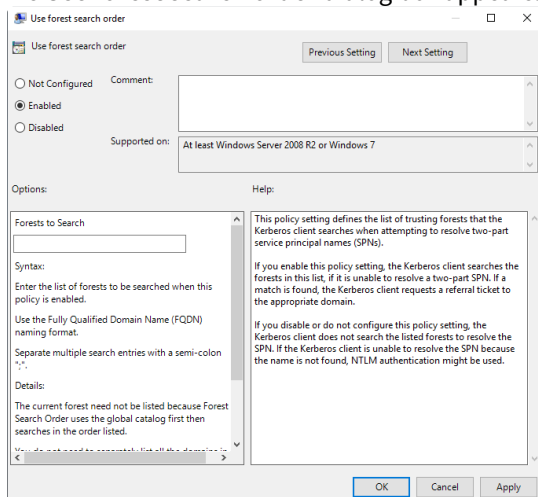
11. Expand **Computer Configuration > Policies > Administrative Templates > System > Kerberos**.



12. In the **Settings** pane, select **Use Forest Search Order**.

13. Select **Action > Edit** to edit the **Use Forest Search Order** setting.

The **Use forest search order** dialog box appears.



14. Select **Enabled**.

15. In the **Options** pane, in the **Forests to Search** field, enter the list of trusted forests that Kerberos clients will search when attempting to resolve a two-part SPN that does not exist in the local forest. Separate each forest with a semicolon. For example:

example.com;example.net;example.org

16. Click **OK**.

Creating a Kerberos Service Account for Kerberos authentication

To use Kerberos authentication, you must create a Kerberos Service Account (also called a Kerberos principal) in Active Directory domain controller. You must specify this Kerberos Service Account when generating a Kerberos keytab file.

A Kerberos Service Account is a standard Active Directory user which belongs to the top-level parent domain. No special permissions are required for this user account.

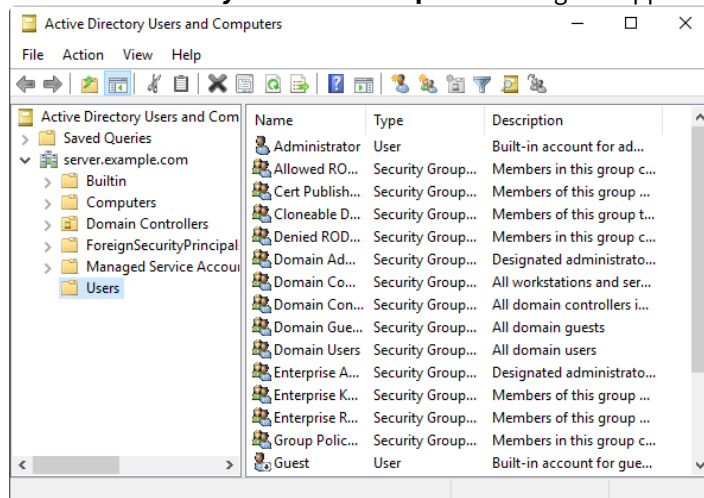
i Certificate Enrollment Gateway supports connections to an entire Domain Forest. Certificate Enrollment Gateway must point to the top-level domain of the forest to work across the entire forest.

You must create the same Kerberos account for all forests in cross-forest deployments.

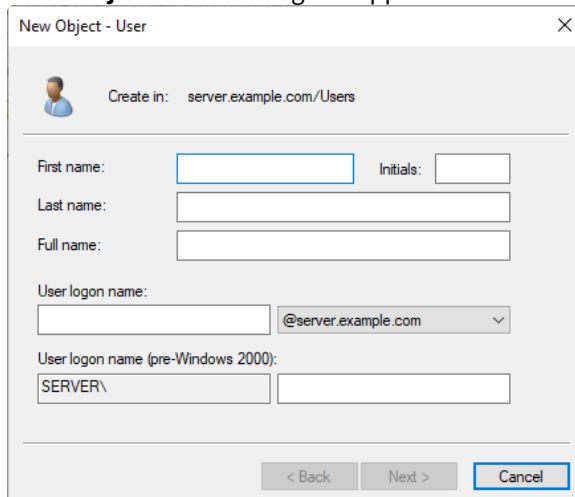
To create a Kerberos Service Account

1. Log in to the server hosting the Active Directory domain controller as a domain administrator or a user who is a member of the built-in Account Operators domain group.
2. Open the Active Directory Users and Computers administrative tool (select **Start > Windows Administrative Tools > Active Directory Users and Computers**).

The **Active Directory Users and Computers** dialog box appears.



3. Right-click the folder where you want to create the new account and select **New > User**. A **New Object – User** dialog box appears.



New Object - User

Create in: server.example.com/Users

First name: Initials:

Last name:

Full name:

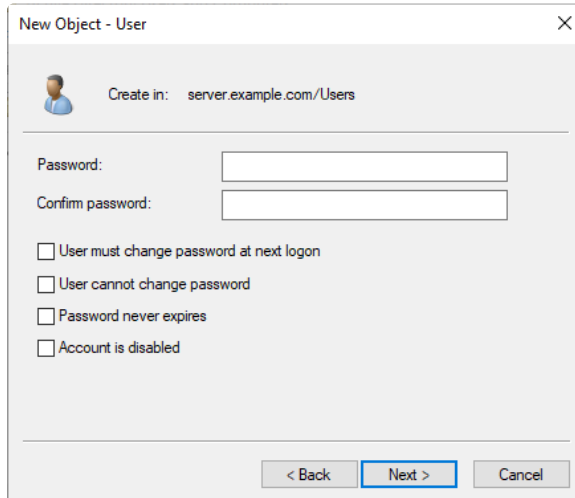
User logon name: @server.example.com

User logon name (pre-Windows 2000): SERVER\

< Back Next > Cancel

4. Using the **First name**, **Last name**, and **Full name** fields, enter a name for the new user account. At a minimum, you must enter a value into the **Full name** field. Entering values into the **First name** and **Last name** field will automatically fill the **Full name** field.
5. In the **User logon name** field, enter a Windows logon name for the user account.
6. (Optional.) In the **User logon name (pre-Windows 2000)** field, enter a logon name for the user account for pre-Windows 2000 computers.

7. Click **Next**.



The 'New Object - User' dialog box shows the 'Create in' field set to 'server.example.com/Users'. It has two text input fields for 'Password' and 'Confirm password'. Below these are four unchecked checkboxes: 'User must change password at next logon', 'User cannot change password', 'Password never expires', and 'Account is disabled'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

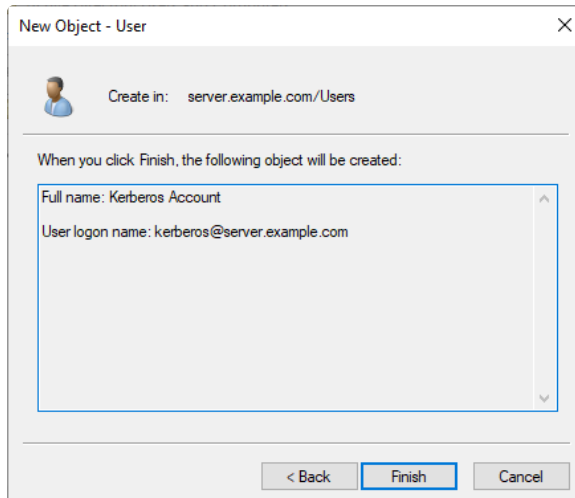
8. In the **Password** field, enter a password for the user account.

9. In the **Confirm password** field, enter the password again to confirm the password.

10. Deselect **User must change password at next logon**.

11. To avoid service interruptions because of an expired password, select **Password never expires**. If the password ever expires, you will need to reset the password, recreate the Kerberos keytab file, and then update the Certificate Enrollment Gateway configuration.

12. Click **Next**.

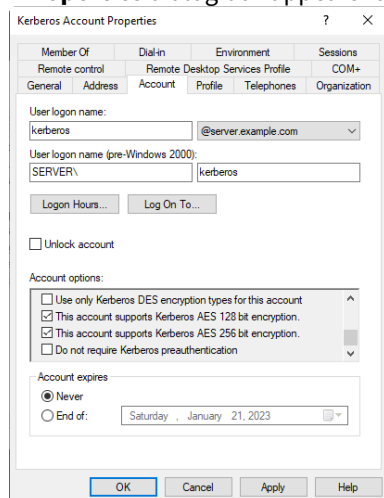


The 'New Object - User' dialog box shows the 'Create in' field set to 'server.example.com/Users'. It displays a summary of the object to be created: 'Full name: Kerberos Account' and 'User logon name: kerberos@server.example.com'. At the bottom are three buttons: '< Back', 'Finish', and 'Cancel'.

13. Record the user logon name of the account (such as `kerberos@example.com`). You will use this logon name later to create the Kerberos keytab file.

14. Click **Finish**.

15. Double-click the account you just created.
A **Properties** dialog box appears for the account.



16. Click the **Account** tab.
17. Under **Account options**:
 - Select **This account supports Kerberos AES 128 bit encryption**.
 - Select **This account supports Kerberos AES 256 bit encryption**.
18. Click **OK**.

Creating a service logon account for read-only access to Active Directory

For WSTEP enrollment, Certificate Enrollment Gateway requires a domain user account for read-only access to LDAP and the Global Catalog in Active Directory. This domain user account must be a service account without any special permissions.

If you will use Kerberos authentication, it is recommended that you use the Kerberos Service Account for read-only access to Active Directory instead of creating a separate service account for read-only access to Active Directory. For information about creating the Kerberos Service Account, see [Creating a Kerberos Service Account for Kerberos authentication](#).

Active Directory role requirements for running the Entrust-provided PowerShell scripts

Entrust provides some Windows PowerShell scripts for configuring WSTEP enrollment with Certificate Enrollment Gateway. You can use these PowerShell scripts to install and configure the Certificate Enrollment Policy Web Service (CEP Service), and an enrollment service for each CA that will issue certificates to the WSTEP endpoints.

To run the PowerShell scripts provided by Entrust, the user account must have the Active Directory roles "Domain Admin" and "Enterprise Admin".

Active Directory schema requirements

For WSTEP enrollment with Certificate Enrollment Gateway, your Windows domain must have the 2016 Active Directory schema or later.

To check the current Active Directory schema version

1. Log in to the server hosting Active Directory.
2. Open a PowerShell window. Select **Start > Windows PowerShell > Windows PowerShell**.
3. Enter the following command:

```
Get-ADObject (Get-ADRootDSE).schemaNamingContext -properties objectVersion
```

The version returned by the command must be 87 or greater.

WSTEP integration architecture

In a WSTEP integration architecture, a Windows enrollment client can connect to a Domain Controller through the Certificate Enrollment Policy Web Service and request certificates from multiple Certification Authorities (CAs).

The following topics describe the components in the WSTEP integration architecture:

- [Certification Authority](#)
- [Entrust CA Gateway](#)
- [Entrust Certificate Enrollment Gateway](#)
- [Cross-forest trust](#)
- [Domain Controller](#)
- [Certificate Enrollment Policy Web Service](#)
- [Enrollment clients](#)

Certification Authority

A Certification Authority (CA) issues certificates to enrollment clients. Entrust CA Gateway can support multiple CAs, called Managed CAs. Each enrollment service object in the Domain Controller will connect to a single Certificate Enrollment Gateway instance and request a certificate from a single CA. To request certificates from multiple CAs, multiple enrollment services must be added to the Domain Controller.

Entrust CA Gateway

Entrust CA Gateway enables full certificate lifecycle management and operational management across all your Entrust-supported Certification Authorities (CAs). Each Entrust CA Gateway client can access one or several CAs. Certificate Enrollment Gateway will send certificate requests to Entrust CA Gateway. Entrust CA Gateway will forward the request to the intended Managed CA, and send the generated certificate back to Certificate Enrollment Gateway.

Entrust Certificate Enrollment Gateway

Each Entrust Certificate Enrollment Gateway instance can connect to multiple Entrust CA Gateway instances, granting access to one or more Certificate Authorities (CAs). Each enrollment service object in the Domain Controller will connect to a single Certificate Enrollment Gateway instance and request a certificate from a single CA. To request certificates from multiple CAs, multiple enrollment services must be added to the Domain Controller.

Cross-forest trust

For WSTEP enrollment, the Domain Controller can use Kerberos authentication to authenticate Windows enrollment clients. Cross-forest trust is a Windows Server feature that allows multiple Active Directory forests to trust each other. With cross-forest trust, a Domain Controller for one forest can use Kerberos V5 LDAP referrals to locate and authenticate enrollment clients that exist in a different forest. For more information about referrals, see the Microsoft documentation.

Domain Controller

A Domain Controller is a server computer hosting Active Directory Domain Services that is responsible for allowing host access to domain resources. The Domain Controller authenticates users, stores user account information, and enforces security policy for a domain.

For WSTEP enrollment, a Domain Controller requires the following objects:

- A certificate enrollment service for each Certification Authority (CA) that will issue certificates to enrollment clients. Each enrollment service will connect to a single CEG Service instance.
- For cross-forest deployments, a crossRef object for each cross-forest domain you must support.

Certificate Enrollment Policy Web Service

The Certificate Enrollment Policy Web Service allows enrollment clients to retrieve certificate enrollment policies from a Certification Authority (CA) when the clients are not permitted to access the Domain Controller. After receiving policy information from the Certificate Enrollment Policy Web Service, enrollment clients can then request a certificate from a certificate enrollment service.

The Windows server hosting the Certificate Enrollment Policy Web Service can be the Domain Controller or any other server in the domain. It is recommended that you install and configure the Certificate Enrollment Policy Web Service on a different server than the Domain Controller. The Certificate Enrollment Policy Web Service must be in same forest as the Domain Controller hosting the certificate templates and enrollment services.

Enrollment clients

For WSTEP enrollment, an enrollment client is a Windows user or a machine that requires a certificate. Enrollment clients are either in a Windows Domain or connected to a Windows Domain. With cross-forest trust (see [Cross-forest trust](#)), enrollment clients from one forest can request a certificate from a Domain Controller in another forest.

Integrating MDM and MDM-SCEP clients with Certificate Enrollment Gateway

This section explains how to integrate Mobile Device Management (MDM) products and MDM-SCEP clients with the Certificate Enrollment Gateway service.

- [Configuring Certificate Enrollment Gateway for MDMWS and MDM-SCEP enrollment](#)
- [Configuring MDM-SCEP clients for enrollment with Certificate Enrollment Gateway](#)
- [Configuring a Mobile Device Management product for enrollment with Certificate Enrollment Gateway](#)

Configuring Certificate Enrollment Gateway for MDMWS and MDM-SCEP enrollment

To configure Certificate Enrollment Gateway for MDM Web Service (MDMWS) and MDM-SCEP enrollment, you must configure the MDMWS enrollment settings in Certificate Enrollment Gateway. You can edit the MDMWS enrollment settings using the Management Console interface.

To configure Certificate Enrollment Gateway for MDMWS and MDM-SCEP enrollment

1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log into the Management Console a user belonging to a role with Certificate Enrollment Gateway management permissions – for example, the initial `admin` administrator user.


 See [Starting up the Management Console](#) for how to manage users and roles.

1. In the **Certificate Enrollment Gateway** pane, click **Manage Solution**.
A **Certificate Enrollment Gateway** page appears.

2. In the left navigation bar, click **Configuration**.
A **Product Configuration** pane appears.
3. Turn on **Enable Advanced Configuration**.
4. Click **Next**.
5. For all SCEP-related protocols (SCEP, MDM-SCEP, and Intune-SCEP), Certificate Enrollment Gateway uses RA certificates to sign and encrypt SCEP PKI messages. For an on-premises CA, you must specify one or more profiles that are defined in CA Gateway used to issue RA certificates.
 - a. Click the **CAGW** tab.
 - b. Configure the **RA Certificate Profile IDs** setting.
6. Click the **MDMWS** tab and configure the following settings.
 - **MDMWS Enrollment Service Configuration**
 - **MDMWS Users**
 - **MDMWS Expired Token Clean-up Cron Job**
 - **MDM-SCEP Token Expire Lifetime**
 - **Enable MDMWS**
7. Configure any other settings if required.
8. After configuring the settings, click **Validate** to validate the settings.
If any configuration errors are detected, correct the errors then click **Validate** again.
9. After validating the configuration settings, click **Next**.
Cryptographic Security Platform uploads the configuration and any attached files, such as P12 credentials.
10. In the **Product Deployment Status** pane, re-deploy Certificate Enrollment Gateway with the updated configuration file by clicking **Deploy**.
A dialog box appears, prompting you to confirm the operation. Click **Yes** to confirm the operation and deploy the Certificate Enrollment Gateway solution.

Configuring MDM-SCEP clients for enrollment with Certificate Enrollment Gateway

MDM-SCEP clients must use one of the following URLs to communicate with Certificate Enrollment Gateway.

 To support macOS (Apple) devices, the URL must start with **http** instead of **https**.

```
http://<CEG-server>/scep/<tenant-ID>/<digitalid-config>/mdm
https://<CEG-server>/scep/<tenant-ID>/<digitalid-config>/mdm
```

Where:

- **<CEG-server>** is the hostname or IP address of the Certificate Enrollment Gateway server.
- **<tenant-ID>** is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- **<digitalid-config>** is a digital ID configuration defined in the CEG Service.

For example:

```
http://cegserver.example.com/scep/tenant1/digitalid-config1/mdm
https://cegserver.example.com/scep/tenant1/digitalid-config1/mdm
```

Configuring a Mobile Device Management product for enrollment with Certificate Enrollment Gateway

This section describes the information required to configure Mobile Device Management (MDM) products to enroll for a certificate using Certificate Enrollment Gateway. For information about using your MDM product, see your MDM product documentation.

- [Enrollment URL for MDMWS clients](#)
- [Issuing a signing certificate to the MDM product](#)
- [Adding the CA certificate chain to the MDM product](#)
- [Supported MDM authentication methods](#)

Enrollment URL for MDMWS clients

Mobile Device Management products must use the following URL to communicate with Certificate Enrollment Gateway:

```
https://<CEG-server>/mdm/services/<tenant-ID>
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.

For example:

```
https://cegserver.example.com/mdm/services/tenant1
```

Issuing a signing certificate to the MDM product

Some MDM products may require a signing certificate to sign data being delivered to MDM devices. For instructions about adding certificates to your MDM product, see your MDM product documentation.

Adding the CA certificate chain to the MDM product

MDM products must trust the CA certificate chain for the Certificate Enrollment Gateway TLS certificate. If the MDM product does not trust the CA certificate chain, the MDM clients will fail to establish a secure TLS connection to Certificate Enrollment Gateway. For instructions about adding certificates to your MDM product, see your MDM product documentation.

Supported MDM authentication methods

Certificate Enrollment Gateway supports username and password authentication to authenticate with MDM products. You must configure at least one username and password credential in the MDM product.

All username and password credentials that Certificate Enrollment Gateway will use to authenticate to the MDM product must be specified in the Certificate Enrollment Gateway MDMWS configuration settings (see [MDMWS](#)).

Integrating SCEP clients with Certificate Enrollment Gateway

This section explains how to integrate SCEP clients with the Certificate Enrollment Gateway service.

- [Google ChromeOS integration use case](#)

- [Configuring SCEP clients for enrollment with Certificate Enrollment Gateway](#)
- [Configuring Certificate Enrollment Gateway for SCEP enrollment](#)

Google ChromeOS integration use case

Google ChromeOS is a cloud-first operating system for Chromebooks and other Google devices. ChromeOS devices can request certificates from the Certificate Enrollment Gateway using the SCEP protocol. SCEP enrollment for ChromeOS is controlled using Google Admin, a Web-based interface for managing users and groups for an organization.

- [ChromeOS integration requirements](#)
- [Configuring Google Admin for SCEP enrollment](#)
- [Downloading and installing the Google Cloud Certificate Connector](#)
- [Testing SCEP enrollment with ChromeOS](#)

ChromeOS integration requirements


Google Admin requirements:

- Google Admin requires either the Chrome Enterprise Upgrade or the Chrome Education Upgrade.
- Google Admin requires the CA certificate chain (from the root CA certificate to the issuing CA certificate) for the on-premises Managed CA or Entrust PKI as a Service (PKIaaS).

Google Cloud Certificate Connector requirements:

- The Google Cloud Certificate Connector must be installed on Domain-joined Windows server.
- The Google Cloud Certificate Connector requires outbound network connectivity to Google Admin.
- The Google Cloud Certificate Connector requires outbound network connectivity to Entrust Certificate Enrollment Gateway.

Entrust Certificate Enrollment Gateway requirements:

 Static challenge passwords are not secure. To increase security, it is recommended that you configure the firewall on the Certificate Enrollment Gateway server to limit incoming traffic for the SCEP service to only the Google Cloud Certificate Connector.

- The SCEP service must be configured with a static challenge password.
- Certificate Enrollment Gateway requires inbound connectivity from the Google Cloud Certificate Connector.

ChromeOS requirements:

- ChromeOS must be enrolled with Google Admin using the **Enterprise enrollment** option. See the Google documentation for instructions about enrolling a device using the **Enterprise enrollment** option (<https://support.google.com/chrome/a/answer/1360534>).
- ChromeOS requires outbound connectivity to Google Admin without the interference of SSL decryption.

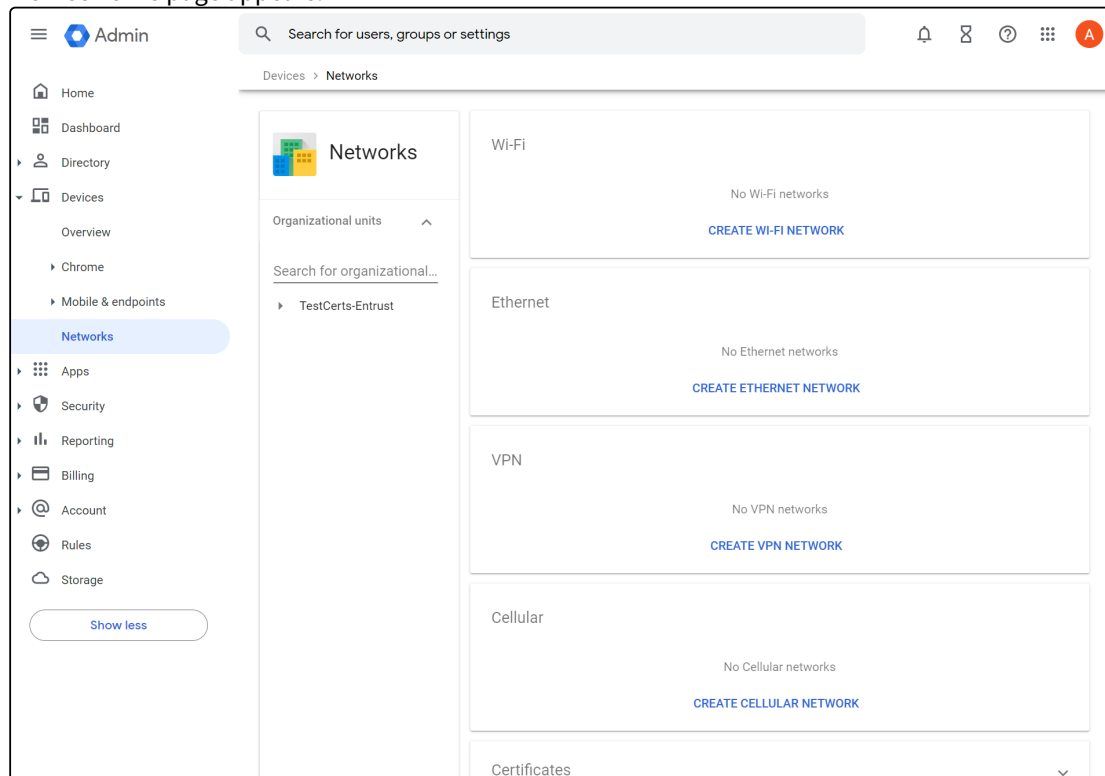
Configuring Google Admin for SCEP enrollment

SCEP enrollment for ChromeOS is controlled using Google Admin, a Web-based interface for managing users and groups for an organization.

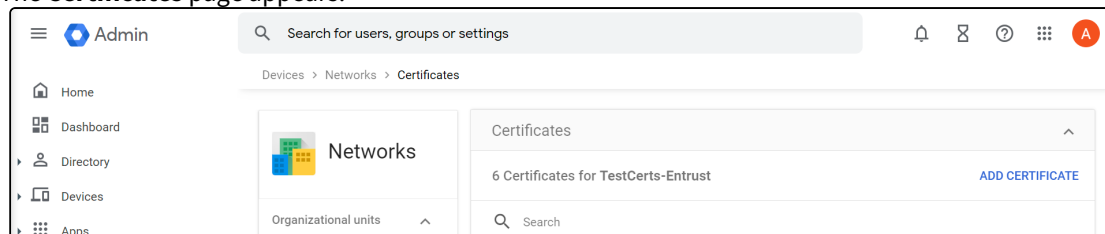
To configure Google Admin for SCEP enrollment

1. Log in to Google Admin (<https://admin.google.com>).

2. Navigate to **Devices > Networks**.
The **Networks** page appears.

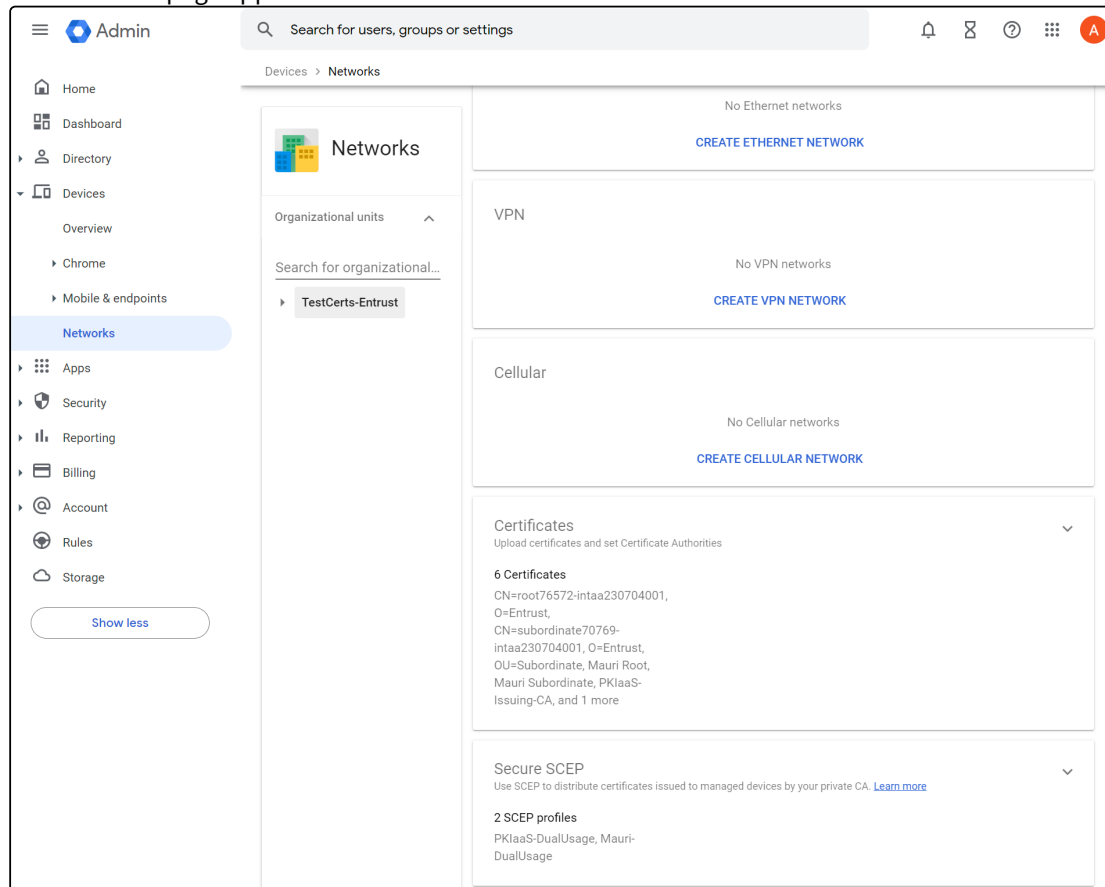


3. Click on the **Certificates** pane.
The **Certificates** page appears.

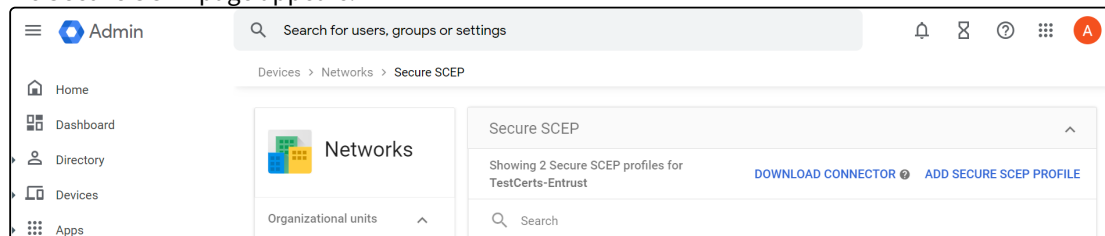


4. Add the entire CA certificate chain (from the root CA to the issuing CA) for the Managed CA. To add a CA certificate:
 - a. Click **Add Certificate**. The **Add Certificate** page appears.
 - b. In the **Name** field, enter a unique friendly name for the CA certificate,
 - c. Click **Upload** and then select the CA certificate you want to upload.
 - d. Select **Chromebook**.
 - e. Click **Add**.
5. Navigate to **Devices > Networks**.

6. The **Networks** page appears.



7. Click on the **Secure SCEP** pane.
The **Secure SCEP** page appears.



8. Create a SCEP profile:
- Click **ADD SECURE SCEP PROFILE**. The **Edit Secure SCEP** page appears.
 - For **Device platforms**, select the Chromebook platforms that will enroll for a certificate over SCEP:
 - Select **Chromebook (user)** for Chromebook users.
 - Select **Chromebook (device)** for Chromebook devices.
 - For **SCEP profile name**, enter a unique name for the SCEP profile.
 - For **Subject name format**, define the desired Subject Name format.

i The key usages you specify in the SCEP profile must match the certificate profile used in the SCEP server URL (SCEP enrollment URL). For example, if both **Key encipherment** and **Signing** are selected, then the certificate profile used in the SCEP server URL must include both encryption and signing key usages. For example in Entrust PKI as a Service (PKIaaS) deployments, if both **Key encipherment** and **Signing** are selected, then the certificate

profile used in the SCEP server URL must be `scep-digital-signature-key-encipherment`.

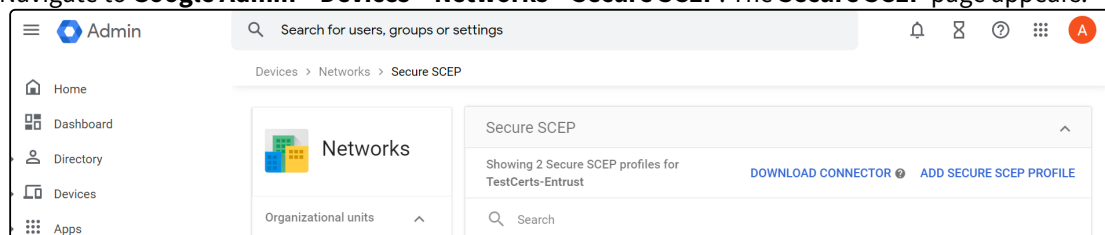
- e. For **Key Usage**, select each key usage that will be included in the issued certificates.
- f. For **Key size (bits)**, select a key size for the issued certificates.
- g. For **Security**, select the security level (attestation requirement) for the issued certificates.
- h. In the **SCEP server URL** field, enter the CEG SCEP Service URL.
- i. For **Certificate validity period (years)**, enter a lifetime (in years).
The certificate validity period will be ignored for SCEP enrollment with Certificate Enrollment Gateway. The lifetime for issued certificates is controlled by the issuing CA. For Entrust PKI as a Service, the default certificate lifetime is 1 year.
- j. For **Renew within days**, enter the renewal period (in days) for certificates. The renewal period is the number of days before a certificate expires. Certificates that will expire within this period will be renewed.
- k. For **Extended key usage**, select the extended key usage extensions that will be included in the issued certificates.
- l. For **Challenge type**, select **Static** and then enter the challenge password defined in the CEG SCEP Service.
- m. For **Certificate Authority**, select the issuing CA certificate (Managed CA certificate) that you uploaded earlier.
- n. (Optional.) For **Network type**, select the network types that will use the SCEP profile.
- o. Click **SAVE**.

Downloading and installing the Google Cloud Certificate Connector

The Google Cloud Certificate Connector is a Windows service that securely distributes certificates and authentication keys from a SCEP server to users' devices. The Google Cloud Certificate Connector must be installed on Domain-joined Windows server.

To download and install the Google Cloud Certificate Connector

1. Log in to <https://admin.google.com>
2. Navigate to **Google Admin > Devices > Networks > Secure SCEP**. The **Secure SCEP** page appears.



3. Click on **DOWNLOAD CONNECTOR**. The **Download connector** page appears.

✕ Download connector

Step 1: Install Google Cloud certificate connector

Download the connector installer on the SCEP server or Windows computer that can access the server and run the installer.

The certificate connector is a Windows service that connects Google Cloud and your on-premises Certificate Authority. [Learn more](#)

Don't start the service until after you download the connector configuration and key in the following steps and move them to the installation folder.

DOWNLOAD

Step 2: Download the connector configuration file

The connector configuration file (config.json) is a customer-specific configuration for the certificate connector. It ensures your certificate traffic is private to only your organization.

DOWNLOAD

Step 3: Get a service account key

The connector uses the secret key (key.json) to authenticate with Google Cloud.

⚠

If you get a new key, the current key is invalidated. Only get a new key if the current key is lost or compromised.

GENERATE KEY

Step 4: Start the connector service

On the computer, move the connector configuration file (config.json) and the secret key (key.json) to the connector installation folder, typically:

C:\Program Files\Google\Google Cloud Certificate Connector

Then open the Windows Services manager and start the Google Cloud Certificate Connector.

If the connector is deployed on multiple computers, you can use the same configuration file and secret key on all of them. [Learn more](#)

FINISH

4. In the **Step 1** pane, click **DOWNLOAD** to download the installer for Google Cloud Certificate Connector.
5. In the **Step 2** pane, click **DOWNLOAD** to download the configuration file (`config.json`) for Google Cloud Certificate Connector.
6. In the **Step 3** pane, click **GENERATE KEY** to generate and download a key file (`key.json`) for Google Cloud Certificate Connector.

7. Copy the installer, configuration file (`config.json`), and key file (`key.json`) to a Domain-joined Windows server.
8. On the Domain-joined Windows server, run the installer to install Google Cloud Certificate Connector.
9. Copy the `config.json` and `key.json` files into the Google Cloud Certificate Connector installation folder.
10. Start Google Cloud Certificate Connector. Open the Services administrative tool (select **Start > Windows Administrative Tools > Services**), and start **Google Cloud Certificate Connector**.

Testing SCEP enrollment with ChromeOS

To test SCEP enrollment with ChromeOS:

1. Enroll a Chromebook into Google Admin using the Enterprise Enrollment option.
2. Log in to the Chromebook.
3. Open Google Chrome.
4. Browse to <chrome://policy>.
5. Ensure that a device or user policy for client certificates exists (either **RequiredClientCertificateForDevice** or **RequiredClientCertificateForUser**).
 - The **RequiredClientCertificateForDevice** policy corresponds to the **Chromebook (device)** device platform in the SCEP profile.
 - The **RequiredClientCertificateForUser** policy corresponds to the **Chromebook (user)** device platform in the SCEP profile.
6. Browse to <chrome://certificate-manager>.
7. The name of the SCEP certificate should appear in the list.
8. Click on the SCEP certificate to view details.
9. Validate that no errors are displayed for the certificate.

Configuring SCEP clients for enrollment with Certificate Enrollment Gateway

SCEP clients must use one of the following URLs to communicate with Certificate Enrollment Gateway:

i The following SCEP enrollment URL requires a trailing forward-slash (/). To support macOS (Apple) devices, the URL must start with `http` instead of `https`.

```
http://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/  
https://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the SCEP client.
- `<profile-ID>` is the profile ID defined in CA Gateway that defines the certificate type issued to the SCEP client. For Entrust PKI as a Service, the profile ID is one of the following:
 - `scep-digital-signature-key-encipherment`
 - `scep-digital-signature`
 - `scep-key-encipherment`
 - `scep-non-repudiation`

For example:

```
http://cegserver.example.com/scep/tenant1/example_ca1/scep-digital-signature/  
https://cegserver.example.com/scep/tenant1/example_ca1/scep-digital-signature/
```

Some SCEP clients will append an additional parameter to all SCEP URLs. For these clients, you must append `nop/` to the SCEP URL. For example:

```
http://cegserver.example.com/scep/tenant1/example_ca1/scep-digital-signature/nop/  
https://cegserver.example.com/scep/tenant1/example_ca1/scep-digital-signature/nop/
```

Configuring Certificate Enrollment Gateway for SCEP enrollment

To configure Certificate Enrollment Gateway for SCEP enrollment, you must configure the SCEP enrollment settings in Certificate Enrollment Gateway. You can edit the SCEP enrollment settings using the Management Console interface.

To configure Certificate Enrollment Gateway for SCEP enrollment

1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log into the Management Console a user belonging to a role with Certificate Enrollment Gateway management permissions – for example, the initial `admin` administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

3. In the **Certificate Enrollment Gateway** pane, click **Manage Solution**.
A **Certificate Enrollment Gateway** page appears.
4. In the left navigation bar, click **Configuration**.
A **Product Configuration** pane appears.
5. Turn on **Enable Advanced Configuration**.
6. Click **Next**.
7. For all SCEP-related protocols (SCEP, MDM-SCEP, and Intune-SCEP), Certificate Enrollment Gateway uses RA certificates to sign and encrypt SCEP PKI messages. For an on-premises CA, you must specify one or more profiles that are defined in CA Gateway used to issue RA certificates.
 - a. Click the [CAGW](#) tab.
 - b. Configure the [RA Certificate Profile IDs](#) setting.
8. Click the [SCEP](#) tab and configure the following settings.
 - [Enable SCEP](#)
 - [SCEP Enrollment Service Configurations](#)
9. Configure any other settings if required.
10. After configuring the settings, click **Validate** to validate the settings.
11. If any configuration errors are detected, correct the errors then click **Validate** again.
12. After validating the configuration settings, click **Next**.
13. Cryptographic Security Platform uploads the configuration and any attached files, such as P12 credentials.

14. In the **Product Deployment Status** pane, re-deploy Certificate Enrollment Gateway with the updated configuration file by clicking **Deploy**.
A dialog box appears, prompting you to confirm the operation. Click **Yes** to confirm the operation and deploy the Certificate Enrollment Gateway solution.

Integrating Microsoft Intune with Certificate Enrollment Gateway

Microsoft Intune is a Microsoft cloud-based service that manages mobile devices and applications. It integrates with other Enterprise Mobility and Security components for identity and access control and data protection.

In Microsoft Intune, you can add non-Microsoft Certification Authorities (CAs) and have these CAs issue and validate certificates using the Simple Certificate Enrollment Protocol (SCEP). SCEP is a PKI communication protocol that allows administrators to automatically and securely issue certificates to mobile devices that support SCEP.

Certificate Enrollment Gateway can receive SCEP requests with a CSR (certificate signing request) from Intune-supported devices and send the CSR to Intune for validation.

This section describes how to integrate Entrust Certificate Enrollment Gateway with the Microsoft Intune service.

- [Updating the client secret \(application key\) used by the integration](#)
- [Configuring Certificate Enrollment Gateway for Microsoft Intune](#)
- [Configuring Microsoft Intune for Certificate Enrollment Gateway](#)
- [How Certificate Enrollment Gateway works with Microsoft Intune](#)

Updating the client secret (application key) used by the integration

Certificate Enrollment Gateway authenticates to Microsoft Intune using a client secret (also called an application key). Client secrets are created in Intune, and will expire after a configurable amount of time, such as two years. If the client secret used by Certificate Enrollment Gateway expires, Certificate Enrollment Gateway cannot authenticate to Intune, and therefore can no longer issue certificates to SCEP clients.

Intune allows you to create multiple client secrets. Before a client secret used by Certificate Enrollment Gateway expires, you should create a new client secret in Intune, and then change the application key in Certificate Enrollment Gateway. Certificate Enrollment Gateway can then use the updated application key to authenticate to Intune.

To generate a new client secret

1. Log in to the Microsoft Azure portal.
2. Under **Azure services**, click **Azure Active Directory**.
3. Click **App Registrations**.
4. Select the application you created earlier for the CEG Service.
5. Click **Certificates & secrets**.
6. Click **New client secret**. The **Add a client secret** page appears.
7. For **Description**, enter a description of the client secret.
8. For **Expires**, select a lifetime for the client secret.
9. Click **Add**. The client secret is displayed under the **Client secrets** pane.
10. Record the client secret. For example:

`abcdefghijklmnopqrstuvwxyz123456`

The client secret is also known as the Application Key. You need this value to update the application key used by Certificate Enrollment Gateway to connect to Microsoft Intune.

To update Certificate Enrollment Gateway to use the new application key

1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log into the Management Console a user belonging to a role with Certificate Enrollment Gateway management permissions – for example, the initial `admin` administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

3. In the **Certificate Enrollment Gateway** pane, click **Manage Solution**.
A **Certificate Enrollment Gateway** page appears.
4. In the left navigation bar, click **Configuration**.
A **Product Configuration** pane appears.
5. Turn on **Enable Advanced Configuration**.
6. Click **Next**.
7. For the Intune settings (see [Intune](#)), update each **Registered Azure Application Key (Client Secret)** setting to use the new application key (client setting) value.
8. After configuring the settings, click **Validate** to validate the settings.
If any configuration errors are detected, correct the errors then click **Validate** again.
9. After validating the configuration settings, click **Next**.
Cryptographic Security Platform uploads the configuration and any attached files, such as P12 credentials.
10. In the **Product Deployment Status** pane, re-deploy Certificate Enrollment Gateway with the updated configuration file by clicking **Deploy**.
A dialog box appears, prompting you to confirm the operation. Click **Yes** to confirm the operation and deploy the Certificate Enrollment Gateway solution.

Configuring Certificate Enrollment Gateway for Microsoft Intune

To configure Certificate Enrollment Gateway for Microsoft Intune, you must configure the Intune connection settings in Certificate Enrollment Gateway. You can edit the Intune connection settings using the Management Console interface.

To configure Certificate Enrollment Gateway for Microsoft Intune

1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log into the Management Console a user belonging to a role with Certificate Enrollment Gateway management permissions – for example, the initial `admin` administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

3. In the **Certificate Enrollment Gateway** pane, click **Manage Solution**.
A **Certificate Enrollment Gateway** page appears.
4. In the left navigation bar, click **Configuration**.
A **Product Configuration** pane appears.

5. Turn on **Enable Advanced Configuration**.
6. Click **Next**.
7. For all SCEP-related protocols (SCEP, MDM-SCEP, and Intune-SCEP), Certificate Enrollment Gateway uses RA certificates to sign and encrypt SCEP PKI messages. For an on-premises CA, you must specify one or more profiles that are defined in CA Gateway used to issue RA certificates.
 - a. Click the [CAGW](#) tab.
 - b. Configure the [RA Certificate Profile IDs](#) setting.
8. Click the [Intune](#) tab, and configure the following settings.
 - [Intune-SCEP Enrollment Service Configurations](#)
 - [Intune Revocation Cron Job](#)
 - [Enable Intune-SCEP](#)
9. Configure any other settings if required.
10. After configuring the settings, click **Validate** to validate the settings.
If any configuration errors are detected, correct the errors then click **Validate** again.
11. After validating the configuration settings, click **Next**.
Cryptographic Security Platform uploads the configuration and any attached files, such as P12 credentials.
12. In the **Product Deployment Status** pane, re-deploy Certificate Enrollment Gateway with the updated configuration file by clicking **Deploy**.
A dialog box appears, prompting you to confirm the operation. Click **Yes** to confirm the operation and deploy the Certificate Enrollment Gateway solution.

Configuring Microsoft Intune for Certificate Enrollment Gateway

To work with Certificate Enrollment Gateway, you must register and configure an application for Certificate Enrollment Gateway, import the issuing CAs as trusted third-party CAs, and configure a SCEP certificate profile in Microsoft Intune. When configuring Microsoft Intune, you must obtain and record information that Certificate Enrollment Gateway requires to connect to your Microsoft Intune instance.

- [Obtaining information required to configure Certificate Enrollment Gateway for Microsoft Intune](#)
- [Configuring SCEP certificate profiles](#)
- [Configuring identity protection profiles for Windows Hello for Business](#)
- [Adding CAs to Microsoft Intune as trusted third-party CAs](#)
- [Adding API permissions to the CEG Service application](#)
- [Generating and importing a TLS certificate for certificate-based authentication with Certificate Enrollment Gateway](#)
- [Generating a client secret for password-based authentication with Certificate Enrollment Gateway](#)
- [Registering an application for Certificate Enrollment Gateway](#)

Obtaining information required to configure Certificate Enrollment Gateway for Microsoft Intune

To integrate with Microsoft Intune, Certificate Enrollment Gateway requires the following Microsoft Intune information.

- Application (client) ID. For example:

00000000-0000-0000-0000-000000000000

- Tenant ID.
The Tenant ID is the domain text after the @ sign in to your account. For example, if your account is `admin@test.example.com`, then your tenant ID is `test.example.com`.
- Application Key (Authentication Key), if you generated a client secret in Microsoft Intune. The application key is the client secret you generated earlier. For example:

abcdefghijklmnopqrstuvwxyz123456

If you will use certificate-based authentication, you do not need an application key.

You may have already obtained and recorded this information when you configured Microsoft Intune for Certificate Enrollment Gateway.

Configuring SCEP certificate profiles


To issue certificates with SCEP, you must create one or more SCEP certificate profiles in Microsoft Intune. A SCEP certificate profile defines various properties of a certificate issued to users or devices over SCEP, including the subject name format and subject alternative name extensions.

When configuring a SCEP certificate profile, you must provide the URL to the CEG Intune-SCEP Enrollment Service in Certificate Enrollment Gateway. Some other settings may also require specific values to work with work with Windows Hello for Business.

To configure a SCEP certificate profile

1. Log in to the Microsoft Azure portal.
2. Log in to Intune.
3. Click **Devices**.
4. Under **Policy**, click **Device configuration**.
5. Click **Create profile**.
The **Create profile** page appears.
6. For **Name**, enter a unique name to identify the SCEP certificate profile.
7. For **Description**, enter a description for the SCEP certificate profile.
8. For **Platform**, select a device platform that will use the trusted certificate. To work with Windows Hello for Business, select **Windows 10 and later**.
9. For **Profile type**, select **SCEP certificate**.
10. In the **SCEP Certificate** pane, provide the information that will be included in the CSR (certificate signing request):
 - a. For **Certificate type**, select the type of certificate that will be issued.
 - b. For **Subject name format**, enter the subject name format. To work with Windows Hello for Business, enter `CN={{UserPrincipalName}}`.
 - c. For **Subject alternative name**, select the subject alternative name extensions that will be included in the CSR.
 - d. For **Certificate validity period**, select a lifetime for the certificate—for example, 1 year.
The validity period must not exceed the maximum validity period that is permitted by the Managed CA. For Entrust PKI as a Service, the maximum validity period is 3 years. .
For iOS devices, the validity period will be defined by the Managed CA. iOS devices will ignore the validity period defined in the SCEP certificate profile. For Entrust PKI as a Service, the validity period for certificates issued to iOS devices will be 3 years.
 - e. For **Key storage provider (KSP)**, select a key storage provider. To work with Windows Hello for Business, select **Enroll to Windows Hello for Business, otherwise fail**.
 - f. For **Key usage**, select a key usage for the certificate.
Certificate Enrollment Gateway will ignore the key usage value set in the SCEP certificate profile. The certificate profile defined in CA Gateway controls the key usage of the certificate.
The profile ID of the certificate profile is part of the SCEP Server URL. Ensure that the key usage defined in the SCEP certificate profile is compatible with the certificate profile defined in CA Gateway.
 - g. For **Key size (bits)**, select the size of the key in bits—for example, 2048.
 - h. For **Root Certificate**, select a trusted root certificate profile that you created previously.
 - i. For **Hash Algorithm**, select SHA-2. Certificate Enrollment Gateway supports only SHA-2 as the hash algorithm.

- j. For **Extended key usage**, add values for the certificate's intended purpose.
 - In most cases, the certificate requires Client Authentication so that the user or device can authenticate to a server.
 - To work with Windows Hello for Business, add Smart Card Logon (OID 1.3.6.1.4.1.311.20.2.2).
- k. For **Renewal threshold (%)**, enter the percentage of the certificate lifetime that remains before the certificate should be renewed.
- l. For **SCEP Server URLs**, enter one of the following Certificate Enrollment Gateway URLs:

 The following Intune-SCEP enrollment URL requires a trailing forward slash (/). To support macOS devices, the URL must start with `http` instead of `https`.

```
https://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/intune/  
http://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/intune/
```

See below for a description of each field.

- `<CEG-server>`
- `<tenant-ID>`
- `<CA-ID>`
- `<profile-ID>`

For example:

```
https://cegserver.example.com/scep/tenant1/example-ca1/intune-digital-  
signature/intune/  
http://cegserver.example.com/scep/tenant1/example-ca1/intune-digital-  
signature/intune/
```

- m. Enter values for any other settings as required.
11. Click **OK**.
 12. Click **Create** to create the SCEP certificate profile.
 13. Click **Assignments**.
 14. For **Include**, select the Azure Active Directory groups you want to include with the certificate profile.
 15. For **Exclude**, select the Azure Active Directory groups you want to exclude from the certificate profile.
 16. Click **Save**.

`<CEG-server>`

The hostname or IP address of the Certificate Enrollment Gateway server.

`<tenant-ID>`

The unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.

`<CA-ID>`

The CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the SCEP client.

`<profile-ID>`

The profile ID defined in CA Gateway that defines the certificate type issued to the SCEP client. For Entrust PKI as a Service, the profile ID is one of the following:

- `intune-digital-signature-key-encipherment`
- `intune-digital-signature`

- intune-key-encipherment
- intune-non-repudiation

Configuring identity protection profiles for Windows Hello for Business

Windows Hello for Business is a method for signing in to Windows devices by replacing passwords, smart cards, and virtual smart cards. To support Windows Hello for Business with Microsoft Intune, you must create one or more identity protection profiles. Each identity protection profile will enable Windows Hello for Business for devices and users, and configure various PIN and authentication settings.

To configure an identity protection profile for Windows Hello for Business


1. Log in to the Microsoft Azure portal.
2. Log in to Intune.
3. Click **Devices**.
4. Under **Policy**, click **Configuration profiles**.
5. Click **Create profile**.
The **Create profile** page appears.
6. For **Platform**, select **Windows 10 and later**.
7. For **Profile type**, select **Templates**.
8. Search or select **Identity protection**, then click **Create**.
9. For **Name**, enter a unique name to identify the identity protection profile.
10. For **Description**, enter a description for the identity protection profile.
11. Scroll down to the **Identity protection** pane.
12. Under **Configuration settings**, configure the following settings:
 - a. For **Configure Windows Hello for Business**, select **Enabled**.
 - b. For **Minimum PIN length**, enter the minimum PIN length.
 - c. For **Maximum PIN length**, enter the maximum PIN length.
 - d. For **Lowercase letters in PIN**, select whether lowercase letters are not allowed, allowed but not required, or required in a PIN.
 - e. For **Uppercase letters in PIN**, select whether uppercase letters are not allowed, allowed but not required, or required in a PIN.
 - f. For **Special characters in PIN**, select whether special characters (non-alphanumeric characters) are not allowed, allowed but not required, or required in a PIN.
 - g. For **PIN expiration (days)**, select the number of days a PIN can be used before it expires. Users must change their PIN after the configured number of days.
 - h. For **Remember PIN history**, select how many previous PINs are remembered. When users change their PIN, they cannot reuse this number of previously-used PINs.
 - i. For **Enable PIN recovery**, select **Enable** to allow users to recover their PIN using the Windows Hello for Business PIN recovery service.
 - j. For **Use a Trusted Platform Module (TPM)**, select **Enable** to allow only devices with an accessible TPM to provision Windows Hello for Business.
 - k. For **Allow biometric authentication**, select **Enable** to allow Windows Hello for Business to authenticate using biometric authentication.
 - l. For **Use enhanced anti-spoofing, when available**, select **Enable** to use anti-spoofing features on the device when available.
 - m. For **Certificate for on-premise resources**, select **Enable** to allow Windows Hello for Business to use certificates for authentication to on-premises resources.
 - n. For **Use security keys for sign-on**, select **Enable** to allow users to sign in with Windows Hello security key.
13. Click **Next**.
14. Under **Assignments**:
 - a. For **Include**, select the Azure Active Directory groups you want to include with the identity protection profile.

- b. For **Exclude**, select the Azure Active Directory groups you want to exclude from the identity protection profile.
15. Click **Next**.
16. Under **Applicability Rules**:
 - a. If required, configure any rules to work with your environment.
 - b. Click **Next**.
17. Under **Review + create**:
 - a. Review the identity protection profile. Change any settings if required.
 - b. Click **Create** to create the identity protection profile.

Adding CAs to Microsoft Intune as trusted third-party CAs

CA Gateway can issue digital certificates for one or more Certification Authorities (CAs). Each of these CAs is called a Managed CA.

For each Managed CA in CA Gateway that will issue certificates, you must add the Managed CA to Microsoft Intune as a trusted third-party CA. To add a trusted CA to Microsoft Intune, you must create a trusted certificate profile in Microsoft Intune. When creating a trusted certificate profile, you will import the CA certificate of the Managed CA.

 If the CA is an intermediate CA (also called a subordinate CA) and not the root CA, you must add each CA certificate in the certificate chain as a trusted third-party CA.

Each Managed CA will also act as a root of trust for one or more SCEP certificate profiles (see [Configuring SCEP certificate profiles](#)).

To add a CA to Microsoft Intune as a trusted third-party CA

1. Obtain the CA certificate of the Managed CA.
If the Managed CA is an intermediate CA (also called a subordinate CA) and not the root CA, you must add each CA certificate in the certificate chain as a trusted third-party CA.
2. Log in to Intune.
3. Click **Devices**.
4. Click **Configuration profile**.
5. Click **Create Profile**.
The **Create profile** page appears.
6. For **Platform**, select a device platform that will use the trusted certificate.
7. For **Profile type**, select **Trusted certificate**.
8. For **Name**, enter a unique name to identify the trusted certificate profile.
9. For **Description**, enter a description for the trusted certificate profile.
10. In the **Trusted certificate** pane, select the CA certificate you obtained earlier, then click **OK**.
11. Click **Create** to create the certificate profile.
12. Click **Assignments**.
13. For **Include**, select the Azure Active Directory groups you want to include with the certificate profile.
14. For **Exclude**, select the Azure Active Directory groups you want to exclude from the certificate profile.
15. Click **Save**.

Adding API permissions to the CEG Service application

After registering an application for the CEG Service, you must add the following API permissions to the application.

API Permission category	Permissions
Intune	scep_challenge_provider (SCEP challenge validation)

API Permission category	Permissions
Microsoft Graph	Application.Read.All (Read all applications)

You must also grant administrative consent for these permissions to the application.

To add required API permissions to the CEG Service application

1. Log in to the Microsoft Azure portal.
2. Under Azure services, click Azure Active Directory.
3. Click App Registrations.
4. Select the application you created earlier for the CEG Service.
5. Click **API permissions**.
6. To add the required Intune API permissions:
 - a. Click **Add a permission**. The Request API permissions page appears.
 - b. Click **Microsoft APIs**.
 - c. Click **Intune**.
 - d. Select **Application permissions**.
 - e. Select the following Intune application permissions:
 - Select **scep_challenge_provider** (SCEP challenge validation).
 - f. Click **Add permissions**.
7. To add the required Microsoft Graph API permissions:
 - a. Click **Add a permission**. The Request API permissions page appears.
 - b. Click **Microsoft APIs**.
 - c. Click **Microsoft Graph**.
 - d. Select **Application permissions**.
 - e. Select the following permissions:
 - Select **Application.Read.All** (Read all applications).
 - f. Click **Add permissions**.
8. When prompted, click **Yes** to confirm consent.

Generating and importing a TLS certificate for certificate-based authentication with Certificate Enrollment Gateway

Certificate Enrollment Gateway can authenticate to Microsoft Intune using one of the following authentication methods:

- Password-based authentication: Certificate Enrollment Gateway authenticates to Microsoft Intune using an application key (also called an authentication key or client secret) generated in Microsoft Intune.
- Certificate-based authentication: Certificate Enrollment Gateway authenticates to Microsoft Intune using a trusted certificate. The certificate must be imported into Microsoft Intune.

You cannot generate a TLS certificate using Microsoft Intune. You must generate a certificate using another tool, and then import the certificate into Microsoft Intune. Microsoft Intune and Certificate Enrollment Gateway must use the same certificate for authentication.

This section provides instructions about how you can use the TLS bootstrapping feature of Certificate Enrollment Gateway to generate a TLS certificate for certificate-based authentication. You can then import this certificate into Microsoft Intune.

To generate a TLS certificate file for certificate-based authentication using TLS bootstrapping

1. Log in to the server hosting the Certificate Enrollment Gateway.
2. Generate a TLS certificate (`tls.crt`) using the TLS bootstrapping feature of Certificate Enrollment Gateway. For instructions about using the TLS bootstrapping feature, see the *Certificate Enrollment Gateway Deployment Guide*. The value of the distinguished name (DN) does not need to be a fully qualified domain

name (FQDN).

You can now import the TLS certificate into Microsoft Intune as described in the following procedure. You must also complete the following steps to convert the TLS certificate (`tls.crt`) and associated private key (`tls.key`) into a PKCS #12 (P12) file. Certificate Enrollment Gateway requires a P12 file for certificate-based authentication to Microsoft Intune.

3. To convert the PEM-formatted TLS certificate and private into a P12 file (AppKey.p12) for Certificate Enrollment Gateway, enter the following command:

```
openssl pkcs12 -export -out AppKey.p12 -in tls.crt -inkey tls.key
```

Certificate Enrollment Gateway requires a P12 file for certificate-based authentication to Microsoft Intune.

4. When prompted, enter a password for the P12 file.
5. Copy the P12 file you just created (`AppKey.p12`) file into the Certificate Enrollment Gateway configuration directory, the same directory hosting the `config.yml` file.
6. Reload the Certificate Enrollment Gateway package to apply the changes.

To import the TLS certificate into Microsoft Intune

1. Log in to the Microsoft Azure portal.
2. Under **Azure services**, click **Azure Active Directory**.
3. Click **App Registrations**.
4. Select the application you created earlier for the CEG Service.
5. Click **Certificates & secrets**.
6. Click **Upload certificate**.
7. Select the TLS certificate
8. Click **Add**.

Information about the certificate is displayed under the **Certificates** pane.

Generating a client secret for password-based authentication with Certificate Enrollment Gateway

Certificate Enrollment Gateway can authenticate to Microsoft Intune using one of the following authentication methods:

- Password-based authentication: Certificate Enrollment Gateway authenticates to Microsoft Intune using an application key (also called a client secret) generated in Microsoft Intune.
- Certificate-based authentication: Certificate Enrollment Gateway authenticates to Microsoft Intune using a trusted certificate. The certificate must be imported into Microsoft Intune.

This section describes how to generate a client secret for the application you registered earlier in Microsoft Intune. Certificate Enrollment Gateway can then use this secret to authenticate to Intune.

To generate a client secret

1. Log in to the Microsoft Azure portal.
2. Under **Azure services**, click **Azure Active Directory**.
3. Click **App Registrations**.
4. Select the application you created earlier for the CEG Service.
5. Click **Certificates & secrets**.
6. Click **New client secret**.
The **Add a client secret** page appears.
7. For **Description**, enter a description of the client secret.
8. For **Expires**, select a lifetime for the client secret.
9. Click **Add**.

The client secret is displayed under the **Client secrets** pane.

10. Record the client secret. For example:

```
abcdefghijklmnopqrstuvwxyz123456
```

The client secret is also known as the Application Key. You need this value later to configure Certificate Enrollment Gateway for Microsoft Intune.

Registering an application for Certificate Enrollment Gateway

For Certificate Enrollment Gateway to run custom challenge validation with Intune, you must register a new application in Azure Active Directory. This application will give delegated rights to Intune to validate SCEP requests.

To register an application for the CEG Service

1. Log in to the Microsoft Azure portal.
2. Under **Azure services**, click **Azure Active Directory**.
3. Click **App Registrations**.
4. Click **Register an application**.
The **Register an application** page appears.
5. For **Name**, enter a unique application name. For example, `Entrust SCEP Service`.
6. For **Supported account types**, select **Accounts in any organizational directory**.
7. Do not provide any values for **Redirect URI**. Intune does not need to redirect back to Certificate Enrollment Gateway after issuing the certificate.
8. Click **Register**.
After registering the application, an **Overview** page appears for the application.
9. Record the **Application (client) ID** value. For example:

```
00000000-0000-0000-0000-000000000000
```

You need this value later to configure Certificate Enrollment Gateway for Microsoft Intune.

10. Record your Tenant ID. You need this value later to configure Certificate Enrollment Gateway for Microsoft Intune. The Tenant ID is the domain text after the @ sign in to your account. For example, if your account is `admin@test.example.com`, then your tenant ID is `test.example.com`.

How Certificate Enrollment Gateway works with Microsoft Intune

Traditional SCEP enrollment uses a static password for authentication. This static password is vulnerable to brute force attacks. Entrust worked with Microsoft Intune to co-develop a secure authentication mechanism for SCEP enrollment.

Certificate Enrollment Gateway can receive SCEP requests with a CSR (certificate signing request) from Windows clients, and send the CSR to Intune for validation.

Certificate Enrollment Gateway works with Intune as follows:

1. Microsoft Intune pushes a certificate profile and SCEP challenge to a Windows client.
2. The Windows client sends a SCEP request with a CSR from the Intune system to the Certificate Enrollment Gateway.
3. During the validation process of the SCEP request, Certificate Enrollment Gateway sends the CSR to the Intune service to validate the CSR.
4. If the CSR is valid:
 - a. Certificate Enrollment Gateway sends the CSR to Entrust CA Gateway, which forwards the CSR to the Managed CA for processing. A Gateway can issue digital certificates for one or more Certification Authorities (CAs). Each of these CAs is called a Managed CA.

- b. The Managed CA processes the request, and issues a certificate for the device.
 - c. The Managed CA sends the certificate back to CA Gateway, which forwards the certificate back to Certificate Enrollment Gateway.
5. Certificate Enrollment Gateway returns the certificate to the Windows client. The Windows client will import the certificate into the client's certificate store.
6. Upon success or failure, Certificate Enrollment Gateway calls the Intune system to relay the status information.
7. With the certificate, the Windows client can access protected resources.

For more information about how non-Microsoft CAs work with Microsoft Intune, see the Microsoft documentation.

Integrating ACMEv2 clients with Certificate Enrollment Gateway

The following topics explain how to integrate ACMEv2 clients with the Certificate Enrollment Gateway service.

- [ACMEv2 client examples](#)
- [Configuring ACMEv2 clients for enrollment with Certificate Enrollment Gateway](#)
- [Configuring Certificate Enrollment Gateway for ACMEv2 enrollment](#)

ACMEv2 client examples

The following topics provide some examples about how to request certificates from Entrust Certificate Enrollment Gateway using some common ACMEv2 clients.

- [Cert-manager.io example](#)
- [acme.sh example](#)
- [Win-acme example](#)
- [Certbot example](#)

For complete information about using these ACMEv2 clients, see the ACMEv2 client documentation.

Cert-manager.io example

Cert-manager.io adds certificates and certificate issuers as resource types in Kubernetes clusters, and can simplify the process of obtaining, renewing, and using those certificates. You can use Cert-manager.io to request certificates from Certificate Enrollment Gateway using the ACMEv2 protocol.

i The instructions in this example use Cert-manager.io installed in a Kubernetes cluster using Helm. Other methods of configuring and deploying Cert-manager.io are available, but are not documented in this guide.

- [Configuring Cert-manager.io for Certificate Enrollment Gateway with ACMEv2](#)
- [Deploying Kubernetes and Cert-manager.io](#)
- [Preparing Linux for HTTPS \(optional\)](#)
- [Cert-manager.io prerequisites](#)

Configuring Cert-manager.io for Certificate Enrollment Gateway with ACMEv2

The following procedures configure Cert-manager.io to request and receive certificates using DNS-01 and HTTP-01 validation. Configuring Cert-manager.io requires configuring a series of YAML files, then applying those files to Cert-manager.io. After applying the files, Cert-manager.io will automatically request the files from Certificate Enrollment Gateway.

For HTTP-01 validation, the following example uses Cert-manager.io's ingress-shim features. In this example, you will create a dummy back-end service (echo), and then an Ingress. The Ingress routes traffic into the cluster, and requests TLS certificates for the services to which it is routing.

For this example, you will create the following files:

- `dns-issuer.yaml` , to define the DNS issuer for DNS-01 validation.
- `dns-cert.yaml` , to define the DNS certificate for DNS-01 validation.
- `http-issuer.yaml` , to define the HTTP issuer for HTTP-01 validation.
- `echo.yaml` , to define the echo (dummy back-end) service for HTTP-01 validation.

In this example, the echo service is a dummy back-end to show how to secure an existing service on the Kubernetes cluster.

- `http-ingress.yaml` , to define the Ingress for HTTP-01 validation.

To create the YAML files for Cert-manager.io

1. Create a new file named `dns-issuer.yaml` with the following contents. Read the comments and modify the content as required.

```
---
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: test-dns
  namespace: default
spec:
  dnsNames:
    #NOTE: This only works if the DNS ClusterIssuer has permission to update
    "example.com" records
    - dns.example.com
  secretName: test-dns
  issuerRef:
    name: ceg-issuer-dns
    kind: ClusterIssuer
```

2. Create a new file named `dns-cert.yaml` with the following contents. Read the comments and modify the content as required.

```
---
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: test-dns
  namespace: default
spec:
  dnsNames:
    #NOTE: This only works if the DNS ClusterIssuer has permission to update
    "example.com" records
    - dns.example.com
  secretName: test-dns
  issuerRef:
    name: ceg-issuer-dns
    kind: ClusterIssuer
```

3. Create a new file named `http-issuer.yaml` with the following contents. Read the comments and modify the content as required.

```
---
apiVersion: cert-manager.io/v1
kind: ClusterIssuer
metadata:
  name: ceg-issuer-http
  namespace: cert-manager
spec:
  acme:
    # Uncomment the following line to allow insecure TLS connections.
    #skipTLSVerify: true
    # The ACME server URL
    server: https://cegserver.example.com/acme/tenant1/example_ca1/
  privateKeySecretRef:
    # Email address used for ACME registration
    email: certmanager@example.com
    # Name of a secret used to store the ACME account private key
    name: ceg-acme-account-key-http
    # Enable the HTTP-01 challenge provider
    solvers:
    - http01:
        ingress:
          class: traefik
```

4. Create a new file named `echo.yaml` with the following contents.

```
---
apiVersion: v1
kind: Service
metadata:
  name: echo
spec:
  ports:
    - port: 80
      targetPort: 5678
  selector:
    app: echo
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: echo
spec:
  selector:
    matchLabels:
      app: echo
  replicas: 1
```

```
template:
  metadata:
    labels:
      app: echo
  spec:
    containers:
      - name: echo
        image: hashicorp/http-echo
        args:
          - "-text=echo"
        ports:
          - containerPort: 5678
```

5. Create a new file named `http-ingress.yaml` with the following contents. Read the comments and modify the content as required.

```
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: echo1-traefik-ingress
  namespace: default
  annotations:
    kubernetes.io/ingress.class: traefik
    cert-manager.io/cluster-issuer: ceg-issuer-http
spec:
  tls:
    - hosts:
        # Change the hostname here to the one you want a TLS Certificate for.
        # NOTE: CEG's must resolve the following hostname to cert-manager.io's IP
        Address.
        - echo1.example.com
      secretName: echo-tls
  rules:
    # The following host must match the host in the "tls" section a few lines up.
    - host: echo1.example.com
      http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: echo
                port:
                  number: 80
```

To apply the YAML files to Kubernetes and request certificates

1. Apply the files with the following commands.

```
kubectl apply -f dns-issuer.yaml
kubectl apply -f dns-cert.yaml
kubectl apply -f http-issuer.yaml
kubectl apply -f http-echo.yaml
kubectl apply -f http-ingress.yaml
```

2. After applying the files, Cert-manager.io has been configured to request two different certificates over two different ClusterIssuers, one certificate for DNS-01 validation, and one certificate for HTTP-01 validation. The certificates will automatically be requested by Cert-manager.io.
3. To view the status of all cert-manger.io ACMEv2 objects, enter the following command:

```
kubectl get
Issuers,ClusterIssuers,Certificates,CertificateRequests,Orders,Challenges --
all-namespaces
```

Deploying Kubernetes and Cert-manager.io

This section describes how to deploy a single-node Kubernetes, and then how to deploy Cert-manager.io into it.

To deploy Kubernetes and Cert-manager.io

1. Install K3s Lightweight Kubernetes by running the following commands:

```
curl -sL https://get.k3s.io | sh -
export PATH=$PATH:/usr/local/bin
```

2. Enable the use of kubectl permanently, by ensuring that `/usr/local/bin` appears as part of the `PATH` environment variable in the `~/.bash_profile` file.
3. Install Helm by running the following commands:

```
curl https://raw.githubusercontent.com/helm/helm/master/scripts/get-helm-3 |
bash
echo "export KUBECONFIG=/etc/rancher/k3s/k3s.yaml" >> ~/.bash_profile
export KUBECONFIG=/etc/rancher/k3s/k3s.yaml
```

4. Add the Cert-manager.io repository to Helm by running the following commands:

```
helm repo add jetstack https://charts.jetstack.io
helm repo update
```

5. Install Cert-manager.io using Helm by entering the following command:

```
helm upgrade -i -n cert-manager cert-manager jetstack/cert-manager --set
installCRDs=true --create-namespace --version v1.6.0-beta.0 --wait
```

6. (Secure HTTP Only) If you want to use Cert-manager.io with trusted HTTPS connections, then you must add the TLS CA certificate chain into the cluster. Create a `private-ca-bundle.pem` file.

- a. This file contains a concatenation of all PEM certificates in the CA certificate chain, starting with the issuing CA first and ending with the root CA last. For example:

```
-----BEGIN CERTIFICATE-----
MIIF0TCCA7mgAwIBAgIQCy...
...
V8HU0ts=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFUDCCAzigAwIBAgIQRv...
...
XLy202FpMk40J031gqbnD0usrY8=
-----END CERTIFICATE-----
```

- b. Create a config-map from the `private-ca-bundle.pem` file by running the following command:

```
kubectl create configmap private-ca-bundle -n cert-manager --from-
file=private-ca-bundle.pem
```

- c. Update the Cert-manager.io deployment to use the config-map using Helm, by running the following command:

```
helm upgrade -i -n cert-manager cert-manager jetstack/cert-manager \
--version v1.6.0-beta.0 \
--set installCRDs=true \
--set volumes[0].name=ca-certs,volumes[0].configMap.name=private-ca-
bundle \
--set volumeMounts[0].name=ca-certs,volumeMounts[0].mountPath=/etc/ssl/
certs \
--wait --wait-for-jobs
```

You have now deployed a single-node Kubernetes cluster and installed Cert-manager.io. Certificate Enrollment Gateway's TLS certificate chain is also trusted at the Cert-manager.io namespace, cluster, and operating system levels. The certificate chain still needs to be configured at the pod level.

Preparing Linux for HTTPS (optional)

i This section is required only if the Kubernetes cluster that will host Cert-manager.io will use a trusted HTTPS connection to connect to Certificate Enrollment. If you will not use a trusted HTTPS connection, you can skip this section. You must complete this step before deploying the Kubernetes cluster.

To configure Linux to trust a CA certificate chain, complete the following steps.

To configure Linux to trust a CA certificate chain

1. Transfer Certificate Enrollment Gateway's trust certificate chain (from the issuing CA certificate to the root CA certificate) to the Linux server that will host Cert-manager.io. The certificate files must be in PEM format.
2. Log in to the Linux server that will host Cert-manager.io.
3. Copy the certificates (trust chain) into the following directory:

```
/etc/pki/ca-trust/source/anchors
```

4. Enter the following command to update the file permissions for `ca-bundle.crt` so everyone can read the file:

```
sudo chmod +r ./ca-bundle.crt
```

5. Run the following command to update the `ca-bundle.crt` file at the operating system level:

```
sudo update-ca-trust extract
```

6. Verify that the certificates were added to the following file:

```
/etc/pki/tls/certs/ca-bundle.crt
```

Cert-manager.io prerequisites

To use Cert-manager.io with Certificate Enrollment Gateway:

- If you will use secure HTTPS with Cert-manager.io, copy Certificate Enrollment Gateway's TLS certificate chain to the server that will host Cert-manager.io.
- For HTTP-01 validation, the DNS server must resolve the requested DNS name to the IP address of the server hosting Cert-manager.io.
- For DNS-01 validation, nonsecure and secure dynamic updates must be enabled for the domain for which Cert-manager.io is requesting certificates.
- Obtain the ACMEv2 enrollment URL used to request a certificate from Certificate Enrollment Gateway. For details, see [ACMEv2 enrollment URL](#). You need this URL later when configuring Cert-manager.io.

acme.sh example

Acme.sh is UNIX shell script that implements the ACMEv2 client protocol. You can use acme.sh to request certificates from Certificate Enrollment Gateway using the ACMEv2 protocol.

To request a certificate using Acme.sh, enter the following command:

```
acme.sh --issue --standalone [--httpport <port>] -d <domain> --server <CEG-ACME-URL>  
--ca-bundle <ca-file>
```

Parameters in square brackets are optional parameters. Where:

- `--standalone` requests a certificate if you do not want to use (or do not have) existing server software.
- `--httpport <port>` specifies the standalone HTTP listen port. If not specified, the port defaults to port 80. The port (such as port 80) must be available and allowed through any configured firewalls. If another application such as a Web server is running and using the port, disable the application.
- `<domain>` is a domain to include in the certificate. You can specify multiple domains using multiple `-d <domain>` parameters. For example:

```
-d example.com -d www.example.com
```

- `<CEG-ACME-URL>` is the ACMEv2 enrollment URL used to request a certificate from Certificate Enrollment Gateway. For details, see [ACMEv2 enrollment URL](#).
- `<ca-file>` is the path and file name of the CA certificate bundle, used to verify the Certificate Enrollment Gateway server certificate.

For example:

```
acme.sh --issue --standalone -d example.com -d www.example.com --server https://  
cegserver.example.com/acme/tenant1/example_ca1/privatessl_tls_client/directory --ca-  
bundle /tmp/root-ca.crt
```

Win-acme example

Win-acme is an ACMEv2 client for Windows operating systems. You can use win-acme to request certificates from Certificate Enrollment Gateway using the ACMEv2 protocol.

To request a certificate using Win-acme

1. Import your root CA certificate into the Windows trust store.
2. Open a Command Prompt. Select **Start > Windows System > Command Prompt**.
3. Navigate to the location where Win-acme is installed.
4. Enter the following command:

```
wacs.exe --baseuri <CEG-ACME-URL> --accepttos --target manual --host <hosts> --  
force
```

Where:

- `<CEG-ACME-URL>` is the ACMEv2 enrollment URL used to request a certificate from Certificate Enrollment Gateway. For details, see [ACMEv2 enrollment URL](#).
- `--accepttos` will force Win-acme to automatically accept the ACMEv2 terms of service.
- `--source manual` will use the manual plugin, allowing you to provide the host names for a certificate.
- `<hosts>` is a comma-separated list of host names to include in the certificate. The first host name listed will become the common name of the certificate. Subsequent host names will be added to the certificate as subjectAltName extensions only.
- `--force` will force a renewal if a valid certificate already exists.

For example:

```
wacs.exe --baseuri https://cegserver.example.com/acme/tenant1/example_ca1/  
privatessl_tls_client/directory --accepttos --target manual --host  
www.example.com,example.com --force
```

5. Win-acme connects to Certificate Enrollment Gateway, and prompts you to select a task:

```
A simple Windows ACMEv2 client (WACS)
```

```
Software version 2.1.17.1065 (release, pluggable, standalone, 64-bit)
Connecting to https://cegserver.example.com/acme/tenant1/example_ca1/
privatessl_tls_client/
directory...
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (0 total)
O: More options...
Q: Quit

Please choose from the menu
```

6. Enter **N** to create a new certificate with the default settings.
7. Win-acme prompts you to provide one or email addresses to receive notifications about problems and abuse:

```
Enter email(s) for notifications about problems and abuse (comma-separated):
```

8. Enter an email address. Certificate Enrollment Gateway will not send email messages to this email address.
9. Win-acme requests the certificate. If the certificate is successfully created, Win-acme installs the certificate and creates a scheduled task for renewing the certificate.

Certbot example

Certbot is a free, open-source software tool for automatically using digital certificates on Web sites to enable HTTPS. You can use Certbot to request certificates from Certificate Enrollment Gateway using the ACMEv2 protocol.

- [Preparing to use Certbot](#)
- [Using Certbot to request a certificate](#)

Preparing to use Certbot

Before using Certbot, configure Certbot to trust your root CA certificate using the `REQUESTS_CA_BUNDLE` environment variable.

- For example, to set the `REQUESTS_CA_BUNDLE` environment variable on Windows:

```
set REQUESTS_CA_BUNDLE=<root-CA-cert-file>
```

Where `<root-CA-cert-file>` is the path and file name of the root CA certificate file. For example:

```
set REQUESTS_CA_BUNDLE= "C:\root_ca.crt"
```

- For example, to set the `REQUESTS_CA_BUNDLE` environment variable on Linux:

```
sudo REQUESTS_CA_BUNDLE=<root-CA-cert-file>
```

Where `<root-CA-cert-file>` is the path and file name of the root CA certificate file. For example:

```
sudo REQUESTS_CA_BUNDLE=/tmp/root_ca.crt
```

Using Certbot to request a certificate

To request a certificate using Certbot, enter the following command:

```
certbot certonly -d <domain> --<CEG-ACME-URL> --standalone --no-eff-email --agree-tos  
-m <email-address>
```

Where:

- `<domain>` is a domain to include in the certificate. You can specify multiple domains using multiple `-d <domain>` parameters. For example:

```
-d example.com -d www.example.com
```

- `<CEG-ACME-URL>` is the ACMEv2 enrollment URL used to request a certificate from Certificate Enrollment Gateway. For details, see [Configuring ACMEv2 clients for enrollment with Certificate Enrollment Gateway](#).
- `--standalone` requests a certificate if you do not want to use (or do not have) existing server software. Certbot will bind on port 80 to perform domain validation. Port 80 must be available and allowed through any configured firewalls. If another application such as a Web server is running and using port 80, disable the application.
- `--no-eff-email` forces Certbot to not share your e-mail address with the Electronic Frontier Foundation.
- `--agree-tos` will cause Certbot to automatically agree to the terms of service of the ACMEv2 server (Certificate Enrollment Gateway).
- `<email-address>` is the email address that Certbot uses when registering the ACME account with Certificate Enrollment Gateway. Certificate Enrollment Gateway will not send email messages to this email address.

For example:

```
certbot certonly -d example.com -d www.example.com --server https://  
cegserver.example.com/acme/tenant1/example_ca1/privatessl_tls_client/directory --  
standalone --no-eff-email --agree-tos -m notifications@example.com
```

Configuring ACMEv2 clients for enrollment with Certificate Enrollment Gateway

This section describes the information required to configure ACMEv2 clients to enroll for a certificate using Certificate Enrollment Gateway. For information about using your ACMEv2 client, see the documentation for your ACMEv2 client.

- [Enrollment URL for ACMEv2 clients](#)
- [Supported algorithms for CSRs](#)

- [Adding the CA certificate chain to the ACMEv2 client](#)
- [Supported validation methods](#)
- [About CSRs with an empty Subject DN](#)

Enrollment URL for ACMEv2 clients

ACMEv2 clients must use the following URL to communicate with Certificate Enrollment Gateway:

```
https://<CEG-server>/acme/<tenant-ID>/<CA-ID>/<profile-ID>/directory
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the ACMEv2 endpoint.
- `<profile-ID>` is the profile ID defined in CA Gateway that defines the certificate type issued to the ACMEv2 client. For Entrust PKI as a Service, the profile ID is one of the following:
 - `privatessl-tls-client-server`
 - `privatessl-tls-server`
 - `privatessl-tls-client`

For example:

```
https://cegserver.example.com/acme/tenant1/example_ca1/privatessl_tls_client/directory
```

Supported algorithms for CSRs

When an ACMEv2 client requests a certificate, the CSR (certificate signing requests) must use an algorithm supported by Certificate Enrollment Gateway.

The ACMEv2 service of the Certificate Enrollment Gateway supports the following algorithms for CSRs (certificate signing requests):

- RSA-2048, RSA-3072, RSA-4096
- EC P-256, EC P-384, EC P-521

Adding the CA certificate chain to the ACMEv2 client

ACMEv2 clients must trust the CA certificate chain for the Cryptographic Security Platform cluster's TLS certificate. The cluster's TLS certificate secures Certificate Enrollment Gateway's TLS traffic. If ACMEv2 clients do not trust the CA certificate chain, the clients will fail to establish a secure TLS connection to Certificate Enrollment Gateway.

✗ While some ACMEv2 clients may allow insecure TLS connections, you should avoid these connections for security reasons.

See your ACMEv2 client documentation for instructions about adding certificates to the ACMEv2 client.

Supported validation methods

During enrollment, ACMEv2 clients must pass one of the following validation methods:

Method	Required configuration
DNS-01	Certificate Enrollment Gateway and the ACMEv2 client must point to the same DNS server. Certificate Enrollment Gateway must be able to query for DNS TXT records generated by the ACMEv2 client.
HTTP-01	Certificate Enrollment Gateway must resolve the hostname of the FQDN in the CSR. The hostname must resolve to the IP address of the ACMEv2 client. The ACMEv2 client must listen on port 80 to use HTTP-01 validation.

About CSRs with an empty Subject DN

Some ACMEv2 clients may send a CSR with an empty Subject DN. However, certificates issued by Entrust Certificate Authority instances will have a non-empty Subject DN. If an ACMEv2 client sends a CSR with an empty Subject DN, Certificate Enrollment Gateway will use the first Subject Alternative Name value in the CSR as the Subject DN.

Certificate Enrollment Gateway will not modify the Subject DN in the CSR. Certificate Enrollment Gateway will send the CSR unaltered to CA Gateway for processing, and send the Subject DN separately as a CA Gateway request parameter.

Configuring Certificate Enrollment Gateway for ACMEv2 enrollment

To configure Certificate Enrollment Gateway for ACMEv2 enrollment, you must configure the ACMEv2 enrollment settings in Certificate Enrollment Gateway. You can edit the ACMEv2 enrollment settings using the Management Console interface.

To configure Certificate Enrollment Gateway for ACMEv2 enrollment

1. Open the following URL in a Web browser.

```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log into the Management Console a user belonging to a role with Certificate Enrollment Gateway management permissions – for example, the initial `admin` administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

3. In the **Certificate Enrollment Gateway** pane, click **Manage Solution**.
4. A **Certificate Enrollment Gateway** page appears.
5. In the left navigation bar, click **Configuration**.
A **Product Configuration** pane appears.
6. Turn on **Enable Advanced Configuration**.
7. Click **Next**.
8. Click the **ACMEv2** tab and configure the following settings.
 - [ACMEv2 HTTP-01 Redirect on POST](#)
 - [ACMEv2 HTTP-01 Retry Interval](#)
 - [ACMEv2 HTTP-01 Retry Count](#)
 - [ACMEv2 DNS-01 Query Timeout](#)

- [ACMEv2 DNS-01 Nameservers](#)
 - [Delete Expired Authorizations Cron Job](#)
 - [Delete Expired Order Cron Job](#)
 - [ACMEv2 Order Expiry Interval](#)
 - [Enable ACMEv2](#)
9. Configure any other settings if required.
 10. After configuring the settings, click **Validate** to validate the settings.
If any configuration errors are detected, correct the errors then click **Validate** again.
 11. After validating the configuration settings, click **Next**.
Cryptographic Security Platform uploads the configuration and any attached files, such as P12 credentials.
 12. In the **Product Deployment Status** pane, re-deploy Certificate Enrollment Gateway with the updated configuration file by clicking **Deploy**.
A dialog box appears, prompting you to confirm the operation. Click **Yes** to confirm the operation and deploy the Certificate Enrollment Gateway solution.

10 Managing Timestamping Authority

See below for configuring, deploying, and administrating the Timestamping Authority solution.

- [Timestamping Authority overview](#)
- [Loading the HSM configuration on Timestamping Authority](#)
- [Configuring Entrust Certificate Authority for Timestamping Authority](#)
- [Generating a timestamping certificate and key pair](#)
- [Configuring and deploying Timestamping Authority](#)
- [Testing the timestamping service](#)



As explained in [Manually starting starting the chrony service](#), you must manually start the `chrony` service after restarting a node.

Timestamping Authority overview

The Timestamping Authority solution responds to timestamp requests to prove that a digital document, message, or transaction:

- Existed at a certain point in time.
- Has not been altered since.

To respond these requests:

- Multiple clients send requests to the timestamping service of Timestamping Authority.
- One or several Hardware Security Modules (HSMs) manage the timestamp signing key.
- One or several Network Time Protocol (NTP) servers provide an accurate and reliable time source.

Loading the HSM configuration on Timestamping Authority

See in following table the required commands for loading the configuration of a Hardware Security Module meeting the [HSM requirements](#).



Skip this step if you use software cryptography (not recommended).

HSM	Command	Additional steps
Entrust nShield HSM	<code>tsactl import-nshield</code>	See Administrating nShield HSM integration
Thales HSM	<code>tsactl import-thales</code>	—

Configuring Entrust Certificate Authority for Timestamping Authority

If you will use Entrust Certificate Authority for [Generating a timestamping certificate and key pair](#), you may need to create a new certificate type. Otherwise, you can skip this section.

i To issue the Timestamping Authority certificate with Entrust Certificate Authority, you may need to create a new certificate type. In the latest Entrust Certificate Authority 10.0.x releases, a Time-Stamp Authority (TimeStamp_1K) certificate type may already be predefined in the certificate specifications. This certificate type includes the proper certificate extensions for signing timestamp responses.

The following procedures describe how to create the Time-Stamp Authority (TimeStamp_1K) certificate type if it does not already exist.

To add the Time-Stamp Authority certificate type to Entrust Certificate Authority

1. Log in to Entrust Certificate Authority administration portal.
2. Select **File > Certificate Specifications > Export** and export the certificate specifications.
3. Open the certificate specifications file in a text editor.
4. Add the following lines to the [Certificate Types] section.

```
TimeStamp_1k=enterprise,Time-Stamp Authority,Time-Stamp Authority certificate
-no directory entry
```

5. Add the following lines to the [Extension Definitions] section.

```
;-----
;- Cert Type: TimeStamp_1k
;- This cert type needs to be mapped to cert def policy enforcing:
; - Certificate lifetime:
; - Exclude privateKeyUsagePeriod: 1
; - Exclude basicConstraints: 1
; - Exclude entrustVersInfo: 1
;-----
[TimeStamp_1k Certificate Definitions]
1=Verification
;
[TimeStamp_1k Verification Extensions]
;Key Usage: Digital Signature
keyusage=2.5.29.15,n,m,BitString,1
;Extended Key Usage: Time Stamping
extkeyusage=2.5.29.37,c,o,SeqOfObjectIdentifier,1.3.6.1.5.5.7.3.8
; Certificate Policies: DER encode the <Policy-OID>
; Policy-OID=<Policy-OID> - This OID is optional, the customer might not have a
policy OID.
;certificatepolicies=2.5.29.32,n,o,DER,<DER encoded value of the above OID>
; AuthorityInfo Access:
; - OCSP server URL: <OCSP-HTTP-URL>
; - Issuing CA certificate URL: <CA-Cert-HTTP-URL>
;aia=1.3.6.1.5.5.7.1.1,n,m,DER,<DER encoded value of the above two URLs>
;
```

6. (Optional.) You can add a certificatePolicies extension to the certificate type. The certificatePolicies extension contains policy information, such as how your CA operates and the intended purpose of the issued certificate. Typically, different certificate policies will relate to different applications which may use the certified key. The Certificate Policies extension contains a sequence of one or more policy information terms. Each policy information term consists of an object identifier (OID) and

optional qualifiers. In an end entity certificate, the policy information terms indicate the policy under which the certificate has been issued, and the purposes for which the certificate may be used. To add a certificatePolicies extension to the certificate type:

- a. DER-encode a list of one or more policy OIDs. Entrust provides an entDerEncoder utility for Entrust Certificate Authority that you can use to DER-encode data for certificate extensions. For instructions about using the entDerEncoder utility, see the Entrust Certificate Authority documentation.
 - b. Uncomment the `certificatepolicies=` entry and replace `<DER encoded value of the above OID>` with the DER-encoded value you obtained in the previous step.
7. (Optional.) You can add an authorityInformationAccess extension to the certificate type. The Authority Information Access (AIA) certificate extension indicates how to access information and services for the CA that issued the certificate. Information and services may include online validation services and CA policy data. To add a certificatePolicies extension to the certificate type:
- a. DER-encode the HTTP URL of the CA certificate. Entrust provides an entDerEncoder utility for Entrust Certificate Authority that you can use to DER-encode data for certificate extensions. For instructions about using the entDerEncoder utility, see the Entrust Certificate Authority documentation.
 - b. Uncomment the `aia=` entry and replace `<DER encoded value of the above URL>` with the DER-encoded value you obtained in the previous step.
8. Add the following lines to the `[Advanced Settings]` section.

```
[TimeStamp_1k Advanced]
noBasicConstraints=1
noPrivateKeyUsage=1
noEntrustVersInfo=1
cdpLdapDnLast=1
noUserInDirectory=1
;noCRLDistPoints=1
```

9. Save and close the file.
10. Select **File > Certificate Specifications > Import** and import the certificate specifications back into Entrust Certificate Authority.

Generating a timestamping certificate and key pair

Each TSA issuer in Timestamping Authority needs a certificate to sign timestamping responses. You can:

- Use a different certificate for every TSA issuer.
- Share a certificate among multiple TSA issuers.

See below for generating a timestamping certificate and key pair.

- [Issuing a timestamping certificate](#)
- [Generating a timestamping key pair](#)

Issuing a timestamping certificate

Use your CA to process the CSR obtained in [Generating a timestamping key pair](#) and issue a certificate with the following extension values.

Extension	Value
Key Usage	digitalSignature
Extended Key Usage	timeStamping


See below for how to issue this certificate with Entrust products.

- [Issuing a timestamping certificate with Entrust Certificate Authority](#)
- [Issuing a timestamping certificate with the Certificate Authority solution](#)

Issuing a timestamping certificate with Entrust Certificate Authority

If you are using Entrust Certificate Authority, you can run one of the following applications to issue the timestamping certificate:

- The CSR Enrollment Services (CSRES) provided by the Entrust Administration Services.
- The Profile Creation Utility included in products such as Entrust Administration Services or available as a separate download with Entrust CA Gateway.

 See [Configuring Entrust Certificate Authority for Timestamping Authority](#) for instructions on configuring Entrust Certificate Authority.

Issuing a timestamping certificate with the Certificate Authority solution

Follow the steps below to issue a timestamping certificate using the Certificate Authority solution provided by Cryptographic Security Platform.

- [Creating a Certificate Authority to issue timestamping certificates](#)
- [Creating a timestamping certificate request](#)
- [Processing the timestamping certificate request](#)

Creating a Certificate Authority to issue timestamping certificates

Follow the steps described in [Managing Certificate Authority](#) to create:

- A root Certificate Authority.
- An issuing Certificate Authority with at least one signature profile – for example, the `wstep-digital-signature` profile described in [Active Directory \(WSTEP\) certificate profiles](#).

Creating a timestamping certificate request

Create a CA Gateway certificate enrollment request – for example:

```
1  {
2    "csr": "MIIDVzCCAb8...",
3    "profileId": "wstep-digital-signature",
4    "requiredFormat": {
5      "format": "X509"
6    },
7    "optionalCertificateRequestDetails": {
```

```

 8      "extensions": [
 9          {
10              "oid": "2.5.29.37",
11              "critical": true,
12              "value": "1.3.6.1.5.5.7.3.8"
13          }
14      ],
15      "validity_period": "2024-11-06T13:00Z/2026-07-06T13:00:00Z"
16  }
17  }

```

See below for the values required by each request field.

Field	Line	Value
csr	2	The base64-encoded Certificate Signing Request previously generated in Generating a timestamping key pair as a single line.
extensions	8	The same fields and values as in the above example (to select the timestamping extended key usage).
validity_period	15	The validity period for the issued certificate. The expiry date in this period cannot exceed the expiry date of the issuing CA certificate.

Processing the timestamping certificate request

See below for processing the timestamping certificate request and obtaining the issued certificate.

To process the timestamping certificate request

1. Use a REST client to process the request as explained in [Issuing certificates with a REST client](#).
2. Edit the REST response and copy the base64-encoded string in the `body` field.
3. Save the string in a file with the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters – for example:

```

-----BEGIN CERTIFICATE-----
MIIICDCCBlIqAwIBAgITMwEf/Fvr7NDwanyerAAAAAR/8WzANBgkqhkiG9w0BAQwF
ADBdMQswCQYDVQQGEwJVUzEeMBwGA1UEChMVMTWljcm9zb2Z0IENvcnBvcmlF0aW9u
...
Ud085g==
-----END CERTIFICATE-----


```

4. Use this certificate file as the [TSA certificate](#) when configuring the solution.

Generating a timestamping key pair


To generate the timestamping key pair, run the `tsactl create-key` command in any Cryptographic Security Platform node. The command will output a CSR that you can use to generate the certificate – for example:

```
$ sudo tsactl create-key -k RSA2048 -s "CN=TSA" -o /tmp/certreq.txt -t mytoken -v
thales
Created key with id 4a00a4617d1afd5ad626955132dd0d396a69ed24
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIICqDCCAQACAQAwMzExMC8GA1UEAxMoNGEwMGE0NjE3ZDFhZmQ1YWQ2MjY5NTUx
...
etTv+pac+nJKW8fw
-----END CERTIFICATE REQUEST-----
```

 As explained in [tsactl create-csr](#) you can create a certificate request for a key that already exists on the HSM.

Configuring and deploying Timestamping Authority

See below for configuring and deploying Timestamping Authority with the Management Console.

 Repeat the following steps each time a configuration update is required. Do not forget to click **Deploy** to make the changes effective.

To configure and deploy Timestamping Authority with the Management Console

1. Open the following URL in a Web browser.

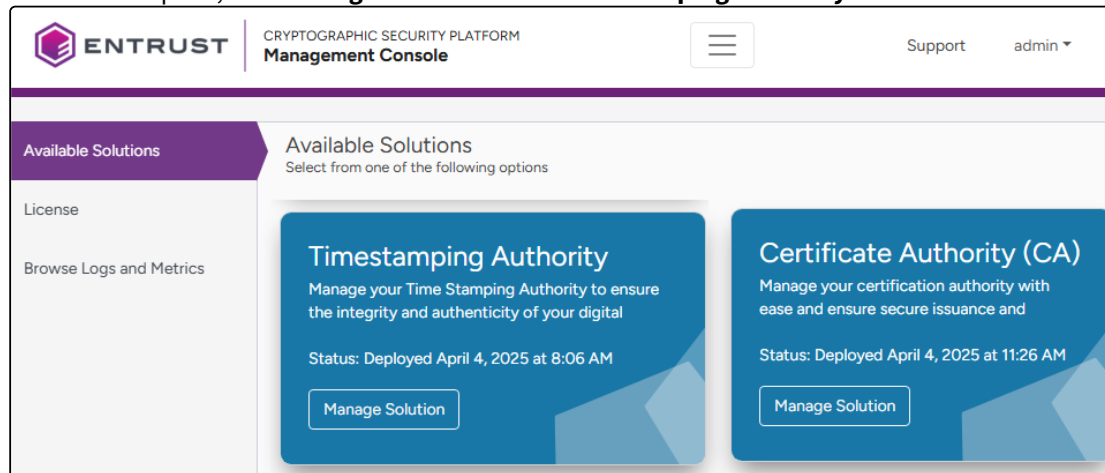
```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

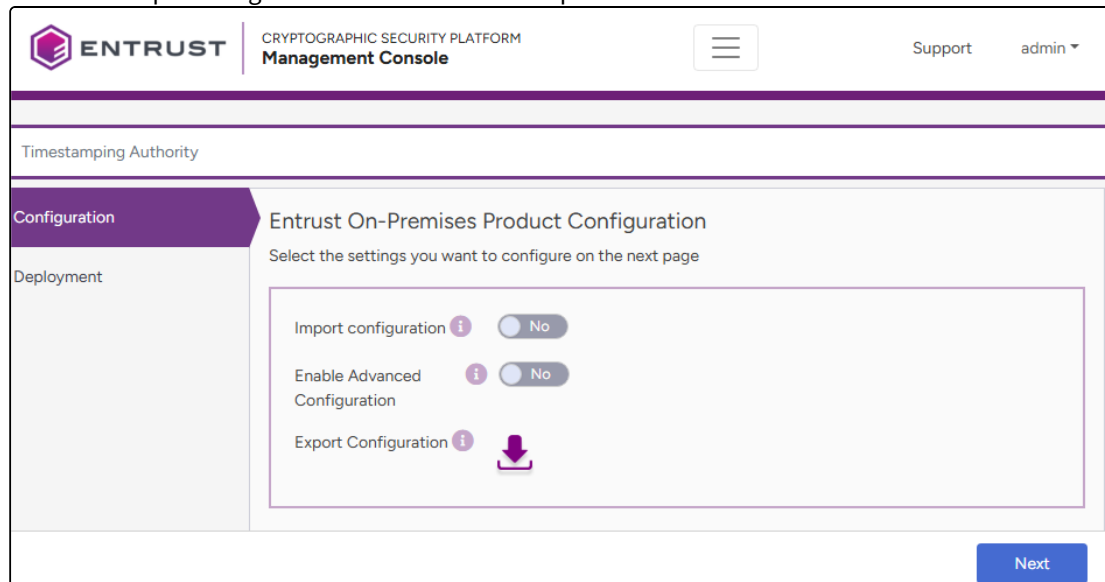
2. Log into the Management Console a user belonging to a role with Timestamping Authority management permissions – for example, the initial `admin` administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

- In the content pane, click **Manage Solution** under **Timestamping Authority**.



- Activate the **Import configuration** toggle switch if you want to import configuration settings from a file, such as a sample configuration file included in the product release.



- Active the **Enable Advanced Configuration** if you want to configure the full set of configuration parameters supported by the solution.
- Click **Next**.
- Configure the solution settings described in the following sections.
 - [Tsa issuers](#)
 - [Clock service](#)
 - [Tsa Server](#)
 - [Hsm](#)
- Click **Validate** to validate the configured settings.
- Correct any detected configuration error until the **Validate** option displays no warnings.
- Optionally, click the **Download** button to export the current configuration. You can later import this configuration using the already mentioned **Import configuration** toggle switch.
- Click **Submit** and wait while Cryptographic Security Platform uploads the configuration and any attached file, such as a P12 file with authentication credentials.
- Click **Deploy**.

Tsa issuers

Select the **TSA issuers** tab of the **Configuration** page to configure at least one timestamp issuer.

- [TST profile](#)
- [CA chain](#)
- [TSA certificate](#)
- [Log timestamp response](#)
- [Issuer ID](#)

Mandatory: Yes.

TST profile

Configure the timestamping policy for generating timestamp responses.

- [Accuracy](#)
- [Allowed hash algorithms](#)
- [Ordering](#)
- [Policy ID](#)
- [Qualified timestamp extension](#)
- [Serial number length](#)
- [Signature digest algorithm](#)

Mandatory: Yes.

Accuracy

The allowed deviation from the `genTime` generation time of the timestamp response.

Mandatory: No. When omitted, this optional value is not present in the `TSTInfo` response field.

Allowed hash algorithms

The list of allowed hash algorithms. Supported values are:

- sha1
- sha224
- sha256
- sha384
- sha512



The Timestamping Authority solution will not timestamp data hashed with other algorithms.

Mandatory: No. This optional value defaults to the following list.

- sha224
- sha256
- sha384
- sha512

Ordering

Check to sort timestamps based on the `genTime` field, regardless of the accuracy of the `genTime` generation time in the timestamp response.

Mandatory: No. This option is disabled by default.

Policy ID

The identifier of the timestamping policy.

Mandatory: Yes.

Qualified timestamp extension

Check this box to add a `qcStatements` statement with the `esi4-qtstStatement-1` extension as required for qualified electronic timestamps.

Mandatory: No. This optional value defaults to `false` (unchecked).


Serial number length

The allowed length in bytes of the timestamp serial numbers, as a number in the 8-20 range.

Mandatory: No. This optional value defaults to 8 bytes.

Signature digest algorithm


The algorithm for hashing the timestamped data.

 The selected algorithm must be included in the **Allowed hash algorithms** list.

Mandatory: No. This optional value defaults to "sha256".

CA chain

Click **Select Files** to import the Certificate Authority certificates that will be included in the timestamp responses.

 Each certificate file must contain a certificate in PEM format and Base64 encoding.

Mandatory: Yes.

TSA certificate

The certificate described in [Generating a timestamping certificate and key pair](#). Click **Select Files** to import this certificate from file.

 Each certificate file must contain a certificate in PEM format and Base64 encoding.

Mandatory: Yes.

Log timestamp response

Check this box to log the encoded timestamp response under the following tag.

`tsa-timestampresponse-encoded`

Mandatory: No. This optional value defaults to `false` (unchecked).

Issuer ID

A user-defined identifier for the configured timestamp issuer. The clients of this issuer will send requests to the following URL.

```
http://<host>/tsa/<issuerID>
```

Mandatory: Yes.

Clock service

Select the **Clock server** tab of the **Configuration** page to configure the clock service settings.

- [Connection timeout](#)
- [Poll interval](#)
- [Maximum allowed error](#)

Mandatory: Yes.

Connection timeout

The maximum period allowed for establishing a connection with the `chrony` client.

Mandatory: No. This optional value defaults to 1 second.

Poll interval

The period between successive connections to the `chrony` client for checking the clock health.

Mandatory: Yes.

Maximum allowed error

The maximum allowed time difference between the Timestamping Authority clock and the `chrony` client. When the difference exceeds the selected period, The Timestamping Authority solution:

1. Considers that the clock is not valid (bad clock).
2. Logs an error when trying to timestamp data.

See below for the main fields on the recorded error log.

Error log field	Value
level	info
msg	ProcessTimeStampRequest.Failed
tsa-log.tsa-pkistatus-string	TimeNotAvailableTSError
cause.cause.cause.msg	BadClock

Mandatory: Yes.

Tsa Server


Select the **Tsa server** tab of the **Configuration** page to configure the below timestamping server settings.

- [Keep alive](#)
- [Listen limit](#)
- [Graceful timeout](#)
- [Max body bytes](#)
- [Max header bytes](#)
- [Idle timeout](#)
- [Write timeout](#)
- [Read timeout](#)

Mandatory: No.

Keep alive

The TCP keep-alive timeouts on accepted connections.

 When this period expires, the server prunes dead TCP connections.

Mandatory: No. This optional value defaults to 3 minutes.

Listen limit

The maximum number of outstanding requests.

Mandatory: No. This optional value defaults to 0 (no limit).

Graceful timeout

The grace period before shutting down the server.

Mandatory: No. This optional value defaults to 15 seconds.

Max body bytes

The maximum number of bytes allowed in the request body.

Mandatory: No. This optional value defaults to 8192.

Max header bytes

The maximum number of bytes allowed for keys and values in the request header, including the request line.

Mandatory: No. This optional value defaults to 1024.

Idle timeout

The maximum period to wait for the next request when keep-alives are enabled.

Mandatory: No. This optional value defaults to 10 seconds.

Write timeout

The maximum period allowed for writing a response. When this period expires, the request gets the following response.

```
Code=503,Reason=Service Unavailable
```

Mandatory: No. This optional value defaults to 60 seconds.

Read timeout

The maximum allowed period for reading an entire request, including the body. When this period expires, the request gets the following response.

```
Code=503,Reason=Service Unavailable
```

Mandatory: No. This optional value defaults to 60 seconds.

Hsm

Select the **Hsm** tab of the **Configuration** page to configure the connection with the HSM (Hardware Security Module).

- [Number of sessions](#)
- [HSM PIN](#)
- [Token Label](#)
- [Vendor](#)

Mandatory: Yes.

Number of sessions

The maximum number of concurrent PKCS #11 sessions on the HSM.

Mandatory: When the **Vendor** value is `nshield` or `thales`.

HSM PIN

The PIN (Personal Identification Number) of the HSM (Hardware Security Module).

Mandatory: When the **Vendor** value is `nshield` or `thales`.

Token Label


The label of the HSM token that contains the private key for timestamp signing.

Mandatory: When the **Vendor** value is `nshield` or `thales`.

Vendor

The vendor of the security module.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

 It is recommended to select a Hardware Security Module (HSM).

Mandatory: Yes.

Testing the timestamping service

To test the Timestamping Authority service, you can send timestamp requests as follows.

- [Creating the timestamp request](#)
- [Validating the timestamp request](#)
- [Sending the request to Timestamping Authority](#)
- [Parsing the timestamp response](#)
- [Verifying the response against the data](#)
- [Verifying the response against the request](#)

Creating the timestamp request

Create the timestamp request. For example:

```
openssl ts -query -data data.txt -sha256 -cert -out tsareq.tsq
```

See below for a description of each option.

Parameter	Description
-data <file>	Create a timestamp request for the data in the <code><file></code> file.
-sha256	Use the SHA256 algorithm to hash the data.
-cert	Add to the response the certificate described in Issuing a timestamping certificate .
-out <file>	Save the generated request in the <code><file></code> file.

The command saves the request in the `tsareq.tsq` file.

Validating the timestamp request

Validate the generated request.

```
openssl ts -query -in tsareq.tsq -text
```

Sending the request to Timestamping Authority

Send the timestamp request to Timestamping Authority. For example:

```
curl -H "Content-Type: application/timestamp-query" -H "Accept: application/timestamp-reply" --data-binary "@tsareq.tsq" http://<machine>/tsa/<issuerID> --output tsarep.tsr
```

Where:

- `<machine>` is the IP address or domain name of the Entrust Cryptographic Security Platform node hosting Timestamping Authority.
- `<issuerID>` is the value of the [Issuer ID](#) configuration parameter.

The command saves the response in the `tsarep.tsr` file.

Parsing the timestamp response

Parse the timestamp response to validate the format.

```
openssl ts -reply -in tsarep.tsr -text
```

Verifying the response against the data

Verify the timestamp response against the original data.

```
openssl ts -verify -in tsarep.tsr -CAfile ca.pem -data data.txt
```

Where `ca.pem` is the Certificate Authority certificate for validating the certificate described in [Issuing a timestamping certificate](#).

Verifying the response against the request

Verify the response against the timestamp request.

```
openssl ts -verify -in tsarep.tsr -CAfile ca.pem -queryfile tsareq.tsq
```

11 Managing Validation Authority

See below for configuring, deploying, and administering the Validation Authority solution.

- [CSP Validation Authority overview](#)
- [Loading the HSM configuration on Validation Authority](#)
- [Initializing the Validation Authority database](#)
- [Configuring a certificate information source for Validation Authority](#)
- [Generating a VA certificate and key pair](#)
- [Configuring Entrust Certificate Authority for CSP Validation Authority](#)
- [Configuring and deploying Entrust Validation Authority](#)
- [Testing the OCSP Responder](#)

CSP Validation Authority overview

The Validation Authority solution responds to OCSP requests on the validation status of the certificates issued by a Certificate Authority. To respond to these requests, the Validation Authority solution connects with different components.


- [OCSP client](#)
- [Certificate Authority](#)
- [Certificate information source](#)
- [Hardware Security Module](#)
- [Database](#)

OCSP client

Multiple clients send OCSP requests to the OCSP Responder service of the Validation Authority solution.

Certificate Authority

The Validation Authority solution checks the status of certificates issued by one or multiple Certificate Authorities (CAs).

 As explained in [Managing Certificate Authority](#), the Certificate Authority solution provides built-in CRL and OCSP services. Therefore, you do not need an Validation Authority for CAs created with the Certificate Authority solution.


Certificate information source

Through Entrust CA Gateway, Entrust solutions obtain a direct feed of issued certificates from each supported Certificate Authority (CA). See the following table for the CA Gateway deployment required by each type of CA.

CA type	CA Gateway deployment
Certificate Authority running on Cryptographic Security Platform	Create a Certificate Authority instance, as explained in Managing Certificate Authority , and select the built-in CA Gateway service of this CA.

CA type	CA Gateway deployment
External Certificate Authority	Start up the Entrust CA Gateway solution and connect it with the external CA as explained Managing CA Gateway .

Alternatively, the Validation Authority solution can obtain revocation information from a full or "combined" CRL published in an LDAP or HTTP server.

 Validation Authority does not support partitioned CRLs.

Hardware Security Module


A Hardware Security Module (HSM) manages one or several OCSP signing keys.

Database

A database stores the status of the certificates.

Loading the HSM configuration on Validation Authority

See in following table the required commands for loading the configuration of a Hardware Security Module meeting the [HSM requirements](#).

 Skip this step if you use software cryptography (not recommended).

HSM	Command	Additional steps
Entrust nShield HSM	evactl import-nshield	See Adminitrating nShield HSM integration
Thales HSM	evactl import-thales	—

Initializing the Validation Authority database

Create an external database meeting the [Database requirements](#), and initialize this database as explained in the following sections.

- [Running the Validation Authority database scripts](#)
- [Setting the variables of the Validation Authority database scripts](#)
- [Downloading the Validation Authority database scripts](#)

Running the Validation Authority database scripts

See below for creating the Validation Authority database in the DBMS of your choice.

- [Creating the database on Oracle](#)
- [Creating the database on PostgreSQL](#)

- [Creating the database on SQL Server](#)

i The syntax of the below commands assumes a Linux operating system. Running these commands on a Windows machine may require a different syntax – for example, evaluating the `<var>` variables with the `%<var>%` syntax.

Creating the database on Oracle

Run the `certstatus_initial_schema.sql` and `metadata_initial_schema.sql` scripts to create the database objects on Oracle.

```
sqlplus "$USERNAME/$PASSWORD@tcp://$HOSTNAME/$DBNAME" @./  
certstatus_initial_schema.sql  
sqlplus "$USERNAME/$PASSWORD@tcp://$HOSTNAME/$DBNAME" @./metadata_initial_schema.sql
```

Run the `create_users.sql` script to create the database users on Oracle.

```
sqlplus "$USERNAME/$PASSWORD@tcp://$HOSTNAME/$DBNAME" @./create_users.sql $USERNAME  
$STATUSFEEDER_DB_USER $STATUSFEEDER_DB_PASSWORD $OCSPRESPONDER_DB_USER  
$OCSPRESPONDER_DB_PASSWORD
```

Creating the database on PostgreSQL

Run the `certstatus_initial_schema.sql` and `metadata_initial_schema.sql` scripts to create the database objects on PostgreSQL.

```
PGPASSWORD=$PASSWORD psql -d $DBNAME -U $USERNAME -h $HOSTNAME -v "ON_ERROR_STOP=1"  
-f ./certstatus_initial_schema.sql  
PGPASSWORD=$PASSWORD psql -d $DBNAME -U $USERNAME -h $HOSTNAME -v "ON_ERROR_STOP=1"  
-f ./metadata_initial_schema.sql
```

Run the `create_users.sql` script to create the database users on PostgreSQL.

```
PGPASSWORD=$PASSWORD psql -d $DBNAME -U $USERNAME -h $HOSTNAME \  
-v STATUSFEEDER_DB_USER=$STATUSFEEDER_DB_USER \  
-v OCSPRESPONDER_DB_USER=$OCSPRESPONDER_DB_USER \  
-v STATUSFEEDER_DB_PASSWORD=$STATUSFEEDER_DB_PASSWORD \  
-v OCSPRESPONDER_DB_PASSWORD=$OCSPRESPONDER_DB_PASSWORD \  
-v "ON_ERROR_STOP=1" -f ./create_users.sql
```

Creating the database on SQL Server

Run the `certstatus_initial_schema.sql` and `metadata_initial_schema.sql` scripts to create the database objects on SQL Server.

```
sqlcmd -S "$HOSTNAME" -U "$USERNAME" -P $PASSWORD -v DBNAME="$DBNAME" -i ./
certstatus_initial_schema.sql
sqlcmd -S "$HOSTNAME" -U "$USERNAME" -P $PASSWORD -v DBNAME="$DBNAME" -i ./
metadata_initial_schema.sql
```

Run the `create_users.sql` script to create the database users on SQL Server.

```
sqlcmd \
-S "$HOSTNAME" -U "$USERNAME" -P $PASSWORD \
-v STATUSFEEDER_DB_USER="$STATUSFEEDER_DB_USER" \
-v OCSPRESPONDER_DB_USER="$OCSPRESPONDER_DB_USER" \
-v STATUSFEEDER_DB_PASSWORD="$STATUSFEEDER_DB_PASSWORD" \
-v OCSPRESPONDER_DB_PASSWORD="$OCSPRESPONDER_DB_PASSWORD" \
-v DBNAME="$DBNAME" \
-i ./create_users.sql
```

Setting the variables of the Validation Authority database scripts

To run the database scripts, you will need to provide the following values, either in the execution command line or as environment variables.

Variable	Value
DBNAME	The database name.
HOSTNAME	The name of the host to connect to.
USERNAME	The name of a DBMS user with permission to create tables, create users, and grant user permissions.
PASSWORD	The password of the database user.
OCSPRESPONDER_DB_PASSWORD	The password of the OCSP Responder user with Read permissions on the certStatus and metadata tables.
OCSPRESPONDER_DB_USER	The name of the OCSP Responder user with Read permissions on the certStatus and metadata tables.
STATUSFEEDER_DB_PASSWORD	The password of the Status Feeder user with Read and Write permissions on the certStatus and metadata tables.
STATUSFEEDER_DB_USER	The name of the Status Feeder user with Read and Write permissions on the certStatus and metadata tables.

Downloading the Validation Authority database scripts

See below for instructions on downloading the Validation Authority database scripts.

To download the Validation Authority database scripts


1. Log in to the secure trustedcare.entrust.com portal with your customer credentials.
2. Select the **PRODUCTS** tab.
3. Click **Cryptographic Security Platform**.
4. Select the product version.
5. In the **SOFTWARE DOWNLOADS** tab, download the compressed file containing the database scripts.
6. Extract the contents of the compressed file. In Linux operating system, run:

```
tar -xvf eva-database-scripts.tar.gz
```

Configuring a certificate information source for Validation Authority

You need one of the following sources of information on the certificate validity status.

- [CA Gateway for Validation Authority](#)
- [Certificate Revocation List](#)

 When [Configuring and deploying Entrust Validation Authority](#), the certificate information source is selected using the [Certificates Source](#) parameter.

CA Gateway for Validation Authority


When using CA Gateway as the source of certificate information, perform the steps below for Validation Authority to authenticate on CA Gateway.

- [Generating the CA Gateway client PKCS #12](#)
- [Configuring the client PKCS #12 in CA Gateway](#)
- [Importing the CA Gateway client PKCS #12 in Validation Authority](#)

Generating the CA Gateway client PKCS #12

Use your CA to generate a PKCS #12 containing:

- A TLS client certificate for Validation Authority to authenticate on CA Gateway.
- The private key of the certificate.

 The PKCS #12 cannot contain more than one client certificate.

To generate the PKCS #12 with Entrust Certificate Authority:

- Select the **1-Key-Pair User (1-Key-Pair User with Dual Usage Key)** certificate type to generate a PKCS #12 with a single client certificate.
- Check the **Export PKCS #12** and **All exportable** options so the user can export the generated PKCS #12.

 See the Entrust Certificate Authority documentation for more detailed information.

Configuring the client PKCS #12 in CA Gateway

Configure the CA Gateway client PKCS #12 in CA Gateway.

To configure the client PKCS #12 in CA Gateway

1. Access the CA Gateway configuration page as explained in [Configuring and deploying CA Gateway](#).
2. Select the [Server](#) tab.
3. Click **Select Files** under [Trust Store](#) and upload a PKCS #12 file containing:
 - The CA certificates already included in the previous Trust Store (if any).
 - The certificate of the CA that issued the CA Gateway client PKCS #12.
4. Select the [Clients](#) tab.
5. In the [Subject DN](#) settings of a client, enter the distinguished name (DN) of the CA Gateway client certificate.
6. Make the changes effective and redeploy CA Gateway.

Importing the CA Gateway client PKCS #12 in Validation Authority

Run the `evactl import-p12` command to import the CA Gateway client PKCS #12 – for example:

```
$ sudo evactl import-p12 -f eva-cagw.p12
```

Certificate Revocation List

Entrust Validation Authority supports obtaining certificate validity status information from a CRL (Certificate Revocation List) with the following configuration.

CRL setting	Supported value
CRL Encoding	DER
CRL host	HTTP or LDAP server
CRL type	Full or "combined" CRL (because Entrust Validation Authority does not support partitioned CRLs).
CRL issuer	A CA of any manufacturer.

Generating a VA certificate and key pair

Each CA configured in Validation Authority needs a certificate to sign OCSP responses. You can:

- Use a different certificate for every CA.
- Share a certificate among multiple CAs.

Perform the steps below for every certificate you want to use.

- [Generating a VA key pair](#)
- [Issuing a VA certificate](#)

Generating a VA key pair

To generate a VA key pair, run the [evactl create-key](#) command in any Cryptographic Security Platform node. The command will output a CSR that you can use to generate the VA certificate – for example:

```
$ sudo evactl create-key -k RSA2048 -s "CN=OCSP Server" -o /tmp/certreq.txt -t mytoken -v thales
Created key with id 4a00a4617d1afd5ad626955132dd0d396a69ed24
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIICqDCCAACAQAwMzExMC8GA1UEAxMoNGEwMGE0NjE3ZDFhZmQ1YWQ2MjY5NTUx
...
etTv+pac+nJKW8fw
-----END CERTIFICATE REQUEST-----
```

i As explained in [evactl create-csr](#), you can create a certificate request for a key that already exists on the HSM.

Issuing a VA certificate

Use your CA to process the CSR obtained in [Generating a VA key pair](#) and issue a certificate with the following extension values.

Extension	Value
Key Usage	digitalSignature
Extended Key Usage	OCSPSigning

See below for how to issue this certificate with Entrust products.

- [Issuing an OCSP responder VA certificate with Entrust Certificate Authority](#)
- [Issuing an OCSP responder VA certificate with the CSP Certificate Authority solution](#)

Issuing an OCSP responder VA certificate with Entrust Certificate Authority

If you are using Entrust Certificate Authority, you can run one of the following applications to issue the VA certificate:


- The CSR Enrollment Services (CSRES) provided by the Entrust Administration Services.
- The Profile Creation Utility included in products such as Entrust Administration Services or available as a separate download with Entrust CA Gateway.

i See [Configuring Entrust Certificate Authority for CSP Validation Authority](#) for how to configure Entrust Certificate Authority.

Issuing an OCSP responder VA certificate with the CSP Certificate Authority solution

Follow the steps below to issue an OCSP responder VA certificate using the Certificate Authority solution provided by Cryptographic Security Platform.

- [Creating a Certificate Authority to issue OCSP responder VA certificates](#)
- [Creating a timestamping certificate request](#)
- [Processing the timestamping certificate request](#)

 The Certificate Authority solution provides built-in CRL and OCSP capabilities. Therefore, you do not need the Validation Authority to check the validity status of certificates issued by CA instances managed by the Certificate Authority solution.

Creating a Certificate Authority to issue OCSP responder VA certificates

Follow the steps described in [Managing Certificate Authority](#) to create:

- A root Certificate Authority.
- An issuing Certificate Authority with at least one signature profile – for example, the `wstep-digital-signature` profile described in [Active Directory \(WSTEP\) certificate profiles](#).

Creating a timestamping certificate request

Create a CA Gateway certificate enrollment request – for example:

```
1  {
2    "csr": "MIIDVzCCAb8...",
3    "profileId": "wstep-digital-signature",
4    "requiredFormat": {
5      "format": "X509"
6    },
7    "optionalCertificateRequestDetails": {
8      "extensions": [
9        {
10         "oid": "2.5.29.37",
11         "critical": true,
12         "value": "1.3.6.1.5.5.7.3.9"
13       }
14     ],
15     "validity_period": "2024-11-06T13:00Z/2026-07-06T13:00:00Z"
16   }
17 }
```

See below for the values required by each request field.

Field	Line	Value
csr	2	The base64-encoded Certificate Signing Request previously generated in Generating a VA key pair as a single line.

Field	Line	Value
extensions	8	The same fields and values as in the above example (to select the OCSP signing extended key usage).
validity_period	15	The validity period for the issued certificate. The expiry date in this period cannot exceed the expiry date of the issuing CA certificate.

Processing the timestamping certificate request

See below for processing the timestamping certificate request and obtaining the issued certificate.

To process the timestamping certificate request

1. Use a REST client to process the request as explained in [Issuing certificates with a REST client](#).
2. Edit the REST response and copy the base64-encoded string in the `body` field.
3. Save the string in a file with the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters – for example:

```
-----BEGIN CERTIFICATE-----
MIIICDCCBliAwIBAgITMwEf/Fvr7NDwanyeRAAAAR/8WzANBgkqhkiG9w0BAQwF
ADBdMQswCQYDVQQGEwJVUzEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcnF0aW9u
...
Ud085g==
-----END CERTIFICATE-----
```

4. Use this certificate file as the VA certificate when configuring the [OCSP Responder](#) settings.

Configuring Entrust Certificate Authority for CSP Validation Authority

Follow the steps below if Validation Authority will obtain certificate information from an Entrust CA Gateway instance integrated with Entrust Certificate Authority.

- [Adding the OCSP Server certificate type to Entrust Certificate Authority](#)
- [Configuring the CA Gateway administrator role in Entrust Certificate Authority](#)

Adding the OCSP Server certificate type to Entrust Certificate Authority

If not already added, add the OCSP Server (OCSP_1K) certificate type you will later use for [Generating a VA certificate and key pair](#).

i In the latest Entrust Certificate Authority 10.0.x releases, an OCSP Server (OCSP_1K) certificate type may already be predefined in the certificate specifications. This certificate type includes the proper certificate extensions for signing OCSP responses.

To add the OCSP Server certificate type to Entrust Certificate Authority

1. Log in to the Entrust Certificate Authority administration portal.
2. Select **File > Certificate Specifications > Export** and export the certificate specifications.

3. Open the certificate specifications file in a text editor.
4. Add the following lines to the `[Certificate Types]` section.

```
OCSP_1K=enterprise,OCSP server,OCSP server certificate -no directory entry
```

5. Add the following lines to the `[Extension Definitions]` section.

```
-----
;- Cert Type: OCSP_1K
;- This cert type needs to be mapped to cert def policy enforcing:
; - Certificate lifetime:
; - Exclude privateKeyUsagePeriod: 1
; - Exclude basicConstraints: 1
; - Exclude entrustVersInfo: 1
; - Exclude CDP: 1
;-----
[OCSP_1K Certificate Definitions]
1=Verification
;
[OCSP_1K Verification Extensions]
;Key Usage: Digital Signature
keyusage=2.5.29.15,n,m,BitString,1
;Extended Key Usage: OCSP Signing
extkeyusage=2.5.29.37,n,o,SeqOfObjectIdentifier,1.3.6.1.5.5.7.3.9
ocspnocheck=1.3.6.1.5.5.7.48.1.5,n,o,DER,0500
; Certificate Policies: DER encode the <Policy-OID>
; Policy-OID=<Policy-OID> - This OID is optional, the customer might not have a
policy OID.
;certificatepolicies=2.5.29.32,n,o,DER,<DER encoded value of the above OID>
; AuthorityInfo Access:
; - Issuing CA certificate URL: <CA-Cert-HTTP-URL>
;aia=1.3.6.1.5.5.7.1.1,n,m,DER,<DER encoded value of the above URL>
;
```

6. (Optional.) You can add a `certificatePolicies` extension to the certificate type. The `certificatePolicies` extension contains policy information, such as how your CA operates and the intended purpose of the issued certificate. Typically, different certificate policies will relate to different applications which may use the certified key. The Certificate Policies extension contains a sequence of one or more policy information terms. Each policy information term consists of an object identifier (OID) and optional qualifiers. In an end entity certificate, the policy information terms indicate the policy under which the certificate has been issued, and the purposes for which the certificate may be used. To add a `certificatePolicies` extension to the certificate type:
 - a. DER-encode a list of one or more policy OIDs. Entrust provides an `entDerEncoder` utility for Entrust Certificate Authority that you can use to DER-encode data for certificate extensions. For instructions about using the `entDerEncoder` utility, see the Entrust Certificate Authority documentation.
 - b. Uncomment the `certificatepolicies=` entry and replace `<DER encoded value of the above OID>` with the DER-encoded value you obtained in the previous step.
7. (Optional.) You can add an `authorityInformationAccess` extension to the certificate type. The Authority Information Access (AIA) certificate extension indicates how to access information and

services for the CA that issued the certificate. Information and services may include online validation services and CA policy data. To add a certificatePolicies extension to the certificate type:

- a. DER-encode the HTTP URL of the CA certificate. Entrust provides an entDerEncoder utility for Entrust Certificate Authority that you can use to DER-encode data for certificate extensions. For instructions about using the entDerEncoder utility, see the Entrust Certificate Authority documentation.
 - b. Uncomment the `aia=` entry and replace `<DER encoded value of the above URL>` with the DER-encoded value you obtained in the previous step.
8. Add the following lines to the `[Advanced Settings]` section.


```
[OCSP_1K Advanced]
noBasicConstraints=1
noPrivateKeyUsage=1
noEntrustVersInfo=1
;cdpLdapDnLast=1
noUserInDirectory=1
noCRLDistPoints=1
```

9. Save and close the file.
10. Select **File > Certificate Specifications > Import** and import the certificate specifications back into Entrust Certificate Authority.
11. In the tree view, select **Security Policy > Certificate Categories > Enterprise > Certificate Types > OCSP Responder (OCSP Responder Certificates) > Verification**.
12. Click the **Certificate definition Policy** field, and then select **Verification_p10 Policy** from the drop-down list.

Configuring the CA Gateway administrator role in Entrust Certificate Authority


When configuring a role for the Entrust CA Gateway administrator in Entrust Certificate Authority, make sure the role has permissions to administer:

- All roles
- All certificate types

 If the Entrust CA Gateway administrator role does not have enough permission, Validation Authority will only receive information on a subset of the issued certificates.

Configuring and deploying Entrust Validation Authority

See below for configuring and deploying Validation Authority with the Management Console.

 Repeat the following steps each time a configuration update is required. Do not forget to click **Deploy** to make the changes effective.

To configure and deploy Validation Authority with the Management Console

1. Open the following URL in a Web browser.

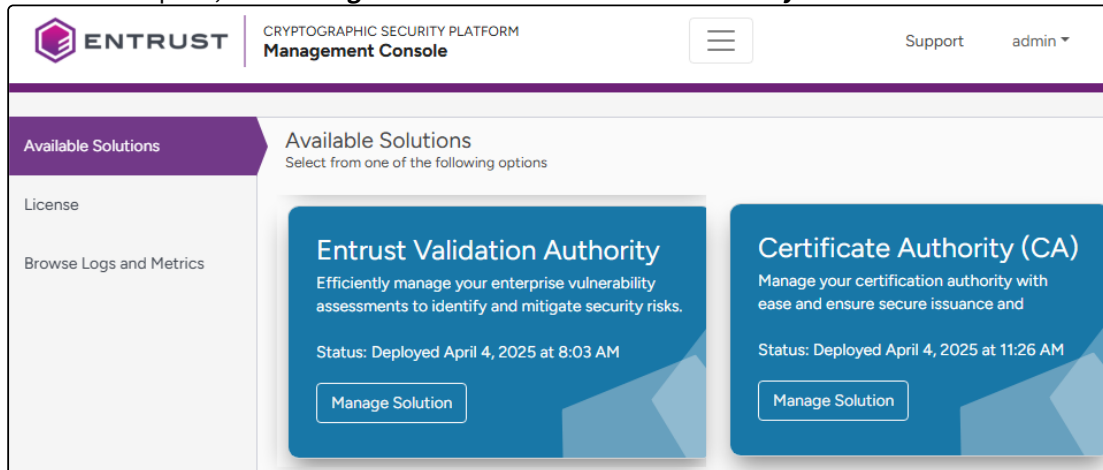
```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

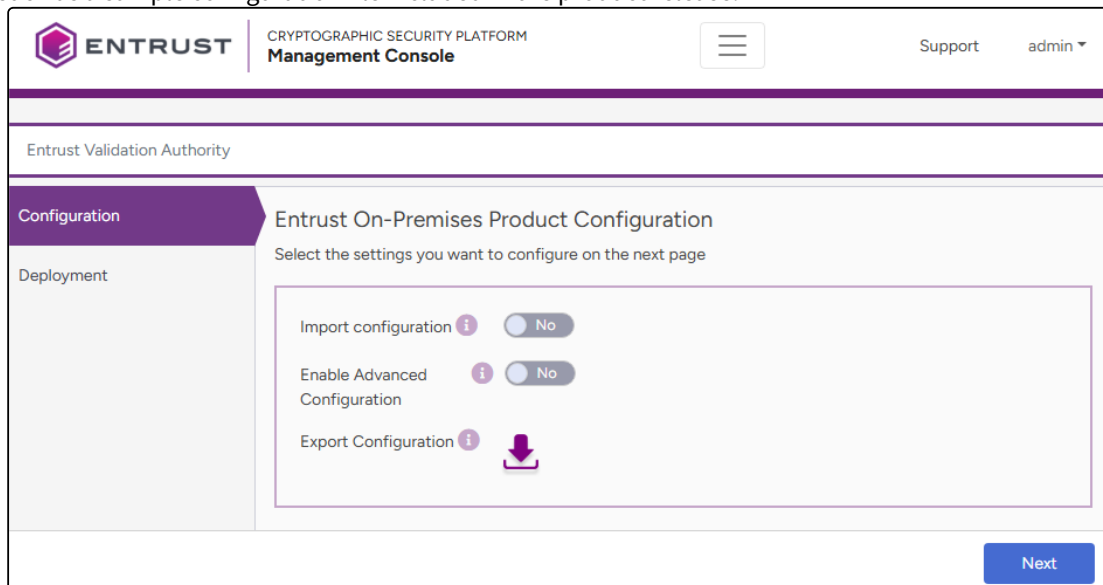
- Log into the Management Console a user belonging to a role with Validation Authority management permissions – for example, the initial `admin` administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

- In the content pane, click **Manage Solution** under **Validation Authority**.



- Activate the **Import configuration** toggle switch if you want to import configuration settings from a file, such as a sample configuration file included in the product release.



- Active the **Enable Advanced Configuration** if you want to configure the full set of configuration parameters supported by the solution.
- Click **Next**.
- Configure the solution settings described in the following sections.
 - [Database](#)
 - [Hsm](#)
 - [OCSF Responder-Server](#)
 - [LDAP Servers](#)

- [Certificate Authorities](#)

8. Click **Validate** to validate the configured settings.
9. Correct any detected configuration error until the **Validate** option displays no warnings.
10. Optionally, click the **Download** button to export the current configuration. You can later import this configuration using the already mentioned **Import configuration** toggle switch.
11. Click **Submit** and wait while Cryptographic Security Platform uploads the configuration and any attached file, such as a P12 file with authentication credentials.
12. Click **Deploy**.

Database

Select the **Database** tab of the **Configuration** page to configure the database connection

- [Driver](#)
- [JDBC URL](#)
- [Host](#)
- [Port](#)
- [Database name](#)
- [OCSP Responder User](#)
- [OCSP Responder password](#)
- [Status Feeder User](#)
- [Status Feeder password](#)
- [Max connections](#)
- [Connection timeout](#)
- [SSL mode](#)
- [SSL validation certificate](#)

Mandatory: Yes

Driver

The driver for connecting to the database.

Driver	Database Management System
oracle	Oracle SQL
postgres	PostgreSQL
sqlserver	Microsoft SQL Server

 See [Database requirements](#) for the supported DBMS versions.

Mandatory: Yes.

JDBC URL

The JDBC URL to connect to the database when **Driver** is [oracle](#). For example, to connect with a database hosted in multiple Oracle nodes:

```
(DESCRIPTION=(ADDRESS_LIST=(LOAD_BALANCE=yes)(FAILOVER=on)(ADDRESS=(PROTOCOL=TCP)
(HOST=host1.domain.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=host2.domain.com)
(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=ServiceName)))
```

Do not include the following prefix in the parameter value:

```
jdbc:oracle:thin:@
```

Mandatory: database connection settings support the following combinations.

Driver	Database name	Host	Port	JDBC URL
oracle	✓	✓	✓	✗
oracle	✗	✗	✗	✓
postgres	✓	✓	✓	✗
sqlserver	✓	✓	✓	✗

⚠ Remove any unnecessary parameters.

Host

The IP address or hostname of the database host.

Mandatory: database connection settings support the following combinations.

Driver	Database name	Host	Port	JDBC URL
oracle	✓	✓	✓	✗
oracle	✗	✗	✗	✓
postgres	✓	✓	✓	✗
sqlserver	✓	✓	✓	✗

⚠ Remove any unnecessary parameters.

Port

The TCP port where the database listens.

Mandatory: database connection settings support the following combinations.

Driver	Database name	Host	Port	JDBC URL
oracle	✓	✓	✓	✗
oracle	✗	✗	✗	✓
postgres	✓	✓	✓	✗
sqlserver	✓	✓	✓	✗

⚠ Remove any unnecessary parameters.

Database name

The same value assigned to the `DBNAME` parameter when [Setting the variables of the Validation Authority database scripts](#).

Mandatory: database connection settings support the following combinations.

Driver	Database name	Host	Port	JDBC URL
oracle	✓	✓	✓	✗
oracle	✗	✗	✗	✓
postgres	✓	✓	✓	✗
sqlserver	✓	✓	✓	✗

⚠ Remove any unnecessary parameters.

OCSP Responder User

The same user identifier assigned to the `OCSPRESPONDER_DB_USER` parameter when [Setting the variables of the Validation Authority database scripts](#).

Mandatory: Yes.

OCSP Responder password

The same password assigned to the `OCSPRESPONDER_DB_PASSWORD` parameter when [Setting the variables of the Validation Authority database scripts](#).

Mandatory: Yes.

Status Feeder User

The same user identifier assigned to the `STATUSFEEDER_DB_USER` parameter when [Setting the variables of the Validation Authority database scripts](#).

Mandatory: Yes.

Status Feeder password

The same password assigned to the `STATUSFEEDER_DB_PASSWORD` parameter when [Setting the variables of the Validation Authority database scripts](#).

Mandatory: Yes.

Max connections

The number of maximum concurrent database connections. as an integer equal to or greater than 1.

✗ Since three internal services of Validation Authority utilize this value, the database must support at least three times the maximum concurrent connections set by this parameter.

Mandatory: Yes.

Connection timeout

The timeout for database connections.

Mandatory: No. This optional value defaults to 5 seconds.

SSL mode

✔ to enable SSL security in the database connection; ✗ otherwise.

✗ The ✗ option is for testing environments only.

Mandatory: Yes.

SSL validation certificate

The CA certificate for validating the database SSL certificate.

⚠ As explained in [Database SSL certificate](#), the SSL certificate for the database host must include the IP address or FQDN of the host.

Mandatory: When SSL mode is **enable**, and **Driver** is **postgres** or **sqlserver**. See the following table for details.

Driver	SSL mode	SSL validation certificate
postgres	enabled	Click Select Files to import a file containing this certificate in PEM format and Base64 encoding.
oracle	enabled	Use the Oracle utilities to set this certificate.
sqlserver	enabled	Click Select Files to import a file containing this certificate in PEM format and Base64 encoding.

Hsm

Select the **Hsm** tab of the **Configuration** page to configure the connection with the HSM (Hardware Security Module).


- [Vendor](#)
- [Token label](#)
- [HSM PIN](#)
- [Number of sessions](#)

Mandatory: Yes.

Vendor

The vendor of the security module.


Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

 It is recommended to select a Hardware Security Module (HSM).

Mandatory: Yes.

Token label

The label of the token that contains the private keys of the OCSP server certificate.

 See [Generating a VA certificate and key pair](#) for how to generate the OCSP server certificate keys.

Mandatory: When the **Vendor** value is `nshield` or `thales`.

HSM PIN

The PIN (Personal Identification Number) of the HSM (Hardware Security Module).

Mandatory: When the **Vendor** value is `nshield` or `thales`.

Number of sessions

The maximum number of concurrent PKCS #11 sessions on the HSM.

Mandatory: When the **Vendor** value is `nshield` or `thales`.

OCSP Responder-Server

Select the **OCSP Responder-Server** tab of the **Configuration** page to configure optional OCSP responder settings.

- [Read timeout](#)
- [Write timeout](#)
- [Idle timeout](#)
- [Max header bytes](#)
- [Max body bytes](#)
- [Graceful timeout](#)
- [Listen limit](#)
- [Keep alive](#)
- [Response Profile ID](#)
- [HTTP Error](#)
- [Retry Unknown Certificates](#)

Mandatory: No

Read timeout

The maximum allowed period for reading an entire request, including the body. When this period expires, the request gets the following response.

```
Code=503,Reason=Service Unavailable
```

Mandatory: No. This optional value defaults to 60 seconds.

Write timeout

The maximum period allowed for writing a response. When this period expires, the request gets the following response.

```
Code=503,Reason=Service Unavailable
```

Mandatory: No. This optional value defaults to 60 seconds.

Idle timeout

The maximum period to wait for the next request when keep-alives are enabled.

Mandatory: No. This optional value defaults to 10 seconds.

Max header bytes

The maximum number of bytes allowed for keys and values in the request header, including the request line.

Mandatory: No. This optional value defaults to 1024.

Max body bytes

The maximum number of bytes allowed in the request body.

Mandatory: No. This optional value defaults to 8192.

Graceful timeout

The grace period before shutting down the server.

Mandatory: No. This optional value defaults to 15 seconds.


Listen limit

The maximum number of outstanding requests.

Mandatory: No. This optional value defaults to 0 (no limit).

Keep alive

The TCP keep-alive timeouts on accepted connections.

 When this period expires, the server prunes dead TCP connections.

Mandatory: No. This optional value defaults to 3 minutes.



Response Profile ID



The identifier of the profile for generating OCSP responses.


Mandatory: No. This optional value defaults to the **basic** identifier of the only supported profile. This profile:

1. Sets `byKey` as responder identifier.
2. If present in the request, copies the `id-pkix-ocsp-nonce` extension value in the response.
3. Signs the response with the SHA-256 algorithm.

HTTP Error


The HTTP error returned in the OCSP response body for failed requests. See the table below for the value returned when enabling  or disabling  this parameter.


Request type		
Invalid request	HTTP 400	HTTP 200
Valid request that could not be processed	HTTP 404	HTTP 200

Mandatory: No. This optional value defaults to .

Retry Unknown Certificates

Retry fetching the status of certificates classified as unknown after the initial retrieval.


 This setting is only effective for certificate profiles that enable the **revokedIfUnknown** parameter.

Mandatory: No. This optional value defaults to .

LDAP Servers

In the **LDAP Servers** tab, click + LDAP Server and add the following parameters for each LDAP server.

- [URL](#)
- [Username](#)
- [Password](#)

 The identifier of each LDAP server must match an identifier configured in the [Certificate Revocation list in LDAP server](#) settings.

Mandatory: Yes.

URL

The URL of the LDAP server in the following format:

```
ldap://<host>:<port>
```

For example:

```
ldap://ldap.example.com:389
```

Mandatory: Yes.

Username

The user name for binding to the LDAP server.

Mandatory: When the binding to the LDAP server is not anonymous.

Password

The user password.

Mandatory: When the user requires password authentication.

Certificate Authorities

In the **Certificate Authorities** tab, add the following parameters for each Certificate Authority that will issue certificates validated by Validation Authority.

- [CA ID](#)
- [Certificates Source](#)
- [CSP CA Gateway](#)
- [Certificate Revocation List](#)
- [Certificate Revocation List in HTTP server](#)
- [Certificate Revocation list in LDAP server](#)
- [Serial number list HTTP](#)
- [OCSP Responder](#)

Mandatory: Yes.

CA ID

The identifier of the CA that issues the certificates. The values supported by this parameter depend on the [Certificates Source](#) value.

Certificates Source	CA ID
CAGW	The CA identifier in CA Gateway.
CRL	Any user-defined value that uniquely identifies the CA in Validation Authority.

Mandatory: Yes.

Certificates Source

The source informing on the validity status of the issued certificates.

Value	Source
CAGW	An instance of Entrust CA Gateway.
CRL	A CRL (Certificate Revocation List) published on an HTTP or LDAP server.

Before changing this parameter value on a deployed Validation Authority:

1. Stop the solution with the [evactl stop](#) command.
2. Remove all the database records related to the CA.
3. Restart the solution with the [clusterctl deploy](#) command or the management console of Cryptographic Security Platform.

Mandatory: Yes.

CSP CA Gateway

CA Gateway configuration parameters.

- [Push by serial](#)
- [TLS CA certificate](#)
- [TLS client certificate](#)

- [Timeout](#)
- [Batch Size](#)
- [Wait on error duration](#)
- [Wait to pull certs duration](#)
- [URL](#)

Mandatory: When [Certificates Source](#) is **CAGW**.

Push by serial


The certificate information pushed into the Validation Authority database.

- Check this box to push the certificate serial number
- Uncheck this box to push the whole DER encoding of the certificate

Mandatory: No. This optional value defaults to `false` (unchecked).

TLS CA certificate

The CA certificate for validating the CA Gateway TLS server certificate. Click **Select Files** to import this certificate from file.


 Each certificate file must contain a certificate in PEM format and Base64 encoding.

Mandatory: Yes.

TLS client certificate

The identifier of the client CA Gateway certificate described in [CA Gateway for Validation Authority](#).

Mandatory: No. This optional parameter defaults to the latest client certificate imported with the `evactl import-p12` command.

 Run the `evactl list-certs` command to list the available certificates and the latest one imported.

Timeout

The timeout for connections with the CA Gateway server. When a connection attempt with the CA Gateway server exceeds this period:

1. The request fails.
2. Validation Authority tries another connection after the **Wait on error duration** period selected in [CSP CA Gateway](#).

Mandatory: No. This optional value defaults to "5s".

Batch Size

The maximum number of certificates to retrieve in every request to CA Gateway. Select an integer value starting from 1.

 The `cagw/v1/certificate-authorities/<caid>/certificate-events` endpoint of CA Gateway must support the selected value.

Mandatory: No. This optional value defaults to 50.


Wait on error duration

The waiting time before retrying a failed connection with CA Gateway or the Status Feeder internal service.

Mandatory: No. This optional value defaults to "5s".

Wait to pull certs duration

The waiting time for Validation Authority while not receiving new events. When this period expires, Validation Authority sends a new request to CA Gateway.

 When enabling the **Retry Unknown Certificates** setting in the [OCSP Responder-Server](#) tab, this value must be less than or equal to **15s**.

Mandatory: Yes.

URL

The URL of the CA Gateway server. For example:

```
https://127.0.0.1/cagw
```

Mandatory: Yes.




Certificate Revocation List

Configure the following Certificate Revocation List (CRL) configuration parameters.

- [Use SN Lists](#)
- [CRL Host Server](#)
- [CRL warning time](#)
- [Wait on error duration](#)
- [Wait to pull certs duration](#)

Mandatory: When [Certificates Source](#) is **CRL**.

Use SN Lists

 to use certificate serial number lists,  otherwise. Set this value to  when selecting one of the following profile identifiers in the [OCSP Responder](#) tab.

- SNListProfile
- SNListProfileWithArchiveCutOff

Validation Authority will pull a serial number list and return the following status for certificates.

Certificate status	The certificate is in the CRL	The certificate is in the SNL
good		
revoked		
unknown		

Mandatory: Yes.

CRL Host Server

The type of server hosting the CRL.

- HTTP
- LDAP

Mandatory: Yes.

CRL warning time

The period during which to enable the expiration warning for the last processed CRL. When the time remaining before the CRL expiration is shorter than this parameter value, the [CRLExpirationWarning](#) metric is set to 1.

Mandatory: No. This optional value defaults to 4 hours.

Wait on error duration

The waiting time before retrying a failed connection with the CRL server, the Status Feeder internal service or the serial number list server.


Mandatory: No. This optional value defaults to "5s".

Wait to pull certs duration

The period between:

- The last upload of the CRL data into the database.
- The next request to the CRL server.

When **Use SN Lists** is , Validation Authority will pull the CRL and the serial number list.

 When enabling the **Retry Unknown Certificates** setting in the [OCSP Responder-Server](#) tab, this value must be less than or equal to [15s](#).

Mandatory: Yes.

Certificate Revocation List in HTTP server

Configuration parameters of the HTTP server hosting the CRL.

- [Connection timeout](#)
- [CRL HTTP URL](#)

Mandatory: When [CRL Host Server](#) is **HTTP**.

Connection timeout

The timeout for connections with the CRL server. When the connection attempt exceeds this value:

1. The request fails.
2. Validation Authority tries another connection after the **Wait on error duration** period selected in [CSP CA Gateway](#).

Mandatory: No. This optional value defaults to 5 seconds.

CRL HTTP URL

The URL of a CRL hosted in an HTTP server – for example:

```
http://127.0.0.1/crl.crl
```

Mandatory: Yes.

Certificate Revocation list in LDAP server

Configuration parameters of the LDAP server hosting the CRL.

- [CRL Attribute Name](#)
- [CRL Entry Distinguished Name](#)
- [Connection timeout](#)
- [LDAP Server ID](#)

Mandatory: When [CRL Host Server](#) is **LDAP**.

CRL Attribute Name

The name of the attribute that contains the CRL in the corresponding entry of the LDAP server.

Mandatory: No. This optional parameter defaults to:

```
certificateRevocationList;binary
```

CRL Entry Distinguished Name

The Distinguished Name of the entry that contains the CRL in the LDAP server.

Mandatory: Yes.

Connection timeout

The timeout for connections with the CRL server. When the connection attempt exceeds this value:

1. The request fails.
2. Validation Authority tries another connection after the **Wait on error duration** period selected in [CSP CA Gateway](#).

Mandatory: No. This optional value defaults to 5 seconds.

LDAP Server ID

The identifier of the LDAP server.

Mandatory: Yes.

Serial number list HTTP

The configuration settings of the certificate serial number list hosted in an HTTP server.

- [Connection timeout](#)
- [Serial Number list URL](#)

Connection timeout

The timeout for connections with the HTTP server that hosts a list containing the serial numbers of all certificates issued by the CA. When the connection attempt exceeds this value:

1. The request fails.
2. Validation Authority tries another connection after the **Wait on error duration** period selected in [CSP CA Gateway](#).

Mandatory: No. This optional value defaults to 5 seconds.

Serial Number list URL

The URL of a file containing the serial numbers of all certificates issued by the CA.

```
http://<host>[:<port>]/<file>
```

Where:

- **<host>** is the IP address or domain name of an HTTP server host.
- **<port>** is the port where the HTTP server listens in the host. Defaults to 80.
- **<file>** is the server path to a plain text file containing serial numbers, separated with newlines – such as:

```
00B289EFB35CB7DB0DD62F298BEF422DC1
00B28A0F6293B6F436845E2CE0B62D6E73
00B28A28E5E48BDC06C16737CF8648D2FF
00B28A3A7BB7DF5D8D1B1F61BCD612892F
00B28A3AC06981CD9B74474E1C5CC814B9
00B28A50BD25A8FAA1504F3C9C51467575
00B28A6D799142C3FAA4753E6B00B86EE6
00B28A7564BE6D8750E4685C3C9D0C4CF9
00B28AA8422EBE753C1C21424CDF3C36C6
00B28AA9C68891199600518FE18F7E1610
00B28ABEDD9190DDA89088BF2F227CE51F
00B28ADD33D8BC98BC8BBFACBC0001ACBF
00B28AE8334C44358CBF5856945AE8C26C
```

For example:

```
http://myhost:8080/certs/snlist.txt
```

Mandatory: Yes.

OCSP Responder

Configure the following parameters of the OCSP responder service provided by the Certification Authority.

- [VA certificate](#)
- [CA certificate](#)
- [Profile ID](#)

VA certificate

The certificate described in [Generating a VA certificate and key pair](#). Click **Select Files** to import this certificate from file.

i Each certificate file must contain a certificate in PEM format and Base64 encoding.

Mandatory: Yes.

CA certificate

Click **Select Files** to import the certificate of the CA that issues the certificates validated by Entrust Validation authority.

i Each certificate file must contain a certificate in PEM format and Base64 encoding.

Mandatory: Yes.

Profile ID

The identifier of the profile for processing the certificate status before generating an OCSP response. See below for the response settings defined by each profile.

Profile identifier	nextUpdate	id-pkix-ocsp-archive-cutoff	Status if unknown	Revocation date
basic	—	—	revoked	Jan 1 00:00:00 1970 GMT
archiveCutOff	—	notBefore date of the CA certificate	revoked	Jan 1 00:00:00 1970 GMT
nextUpdate	thisUpdate + 8 hours	—	revoked	Jan 1 00:00:00 1970 GMT
archiveCutOffWithNextUpdate	thisUpdate + 8 hours	notBefore date of the CA certificate	revoked	Jan 1 00:00:00 1970 GMT
CRLProfile	—	—	good	—
CRLProfileWithArchiveCutOff	—	notBefore date of the CA certificate	good	—
SNListProfile	—	—	unknown	—
SNListProfileWithArchiveCutOff	—	notBefore date of the CA certificate	unknown	—

See the below for the [Certificates Source](#) and [Use SN Lists](#) values supported by each profile.

Profile identifier	Certificates Source	Use SN Lists
basic	CAGW	—
archiveCutOff	CAGW	—
nextUpdate	CAGW	—
archiveCutOffWithNextUpdate	CAGW	—
CRLProfile	CRL	False
CRLProfileWithArchiveCutOff	CRL	False
SNListProfile	CRL	True
SNListProfileWithArchiveCutOff	CRL	True

Mandatory: Yes.

Testing the OCSP Responder

After deploying Validation Authority, you can test the OCSP Responder service as follows.

- [Testing the OCSP Responder with openssl](#)
- [Testing the OCSP Responder with the health check endpoint](#)

Testing the OCSP Responder with openssl

Run the following `openssl` command to test the OCSP Responder service.

```
openssl ocsp -issuer <ca_cert> -serial <sn> -url <url> -VAfile <va_cert>
```


For example:

```
$ openssl ocsp -issuer issuer.pem -serial 0x000000002439fa8f5fe6370bb20ccb2556da6991
-url http://10.1.141.37/eva -VAfile ./VAFile.pem
Response verify OK
0x000000002439fa8f5fe6370bb20ccb2556da6991: good
      This Update: Nov  7 18:52:34 2022 GMT
      Next Update: Nov  8 02:41:13 2022 GMT
```

See below for a description of each command option.

- `-issuer <ca_cert>`
- `-serial <sn>`

- `-url <url>`
- `-VAfile <va_cert>`

 The OCSP Responder service reboots when losing connection with the HSM. Run the [evactl check all](#) command to check the HSM connection and other settings.

`-issuer <ca_cert>`

Validate the status of a certificate issued by the `<ca_cert>` CA. Where `<ca_cert>` is the file path of the CA certificate.

`-serial <sn>`

Validate the status of the certificate with the `<sn>` serial number.

`-url <url>`

Connect to the `<url>` Validation Authority service. Where `<url>` is an URL in the following format.

```
http://<host>/eva
```

Where `<host>` is the IP address or hostname of the host running Validation Authority.

`-VAfile <va_cert>`

Validate the response with the `<va_cert>` certificate. Where `<va_cert>` is the file path of the certificate:

- Generated as explained in [Generating a VA certificate and key pair](#).
- Selected as VA certificate when configuring the [OCSP Responder](#) settings.

Testing the OCSP Responder with the health check endpoint

Entrust Validation Authority exposes the following endpoint to check the health of the database and HSM connections.

```
http://<host>/eva/health
```

This endpoint returns an HTTP 503 response when the health check fails.

12 Managing CA Gateway

See below for configuring, deploying, and administering the CA Gateway solution.

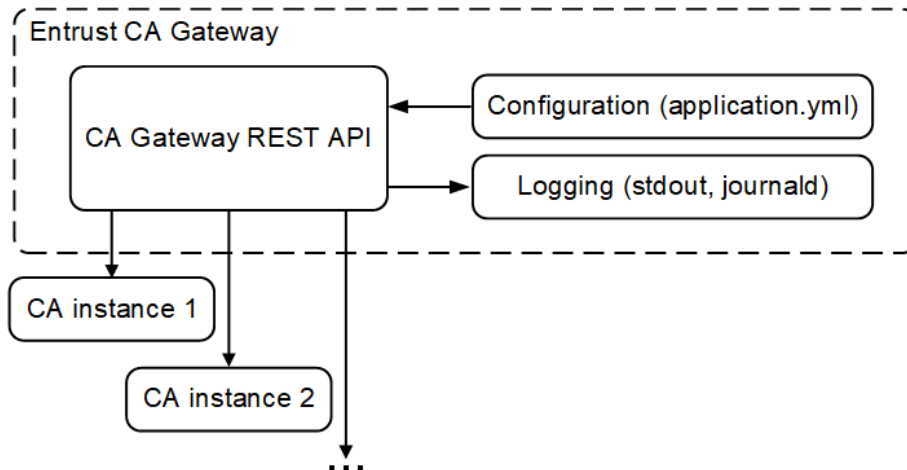
✗ As explained in [Starting up CSP](#), do not perform system operations other than those described in this guide. Specifically, the user and group identifiers 1339 are reserved for CA Gateway images, so the host server should not use them.

- [CA Gateway architecture](#)
- [Obtaining the Gateway server certificate](#)
- [Integrating Certificate Authorities with CA Gateway](#)
- [Configuring and deploying CA Gateway](#)
- [Issuing public trust certificates with CA Gateway](#)
- [Adminstrating CA Gateway](#)
- [CSP CA Gateway endpoints](#)
- [CA Capabilities reference](#)

See [Browsing logs with Grafana](#) for how to browse Certificate Authority logs.

CA Gateway architecture

CA Gateway is a lightweight, container-based module implementing a CA-agnostic Certificate Lifecycle and Policy Management API. Using CA Gateway, your applications can provide certificate issuance, renewal, and revocation actions across different Certification Authorities (CAs). CA Gateway provides policy retrieval capabilities so applications can customize API and user-facing dialogs to ensure that certificate actions conform to organizational policies.



See below for a description of each component.

- [Client](#)
- [Integrator](#)
- [Tenant](#)
- [Managed CA](#)

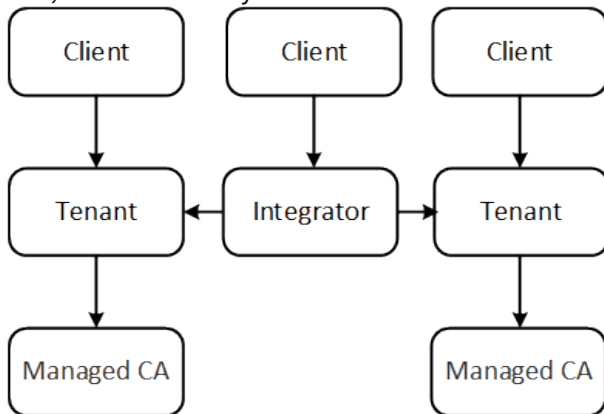
i CA-specific plugins communicate with the underlying CAs through mutually authenticated TLS.

Client

Each client is an authorized end entity of the CA Gateway API and is mapped either to a tenant or an integrator.

- Clients mapped to an integrator can access many Managed CAs.
- Clients mapped to a tenant can access only that tenant's Managed CA.

Thus, each CA Gateway client can access one or several CAs.



The CA Gateway API is regularly updated to add functionalities. Therefore, client applications:

- Should tolerate and ignore new fields.
- Should be recompiled against the new data model of each CA Gateway release.

Integrator

Each integrator is an access controller for one or more tenants.

Tenant

Each tenant is an access controller for a Managed CA. Thus, each tenant:

- Has only one integrator.
- Controls access to a different CA.

Managed CA

Each "managed CA" is a set of information that CA Gateway uses to connect to a CA. For example:


- Microsoft Active Directory Certificate Services.
- AWS Certificate Manager Private Certificate Authority.
- Entrust Certificate Authority.

Obtaining the Gateway server certificate

CA Gateway requires a digital certificate for securing communications between the CA Gateway and authorized clients. See below to generate this certificate for a production environment.

- [Generating the server key pair](#)
- [Obtaining the key pair CSR](#)
- [Obtaining the server certificate](#)
- [Importing the server certificate into the keystore](#)

- [Importing CA certificates into a truststore](#)
- [Reusing the Cryptographic Security Platform TLS certificate](#)

 The certificate must contain the server's fully qualified domain name (FQDN) as a DNS type Subject Alternative Name (subjectAltName) extension.

Generating the server key pair

On a machine with Java installed, run the following command to generate the server key pair.

```
keytool -genkeypair -alias <ALIAS> -dname <DN> -keyalg <KEYALG> -keysize <KEYSIZE>  
-sigalg sha256WithRSA -ext san=dns:<DNS> -keystore <KEYSTORE> [-keypass <KEYPASS>] [-  
storepass <STOREPASS>]
```

See the following table for a description of each flag.

Flag	Value
-alias	An alias for the key pair.
-dname	The DN for the key pair (and later, the certificate). Use the DN format expected by the CA that will issue the certificate.
-keyalg	The algorithm for the key pair (for example, RSA).
-keysize	The Key size. Select a secure key size (for example, 2048).
-ext	The DNS-type value of the Subject Alternative Name (subjectAltName) extension.
-keystore	The full path of the keystore file. If the keystore does not exist, the keytool utility will create it.
-keypass	The password of the private key. When you omit this option, the tool prompts for a password.
-storepass	The password for the keystore. When you omit this option, the tool prompts for a password.

Obtaining the key pair CSR

Create a Certificate Signing Request (CSR) by entering the following command:

```
keytool -certreq -alias <ALIAS> -file <FILE> -storetype pkcs12 -keystore <KEYSTORE>
[-storepass <STOREPASS>]
```

For example:

```
> keytool -genkeypair -alias example_alias -dname "cn=CA Gateway,ou=CA
Entry,o=Example,c=US" -keyalg RSA -keysize 2048 -sigalg sha256WithRSA -ext
san=dns:domain.example.com -keystore /CAGW/config/keystore.ks
> keytool -certreq -alias example_alias -file /tmp/cagw/cagw_csr.txt -keystore /CAGW/
config/keystore.ks
```

See the following table for a description of each option.

Option	Value
-alias	The alias previously specified when Generating the server's key pair.
-file	The full path of the CSR file.
-keystore	The full path of the keystore file.
-storepass	The password of the keystore. When you omit this option, the tool prompts for a password.

Obtaining the server certificate

Issue the certificate with either:

- Your on-premises CA, such as Entrust Certificate Authority.
- A trusted certificate provider such as the Entrust Certificate Services at store.entrust.com.

Importing the server certificate into the keystore

Import the certificate into the keystore:

```
keytool -importcert -alias <ALIAS> -file <FILE> -keystore <KEYSTORE>
```

For example:

```
keytool -importcert -alias example_alias -file /tmp/cagw/cagw_cert.p7b-keystore /
home/myuser/cagw/config/keystore.ks
```

See the following table for a description of each option.

Option	Value
-alias	The alias previously specified when Generating the server's key pair.
-file	The full path of the PKCS #7 file containing the certificate and the certificate chain.
-keystore	The full path of the keystore file.

Importing CA certificates into a truststore

For each managed Certificate Authority, CA Gateway requires the following certificates.

CA type	Required certificates
Root	The self-signed root CA certificate.
Subordinate	The complete CA certificate chain, from the subordinate CA certificate up to the root CA certificate.

Import these certificates in either:

- The Truststore used when Importing the server certificate into the keystore.
- A new Truststore.

To import a CA certificate into a truststore using the Java `keytool` utility, run the following command.

```
keytool -importcert -trustcacerts -alias <ALIAS> -file <FILE> -keystore <KEYSTORE> [-storepass <STOREPASS>]
```

For example:

```
keytool -import -trustcacerts -alias managed_ca1 -file /tmp/cagw/managed_ca1.cer  
-keystore /home/myuser/cagw/config/keystore.ks
```

See the following table for a description of each parameter.

Option	Value
-alias	The alias of the CA certificate.
-file	The full path of the CA certificate file.

Option	Value
-keystore	The full path of the Java keystore file. If not present, the keystore is created.
-storepass	The password of the Java keystore. When you omit this option, the tool prompts for a password.

Reusing the Cryptographic Security Platform TLS certificate

As TLS certificate for CA Gateway, you can use the same TLS server certificate described in [Replacing the default TLS certificate](#)

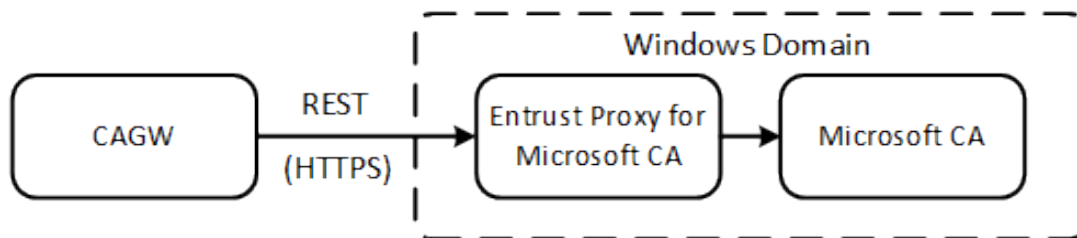
Integrating Certificate Authorities with CA Gateway

The sections below explain how to integrate CA Gateway with Certificate Authorities of different providers.

- [Integrating a Microsoft CA](#)
- [Integrating an AWS CA](#)
- [Integrating an ECS CA](#)
- [Integrating an Entrust Certificate Authority](#)

Integrating a Microsoft CA

As illustrated by the following figure, CA Gateway manages each Microsoft CA instance through an Entrust Proxy for Microsoft CA.



In this architecture, CA Gateway is a client of Microsoft CA. See in the following sections how to configure the Entrust Proxy for Microsoft CA and CA Gateway to manage Microsoft CAs.

- [Setting up the Entrust Proxy for Microsoft CA](#)
- [Integrating a Microsoft CA with the Entrust Proxy](#)

i Only Microsoft Enterprise CA is supported; standalone CA is not supported.

Setting up the Entrust Proxy for Microsoft CA

Install and configure the Entrust Proxy for Microsoft CA.

- [Installing the Entrust Proxy for Microsoft CA](#)
- [Issuing the SSL certificates](#)
- [Generating a client keystore for CA Gateway](#)

- [Generating a truststore for CA Gateway](#)
- [Generating the server keystore of the Entrust Proxy for Microsoft CA](#)
- [Running the Entrust Proxy for Microsoft CA](#)

Installing the Entrust Proxy for Microsoft CA

Install the Entrust Proxy for Microsoft CA, as explained in the following sections.

- [System requirements for the Entrust Proxy for Microsoft CA](#)
- [Configuring the Windows domain account](#)
- [Downloading the Entrust Proxy for Microsoft CA installer](#)
- [Configuring logs](#)
- [Running the Entrust Proxy for Microsoft CA installer](#)
- [Un-Installing the Entrust Proxy for Microsoft CA](#)

System requirements for the Entrust Proxy for Microsoft CA

To install the Entrust Proxy for Microsoft CA, you need a machine with Windows Server 2016 (x64) or above and one of the following LTS (Long Term Support) Java distributions.

- Oracle Java x86_64 version 17
- OpenJDK 17
- AdoptOpenJDK 17

An environment variable JAVA_HOME should exist pointing to the path of java installation.

The PATH environment variable should be extended to include %JAVA_HOME%\bin

To check the Java version and architecture details, run:

```
java -XshowSettings:properties -version
```

Configuring the Windows domain account

Configure the Windows login account of the Entrust Proxy for Microsoft CA. See below for the supported combinations when the Entrust Proxy for Microsoft CA and the Domain Controller share the same server or run on different servers.

User	Service startup type	Same server	Different servers
A local service account	Automatic or Automatic (Delayed Start)	✓	✓
A user of the Domain Admin group	Automatic (Delayed Start)	✓	✗

In either case, enable only the following user permissions.


- Issue and Manage Certificates
- Request Certificates

Downloading the Entrust Proxy for Microsoft CA installer

Download and extract the Entrust Proxy for Microsoft CA installer files.

To download the Entrust Proxy for Microsoft CA installer

1. Log in trustedcare.entrust.com
2. Go to **PRODUCTS > Cryptographic Security Platform**
3. Select the latest version.
4. Click the download link of the Entrust Proxy for Microsoft CA.
5. Unzip the compressed file contents to your selected installation directory on the Windows machine – for example, in `c:\mscaproxy`

 Installing into `c:\Program Files` may not be functional due to windows privilege enforcement.

Configuring logs

Optionally, edit the configuration files to modify the default log recording settings.

Configuration file	Parameter	Value	Additional steps
MSCAProxy.xml	logpath	The folder where to save logs.	Re-run the Entrust Proxy for Microsoft CA installer if you edit this file after the installation.
config\application.yml	com.entrust.mscaproxy	The supported log levels. Supported values in increasing severity are <code>TRACE</code> , <code>DEBUG</code> , <code>INFO</code> , <code>WARN</code> , <code>ERROR</code> , <code>FATAL</code> and <code>OFF</code> .	Restart the system if you edit this file after the installation.

For example, adding the following code to the `config\application.yml` file sets the log level to `INFO`.

```
logging:
  level:
    root: INFO
    com.entrust.mscaproxy: INFO
```

Running the Entrust Proxy for Microsoft CA installer

Run the following command as an administrator to register the Entrust Proxy for Microsoft CA as a Windows service.

```
MSCAProxy.exe install /p
```

When prompted, type the domain user's username in one of the following formats:

- UPN (User Principal Name)
- `<domainName>\<sAMAccountName>`

Type the password of the domain user and type `y` for allowing the log-on as a service. The installer does not wait for you to press the **Enter** key.

Un-Installing the Entrust Proxy for Microsoft CA

Run the following command as an administrator if you want to uninstall.

```
MSCAProxy.exe uninstall
```

Issuing the SSL certificates

CA Gateway and the Entrust Proxy for Microsoft CA communicate with HTTP over SSL using mutual authentication. Thus, two SSL certificates are required:

- A server SSL certificate for the Entrust Proxy for Microsoft CA.
- A client authentication certificate for CA Gateway.

You can obtain both SSL certificates from any CA. Those steps are outside the scope of this document.

Generating a client keystore for CA Gateway

Generate a `mscaproxyclient.jks` keystore containing:

- The private key of CA Gateway for client authentication.
- The key's certificate.
- The certificate's chain.

See below the required steps.

- [Generating and certifying the key pair](#)
- [Importing the keys and the certificate](#)
- [Deleting temporary files](#)



The following instructions create a Java KeyStore (JKS) with the Java `keytool` command line utility. Consider using a more secure PKCS#12 type instead.


Generating and certifying the key pair

In a temporary directory under the Microsoft Proxy Server, run the following commands to generate and certify a key pair.

```
keytool -genkey -noprompt -alias mscaproxyclient -dname "cn=mscaproxy client" -keyalg  
RSA -keysize 2048 -keystore mscaproxyclient.jks -storepass <STOREPASS> -keypass  
<KEYPASS>
```

```
keytool -certreq -alias mscaproxyclient -file mscaproxyclient.csr -keystore  
mscaproxyclient.jks -storepass <STOREPASS>
```

```
certreq.exe -f -attrib "CertificateTemplate:ClientAuthentication" -config  
"<HOST>\<CA>" mscaproxyclient.csr CertChainFileOut mscaproxyclient.p7b
```

 Depending on the Microsoft CA setup, you may need to manually approve the request and retrieve the certificate.

See the following table for a description of the main parameters.

Option	Value
-attrib	The name of the template authentication template for Microsoft CA you previously created.
-config	The keystore configuration in "<HOST>\<CA>" syntax. Where <HOST> is the Microsoft CA's hostname, and <CA> is the CA name defined when configuring Microsoft CA in CA Gateway.
-dname	A valid certificate distinguished name.
-keypass	The password of the private key
-keystore	The name of the keystore file. Copy this file into the CA Gateway's server
-storepass	The keystore password.

Importing the keys and the certificate

Import the keys and the certificate into the keystore.

```
keytool -import -noprompt -alias mscaproxyclient -file mscaproxyclient.p7b -keystore mscaproxyclient.jks -storepass <STOREPASS>
```


Deleting temporary files

Delete the temporary files.

```
del CertChainFileOut
del CertChainFileOut.rsp
del mscaproxyclient.csr
del mscaproxyclient.p7b
```

Generating a truststore for CA Gateway

You need a `truststore.jks` truststore containing the CA chain of the Entrust Proxy for Microsoft CA's server key.

 The following instructions create a Java KeyStore (JKS) with the Java `keytool` command line utility. Consider using a more secure PKCS#12 type instead.

To generate a truststore for CA Gateway

1. Create an SSL directory under the Entrust Proxy for Microsoft CA installation. For example:

```
c:\mscaproxy\ssl
```

2. In this directory, run the following command to include the certificate of the root CA and all the intermediate CAs.

```
keytool -import -noprompt -alias <CA_ALIAS> -file <CA_ALIAS>.cer -keystore truststore.jks -storepass <STOREPASS>
```

3. Copy the new `truststore.jks` truststore in the CA Gateway server.


Generating the server keystore of the Entrust Proxy for Microsoft CA

You need a keystore containing:

- The SSL authentication certificate of the Entrust Proxy for Microsoft CA.
- The private key of the certificate.
- The validation chain of the certificate.

See below the required steps.

- [Generating the keystore](#)
- [Setting the Subject Name](#)
- [Adding the keystore password to the configuration](#)
- [Adding the truststore password to the configuration](#)
- [Restarting CA Gateway](#)


 The following instructions create a Java KeyStore (JKS) with the Java `keytool` command line utility. Consider using a more secure PKCS#12 type instead.

Generating the keystore

Go to the SSL directory containing the `truststore.jks` file previously generated. For example:

```
c:\mscaproxy\ssl
```

Run the following commands to generate the key.

 The below commands use the default Web Server certificate template. If you need to customize any settings of the Web Server certificate template, use a copy of it.

```
keytool -genkey -noprompt -alias mscaproxy -dname "cn=MS CA proxy server FQDN" -keyalg RSA -keysize 2048 -keystore mscaproxy.jks -storepass <STOREPASS> -keypass <KEYPASS>
```

```
keytool -certreq -alias mscaproxy -ext SAN=dns:MS CA proxy server FQDN -file  
mscaproxy.csr -keystore mscaproxy.jks -storepass <STOREPASS>
```

```
certreq.exe -f -attrib "CertificateTemplate:WebServer" -config "MS CA host name\CA  
name" mscaproxy.csr CertChainFileOut mscaproxy.p7b
```

```
keytool -import -noprompt -alias mscaproxy -file mscaproxy.p7b -keystore  
mscaproxy.jks -storepass <STOREPASS>
```

```
del CertChainFileOut  
del CertChainFileOut.rsp  
del mscaproxy.csr  
del mscaproxy.p7b
```

Where:

- "MS CA proxy server FQDN" is the fully qualified domain name of your Entrust Proxy for Microsoft CA's server.
- <STOREPASS> is the password of the keystore.
- <KEYPASS> is the password of the private key.

Setting the Subject Name

Edit the `application.yml` file of the Entrust Proxy for Microsoft CA installation folder.

```
config\application.yml
```

Uncomment all lines (by removing #) and assign to `subject-dn` the distinguished name set with `-dname` when generating the client keystore. For example:

```
subject-dn: "cn=mscaproxy client"
```

Adding the keystore password to the configuration

Edit the following file.

```
MS CA Proxy Installation\config\key-store-password.scrt
```

Set the following parameter:

```
decrypted=<STOREPASS>
```

Where <STOREPASS> is the password of the keystore described in [Generating the keystore](#).

Adding the truststore password to the configuration

Edit the following file:

```
MS CA Proxy Installation\config\trust-store-password.scrt
```

Set the following parameter.

```
decrypted=<STOREPASS>
```

Where `<STOREPASS>` is the password of the keystore described in [Generating the keystore](#).

Restarting CA Gateway

If the Entrust Proxy for Microsoft CA is running, execute the following command as an administrator to restart it.

```
MSCAProxy.exe restart
```

Running the Entrust Proxy for Microsoft CA

Administrators can run and manage the Entrust Proxy for Microsoft CA with the following commands.

- `MSCAProxy.exe start`
- `MSCAProxy.exe stop`
- `MSCAProxy.exe restart`

Once started, you can check the correct execution of the Entrust Proxy for Microsoft CA using a Chrome browser.

To check the execution of the Entrust Proxy for Microsoft CA

1. Run the following command to generate a PKCS#12 from the `mscaproxyclient.jks` keystore.

```
keytool -importkeystore -srckeystore mscaproxyclient.jks -destkeystore  
mscaproxyclient.p12 -srcstoretype JKS -srcstorepass <SRCSTOREPASS>  
-deststoretype PKCS12 -deststorepass <DESTSTOREPASS>
```

2. Import the generated `mscaproxyclient.p12` file into Chrome.
3. Go to:

```
https://<proxyserver>:8443/MSCAProxy/rest/status/ping
```

4. Check the server response. The "MS CA proxy is running" message indicates a correct operation.

Integrating a Microsoft CA with the Entrust Proxy

After [Setting up the Entrust Proxy for Microsoft CA](#), you can connect it to a Microsoft CA.

- [Adding Microsoft Management Console snap-ins](#)
- [Creating a client authentication template for Microsoft CA](#)
- [Creating the CA enrollment agents](#)

- [Creating the RA recovery agents](#)
- [Creating the RA enrollment agents](#)
- [Enabling supply in the request](#)
- [Configuring Request Handling in the Microsoft CA](#)
- [Enabling SAN attributes in the enrollment request](#)

Adding Microsoft Management Console snap-ins

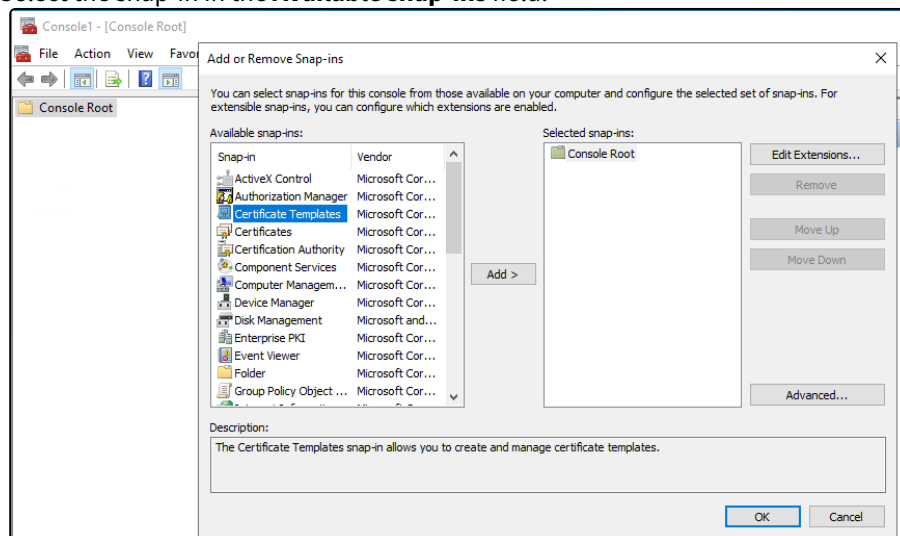
Run the Microsoft Management Console and add the following snap-ins.

- Certificate Templates
- Certificates
- Certificate Authorities

See below for how to add a span-in to the Microsoft Management Console.

To add a Microsoft Management Console snap-in

1. Log into the Microsoft CA server machine.
2. Press **Win + R** to open the **Run** dialog.
3. Type "mmc" and press Enter to open Microsoft Management Console.
4. Select **File > Add Remove Snap-In**.
5. Select the snap-in in the **Available snap-ins** field.



6. Click **Add** to include the snap-in in the **Selected snap-ins** field.
7. Click **OK**.

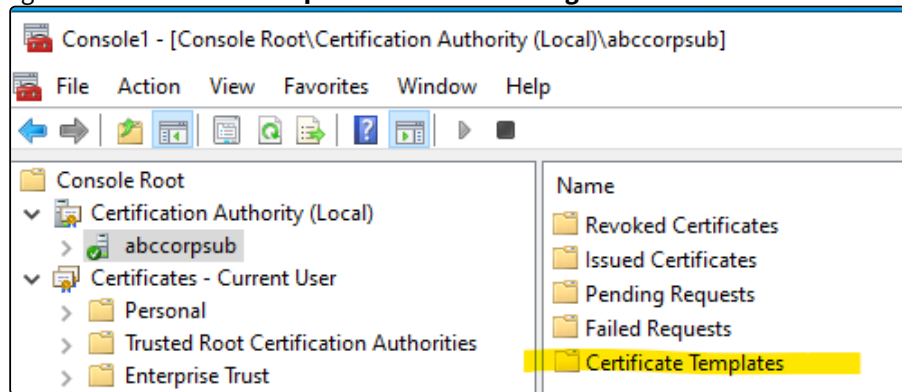
Creating a client authentication template for Microsoft CA

Create an authentication template for enabling client authentication in Microsoft CA.

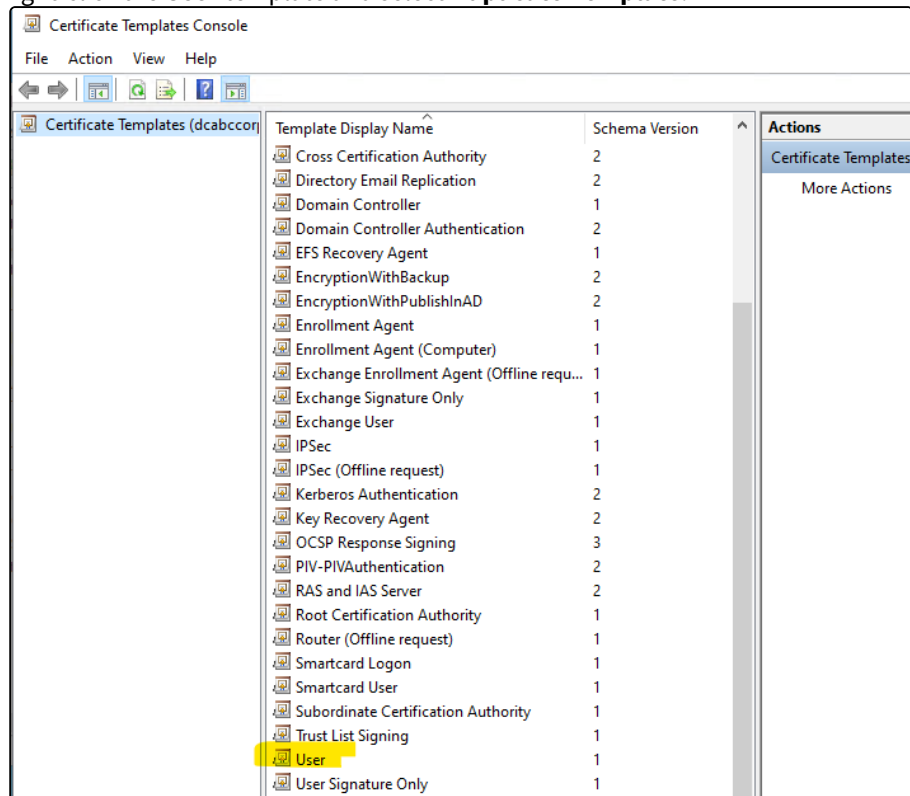
To create a client authentication template for Microsoft CA

1. Log into the Microsoft CA server machine.
2. Press **Win + R** to open the **Run** dialog.
3. Type "mmc" and press Enter to open the Microsoft Management Console.
4. Go to **Certificate Authority**.

5. Right-click **Certificate Templates** and select **Manage**.



6. Right-click the **User** template and select **Duplicate Template**.



7. In the **General** tab of the **Properties of New Template** dialog, set **Template display name** to **Client Authentication**.
8. In the **Subject Name** tab, enable **Supply in the request**.
9. In the **Extensions** tab, edit **Application Policies** to remove **Encrypting File System** and **Secure Email**.
10. Go to **Certificate Authority**.
11. Right-click **Certificate Templates** and select **New >Certificate Template to Issue**.
12. Select **Client Authentication** from the list.

Creating the CA enrollment agents

You must create a CA Enrollment Agent (EA) before creating the RA recovery agents and the RA enrollment agents.

- [Publishing the enrollment template](#)

- [Creating an enrollment certificate for the CA Administrator](#)

i A CA enrollment agent is self-enrolled and internal to the CA, while a RA enrollment agent is co-located with CA Gateway.

Publishing the enrollment template

If not already published, publish the enrollment agent template as explained in this section.

To publish the enrollment agent template

1. Log into the Microsoft CA server machine.
2. Press **Win + R** to open the **Run** dialog.
3. Type "mmc" and press Enter to open Microsoft Management Console.
4. Under the certificate authority name, right-click **Certificate Templates**.
5. Select **New > Certificate Template to issue**.
6. Select **Enrollment Agent**.

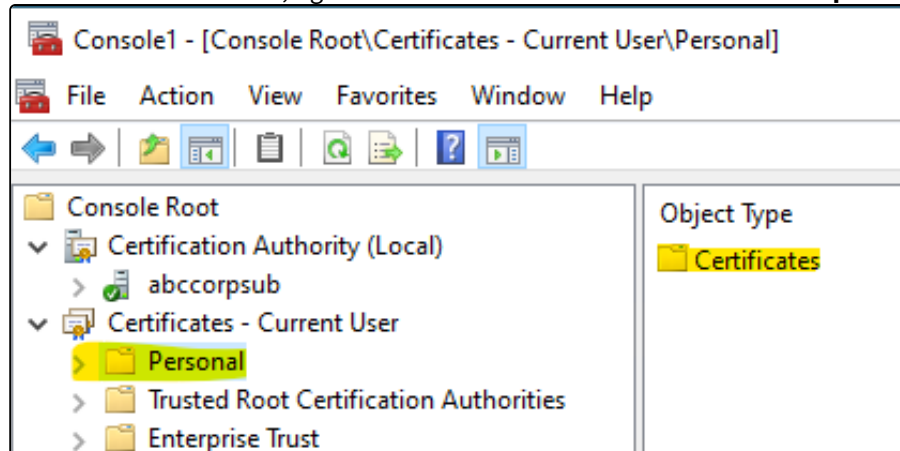
Creating an enrollment certificate for the CA Administrator

Create an enrollment certificate for the CA administrator user of the Microsoft CA server.

✗ Do not export the CA administrator's enrollment key.

To create an enrollment certificate for the administrator

1. In the Microsoft CA server machine, run MMC.
2. Under the **Personal** node, right-click **Certificates** and select **All Tasks > Request New Certificate**.



3. Follow the wizard instructions. When prompted, select the **Enrollment Agent** template.

Creating the RA recovery agents

If you want to store and recover keys generated by the Microsoft CA, create one or more recovery agents as explained below.

To create a recovery agent

1. Log into the Microsoft CA server machine.
2. Press **Win + R** to open the **Run** dialog.
3. Type "mmc" and press Enter to open Microsoft Management Console.
4. Under the Certificate Authority node, right-click **Certificate Template**, and select **Manage**.

5. Right-click **Key Recovery Agent** and select **Duplicate Template**.
6. Configure the following settings in each tab of the **Properties of the New Template** dialog.
 - [General](#)
 - [Request Handling](#)
 - [Issuance Requirements](#)
 - [Security](#)
7. Under the Certificate Authority node, right-click **Certificate Template** and select **New > Certificate Template to issue**.
8. Select the newly created template.
9. Create a user in Active Directory.
10. Under the **Personal** node, right-click **Certificates** and select **Tasks > Advanced Operations > Enroll On Behalf Of**
11. Follow the wizard instructions. When prompted, select the newly created user.
12. Right-click the issued certificate and select **Export**.
13. Follow the wizard instructions. In the **Export Private Key** dialog, select **Yes, export the private key**.

General

Click this tab and write a name for the new template in the **Template display name** field.

Request Handling

Click this tab and check the **Allow private key to be exported** box.



Issuance Requirements

Click this tab and set the following values.

Parameter	Value
CA certificate manager approval	Disable this option
This number of authorized signatures	1
Policy type required in signature	Application policy
Application Policy	Certificate Request Agent

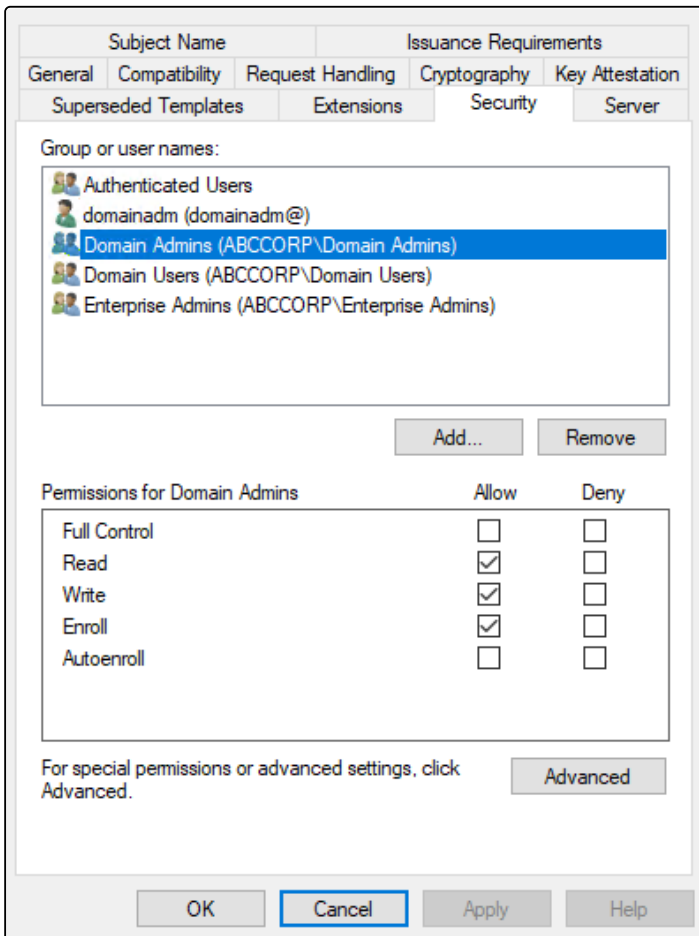
Security

Click this tab and assign the following permissions to the **Domain Admins** user group.

Permissions for Domain Admins	Allow	Deny
Full Control		
Read		

Permissions for Domain Admins	Allow	Deny
Write	✓	
Enroll	✓	
Autoenroll	✗	

For example:



Subject Name Issuance Requirements

General Compatibility Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security Server

Group or user names:

- Authenticated Users
- domainadm (domainadm@)
- Domain Admins (ABCCORP\Domain Admins)**
- Domain Users (ABCCORP\Domain Users)
- Enterprise Admins (ABCCORP\Enterprise Admins)

Add... Remove

Permissions for Domain Admins	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

Advanced

OK Cancel Apply Help

Creating the RA enrollment agents

To publish the issued certificates in Active Directory, you need one or more RA (Registration Authority) enrollment agents. See below for the supported credential generation modes.

- [Creating RA enrollment agent credentials in a keystore file](#)
- [Creating RA enrollment agent credentials in a PKCS#11 HSM](#)

Creating RA enrollment agent credentials in a keystore file

You can create the RA enrollment agent credentials in the following file formats.

- PKCS#12 (Personal Information Exchange Syntax Standard).
- JKS (Java KeyStore).
- JCEKS (Java Cryptography Extension KeyStore).
- PFX (Personal Information Exchange).

See the example below for how to create them in PKCS#12.

To create RA enrollment agent credentials in a keystone file

1. Log into the Microsoft CA server machine.
2. Press **Win + R** to open the **Run** dialog.
3. Type "mmc" and press Enter to open Microsoft Management Console.
4. Under the Certificate Authority node, right-click **Certificate Template**, and select **Manage**.
5. Right-click **Enrollment Agent** and select **Duplicate Template**.
6. Configure the following settings in each tab of the **Properties of the New Template** dialog.
 - [General](#)
 - [Request Handling](#)
 - [Issuance Requirements](#)
 - [Security](#)
7. Under the Certificate Authority node, right-click **Certificate Template** and select **New >Certificate Template to issue**.
8. Select the newly created template.
9. Create a user in Active Directory.
10. Under the **Personal** node, right-click **Certificates** and select **Tasks > Advanced Operations > Enroll On Behalf Of**.
11. Follow the wizard instructions. When prompted, select the newly created user.
12. Right-click the issued certificate and select **Export**.
13. Follow the wizard instructions. In the **Export Private Key** dialog, select **Yes, export the private key**.

General

Click this tab and write a name for the new template in the **Template display name** field.

Request Handling

Click this tab and check the **Allow private key to be exported** box.

Issuance Requirements

Click this tab and set the following values.

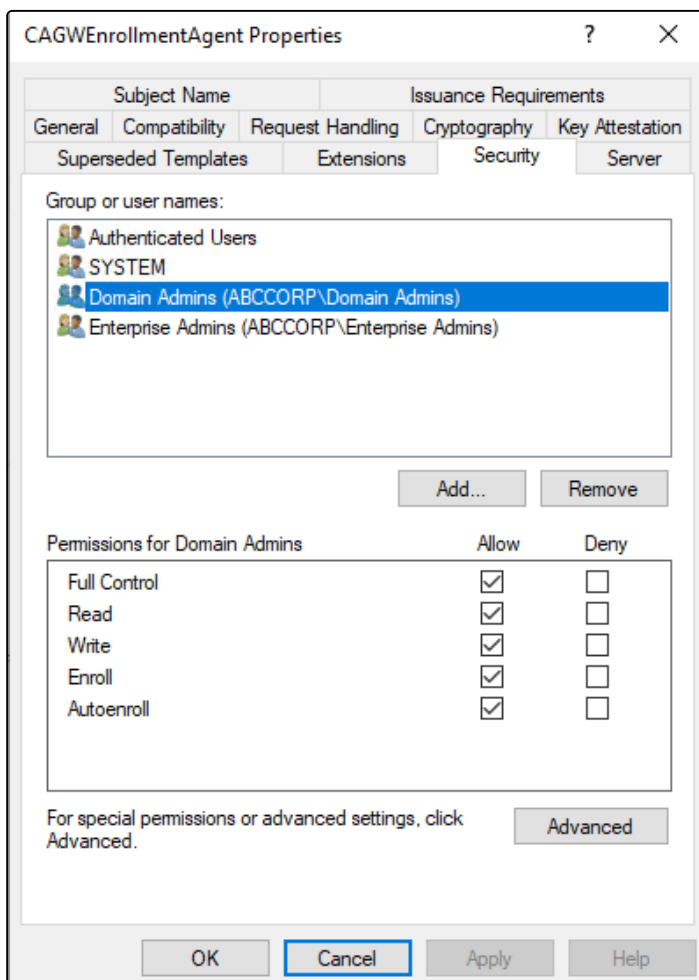
Parameter	Value
This number of authorized signatures	1
Policy type required in signature	Application policy
Application Policy	Certificate Request Agent

Security

Click this tab and assign the following permissions to the **Domain Admins** user group.

Permissions for Domain Admins	Allow	Deny
Full Control	✓	
Read	✓	
Write	✓	
Enroll	✓	
Autoenroll	✓	

For example:



CAGWEnrollmentAgent Properties

Subject Name: Issuance Requirements

General | Compatibility | Request Handling | Cryptography | Key Attestation

Superseded Templates | Extensions | Security | Server

Group or user names:

- Authenticated Users
- SYSTEM
- Domain Admins (ABCCORP\Domain Admins)**
- Enterprise Admins (ABCCORP\Enterprise Admins)

Add... Remove

Permissions for Domain Admins	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>


For special permissions or advanced settings, click Advanced.

Advanced

OK Cancel Apply Help

Creating RA enrollment agent credentials in a PKCS#11 HSM

When creating enrollment agents for the Microsoft CA, you can generate keys in a PKCS#11 HSM along with a CSR. When processing this CSR, the Microsoft CA issues a certificate chain for the RA Enrollment Agent that you can import into the HSM to pair with the private key.

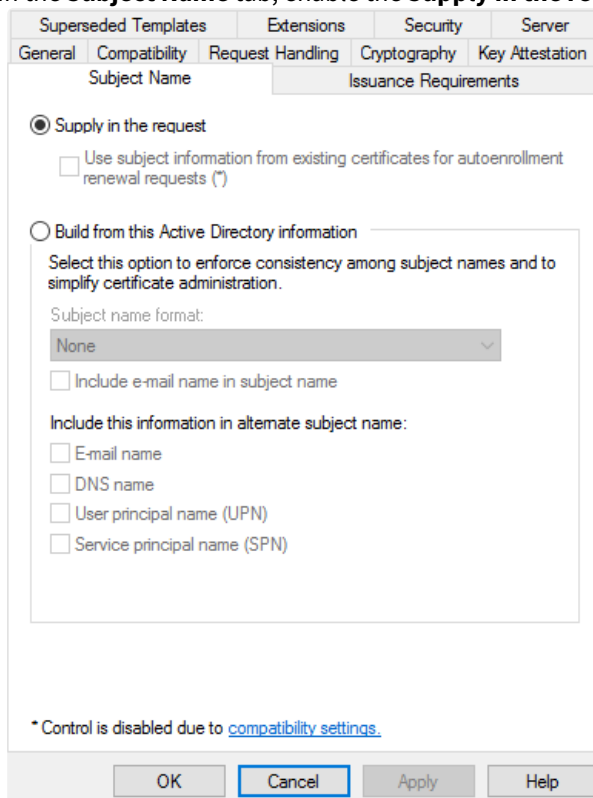
 See the integration guides of the supported HSM for the required operations.

Enabling supply in the request

In all the managed Microsoft CA templates for issuing entity certificates, make sure that the Subject Name is supplied by the certificate request.

To enable supply in the request in a template

1. Log into the Microsoft CA server machine.
2. Press **Win + R** to open the **Run** dialog.
3. Type "mmc" and press Enter to open Microsoft Management Console.
4. Go to **Certificate Authority**.
5. **Right-click Certificate Templates and select Manage.**
6. Right-click the template and select **Properties**.
7. In the **Subject Name** tab, enable the **Supply in the request** radio button.



Superseded Templates Extensions Security Server

General Compatibility Request Handling Cryptography Key Attestation

Subject Name Issuance Requirements

☒ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests (*)

☐ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

☐ DNS name

☐ User principal name (UPN)

☐ Service principal name (SPN)

* Control is disabled due to [compatibility settings](#).

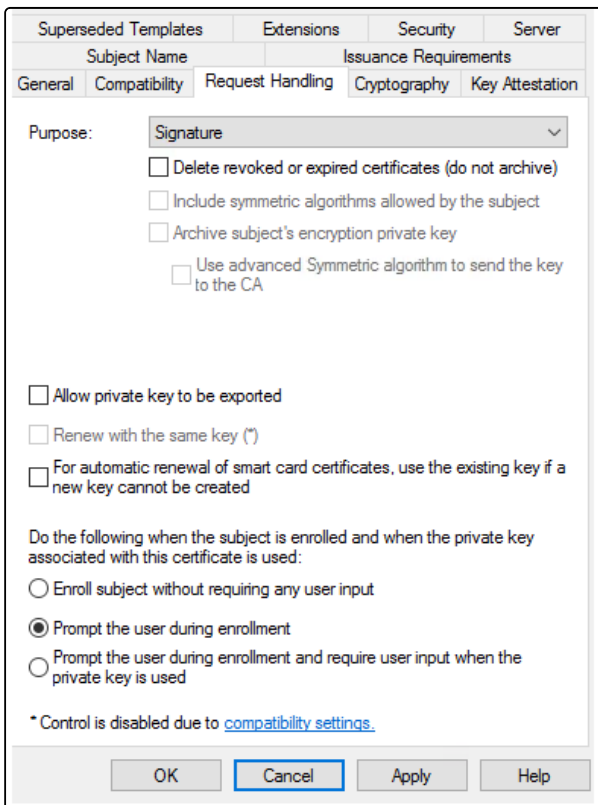
OK Cancel Apply Help

Configuring Request Handling in the Microsoft CA

If the Microsoft CA settings configure **Request Handling** as follows.

Parameter	Value
Purpose	Signature
Delete revoked or expired certificates	
Allow private key to be exported	
For automatic renewal of smart card certificates, use the existing key if a new key cannot be created	
Do the following when the public subject is enrolled and when the private key associated with this certificate is used	Prompt the user during enrollment

As we see, the **Archive subject's encryption private key** option is disabled when selecting the **Signature** template.



Superseded Templates Extensions Security Server

Subject Name Issuance Requirements

General Compatibility Request Handling Cryptography Key Attestation

Purpose: Signature

☐ Delete revoked or expired certificates (do not archive)

☐ Include symmetric algorithms allowed by the subject

☐ Archive subject's encryption private key

☐ Use advanced Symmetric algorithm to send the key to the CA

☐ Allow private key to be exported

☐ Renew with the same key (*)

☐ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

☐ Enroll subject without requiring any user input

☒ Prompt the user during enrollment

☐ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to [compatibility settings](#).


OK Cancel Apply Help

Enabling SAN attributes in the enrollment request

For Microsoft CA to construct the `SubjectAltName` in the issued certificate, you must enable the following flag.

```
Config_CA_Accept_Request_Attributes_SAN
```

You can enable this flag in your remote certificate services implementation or the Microsoft CA server machine, as explained below.

 See the [MS-CSRA] Microsoft document for more information on this flag.

To enable Config_CA_Accept_Request_Attributes_SAN in the Microsoft CA machine

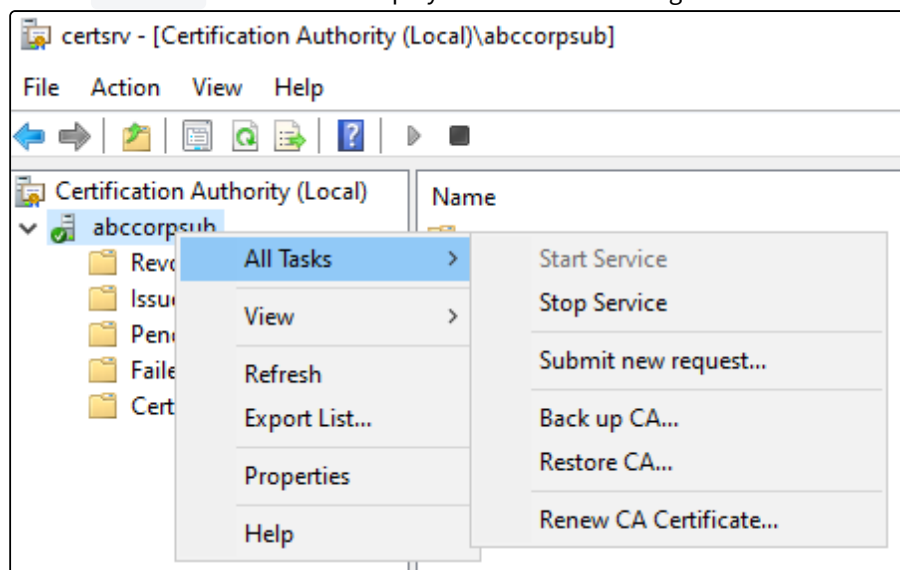
1. Log into the Windows machine hosting the Microsoft CA server.
2. Run the `regedit` command to open the Registry Editor.
3. Select the following registry key (`<CA_CN>` is the Common Name of the Microsoft CA).

```
HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<CA_CN>/
PolicyModules/CertificateAuthority_MicrosoftDefault.Policy/EditFlags
```

4. Calculate an OR of the current key value and `0x000040000` . For example, if the current value is `11014e` , calculate:

```
0x00011014e OR 0x000040000 = 0x0015014e
```

5. Set the OR result as the new key value.
6. Run the `certsrv` command to display the CA service settings.



7. In the navigation tree, right-click the CA name.
8. Select **All Tasks > Stop service** to stop the Microsoft CA server.
9. Select **All Tasks > Start service** to restart the Microsoft CA server.

Integrating an AWS CA

This section explains how to configure CA Gateway for integrating CAs of the Amazon Web Services (AWS).

- [Installing and configuring the AWS CA plugin](#)
- [Handling certificate events with DynamoDB](#)

See the [CA Capabilities reference](#) for a complete description of the operations supported by these CAs.

Installing and configuring the AWS CA plugin

See below for how to install and configure the AWS CA plugin.

- [Exporting the current CA Gateway configuration](#)
- [Copying the AWS-CA plugin installation files](#)
- [Updating the config-schema.json file](#)
- [Updating the CA Gateway configuration](#)

Exporting the current CA Gateway configuration

Create a `<CONFIG>` folder in the machine hosting Cryptographic Security Platform – for example:

```
$ mkdir /tmp/config
```

Run the `clusterctl solution config export` command to export the CA Gateway configuration on the `<CONFIG>` folder – for example:

```
$ sudo clusterctl solution config export -i cagw -f /tmp/config
```

Copying the AWS-CA plugin installation files

Entrust distributes each `<VERSION>` version of the AWS CA plugin in a compressed file with the following name.

```
cagw-plugin-awsca-<VERSION>.zip
```

Once extracted, copy the following contents of this file.

Source	Destination
config/edm/mc/awsca-schema.json	<CONFIG>
lib/*.jar	<CONFIG>/plugins

For example:

```
$ cp config/edm/mc/awsca-schema.json /tmp/config
$ mkdir /tmp/config/plugins
$ cp lib/*.jar /tmp/config/plugins
```

Updating the config-schema.json file

Edit the `config-schema.json` file previously exported to the `<CONFIG>` folder with the rest of the CA Gateway configuration. On this file, update the following settings under `managed-cas`.

Parameter	Update
<code>additionalProperties.properties.connector-name.enum</code>	Add the <code>com.entrust.awsca</code> internal name of the CA plugin.
<code>additionalProperties.properties.connector-name.enumNames</code>	Add the <code>AWS Certificate Authority</code> external name of the CA plugin.
<code>dependencies.connector-name.oneOf</code>	Add a <code>\$file</code> reference to the <code>awsca-schema.json</code> configuration file at the ordered position.

For example:

```
"managed-cas": {
  "title": "Managed CAs",
  "type": "object",
  "additionalProperties": {
    "type": "object",
    "properties": {
      "name": {
        ...
      },
      "issuer-dn": {
        ...
      },
      "connector-name": {
        "title": "Connector Name",
        "enum": [
          "com.entrust.ECS",
          "com.entrust.SecurityManager",
          "com.entrust.MicrosoftCA",
          "com.entrust.awsca"
        ],
        "enumNames": [
          "Entrust Certificate Services",
          "Entrust Certificate Authority",
          "Microsoft Certificate Authority",
          "AWS Certificate Authority"
        ]
      }
    },
    "dependencies": {
      "connector-name": {
        "oneOf": [
          {
            ....
          },
          {

```

```
    "$file": "awsca-schema.json"
  }
]
},
}
```

Updating the CA Gateway configuration

Run the `clusterctl solution config import` command to import the Ca Gateway configuration with the AWS-CA plugin updates. For example:

```
$ sudo clusterctl solution config import -i cagw -f /tmp/config
```

Handling certificate events with DynamoDb

You can handle certificate events with the DynamoDb table hosted in your AWS environment. This method has additional costs but also improved performance: AWS will charge for the DynamoDb service and all of the traffic to and from CA Gateway. With this cost, however, comes increased speed and scalability.

Our testing found that, in the worst case, DynamoDb performs evenly with the AWS Audit Report method. Still, as the number of events in the CA grows, DynamoDb performs significantly faster than the AWS Audit Report method. The improvement is particularly evident when the number of requested events is small compared to the total number of events in the CA. DynamoDb also uses no additional memory in CA Gateway.

When a certificate is issued or revoked by an ACM Private CA:

1. Amazon CloudTrail logs an `IssueCertificate` or `RevokeCertificate` event.
2. An Amazon EventBridge rule triggers an AWS Lambda function.
3. The lambda function receives the event data and extracts the relevant details to create a record.
4. The lambda function saves the record in the DynamoDb table where CA Gateway queries certificate events.

See the following sections for how to configure this method in AWS and CA Gateway.

- [Creating the AWS DynamoDb table](#)
- [Creating the AWS Lambda function](#)
- [Configuring the AWS Lambda function](#)
- [Limiting AWS DynamoDB permissions \(optional\)](#)
- [Limiting AWS Private Certificate Manager permissions \(optional\)](#)
- [Creating the AWS EventBridge rule](#)
- [Configuring the AWS DynamoDB table in CA Gateway](#)

Creating the AWS DynamoDb table

Create an AWS DynamoDb table for storing the certificate events.

To create an AWS DynamoDb table

1. Search for `DynamoDB` in the search box at the top of the AWS Management Console.

2. Navigate to the main page of the DynamoDB service.



3. Select **Create table**.
4. Provide a table name. You will later add the selected name in Creating the AWS Lambda function and Configuring the AWS DynamoDB table in CA Gateway. The Lambda script provided by Entrust uses the certificate-events default table name.
5. Under **Partition key**, enter `certificate_authority_arn` for the primary key and select **String** for the type (default value).
6. Check **Add sort key**.
7. In the resulting text box, enter `time` and select **String** for the type (default value).
8. In the **Table settings** section, do not uncheck **Use default settings** (checked by default) unless you know what you're doing and would like to change these settings for your own needs.
9. Review the configured settings:
 - The partition key must be `certificate_authority_arn`.
 - The sort key must be `time`.
 - The table name is up to you.
10. Click **Create** to create the table.

Creating the AWS Lambda function

Create a Lambda function for storing certificate event records in the AWS DynamoDb table.

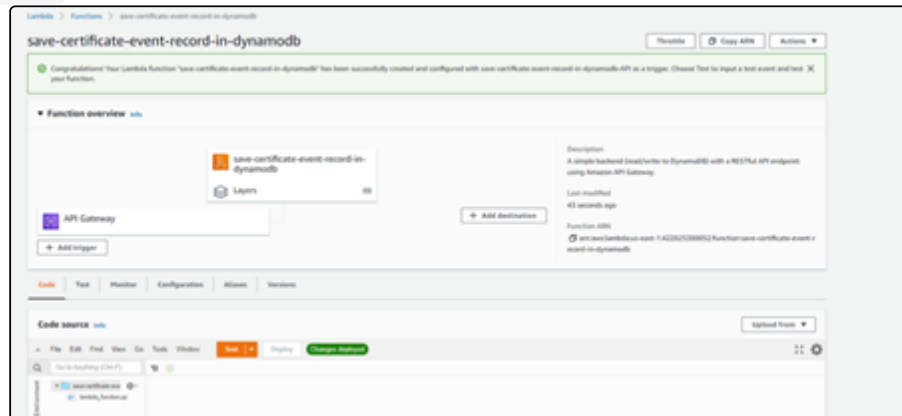
To create the Lambda function

1. Search for `Lambda` in the search box at the top of the AWS Management Console.
2. Navigate to the main page of the Lambda service.
3. Select **Create function**.
4. Select **Use a blueprint**.
5. Search for `microservice-http-endpoint-python` in the **Blueprints** search box.
6. Select the `microservice-http-endpoint-python` blueprint.

7. Click **Configure**.
8. In the resulting page, provide a function name.
9. In **Execution role**, select **Create a new role from AWS policy templates**.
10. Provide a name for the role.
11. Under **Policy templates**, select **Simple microservice permissions: DynamoDB**.
12. In the **API Gateway trigger** section under **API**, select **Create an API**.
13. For **API type**, select **REST API**.
14. For security, select **IAM**.
15. Click **Create function**.
16. Review the performed steps. For example, after selecting the

`save-certificate-event-record-in-dynamodb`

name for the Lambda function, you should go to a page like the following.



Configuring the AWS Lambda function

Configure the Lambda function previously created in Creating the AWS Lambda function .

To configure the Lambda function

1. Copy the contents of the `dynamo-db-lambda.py` file provided with the AWS CA Gateway plugin artifact.
2. Paste the contents under the **Code source** tab to replace the `dynamo-db-lambda.py` contents.
3. Assign to the `TABLE_NAME` variable the name of the DynamoDB table created earlier. For example:

```
TABLE_NAME = "certificate-events"
```

⚠ Be careful if you choose to edit the Lambda code in any other way. The Lambda code is directly responsible for storing certificate event records in the DynamoDB table, so the correctness of CA Gateway certificate events API depends on the correctness of this Lambda code.

4. Click **Deploy** above the code file.
5. Click the **Configuration** tab.
6. On the left pane, select **Permissions**.
7. In the **Execution role** section, click the role associated with this Lambda function. You should see a summary of the Lambda function role in a new tab.
8. In the new tab, click **Attach policies** under **Permissions**.
9. On the resulting page, search for `AWSCertificateManagerPrivateCAReadOnly`.
10. Select the `AWSCertificateManagerPrivateCAReadOnly` policy.
11. Click **Attach policy**. Attaching this policy to the role allows the Lambda function to retrieve certificate content from an AWS private CA.
12. Verify that your role has all of the necessary permissions. The following permissions will suffice.
 - Certificate Manager Private Certificate Authority: List, Read
 - DynamoDB: Read, Write
 - CloudWatch Logs: Write

Limiting AWS DynamoDB permissions (optional)

You may wish to limit the DynamoDB permissions to saving certificate events in the AWS DynamoDb table.

To limit the DynamoDB permissions

1. In the **AWSLambdaMicroserviceExecutionRole** section containing the DynamoDB permissions, click **Edit policy**.
2. In the JSON tab, replace the value in the Resource field with the ARN of the DynamoDb table previously created in [Creating the AWS DynamoDb table](#). To get this ARN in the DynamoDB service console, go to the **Table details** section and click the **Overview** tab.

Limiting AWS Private Certificate Manager permissions (optional)

You may wish to limit Certificate Manager Private CA permissions to the CA(s) the Lambda code will access. As the policy already attached to the Lambda role is a pre-packaged AWS-managed policy, you won't be able to edit it. Instead, you'll have to create a policy.

To limit the Private Certificate Manager permissions

1. Remove the **AWSCertificateManagerPrivateCAReadOnly** policy by clicking the **X** to the right of it. Confirm this action when prompted.
2. Click **Attach policies**.
3. Click **Create policy**.
4. Create the policy either via the **Visual editor** or the **JSON** editor.

Creating the AWS EventBridge rule

Create an AWS EventBridge rule for invoking the Lambda function.

To create an EventBridge rule

1. Search for `Amazon EventBridge` in the search box at the top of the AWS Management Console.
2. Navigate to the main page of the Amazon EventBridge service.
3. Select **Create rule**.
4. Provide a name and description for the rule.
5. In the **Define pattern** section, select **Event pattern**.
6. In **Event matching pattern**, select **Pre-defined pattern by service**.
7. In **Service provider** select **AWS**.
8. In **Service name**, select **Certificate Manager Private CA**.
9. In **Event type** select **AWS API Call via CloudTrail**.

10. Select **Specific operation(s)** instead of the default **Any operation**.
11. Add the **IssueCertificate** and **RevokeCertificate** operations.
12. Review the configuration. The **Event pattern** should look like this.

```
{
  "source": ["aws.acm-pca"],
  "detail-type": ["AWS API Call via CloudTrail"],
  "detail": {
    "eventSource": ["acm-pca.amazonaws.com"],
    "eventName": ["IssueCertificate", "RevokeCertificate"]
  }
}
```

13. In the **Select event bus** section, select **AWS default event bus** (selected by default).
14. In the **Select targets** section under the first **Target**, select **Lambda function** (selected by default).
15. Under **Function** select the Lambda function previously created in Creating the AWS Lambda function.
16. Click **Create**.

Configuring the AWS DynamoDB table in CA Gateway

Edit the CA Gateway

`application.yml`

file and configure the following in the AWS-managed CA settings.

Setting	Value
properties.certificate-events-storage-method	"DynamoDb"
properties.dynamodb-table-name	The table name selected in Creating the AWS DynamoDb table .

For example:

```
AWSWITHDYNAMODB:
  name: "AWS Private Root CA"
  issuer-dn: "L=Dallas, CN=WY Root CA 1, ST=Texas, OU=Terraforming, O=Weylan-
Yutani Corporation, C=US"
  connector-name: com.entrust.awsca
  properties:
    aws-region: "us-east-1"
    aws-ca-arn: "arn:aws:acm-pca:us-east-1:422825380052:certificate-authority/
2b33862c-e9f0-490d-9a3a-ad74476f7bca"
    aws-ca-s3-crl-arn: ""
    aws-ca-audit-report-s3-bucket-name: "cagw-audit-report"
    aws-api-url: "https://acm-pca.us-east-1.amazonaws.com:443/"
    aws-user-login-url: "https://edc-admin-services-dev.signin.aws.amazon.com/
console"
    aws-user-arn: "arn:aws:iam::422825380052:user/cagw-ca-user"
    aws-user-access-key-id: "ABCDEFG1234567890123"
    aws-user-secret-access-key: "ABCDEFG123456789012345678901234567890123"
```

```
certificate-events-storage-method: "DynamoDb"  
dynamodb-table-name: "certificate-events"
```

Integrating an ECS CA

See below for configuring CA Gateway for integrating CAs of the Entrust Certificate Services (ECS).


- [Issuing the SSL certificate](#)
- [Creating the API username and key](#)
- [Adding tracking information to the certificate requests](#)

See the [CA Capabilities reference](#) for a complete description of the operations supported by these CAs.

Issuing the SSL certificate

Generate the SSL certificate that CA Gateway will use to authenticate enrollment operations with the ECS-managed CA.

- [Generating the key pair](#)
- [Generating the certificate signing request](#)
- [Issuing the certificate](#)
- [Generating the SSL PKCS#12](#)

 You can run the commands below on the machine hosting CA Gateway or on any machine with OpenSSL installed.

Generating the key pair

Run the following command to generate the key pair.

```
openssl genrsa -out key.pem 2048
```

Generating the certificate signing request

Run the following command to generate the certificate signing request.

```
openssl req -new -key key.pem -out csr.pem
```

When requested for the Common Name, enter a domain or subdomain verified in your account.

Issuing the certificate

Process the certificate signing request to issue a certificate.

To issue the certificate

1. As a Super Admin user, log in to the ECS Portal.
2. Navigate to **Create > SSL/TLS**
3. In the create wizard, paste the generated PEM request contents.
4. Select one of the following extended key usages:
 - **Client Authentication**
 - **Client and Server Authentication.**

5. Complete the wizard steps.
6. Navigate to **Certificates > Managed Certificates > ECS Certificates**.
7. Record the **Tracking ID** value for future use.
8. Go to **Actions > Pickup**.
9. Type the password, if required.
10. Select the **WS_FTP** server type.
11. Download a Zip file containing the issued certificate, the certification chain, and the root certificate.

Generating the SSL PKCS#12

Generate a PKCS#12 containing the SSL keys and certificates – for example:

```
openssl pkcs12 -export -in ServerCertificate.crt -certfile chain.pem -inkey key.pem  
-out restapi.p12
```

You will later set this PKCS#12 as either a file path or a base64 encoding. To encode the PKCS#12 in Base64, run:

```
base64 restapi.p12 -w 0 > restapi.txt
```

Where the `-w 0` option formats the output as one line without line breaks.

Creating the API username and key

Create a username and a key for authenticating with the Entrust Certificate Services API.

To create the API username and key

1. Log in to the Entrust Certificate Services portal as a Super Admin user.
2. Navigate to **Administration > Advanced Settings > Localization**.
3. Select **English** in the **Account language** list and click **Save**.
4. Navigate to **Administration > Advanced Settings > API**
5. Use the recorded Tracking ID value to select the SSL certificate.
6. Click on **Generate credentials**
7. Record the displayed username and key.

✗ The system will not display the key again.

Adding tracking information to the certificate requests

In addition to the fields required by the CA Gateway API, certificate requests for ECS CAs must include tracking information. For example:

```
"properties": {  
  "requesterEmail": "requester@mail.com",  
  "requesterPhone": "123456789",  
  "requesterName": "Request Name",  
  "trackingInfo": "tracking info test",  
  "additionalEmails": "test1@mail.com, test2@mail.com",  
  "text4": "this is custom text 4",  
  "date1": "2022-07-01T12:24:27.627Z",  
  "number3": 33  
}
```

```
}
```

As we see in the example, this tracking information can include custom fields to meet customer requirements.

Integrating an Entrust Certificate Authority

As explained in the following sections, CA Gateway requires an administrator profile to integrate an Entrust Certificate Authority.

- [Enabling TLS 1.0 and TLS 1.1](#)
- [Creating a certificate type for the administrator profile](#)
- [Creating a new certificate definition policy for the certificate type](#)
- [Mapping the certificate definition policy to the certificate type](#)
- [Creating a client policy for the administrator profile](#)
- [Creating a role for the administrator profile](#)
- [Creating a user entry for the administrator profile](#)
- [Creating the administrator profile](#)

See the [CA Capabilities reference](#) for a complete description of the operations supported by these CAs.

Enabling TLS 1.0 and TLS 1.1

Some early versions of Entrust Certificate Authority require older versions of TLS disabled by default. To enable these versions:

1. Edit the `application.yml` configuration file.
2. Enable the selected TLS versions under `cagw.deploy.enable`.

Creating a certificate type for the administrator profile

Create a certificate type for the administrator profile CA Gateway will use to connect and perform operations with Entrust Certificate Authority.

To create a certificate type for the administrator profile

1. Export the certificate specifications from the Entrust Certificate Authority:
 - a. Log in to Entrust Certificate Authority for the Entrust Certificate Authority.
 - b. Select **File > Certificate Specifications > Export**.
 - c. Save the file to a location on the computer.
2. Open the certificate specifications file in a text editor.
3. Add the following to the `[Certificate Types]` section:

```
ent_cagwxap_rsa1=enterprise,CAGW Admin,CA Gateway XAP Administrator
```

4. Add the following to the `[Extension Definitions]` section:

```
[ent_cagwxap_rsa1 Certificate Definitions]
1=Dual Usage; Single key dual usage key pair Certificate Type
[ent_cagwxap_rsa1 Dual Usage Extensions]
keyusage=2.5.29.15,c,m,BitString,101; digitalSignature(0) and
keyEncipherment(2)
```

```
; Encodes the entAdminServicesClients policy OID (2.16.840.1.114027.10.4)
certificatepolicies=2.5.29.32,n,o,DER,300D300B06096086480186FA6B0A04
```

5. Save and close the file.
6. Import the certificate specifications back into the Entrust Certificate Authority:
 - a. Log in to Entrust Certificate Authority for the Entrust Certificate Authority.
 - b. Selecting **File > Certificate Specifications > Import**.
 - c. Select the file you edited earlier.

Creating a new certificate definition policy for the certificate type

The certificate type created in [Creating a certificate type for the administrator profile](#) has a Dual Usage certificate definition. You must create a new certificate definition policy for this certificate definition that disables private key backup and enforces generating the key at the client application.

To create a new certificate definition policy for the new certificate type

1. Log in to the Entrust Certificate Authority administration console.
2. In the tree view, expand **Security Policy > User Policies**.
3. Select **Dual Usage Policy**.
4. Select **Policies > User Policies > Selected User Policy > Copy**.
The **Copy User Policy** dialog box appears.
5. In the **Label** field, enter **Dual Usage CAGW Admin Policy**.
6. In the **Common name** field, enter **Dual Usage CAGW Admin Policy**.
7. In the **Add to** drop-down list, select the searchbase where you want to store the user policy.
8. Under **Policy Attributes**:
 - Deselect **Backup private key**.
 - Select **Generate key at client**.
9. Click **OK**.
10. If prompted, authorize the operation. The operation may require more than one authorization. See the Entrust Certificate Authority documentation for details.

Mapping the certificate definition policy to the certificate type

After creating a certificate definition policy, you must map this certificate definition policy to the certificate type.

To map the certificate definition policy to the certificate type

1. Log in to the Entrust Certificate Authority administration portal
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > Certificate Types > CAGW Admin > Dual Usage**.
3. In the **Certificate definition policy** drop-down list, select **Dual Usage CAGW Admin Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation. The operation may require more than one authorization. See the Entrust Certificate Authority documentation for details.

Creating a client policy for the administrator profile

Create a client policy for the administrator profile CA Gateway will use to connect and perform operations with Entrust Certificate Authority.

To create a new client policy for the administrator profile

1. Log in to the Entrust Certificate Authority administration portal.
2. In the tree view, expand **Security Policy > User Policies**.

3. Select **Administrator Policy**.
4. Select **Policies > User Policies > Selected User Policy > Copy**.
The **Copy User Policy** dialog box appears.
5. In the **Label** field, enter `CAGW Admin Policy`.
6. In the **Common name** field, enter `CAGW Admin Policy`.
7. In the **Add to** drop-down list, select the searchbase where you want to store the user policy.
8. Under **Policy Attributes**, select **Permit Server Login usage**.
9. Click **OK**.
10. If prompted, authorize the operation. The operation may require more than one authorization. See the Entrust Certificate Authority documentation for details.

Creating a role for the administrator profile

CA Gateway requires an administrator profile issued by the Entrust Certificate Authority. This profile must have a role with the following permissions.

Permission category	Permissions
Certificates	Administer at least one certificate category. Currently, CA Gateway supports only Enterprise certificate types.
Certificate Types	Administer at least one certificate type.
Groups	<ul style="list-style-type: none">• View• Administer at least one group
License Information	View
Roles	<ul style="list-style-type: none">• View• Administer at least one role.
Searchbases	<ul style="list-style-type: none">• View• Administer at least one searchbase.
Security Policy	<ul style="list-style-type: none">• Force CRLs• View User Policy• View Security Policy• Export Certificate Specification
User Templates	Administer at least one template

Permission category	Permissions
User - General	<ul style="list-style-type: none"> • View • Add • Reactivate • Deactivate/Remove • Change DN • Modify properties • Revoke certificates • Update key pairs • Set for key recovery • Cancel key recovery • Modify key update options • View activation code • Reissue activation code
User - Advanced	Change user's role

 Refer to the Entrust Certificate Authority documentation for more details on role configuration.

To create a new role for the administrator profile

1. Log in to Entrust Certificate Authority administration portal.
2. In the tree view, expand **Security Policy > Roles**.
3. Select **Policies > Roles > New** to create a new role. Alternatively, you can copy the **Administrator** role because this role includes most of the permissions required for the new role.
 - a. Select **Administrator**.
 - b. Select **Policies > Roles > Selected Role > Copy**. A copy of the role appears at the bottom of the list of roles in the tree view, and the new role's properties appear in the right pane.
4. Click the **Role** tab.
 - a. Into the **Unique name** field, enter `CAGW Admin Role`.
 - b. In the **Authorizations** field, enter 1.
 - c. In the **User Policy** drop-down list, select **CAGW Admin Policy**. This is the client policy you created earlier.
 - d. Unselect the **End User** check box. This check box should already be deselected.
5. Click the **Permissions** tab.
6. Configure the permissions documented in the above table and click **Apply**.
7. If prompted, authorize the operation. As explained in the Entrust Certificate Authority documentation, the operation may require more than one authorization.
8. A **Permission Dependencies** pop-up dialog may list additional permissions required for the role to function properly. Add these missing permissions to the role.

Creating a user entry for the administrator profile

Create a user entry in Entrust Certificate Authority for the administrator profile.

To create a user entry for the administrator profile

1. Log in to the Entrust Certificate Authority administration portal.
2. Select **Users > New User** to display the **New User** dialog.
3. Select the following tabs to configure the corresponding fields.

- [Naming](#)
- [General](#)
- [Certificate Info](#)
- [Key Update Options](#)

4. Click **OK**.
5. If prompted, authorize the operation. The operation may require more than one authorization. See the Entrust Certificate Authority documentation for details.
6. Copy the reference number and authorization code required to create the administrator profile. You will require them later to create and activate the user's Entrust digital ID. See the Entrust Certificate Authority documentation for more details about how the Registration number and Authorization codes are used.

Naming

Configure the following fields under this tab.

Field	Value
Type	Select a user type.
User fields	Enter a value for all configuration fields of the selected user type.
Add to	Select a searchbase for the user – for example, select CA Domain Searchbase to add the user entry to the default searchbase.

General

Configure the following fields under this tab.

Field	Value
User role	Select the role described in Creating a role for the administrator profile .
User group(s)	Assign the user to one or more groups.

Certificate Info

Configure the following fields under this tab.

Field	Value
Category	Select Enterprise .
Certificate Type	Select the role described in Creating a role for the administrator profile .

Key Update Options

Under this tab, enable the **Use default key update policy** option.

Creating the administrator profile

To connect and perform operations with Entrust Certificate Authority, CA Gateway requires an administrator profile that is issued by Entrust Certificate Authority.

To create the administrator profile

1. Install JDK (Java Development Kit) 17 and set the `JAVA_HOME` environment library.
2. Log in to <https://trustedcare.entrust.com>
3. Go to **PKI > Authority > CA Gateway**.
4. Download the Profile Creation Utility for your preferred operating system:
 - `cagw-profilecreationutility-linux64-version.zip` for Linux 64-bit.
 - `cagw-profilecreationutility-win64-version.zip` for Windows 64-bit.
5. Extract the file contents.
6. Run the CA Gateway Profile Creation Utility as explained in the following sections.
 - [Creating the administrator profile on software](#)
 - [Using the Profile Creation Utility to create the administrator profile on hardware](#)

Creating the administrator profile on software

As explained in this section, you can store the administrator profile in software as an Entrust Profile File (EPF).

To create the administrator profile on software

1. Run the `<VERSION>` version of the CA Gateway Profile Creation Utility.
 - `cagw-profilecreationutility-<VERSION>/bin/pcu.sh` for Linux.
 - `cagw-profilecreationutility-<VERSION>/bin/pcu.bat` for Windows.
2. Once on the main menu, select option **2** for **Create Entrust profile**.
3. Select option **1** for **File on disk**
4. In **Take settings from an existing entrust.ini file (y/n)?** enter **y** for yes.
5. In **Enter full path to entrust.ini**, enter the path of the local file.
6. In **Enter reference number**, enter the reference number you obtained when creating a user entry for the administrator profile.
7. In **Enter authorization code**, enter the authorization code you obtained when creating a user entry for the administrator profile.
8. In **Enter profile name**, enter a file name for the EPF file. Do not include a file name extension because the utility automatically appends a .epf extension. If you include a .epf extension in the name, it will be added to the file twice.
9. In **Enter profile directory**, enter the directory for the EPF file. The name of this file is the name previously entered in **Enter profile name**.
10. In **Enter profile password**, enter a new password to encrypt and MAC the contents of the EPF.

Using the Profile Creation Utility to create the administrator profile on hardware

For information about creating the administrator profile on hardware, see the CA Gateway integration guide for your hardware security module (HSM).

Configuring and deploying CA Gateway

See below for configuring and deploying CA Gateway with the Management Console.

To configure and deploy CA Gateway with the Management Console

1. Open the following URL in a Web browser.

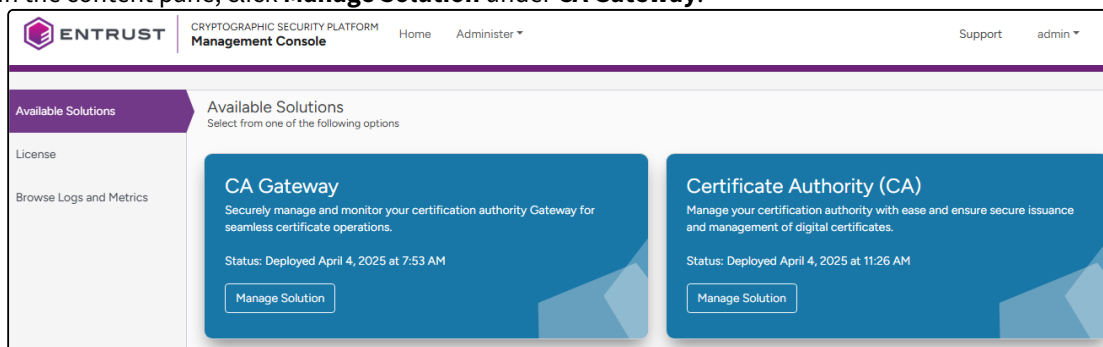
`https://<machine>/management-console`

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

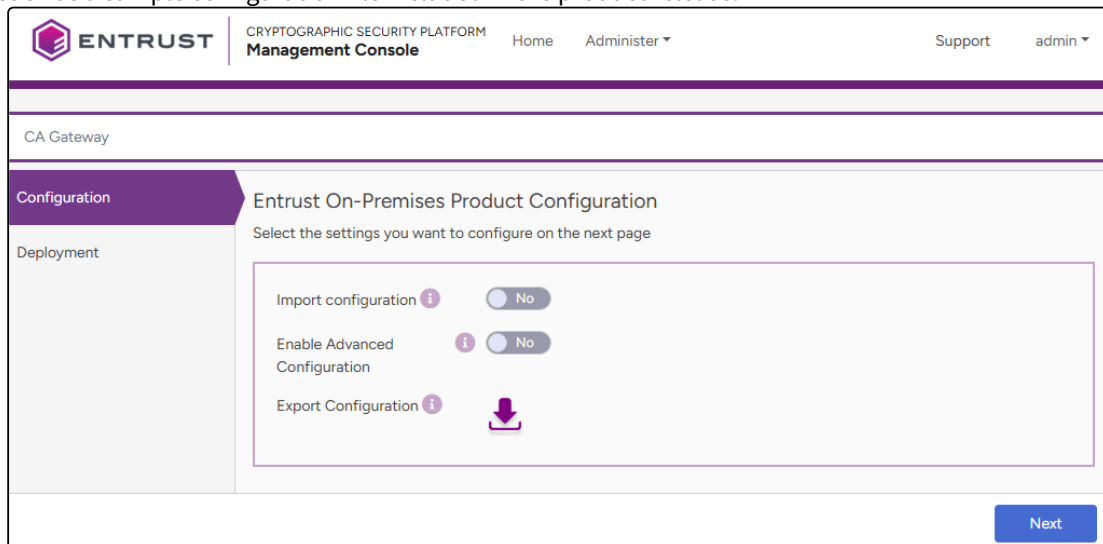
2. Log into the Management Console a user belonging to a role with CA Gateway management permissions – for example, the initial `admin` administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

3. In the content pane, click **Manage Solution** under **CA Gateway**.



1. Activate the **Import configuration** toggle switch if you want to import configuration settings from a file, such as a sample configuration file included in the product release.



2. Click **Next**.
3. Configure the solution settings described in the following sections.
 - [Logging](#)
 - [Server](#)
 - [Connector filters](#)
 - [Authorities](#)
 - [Profiles](#)

- [Tenants](#)
- [Clients](#)
- [Cmpv2](#)
- [TLS CRL-settings](#)

1. Click **Validate** to validate the configured settings.
2. Correct any detected configuration error until the **Validate** option displays no warnings.
3. Optionally, click the **Download** button to export the current configuration. You can later import this configuration using the already mentioned **Import configuration** toggle switch.
4. Click **Submit** and wait while Cryptographic Security Platform uploads the configuration and any attached file, such as a P12 file with authentication credentials.
5. Click **Deploy**.

Logging

Set the following parameters in the **Logging** tab of the **Configuration** page.

Level

Select the level of detail for the root CA Gateway's logger. In increasing severity:

- TRACE
- DEBUG
- INFO
- WARN
- ERROR
- FATAL
- OFF

Each level sets the lowest message level to show. For example, the **WARN** level provides messages with the **WARN**, **ERROR**, and **FATAL** status.


JTK Logging

To enable JSTK logging:

1. Click  in the **Enable** field.
2. Select the log detail in the **JTK Logs Level** list (from 0 to 4, in increasing severity).

JSSE Logging

To enable JSSE logging:

1. Click  in the **Enable** field.
2. Select the log detail in the **JSSE Logs Level** list.

Server

Set the following parameters in the **Server** tab of the **Configuration** page.

- [Comma-separated list of Ciphers](#)
- [Key Alias](#)
- [Key Store](#)
- [Key Store Password](#)

- [Key Store Type](#)
- [Trust Store Type](#)
- [Trust Store](#)
- [Trust Store Password](#)

Comma-separated list of Ciphers

The list of allowed SSL ciphers – for example:

```
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,  
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_128_GCM_SHA256
```

Key Alias

The alias of the SSL key in the keystore.

Mandatory: Yes.

Key Store

The keystore that contains the SSL server certificate. Click **Select Files** to import this keystore from file.

Key Store Password

The password of the keystore that contains the server SSL certificate.

Mandatory: Yes.

Key Store Type

The type of keystore containing the SSL server certificate.

Type	Description
jks	Java keystore
pkcs12	PKCS #12 keystore

Mandatory: Yes.

Trust Store Type

The type of truststore containing the CA certificates.

Type	Description
jks	Java truststore

Type	Description
pkcs12	PKCS #12 truststore

Mandatory: Yes.

Trust Store

Click **Select Files** to import the truststore file.

Trust Store Password

The password of the truststore that contains the CA certificates.

Mandatory: Yes.

Connector filters

Create lists of connector filters.

To create a list of connector filters

1. Click **+ Filter list** in the **Connector filters** tab of the **Configuration** page.
2. Enter an identifier for the new list.
3. For each filter on the list:
 - a. Click **+ Filter**
 - b. Enter a **Name** for the filter.
 - c. Select one of the following identifiers under **Connector Name**.
 - [com.entrust.CAAuthorization](#)
 - [com.entrust.CertificateEvents](#)
 - [com.entrust.CertTransparency](#)
 - d. Click **+ Filter Settings** and add the settings described below for each connector.

com.entrust.CAAuthorization

Filter to conduct CA Authorization checks for certificates intended for public trust. When selecting this filter, configure the following settings under `properties`.

- `check-domains-external-to-cs`
- `check-domains-from-csr`
- `dns-server.<i>.<setting>`
- `issuer-string`
- `log-server.<i>.<setting>`

check-domains-external-to-cs

`true` for CA Gateway to make CAA checks for domains in the subjectAltNames field external to the CSR, `false` otherwise.

Mandatory: No. This optional parameter defaults to `true`.

check-domains-from-csr

`true` for CA Gateway to make CAA checks for domains inside the CSR, `false` otherwise.

Mandatory: No. This optional parameter defaults to `true`.

dns-server.<i>.<setting>

The DNS settings, where "i" is an index starting at 0. You can omit this index when defining a single DNS.

<setting>	Value	Default
ip	The IP address of the local DNS server that CA Gateway will use to look up the DNS issuer resource record.	–
port	The port of the DNS server.	53
timeout-first-seconds	The timeout of the first DNS lookup attempt, in seconds.	3
timeout-second-seconds	Timeout of the second DNS lookup attempt, in seconds. Applicable if the first attempt results in an error.	7
timeout-dsquery-seconds	Timeout in seconds of the Delegation Signer (DS) query when querying DNSSEC support.	7

Mandatory: Yes.

issuer-string

The CAA issuer name, as expected in the DNS resource record. Real-world examples include:

- entrust.net
- pki.goog

The name is owned and defined by the issuer and registered in DNS for any CA to check.

Mandatory: Yes

log-server.<i>.<setting>

The settings of each log server CA Gateway must contact to request the signed CT response. Therefore, you must define at least one server, with `<i>` starting a 0.

<setting>	Value
name	A friendly name for the log server. For example: "Google Log Server".

<setting>	Value
url	The URL of the log server
google	True if the SCTs produced by this log server are Google Chrome compatible.
public-key	The public key of the log server, as a Base64 DER-encoded public key. Log servers typically advertise their keys publicly.
tls-trust-anchor	The trust anchor for the CT Filter to perform the TLS handshake with the log server, as a Base64 DER-encoded certificate.

Mandatory: Yes.

com.entrust.CertificateEvents

Convenience filter to:

1. Read a certificate.
2. Extract data from the certificate.
3. Add the data to the response so that the caller does not have to immediately decode the certificate.

This filter does not require configuring properties.

com.entrust.CertTransparency

Filter to:

1. Collect a set of signed CT log server responses.
2. Ask the underlying CA if the certificates for public trust include these responses in an SCT List extension.

When selecting this filter, configure the following settings under `properties`.

- `connection-timeout-millis`
- `ct-policy-json`
- `log-server.<i>.<setting>`
- `proxy-host-name`
- `proxy-port`
- `socket-timeout-millis`

connection-timeout-millis

The connection timeout for the HTTP communication with the log server, in milliseconds.

Mandatory: No. This optional parameter defaults 5000 milliseconds.

ct-policy-json

The number of log server responses CA Gateway must wait for.

i CA Gateway can cope with slow running or unresponsive log servers when the number of servers configured under `log-server.<i>.setting` exceeds the number of required responses.

The general form of this JSON value is:

```
{
  sct-policy:[
    [<months-threshold>,<threshold-equals>,<google-min-responses>,<non-google-min-responses>]
  ],
  insurance:<insurance>
}
```

See the following table for a description of each parameter.

Parameter	Value
months-threshold	The applicability of the <code>sct-policy</code> policy according to the certificate lifetime, as a number of months. When defining multiple policies, this value determines which policy to apply for issuing a certificate. On the other hand, specifying a high value ensures this policy applies to all certificates issued.
threshold-equals	<code>true</code> for comparing the months-threshold and the actual certificate lifetime with the equals operator ('='); <code>false</code> for comparing with the less than or equals operator ('<=').
google- min- responses	The minimum number of Google-compatible log server responses to include in the issued certificate.
non-google- min-responses	The minimum number of non-Google-compatible log server responses to include in the issued certificate.
insurance	The number of log server responses to collect above the following minimum: <div>google-min-responses + non-google-min-responses</div>

Mandatory: No. This optional parameter defaults to:

```
{
  sct-policy:[
    [39,true,0,1]
  ],
```



```
insurance:0
}
```

In the configuration, you can flatten this default value to:

```
{sct-policy:[[38,true,0,1]],insurance:0}
```

log-server.<i>.<setting>


The settings of each log server CA Gateway must contact to request the signed CT response. Therefore, you must define at least one server, with <i> starting a 0.

<setting>	Value
name	A friendly name for the log server. For example: "Google Log Server".
url	The URL of the log server
google	True if the SCTs produced by this log server are Google Chrome compatible.
public-key	The public key of the log server, as a Base64 DER-encoded public key. Log servers typically advertise their keys publicly.
tls-trust-anchor	The trust anchor for the CT Filter to perform the TLS handshake with the log server, as a Base64 DER-encoded certificate.

Mandatory: Yes.

proxy-host-name

The hostname of the proxy for accessing the CA server.

 The proxy configured using this parameter is part of your corporate infrastructure; it is not an Entrust product.

Mandatory: Only when traffic to the CA server passes through a proxy.

proxy-port

The port for accessing the proxy.

Mandatory: Only when traffic to the CA server passes through a proxy.

socket-timeout-millis

The TCP Socket timeout for the HTTP communication with the log server, in milliseconds.

Mandatory: No. This optional parameter defaults 5000 milliseconds.

Authorities

For each certificate authority, set the following field values in the **Authorities** tab of the **Configuration** page.

- [Minimum keysize](#)
- [Authority settings](#)

Minimum keysize

Configure the minimum sizes supported by all authority keys.

- [Specify whether to disable, log or reject key size violations](#)
- [Minimum RSA Keysize](#)
- [Minimum ECC Keysize](#)

Specify whether to disable, log or reject key size violations

The performed action when an authority key does not meet the [Minimum RSA Keysize](#) or [Minimum ECC Keysize](#) size requirements.

Value	Action
off	Nothing
log	Log the key size
block	Reject the key

Minimum RSA Keysize

The minimum size for all authority RSA keys, as a number of bytes.

Minimum ECC Keysize

The minimum size for all authority ECC (elliptic curve) keys, as a number of bytes.

Authority settings

To register an authority, click the **+** button and configure the following settings.

- [Choose a key name](#)
- [Name](#)
- [Issuer DN](#)
- [Minimum keysize](#)
- [Connector Name](#)

Choose a key name

Type a unique identifier for the authority.

Mandatory: Yes.

Name

A friendly name for the CA.

Mandatory: Yes

Issuer DN

The Distinguished Name (DN) of the CA. For example:

```
CN = Certificate Authority, O = Entrust, Inc, C = US
```

```
CN = "Entrust Class 2 Client CA", OU = "(c) 2010 Entrust, Inc.", OU =  
"www.entrust.net/CPS is incorporated by reference", O = "Entrust, Inc.", C = US
```

As explained in [RFC 2253](#), you can surround the value of each DN field with quote ("" ASCII 34) characters, which are not part of the value. Inside the quoted value, the following characters can occur without any escaping:

- ""
- ,
- "="
- "+"
- "<"
- ">"
- "#"
- ";"

Mandatory: Yes.

Minimum keysize

Configure the minimum sizes supported by this specific authority authority key.

- [Specify whether to disable, log or reject key size violations](#)
- [Minimum RSA Keysize](#)
- [Minimum ECC Keysize](#)

Specify whether to disable, log or reject key size violations

The performed action when this authority key does not meet the [Minimum RSA Keysize](#) or [Minimum ECC Keysize](#) size requirements.

Value	Action
off	Nothing
log	Log the key size
block	Reject the key

Minimum RSA Keysize

The minimum size for this authority RSA key, as a number of bytes.

Minimum ECC Keysize

The minimum size for this authority ECC (elliptic curve) key, as a number of bytes.

Connector Name

The CA connector name. See below for the supported values.

- [com.entrust.ECS](#)
- [com.entrust.MicrosoftCA](#)
- [com.entrust.SecurityManager](#)

com.entrust.ECS

To integrate an ECS certificate authority, select this connector and configure the following settings.

- [ECS URL](#)
- [User Name](#)
- [API Key](#)
- [Enrollment Agent PKCS#12 File](#)
- [Enrollment Agent PKCS#12 Password](#)
- [CA Certificate](#)
- [CA Certificate Chain](#)
- [Client ID defined in ECS for all domain operations](#)
- [Proxy Hostname](#)
- [Proxy Port](#)
- [Proxy username](#)
- [Proxy password](#)
- [Additional ECS Properties](#)

ECS URL

Set this parameter to:

`https://api.entrust.net/enterprise/v2`

Mandatory: Yes.

User Name

The API username for consuming the ECS CA services. See the CA Gateway guide for how to obtain this username.

Mandatory: Yes.

API Key

The API key for consuming the ECS CA services. See the CA Gateway guide for how to obtain this key.

Mandatory: Yes.

Enrollment Agent PKCS#12 File

The PKCS#12 file containing the CA certificate. Click **Select Files** to import this file.

Enrollment Agent PKCS#12 Password

The password of the PKCS#12 file containing the CA certificate.

CA Certificate

The DER and Base64 encoding of the ECS issuing CA certificate. CA Gateway returns the selected certificate when querying the following resource with `$field` set to `ca.cert`.

```
GET /v1/certificate-authorities
```

i You must statically configure this setting because the ECS public API does not yet allow querying certificates from the CA.

Mandatory: Yes.

CA Certificate Chain

The DER and Base64 encoding of the ECS CA certificate chain.

i You must statically configure this setting because the ECS public API does not yet allow querying certificates from the CA.

Mandatory: Yes.

Client ID defined in ECS for all domain operations

The client identifier defined in ECS for all domain operations sent to the ECS API.

i You must statically configure this setting because the ECS public API does not yet allow querying certificates from the CA.

Mandatory: No. This optional parameter defaults to 1.

Proxy Hostname

The hostname of the proxy for accessing the ECS CA server.

Mandatory: Only when traffic to the ECS CA server passes through a proxy.

Proxy Port

The port for accessing the proxy server.

Mandatory: Only when traffic to the ECS CA server passes through a proxy.

Proxy username

The username for authenticating in the proxy server.

Mandatory: Only when the proxy requires authentication.

Proxy password

The password for authenticating in the proxy server.

Mandatory: Only when the proxy requires authentication.

Additional ECS Properties

Click **+ ECS Properties** to add the following settings.

- `api-key`
- `ca.cert`
- `ca.certchain.<i>`
- `client-id-domains`
- `ecs-url`
- `enrollment-agent-p12`
- `enrollment-agent-p12-password`
- `proxy-host-name`
- `proxy-password`
- `proxy-port`
- `proxy-username`
- `rdn-corrections.<i>.rep`
- `rdn-corrections.<i>.rep-with`
- `user-name`

`api-key`

The API key for consuming the ECS CA services. See the CA Gateway guide for how to obtain this key.

Mandatory: Yes.

`ca.cert`

The DER and Base64 encoding of the ECS issuing CA certificate. CA Gateway returns the selected certificate when querying the following resource with `$field` set to `ca.cert`.

```
GET /v1/certificate-authorities
```

i You must statically configure this setting because the ECS public API does not yet allow querying certificates from the CA.

Mandatory: Yes.

`ca.certchain.<i>`

The DER and Base64 encoding of the certificate in the `<i>` position of the ECS CA certificate chain. For example, the certificate specified with the `ca.certchain.0` parameter is the certificate of the CA that issued the certificate specified with the `ca.cert` parameter.

CA Gateway returns the selected certificate when querying the following resource with `$field` set to `ca.chain`.


```
GET /v1/certificate-authorities
```

i You must statically configure this setting because the ECS public API does not yet allow querying certificates from the CA.

Mandatory: Yes.

`client-id-domains`

The client identifier defined in ECS for all domain operations sent to the ECS API.

 You must statically configure this setting because the ECS public API does not yet allow querying certificates from the CA.

Mandatory: No. This optional parameter defaults to 1.

ecs-url

Set this parameter to:

```
https://api.entrust.net/enterprise/v2
```

Mandatory: Yes.

enrollment-agent-p12

The SSL PKCS#12, as a file path or a Base64 encoding.

Mandatory: Yes.

enrollment-agent-p12-password

The password of the SSL PKCS#12.

Mandatory: Yes.

proxy-host-name

The hostname of the proxy for accessing the ECS CA server.

Mandatory: Only when traffic to the ECS CA server passes through a proxy.

proxy-password

The password for authenticating in the proxy server.

Mandatory: Only when the proxy requires authentication.

proxy-port

The port for accessing the proxy server.

Mandatory: Only when traffic to the ECS CA server passes through a proxy.

proxy-username

The username for authenticating in the proxy server.

Mandatory: Only when the proxy requires authentication.

rdn-corrections.<i>.rep

A distinguished name (DN) attribute you want to rename using the [rdn-corrections.<i>.rep-with](#) parameter.

Specifically, some Entrust Certificate Services profiles may include legacy attribute names in the subject of the issued certificates. However, these attribute names may not be compatible with the industry-standard names used by some client applications.

Entrust Certificate Services legacy attribute name	Industry-accepted attribute name
jurisdictionOfIncorporationStateOrProvinceName	jurisdictionStateOrProv
jurisdictionOfIncorporationCountryName	jurisdictionCountryName

In this case, add the following lines to the CA Gateway configuration.

```
rdn-corrections.0.rep: jurisdictionCountryName
rdn-corrections.0.rep-with: jurisdictionOfIncorporationCountryName
rdn-corrections.1.rep: jurisdictionStateOrProvinceName
rdn-corrections.1.rep-with: jurisdictionOfIncorporationStateOrProvinceName
```

Before sending certificate renewal requests to Entrust Certificate Services, CA Gateway will apply this configuration and replace industry-compliant subject attributes with legacy ones.

Example of subject name with industry-compliant attribute names

```
CN=test.com, serialNumber=705421, businessCategory=Private Organization, O=Entrust Corporation, jurisdictionStateOrProv=Delaware, jurisdictionCountryName=US, L=Shakopee, ST=Minnesota
```

Example of subject name with Entrust Certificate Services legacy attribute names

```
CN=test.com, serialNumber=705421, businessCategory=Private Organization, O=Entrust Corporation, jurisdictionOfIncorporationStateOrProvinceName=Delaware, jurisdictionOfIncorporationCountryName=US, L=Shakopee, ST=Minnesota
```

Mandatory: Only when renewing certificates with Entrust Certificate Services.

rdn-corrections.<i>.rep-with

A new name for the distinguished name (DN) attribute you selected with the [rdn-corrections.<i>.rep](#) parameter.

Mandatory: Only when renewing certificates with Entrust Certificate Services.

user-name

The API username for consuming the ECS CA services. See the CA Gateway guide for how to obtain this username.

Mandatory: Yes.

com.entrust.MicrosoftCA

To integrate a Microsoft certificate authority, select this connector and configure the following settings.

- [CA Proxy URL](#)
- [CA Host](#)
- [CA Name](#)

- [LDAP Port](#)
- [LDAPS Port](#)
- [LDAP Host](#)
- [Key Recovery Agent PKCS#12](#)
- [Key Recovery Agent PKCS#12 Password](#)
- [Client Certificate Key Alias](#)
- [Client Certificate Keystore Type](#)
- [Client Certificate Keystore File](#)
- [Client Certificate Keystore Password](#)
- [SSL Truststore Type](#)
- [SSL Truststore File](#)
- [SSL Truststore Password](#)
- [Additional Microsoft CA Properties](#)

CA Proxy URL

The URL of the Entrust Proxy for Microsoft CA, in the following format:

```
https://<server>:8443/MSCAProxy
```

Mandatory: Yes.

CA Host

The CA hostname, as either:

- An IP
- A hostname
- A FQDN

As long as it resolves from the DNS.

Mandatory: Yes.

CA Name


The CA name – for example:

```
abc-issuing
```

Mandatory: Yes.

LDAP Port

The port number for LDAP connections with Microsoft Active Directory (for LDAPS connections, configure [LDAPS Port](#) instead).

 The port is anonymously bound. The Microsoft CA proxy connects to Active Directory to get certificate template information.

This value is typically 389, the well-known port for LDAP.

Mandatory: When not configuring [LDAPS Port](#).

LDAPS Port

The port number for LDAPS connections with Microsoft Active Directory (for LDAP connections, configure [LDAP Port](#) instead).

i The port is anonymously bound. The Microsoft CA proxy connects to Active Directory to get certificate template information.

This value is typically 636, the well-known port for LDAPS.

Mandatory: When not configuring [LDAP Port](#).

LDAP Host

The Microsoft Active Directory, as an IP, a hostname, or an FQDN (as long as it resolves from the DNS). The host must be in the [CA Host](#) domain because:

- CA Gateway only talks to the Entrust Proxy for Microsoft CA.
- The Entrust Proxy for Microsoft CA is on the CA's same domain and talks to the CA.

Mandatory: Yes.

Key Recovery Agent PKCS#12

The path of the key PKCS#12 generated when creating the RA recovery agents (if any). Where `<i>` is an integer greater than or equal to 0.

Mandatory: Only when creating the RA recovery agents.

Key Recovery Agent PKCS#12 Password

The password of the key recovery agent PKCS#12.

Mandatory: Only when creating the RA recovery agents.

Client Certificate Key Alias

The alias of the CA Gateway client key.

Mandatory: Yes.

Client Certificate Keystore Type

Set this parameter to:

JKS

Mandatory: Yes.

Client Certificate Keystore File

The filename of the CA Gateway client JKS.

Mandatory: Yes.

Client Certificate Keystore Password

The password of the CA Gateway client JKS.

Mandatory: Yes.

SSL Truststore Type

The type of CA Gateway trust store. Supported values are:

- JKS
- PKCS12

Mandatory: Yes.

SSL Truststore File

The CA Gateway truststore. Click **Select Files** to import this truststore from file.

SSL Truststore Password

The password of the CA Gateway trust store.

Mandatory: Yes.

Additional Microsoft CA Properties

Click + **Microsoft CA Properties** to add the following settings.

- [ca-host](#)
- [ca-name](#)
- [ca-proxy-url](#)
- [key-recovery-agent-p12-<i>](#)
- [key-recovery-agent-p12-password-<i>](#)
- [ldap-host](#)
- [ldap-port](#)
- [ldaps-port](#)
- [proxy-host-name](#)
- [proxy-password](#)
- [proxy-port](#)
- [proxy-ssl](#)
- [proxy-username](#)

ca-host

The CA hostname, as either:

- An IP
- A hostname
- A FQDN

As long as it resolves from the DNS.

Mandatory: Yes.

ca-name

The CA name – for example:

abc-issuing

Mandatory: Yes.

ca-proxy-url

The URL of the Entrust Proxy for Microsoft CA, in the following format:

```
https://<server>:8443/MSCAProxy
```

Mandatory: Yes.

key-recovery-agent-p12-<i>

The path of the key PKCS#12 generated when creating the RA recovery agents (if any). Where `<i>` is an integer greater than or equal to 0.

Mandatory: Only when creating the RA recovery agents.

key-recovery-agent-p12-password-<i>

The password of the key recovery agent PKCS#12.

Mandatory: Only when creating the RA recovery agents.

ldap-host


The Microsoft Active Directory, as an IP, a hostname, or an FQDN (as long as it resolves from the DNS). The host must be in the [ca-host](#) domain because:

- CA Gateway only talks to the Entrust Proxy for Microsoft CA.
- The Entrust Proxy for Microsoft CA is on the CA's same domain and talks to the CA.

Mandatory: Yes.

ldap-port

The port number for LDAP connections with Microsoft Active Directory (for LDAPS connections, configure [ldaps-port](#) instead).


 The port is anonymously bound. The Microsoft CA proxy connects to Active Directory to get certificate template information.

This value is typically 389, the well-known port for LDAP.

Mandatory: When not configuring [ldaps-port](#).

ldaps-port

The port number for LDAPS connections with Microsoft Active Directory (for LDAP connections, configure [ldap-port](#) instead).


 The port is anonymously bound. The Microsoft CA proxy connects to Active Directory to get certificate template information.

This value is typically 636, the well-known port for LDAPS.

Mandatory: When not configuring [ldap-port](#).

proxy-host-name


The hostname of the proxy for accessing the Microsoft CA server.

 The proxy configured using this parameter is part of your corporate infrastructure. Do not confuse it with the Entrust Proxy for Microsoft CA, which is selected using the [CA Proxy URL](#) parameter.

Mandatory: Only when traffic to the Microsoft CA Proxy passes through a proxy.

proxy-password


The password for authenticating in the proxy.

 The proxy configured using this parameter is part of your corporate infrastructure. Do not confuse it with the Entrust Proxy for Microsoft CA, which is selected using the [CA Proxy URL](#) parameter.

Mandatory: Only when the proxy requires authentication.

proxy-port

The port for accessing the proxy.

 The proxy configured using this parameter is part of your corporate infrastructure. Do not confuse it with the Entrust Proxy for Microsoft CA, which is selected using the [CA Proxy URL](#) parameter.

Mandatory: Only when traffic to the Microsoft Proxy passes through a proxy.


proxy-ssl

Under this section, configure the following authentication settings.

Setting	Value	Mandatory
client-cert-key-alias	The alias of the CA Gateway client key	✓
client-cert-key-store	The filename of the CA Gateway client JKS	✓
client-cert-key-store-password	The password of the CA Gateway client JKS	✓
client-cert-key-store-type	Set this parameter to <code>JKS</code>	✓
ssl-trust-store	The path of the CA Gateway trust store	✓
ssl-trust-store-password	The password of the CA Gateway trust store	✓
ssl-trust-store-type	The type of CA Gateway trust store. Supported values are <code>JKS</code> and <code>PKCS12</code>	✓

proxy-username

The username for authenticating in the proxy.

 The proxy configured using this parameter is part of your corporate infrastructure. Do not confuse it with the Entrust Proxy for Microsoft CA, which is selected using the [CA Proxy URL](#) parameter.

Mandatory: Only when the proxy requires authentication.

com.entrust.SecurityManager

To integrate Entrust Certificate Authority, select this connector and configure the following settings.

- [Security Manager Host](#)
- [PKIX Port](#)
- [LDAP Host](#)
- [LDAP Port](#)
- [LDAPS Port](#)
- [LDAP Principal](#)
- [LDAP Credential](#)
- [XAP Port](#)
- [Admin EPF file](#)
- [Admin EPF Password](#)
- [Initial XAP Connections](#)
- [Max XAP Connections](#)
- [XAP Connection Idle Timer \(seconds\)](#)
- [XAP Connection Socket Timer \(seconds\)](#)
- [XAP Logging](#)
- [XAP Logs Level](#)
- [P11 APF File](#)
- [P11 Library](#)
- [P11 Slot](#)
- [P11 Password](#)
- [Enable niche certificate types](#)
- [Allow 100% PKUP](#)
- [Enable CA Profile Sync](#)

Security Manager Host

The hostname of the Entrust Certificate Authority instance.

Mandatory: Yes

PKIX Port

The PKIX-CMP port number of the Entrust Certificate Authority instance

Mandatory: Yes


LDAP Host

The hostname of the directory instance.

Mandatory: Yes.

LDAP Port


The port number for LDAP connections with the Entrust Certificate Authority directory (for LDAPS connections, configure **LDAPS Port** instead).

 This value is typically 389, the well-known port for LDAP.

Mandatory: When using an LDAP connection.

LDAPS Port

The port number for LDAPS connections with Entrust Certificate Authority (for LDAP connections, configure **LDAP Port** instead).

 This value is typically 636, the well-known port for LDAPS.

Mandatory: When using an LDAPS connection.

LDAP Principal

The name of the LDAP user for logging in to the directory. Save this property in secure storage such as Vault rather than directly in a configuration file.

Mandatory: Yes

LDAP Credential

The password of the LDAP user. Save this property in secure storage such as Vault rather than directly in a configuration file.

Mandatory: Yes

XAP Port

The XAP port number of the Entrust Certificate Authority instance.

Mandatory: Yes.

Admin EPF file

The administrator's Entrust Profile File (EPF) for connecting to Entrust Certificate Authority. Click **Select Files** to import this file.

Mandatory: When saving the user settings in an Entrust Profile File (EPF).

Admin EPF Password

The password for decrypting the administrator's Entrust Profile File (EPF).

Mandatory: When saving the administrator's settings in an EPF.

Initial XAP Connections

The initial number of XAP connections to the Entrust Certificate Authority.

Mandatory: No. This optional parameter defaults to 20 connections.

Max XAP Connections

The maximum number of XAP connections to the Entrust Certificate Authority.

Mandatory: No. This optional parameter defaults to 20 connections.

XAP Connection Idle Timer (seconds)

The idle timeout of the Entrust Certificate Authority XAP connection, in seconds.



Mandatory: No. This optional parameter defaults to 30 seconds.


XAP Connection Socket Timer (seconds)

The socket timeout of the Entrust Certificate Authority XAP connection, in seconds.

Mandatory: No. This optional parameter defaults to 60 seconds.

XAP Logging

 for logging the XAP debugging to file;  otherwise.

Mandatory: No. This optional parameter defaults to .

XAP Logs Level

The XAP debug log level, from 0 (no logging) to 7 (maximum logging).

Mandatory: No. This optional parameter defaults to 0.

P11 APF File

The APF (Auxiliary Profile File). Click **Select Files** to import this file.

Mandatory: When saving the user settings in a PKCS #11 hardware security module (HSM) and archiving old private keys locally (to make them available for other purposes).

P11 Library

The full path of the PKCS#11 native library.

Mandatory: When saving the user settings in a PKCS #11 hardware security module (HSM).

P11 Slot

The slot number of the PKCS#11 slot.

Mandatory: When saving the user settings in a PKCS #11 hardware security module (HSM).

P11 Password

The PKCS#11 user PIN to log in to the PKCS#11 slot.

Mandatory: When saving the user settings in a PKCS #11 hardware security module (HSM).

Enable niche certificate types

 to expose certificate types relating to ePassport applications and legacy software,  otherwise.

Mandatory: No. This optional parameter defaults to .

Allow 100% PKUP

The value of the `PrivateKeyUsagePeriod` extension in certificates issued by Entrust Certificate Authority when the request:

- Includes the `optionalCertificateRequestDetails.validityPeriod` field, and
- Does not include the `optionalCertificateRequestDetails.privateKeyUsagePercentage` field.

See below for the values supported by this setting.

apply-full-pkup	PrivateKeyUsagePeriod
true	The 100% of the <code>optionalCertificateRequestDetails.validityPeriod</code> value.
false	Set by the CA.



As explained in [RFC2459](#), the `PrivateKeyUsagePeriod` extension "allows the certificate issuer to specify a different validity period for the private key than the certificate".

Mandatory: No. This optional value defaults to `true`.

Enable CA Profile Sync

`true` to enable profile synchronization with Entrust Certificate Authority, `false` otherwise. When set to `true`, CA Gateway:

- Mirrors any eligible certificate types and definitions defined in Entrust Certificate Authority as basic CA Gateway certificate profiles without the need to define them in the CA Gateway configuration explicitly.
- Suppresses niche certificate types relating to ePassport applications and legacy software. To expose these types, enable the **Enable niche certificate types** parameter setting of the [com.entrust.SecurityManager](#) connector.

Mandatory: No.

Profiles

In the **Profiles** tab of the **Configuration** page, configure the following settings.

- [Choose a key name](#)
- [Name](#)
- [Copy CN in SubjectDN to SAN](#)
- [Subject Variable Requirements](#)
- [Subject Builder Configuration](#)
- [SAN Requirements](#)
- [Minimum keysize](#)
- [ECS Profile Properties](#)

Choose a key name

Type a unique identifier for the profile.

Mandatory: Yes.

Name

A readable name that describes the profile.

Mandatory: Yes.

Copy CN in SubjectDN to SAN

`true` to enable copying the CN of the Subject DN as Subject Alternative Name, `false` otherwise.

Mandatory: No. This optional parameter defaults to `false`.

Subject Variable Requirements

Under this section, define the subject variables for an enrollment operation with the certificate profile. When CA Gateway clients query the certificate profile, these variables inform the subject variable to supply when enrolling for a certificate using the profile.

- [Name](#)
- [Description](#)
- [Required](#)

Name

The name of the variable.



Mandatory : Yes.



Description

A friendly description of the variable.

Mandatory : Yes.

Required

 if the variable is required,  if the variable is optional. The purpose of this setting is to illustrate the intention of the variable.

 As of CA Gateway 3.1, this setting is enforced by policy. CA Gateway may throw an error if set to  for a variable that is actually required by a template.

Mandatory : Yes.

Subject Builder Configuration

Under this section, define the Subject Builders for constructing the subject DN for the enrollment request.

- [Name](#)
- [Properties](#)

Name

The class name of the subject builder.

- [com.entrust.adminservices.cagw.common.subjects.BasicSubjectBuilder](#)
- [com.entrust.adminservices.cagw.common.subjects.SubAltNameSubjectBuilder](#)
- [com.entrust.adminservices.cagw.common.subjects.TemplateSubjectBuilder](#)

Mandatory: No. This optional parameter defaults to [com.entrust.adminservices.cagw.common.subjects.BasicSubjectBuilder](#).

`com.entrust.adminservices.cagw.common.subjects.BasicSubjectBuilder`

Select this subject builder to append all the supplied subject variables together in the order of arrival.

Sample BasicSubjectBuilder

```
- name: "Use BasicSubjectBuilder"
  unique-id: "CA-1003-PROF-1001"
  subject-builder-config:
    subject-builder-name:
      "com.entrust.adminservices.cagw.common.subjects.BasicSubjectBuilder"
```

Sample subject variables

```
"subjectVariables" : [
  {
    "type" : "cn",
    "value" : "test"
  },
  {
    "type" : "o",
    "value" : "pki"
  }
]
```

Subject DN generated by the sample builder when parsing the sample variables

`cn=test,o=pki`

`com.entrust.adminservices.cagw.common.subjects.SubAltNameSubjectBuilder`

Select this subject builder to construct the Subject DN from the Subject Alternative Name provided in the request or CSR. Specifically, this builder:

1. Pulls out the SAN as per the order of SAN types preference provided in [SAN type order](#) property.
2. Uses the first SAN as the subject by filling the provided template. This SAN type can have only one value.
3. Gives priority to SAN from the request over the SAN provided in CSR.

This subject builder is useful when subject is not provided in both the request and CSR.

Sample SubAltNameSubjectBuilder

```
- name: "Use SubAltNameSubjectBuilder"
  unique-id: "CA-1003-PROF-1003"
  subject-variable-requirements:
    - name: SAN
      description: "Subject Alternative Name"
      required: true
  subject-builder-config:
    subject-builder-name:
      "com.entrust.adminservices.cagw.common.subjects.SubAltNameSubjectBuilder"
    properties:
      template: "cn=<SAN>,ou=CA01,o=pki,test,dc=com"
      san-type-order:
        dNSName,iPAddress,registeredID,rfc822Name,uniformResourceIdentifier
```

Sample subject variables

```
"subjectVariables" : [
  {
    "type" : "Subject Alternative Name",
    "value" : "SAN"
  }
],
"subjectAltNames" : [ {
  "type" : "dNSName",
  "value" : "cagw.test"
} ]
```

Subject DN generated by the sample builder when parsing the sample variables

```
cn=cagw.test,ou=CA01,o=pki,test,dc=com
```

com.entrust.adminservices.cagw.common.subjects.TemplateSubjectBuilder

Select this subject builder to replace DN (Distinguished Name) variables in a template with variables from the CSR (Certificate Signing Request).

- [Example: building the Common Name from Subject Variables](#)
- [Example: building the Common Name when no Subject Variables are provided](#)

Example: building the Common Name from Subject Variables

To build the final DN, the following template expects an enrollment request with subject variables for "First Name" and "Last Name".

```
- name: "Use TemplateSubjectBuilder"
  unique-id: "CA-1003-PROF-1002"
  subject-variable-requirements:
    - name: First Name
      description: "First Name"
      required: true
    - name: Last Name
      description: "Last Name"
      required: true
  subject-builder-config:
    subject-builder-name:
      "com.entrust.adminservices.cagw.common.subjects.TemplateSubjectBuilder"
    properties:
      template: "cn=<First Name> <Last Name>, ou=CA01,o=pki,dc=test,dc=com"
```

For example, when receiving the following request values.

```
"subjectVariables" : [
  {
    "type" : "First Name",
    "value" : "PKI"
  },
  {
    "type" : "Last Name",
    "value" : "Test"
  }
]
```

The template builds the following Distinguished Name.

```
cn=PKI Test,ou=CA01,o=pki,dc=test,dc=com
```

Example: building the Common Name when no Subject Variables are provided

To build the final DN when no Subject Variables are provided, the following template parses the CSR for common name.

 This configuration will not process fields other than CN and UID.

```
- name: "Use TemplateSubjectBuilder"
  unique-id: "CA-1003-PROF-1002"
  subject-builder-config:
    subject-builder-name:
      "com.entrust.adminservices.cagw.common.subjects.TemplateSubjectBuilder"
    properties:
      template: "cn=<cn>,ou=CA01,o=pki,dc=test,dc=com"
```

Parsing a CSR with multiple common names requires indexing the template output, starting with `cn.1` . For example;

```
template: "cn=<cn.1>, cn=<cn.2>, cn=<cn.3>, ou=CA01,o=pki,dc=test,dc=com"
```

 The use of `<CN>` or `<cn>` should be consistent.

Properties

Under this section, configure the following Subject Builder properties.

- [Template](#)
- [SAN type order](#)

Template

The DN template to use for constructing the subject. For example:

```
subject-builder-config:
  subject-builder-name:
    "com.entrust.adminservices.cagw.common.subjects.TemplateSubjectBuilder"
  properties:
    template: "cn=<CN>,ou=CA01,o=pki,dc=hooli,dc=com"
```

Mandatory: When the value of [Name](#) is `com.entrust.adminservices.cagw.common.subjects.SubAltNameSubjectBuilder`.

SAN type order

The SAN types to be used as the subject, in order of preference. Supported SAN types are:

- `dnsName`
- `iPAddress`
- `registeredID`
- `rfc822Name`
- `uniformResourceIdentifier`

Mandatory: When the value of [Name](#) is `com.entrust.adminservices.cagw.common.subjects.SubAltNameSubjectBuilder`.

SAN Requirements

Under this section, define the requirements of the Subject Alternative Name (SubjectAltName) expected during enrollment requests.

- [type](#)
- [required](#)

type

The type for the Subject Alternative Name, as defined by [RFC 5280](#). For example:

- `rfc822Name`

- `dnsName`

Mandatory: Yes.

required

`true` if the Subject Alternative Name is required, `false` if the Subject Alternative Name is optional.

Mandatory: Yes.

Minimum keysize

Configure the minimum sizes supported by the keys.

- [Specify whether to disable, log or reject key size violations](#)
- [Minimum RSA Keysize](#)
- [Minimum ECC Keysize](#)

Specify whether to disable, log or reject key size violations

The performed action when a key does not meet the [Minimum RSA Keysize](#) or [Minimum ECC Keysize](#) size requirements.

Value	Action
off	Nothing
log	Log the key size
block	Reject the key

Minimum RSA Keysize

The minimum size for RSA keys, as a number of bytes.

Minimum ECC Keysize

The minimum size for ECC (elliptic curve) keys, as a number of bytes.

ECS Profile Properties

Under this section, add the following profile settings for each ECS (Entrust Certificate Services) authority.

- [Certificate Type](#)
- [Certificate lifetime](#)
- [Client ID](#)

Certificate Type

The certificate types supported by ECS. For example:

STANDARD_SSL, ADVANTAGE_SSL, EV_SSL, UC_SSL, QWAC_SSL, PSD2_SSL, WILDCARD_SSL, SMIME_ENT

Mandatory: Yes.

Certificate lifetime

The certificate validity period in ISO 8601 format:

P<y>Y<m>M<d>D

For example, `P1Y6M10D` means one year, six months, and ten days. Certificate types such as `SMIME_ENT` restrict allowed values.

Mandatory: Yes.

Client ID

The identifier of the client requesting the certificates.

Mandatory: No. By default, the ECS REST API sets this value to 1.

Microsoft CA Profile Properties

Under this section, add the following profile settings for each Microsoft CA authority.

- [Certificate Template](#)
- [RA Enroll Key Store Provider Config](#)
- [RA Enroll Key Store Provider](#)
- [RA Enroll Key Store](#)
- [RA Enroll Key Store Type](#)
- [RA Enroll Key Store Password](#)
- [RA Enroll Key Alias](#)
- [RA Enroll Key Password](#)
- [Client Key Generation mode](#)

Certificate Template

The Microsoft Certificate name. No spaces.

Mandatory: Yes.

RA Enroll Key Store Provider Config

The SunPKCS11 configuration file described in the Thales Luna integration guide. Click **Select Files** to import this file.

Mandatory: Yes.


RA Enroll Key Store Provider

The security provider of the key store. When creating RA enrollment agent credentials in a Key Store file, supported values are the following.

Value	Security provider
SunJSSE	PKCS#12 and PFX
SUN	JKS
SunJCE	JCEKS

When creating RA enrollment agent credentials in PKCS#11 HSM, supported values are the following.

Value	Security provider
SunPKCS11	nCipher
LunaProvider	Luna

 CA Gateway tries loading the key store with any available security provider when this value is omitted or incorrect.

Mandatory: Yes.

RA Enroll Key Store

The file generated when creating RA enrollment agent credentials in a Key Store file. Supported extensions for this file are:

- p12
- pfx
- Jks
- jceks

Click **Select Files** to import this file.

Mandatory: Yes.

RA Enroll Key Store Type

The type of key store. Supported values are:

- pkcs12
- pfx
- Jks
- jceks

Mandatory: Yes.

RA Enroll Key Store Password

The password of the key store containing the enrollment agent credential. Where the key store is either:

- A key store file.
- An HSM slot.

 We recommend creating the enrollment agent credentials in a PKCS#11 HSM.

Mandatory: Yes.

RA Enroll Key Alias

The alias for accessing the enrollment agent's key in either:

- A key store file.
- An HSM slot. In this case, you can usually omit this value because most HSMs do not protect the slot objects with an additional password.

Mandatory: Yes.

RA Enroll Key Password

The password for accessing the enrollment agent's key in either:

- A key store file.
- An HSM slot. In this case, you can usually omit this value because most HSMs do not protect the slot objects with an additional password.

Mandatory: Yes.

Client Key Generation mode

The client key generation mode.

Value	Key generation mode
true	The client generates the key and provides a CSR for CA Gateway to return an X.509 certificate.
false	CA Gateway returns a PKCS#12 containing the client's key and certificate.

Mandatory: No. This optional parameter defaults to `true`.

Security Manager Profile Properties

Under this section, add the following profile settings for each Entrust Certificate Authority.

- [Certificate Type](#)
- [Certificate Definition](#)
- [LDAP entry creation mode](#)
- [LDAP directory mode](#)
- [User Role](#)
- [User Type](#)

Certificate Type

The Entrust Certificate Authority certificate type to use when processing an enrollment request under the certificate profile. For example:

- `ent_twokeypair`
- `ent_default`

The administrator EPF for the Managed CA must have permission to administer this certificate type.

Mandatory: Yes.

Certificate Definition

The certificate definition for processing enrollment requests under the certificate profile. For example:

- Verification
- Dual usage
- Encryption

This certificate definition must have an assigned certificate definition policy. Otherwise, enrollments will fail.

Mandatory: Yes.

LDAP entry creation mode

The LDAP entry creation mode.

Value	Action
✓	CA Gateway will create the LDAP entry for the user. CA Gateway will connect to the directory using the LDAP credentials specified for the Managed CA.
✗	Entrust Certificate Authority will create an LDAP entry for the user depending on the <code>managed-cas.profiles.directory-mode</code> value.

Mandatory: No. This optional parameter defaults to `true`.

LDAP directory mode

When the **LDAP entry creation mode** option is disabled, this setting controls whether Entrust Certificate Authority creates an LDAP entry for the user.

Value	Action
DO_OP_FAIL_IF_NOT_NEEDED	Perform the repository operation when needed, and fail if not needed.
DO_OP_SUCCEED_IF_NOT_NEEDED	Perform the repository operation when needed, and return success if not needed.
NO_OP	Omit the repository operation and do not check if the operation is needed.
NO_OP_FAIL_IF_NEEDED	Omit the repository operation, but fail if the operation is needed.

In the CA profile, certificate types as `vpn_nodir` include the following `master.certspec` advanced setting under `[Extension Definitions]`.

noUserInDirectory=1

Mandatory: Yes.

User Role

The Entrust Certificate Authority role for processing enrollment requests under the certificate profile (for example, "End User").


 The administrator EPF for the Managed CA must have permission to administer this role.

Mandatory: No.

User Type

The Entrust Certificate Authority user type to use when processing an enrollment request under the certificate profile. For example:

- Person
- Web Server

 The administrator EPF for the Managed CA must have permission to administer this user type.

Mandatory: No. The user type is not required when the **LDAP entry creation mode** option is disabled.

Tenants

Set the following parameters in the **Tenants** tab of the **Configuration** page.

- [Tenants](#)
- [Integrators](#)

Tenants

For each tenant, set the following field values under **Tenants**.

Setting	Value	Mandatory
Name	A friendly name for the tenant.	✓
Unique-Id	A unique identifier for the tenant. When configuring integrators, you will specify this identifier to map an integrator to a tenant.	✓
Certificate Authority Id	The CA unique identifier in CA Gateway. Map each tenant to a different managed CA because errors will occur if you map multiple tenants to the same managed CA.	✓

Integrators

Set the following fields under **Integrators**.

Setting	Value	Mandatory
Name	A friendly name for the integrator	✓
Unique-Id	A unique identifier for the integrator. When creating certificates for clients, you can specify this integrator ID to map a client to an integrator.	✓
Tenant IDs	One or more of the tenant identifiers previously defined when configuring tenants. Map each integrator to a different tenant because errors will occur if you map multiple integrators to the same tenant.	✓

Clients

For each client, set the following field values in the **Clients** tab of the **Configuration** page.

- [Subject DN](#)
- [Tenant ID](#)
- [Integrator ID](#)
- [Role](#)

Subject DN

The subject DN of the client.

⚠ You must issue the client a digital certificate with this subject DN.

Mandatory: Yes.

Tenant ID

One of the tenant identifiers listed under [Tenants](#)

✗ This value is mapped with the client and is mutually exclusive with [Integrator ID](#).

Mandatory: Yes.

Integrator ID

The integrator identifier.

✗ This value is mapped with the client and is mutually exclusive with [Tenant ID](#).

Mandatory: Yes.

Role

One of the following roles.

Role identifier	Role main permissions	Granted by default
integrator	Access to multiple CAs. For example, as an organization providing services or capabilities to customers, such as Identity Management service providers like Microsoft Intune.	Default role for clients mapped to an integrator.
policy-constrained-tenant	View a single CA. For example, as a consumer of the services provided by the Integrator.	Default role for clients mapped to a tenant.
policy-override-tenant	Control the naming information in the certificates requested to Entrust Certificate Authority. The CA policy of the requested certificate profile determines all other certificate content.	—
read-only-integrator	Access multiple CAs and perform <code>get</code> operations on any of them.	—
read-only-tenant	Access one CA and perform <code>get</code> operations.	—

See the following table for a more detailed description of the permissions assigned to each predefined role.

Permission	integrator	policy-override-tenant	policy- constrained-tenant	read-only-integrator	read-only-tenant
Access multiple CAs	✓	Single CA only	Single Entrust Certificate Authority only	✓	Single CA only
Request explicit extensions	✓	✓	✗	✗	✗
Request private key usage period	✓	✓	✗	✗	✗
External public keys (no CSR)	✓	✓	✗	✗	✗

Permission	integrator	policy-override-tenant	policy-constrained-tenant	read-only-integrator	read-only-tenant
Override Proof of Possession	✓	✓	✗	✗	✗
Request explicit validity dates	✓	✓	Can shorten the lifetime in CSR enrollments (relative to the CA policy).	✗	✗
CSR	✓	✓	✓	✗	✗
PKCS#12	✓	✓	✓	✗	✗
Subject DN Naming Info (including subjectDn and previousSubjectDn optional parameters)	✓	✓	✓	✗	✗
Subject Alternative Names	✓	✓	✓	✗	✗
Manage certificates (revoke, suspend, unsuspend)	✓	✓	✓	✗	✗
Search in the certificate inventory	✓	✓	✓	✓	✓
Certificate events	✓	✓	✓	✓	✓

Authorized users can request certificates with the following contents.

- Certificate Lifetimes.
- Certificate naming information: Subject DN (subject to CA DIT constraints), Subject Alternative Names.
- Key Usage
- Private Key Usage Percentage
- Required Certificate Extensions

No client role can request the following extensions from Entrust Certificate Authority.

- authorityKeyIdentifier (2.5.29.35)
- basicConstraints (2.5.29.19)
- cRLDistributionPoints (2.5.29.31)
- cRLNumber (2.5.29.20)

- entrustVersInfo (1.3.0040.113533.7.65.0)
- invalidityDate (1.2.5.29.24)
- issuingDistributionPoint (2.5.29.28)
- netscapeRevocationUrl (2.16.840.1.113730.1.3)
- reasonCode (2.5.29.21)
- subjectKeyIdentifier (2.5.29.14)

✗ CA Gateway will ignore these extensions when included in a CSR sent from a client.

Each role can access any of the REST APIs. However, based on the role, the requested action is scoped to the allowed set of managed CAs.

Mandatory: No. This optional parameter defaults to the lowest privileged role.

Cmpv2

Set the following parameters in the **Cmpv2** tab of the **Configuration** page.

- [Truststore](#)
- [Alias](#)
- [Customization](#)
- [Shared Secret](#)
- [Caching of in-progress CMPv2 transactions](#)

Truststore

Configure the trust-store that contains root CA certificates for verifying CMP messages.

- [Upload file](#)
- [Password](#)
- [Type](#)

Upload file

The truststore that contains the CA certificates. Click **Select Files** to import this truststore from file.

Mandatory: Yes

Password

The password of the truststore that contains the CA certificates.

Mandatory: Yes.

Type

The type of truststore containing the CA certificates.

Type	Description
jks	Java truststore
pkcs12	PKCS #12 truststore

Mandatory: Yes.

Alias

An optional list of trusted root CA certificate aliases. For each alias, define the following settings.

- [Alias](#)
- [DN](#)

Alias

The alias assigned to the certificate when stored in the trust store

Mandatory: Yes.

DN

The DN (Distinguished Name) of the certificate.

Mandatory: Yes.

Customization

An optional list of rules for extending or modifying the specifications. Add the following setting for each custom rule.

- [Choose a key name](#)
- [Minimal RSA public key length](#)
- [Minimal elliptic curve \(EC\) public key length](#)
- [Digest algorithm](#)
- [MAC algorithm](#)
- [Signature class](#)
- [Signing algorithm](#)
- [EC public key algorithm](#)
- [Excluded test](#)

Choose a key name

Write a name for the new rule.

Mandatory: Yes.

Minimal RSA public key length

The minimal key length allowed for RSA public keys.

Mandatory: No. This optional value defaults to 2048 bits.

Minimal elliptic curve (EC) public key length

The minimal key length allowed for EC (Elliptic-curve) public keys.

Mandatory: No. This optional value defaults to 256 bits.

Digest algorithm

The list of supported one-way digest algorithms. Supported list items are:

- SHA-256
- SHA-384

Mandatory: No. When omitting this optional value, both SHA-256 and SHA-384 are supported.

MAC algorithm

The list of supported MAC (Message Authentication Code) algorithms.

Mandatory: No. When omitting this value, a default list is built from the [Digest algorithm](#) value.

Signature class

The list of supported signature algorithm classes. Supported list items are:

- `rsa`
- `ecdsa`

Mandatory: No. When omitting this optional value, both `rsa` and `ecdsa` are supported.

Signing algorithm

The list of supported signing algorithms.

Mandatory: No. When omitting this value, a default list is built from the [Digest algorithm](#) and [Signature-class](#) values.

EC public key algorithm

The list of algorithms of supported EC public keys. Supported list items are:

- `secp256r1`
- `secp384r1`

Mandatory: No. When omitting this optional value, both `secp256r1` and `secp384r1` are supported.

Excluded test

The list of specific tests to be excluded during validation of the message.

Mandatory: No.

Shared Secret

The settings for each connection between the CMP enrollment server and the potential request transmitters.

- [DN of the node sending the message](#)
- [Passcode](#)

Mandatory: Yes.

DN of the node sending the message

The subject's distinguished name of the certificate the enrollment server will use to sign the issued certificates.

 The certificate must be included in the Trust Store selected with the [Truststore](#) field

Mandatory: Yes.

Passcode

A list of request signing keys. Under this field, define each transmitter key with the following settings.

Setting	Value
KID provided in message header	The identifier of the key in the trust-store selected with the Truststore parameter.
Passcode	The password for accessing the key in the trust-store selected with the Truststore parameter.

Mandatory: Define at least one signing key.

Caching of in-progress CMPv2 transactions

The cache settings for the CMPv2 transactions.

- [Maximum Cache Size](#)
- [Initial Cache Capacity](#)
- [Expire After Value](#)
- [Expire After Time Unit](#)

Maximum Cache Size

The maximum number of entries supported by the API cache. Setting this parameter to 0 disables the cache -for example:

Mandatory: Yes

Initial Cache Capacity

The initial number of entries in the API cache.

Mandatory: Yes.

Expire After Value

The number of minutes before removing an entry from the API cache. For example, to remove the entries after 5 minutes:

Mandatory: No. This optional parameter defaults to 60.



Expire After Time Unit

Time unit for the expiry period. This parameter supports the following Java TimeUnit enum constants:

- SECONDS
- MINUTES
- HOURS

TLS CRL-settings

Configure the following TLS authentication settings under **enable**.

Setting	True 	False 
To enable TLSV1 on EDM Deployments	Enable TLS 1.0 in Cryptographic Security Platform installations – for example, to support Entrust Security Manager 8.2 or earlier	Do not enable TLS 1.0 (default value)
To enable TLSV1.1 on EDM Deployments	Enable TLS 1.1 in Cryptographic Security Platform installations.	Do not enable TLS 1.1 (default value)
To enable CRL Check on EDM Deployments	Check CRL distribution points for certificate revocation.	Do not check CRL distribution points (default value)

Issuing public trust certificates with CA Gateway

CA Gateway supports issuing certificates intended to be publicly trusted. See the following sections for how to use this feature with filter lists.

- [CA Authorization](#)
- [Certificate Transparency](#)

 In the current release, only the CA described in [Integrating an Entrust Certificate Authority](#) supports this feature.

CA Authorization

With the configured CAA filter, CA Gateway lookups CAA records for the domain and each parent domain. For example, for the following domain:

`www.acme.com`

CA Gateway performs the following lookups:

`www.acme.com`

`acme.com`

`com`

CA Gateway traverses up the tree in search of CAA records. This CAA check passes if:

- The issuer in a CAA record matches the issuer defined in the `issuer-string` setting of the `com.entrust.CAAuthorization` filter.

- No CAA record defines an issuer or specifies "Any CA". In this case, the domain owner is not asserting a particular issuing CA.
- No CAA record is found. In this case, the domain owner is not asserting a particular issuing CA.

The above applies to each domain requested in the CA Gateway enrollment request. For example, domains inside the CSR, subject to the following flag if applied.

```
optionalCertificateRequestDetails/useSANFromCSR
```

Domains are requested in the separate `subjectAltNames`, or in the following fields externally to the CSR.

```
optionalCertificateRequestDetails/extensions
```

CA Gateway will check CAA records for wildcard domains under RFC8659 .

Defining Multiple DNS Servers

When defining multiple DNS servers, the DNS lookups run in parallel. The check for a domain stops when reaching the number of positive responses defined in the `dns.response-threshold` configuration parameter. Thus, this parameter provides additional assurance by forcing consultation of multiple separate DNS responders while allowing some contingency if a DNS server fails to respond quickly.

For example, when using three DNS servers, setting `dns.response-threshold` to "2" ensures at least two positive DNS checks against two distinct responders while allowing for the unavailability of one of the three responders.

DNS Infrastructure Guidance

Before using the CAA check feature of CA Gateway, read RFC8659 with particular attention to section 5 covering security considerations. This RFC provides rules and advice for CAA checking. Deploying the DNS infrastructure is the responsibility of the customer.

The DNS responders referenced in the CA Gateway configuration are under the CA and CA Gateway responsibility (not under the control of a third-party cache such as Google or CloudFlare). All records received by CA Gateway come from authoritative nameservers. Caching of these records at the responder is allowed.

DNSSEC

As stated by RFC8659 , DNSSEC allows CA Gateway to ensure that an empty resource record (potentially containing the domain owner's stated issuer) is legitimately empty or not empty after a record suppression. CA Gateway will validate DNSSEC if present but still proceed if no DNSSEC applies for the domain.

 CA Gateway does not archive the DNSSEC proof for future audits.

Certificate Transparency

CA Gateway can collect a set of signed CT log server responses and ask the underlying CA if the certificates for public trust include these responses in an SCT List extension. The certificate transparency filter:

1. Sends parallel requests to all of the configured log servers.

2. Waits for sufficient log server responses to arrive. In the filter configuration, a certificate transparency policy states the type and the minimum of required responses.
3. Requests the final certificate to the CA.

This approach allows defining a surplus of log servers to guard against slow or offline servers.

Administrating CA Gateway

Once deployed, you can administrate CA Gateway as explained below.

- [Checking CA Gateway error codes](#)
- [Checking the CA Gateway health](#)
- [Checking the health of a CA](#)

Checking CA Gateway error codes

For a description of each error code recorded in the CA Gateway logs, see the CA Gateway API documentation at:

```
https://<HOST>:<CAGW_HOST_PORT>/<server.servlet.context-path>/docs
```

Where `<HOST>` and `<CAGW_HOST_PORT>` are the hostname and port of the CA Gateway service. CA Gateway logs can also include the following warning message.

```
Version <= 1.4 profile configuration detected for CA <ca>. This configuration syntax is deprecated. Please update.
```

CA Gateway records this warning message when the YAML configuration includes a deprecated profile syntax under:

```
cagw.authorities.managed-cas.<CA>
```

To avoid this message, configure the CA profiles as described in the configuration guide.

Checking the CA Gateway health

Gateway provides the following endpoints to check the health of the CA Gateway server.

- [health](#)
- [diskSpace](#)
- [ping](#)
- [prometheus](#)

Checking the health of a CA

CA Gateway provides the [status](#) endpoint to check the health of a Certificate Authority.

CSP CA Gateway endpoints

CSP CA Gateway provides the following endpoints.

- [diskSpace](#)
- [docs](#)

- [health](#)
- [ping](#)
- [prometheus](#)
- [properties](#)
- [status](#)
- [swagger-ui](#)
- [v1](#)


diskSpace

The following endpoint returns the disk space of the CA Gateway server for a group.

```
https://{host}:9444/{management.endpoints.web.base-path}/health/{group}/diskSpace
```

Where:

- `{host}` is the hostname or IP address of the CA Gateway host server.
- `{management.endpoints.web.base-path}` is the value of the `management.endpoints.web.base-path` parameter in the `application.yml` configuration file.
- `{group}` is one of the groups listed by the [health](#) endpoint.

 To enable this health endpoint, you must configure the `management.endpoints.web.exposure.include` parameter in the `application.yml` file.

For example, to check the disk space for the `custom` group.

```
https://localhost:9444/cagw/management/actuator/health/custom/diskSpace
```

If the server is up, this endpoint will return a response like the following.

```
{"status":"UP","details":  
{"total":1013309239296,"free":765931622400,"threshold":10485760,"exists":true}}
```

docs

The following endpoint provides documentation on using the CA Gateway API for certificate policy, certificate issuance, and certificate lifecycle management.

```
https://{host}:8444/{server.servlet.context-path}/doc
```

Where:

- `{host}` is the hostname or IP address of the CA Gateway host server.
- `{server.servlet.context-path}` is the value of the `server.servlet.context-path` parameter in the `application.yml` configuration file.


health

The following endpoint returns information on the CA Gateway server health.

```
https://{host}:{9444}/{management.endpoints.web.base-path}/health
```

Where:

- `{host}` is the hostname or IP address of the CA Gateway host server.
- `{management.endpoints.web.base-path}` is the value of the `management.endpoints.web.base-path` parameter in the `application.yml` configuration file.

 To enable this health endpoint, you must configure the `management.endpoints.web.exposure.include` parameter in the `application.yml` file.

For example:

```
{"status":"UP","groups":["custom"]}
```

See below for a description of each value.

- [status](#)
- [groups](#)

status

The ping status of the CA Gateway server.

groups

The list of user groups configured in the CA Gateway server.


ping

The following endpoint returns the ping status of the CA Gateway server for a group.

```
https://{host}:9444/{management.endpoints.web.base-path}/health/{group}/ping
```

Where:

- `{host}` is the hostname or IP address of the CA Gateway host server.
- `{management.endpoints.web.base-path}` is the value of the `management.endpoints.web.base-path` parameter in the `application.yml` configuration file.
- `{group}` is one of the groups listed by the [health](#) endpoint.

 To enable this health endpoint, you must configure the `management.endpoints.web.exposure.include` parameter in the `application.yml` file.

For example, to check the ping status for the `custom` group.

```
https://localhost:9444/cagw/management/actuator/health/custom/ping
```

If the server is up, this endpoint will return the following response.

```
{"status":"UP"}
```


prometheus

The following endpoint returns CA Gateway metrics in Prometheus-compliant format.

```
https://{host}:9444/{management.endpoints.web.base-path}/prometheus
```

Where:

- `{host}` is the is the hostname or IP address of the CA Gateway host server.
- `{management.endpoints.web.base-path}` is the value of the `management.endpoints.web.base-path` parameter in the `application.yml` configuration file.

 To enable this health endpoint, you must configure the `management.endpoints.web.exposure.include` parameter in the `application.yml` file.

For example:

```
# HELP jvm_threads_live_threads The current number of live threads including both
daemon and non-daemon threads
# TYPE jvm_threads_live_threads gauge
jvm_threads_live_threads 51.0
# HELP spring_security_filterchains_AnonymousAuthenticationFilter_before_total
# TYPE spring_security_filterchains_AnonymousAuthenticationFilter_before_total
counter
spring_security_filterchains_AnonymousAuthenticationFilter_before_total{security_secu
rity_reached_filter_section="before",spring_security_filterchain_position="0",spring_
security_filterchain_size="0",} 8.0
# HELP jvm_gc_live_data_size_bytes Size of long-lived heap memory pool after
reclamation
# TYPE jvm_gc_live_data_size_bytes gauge
jvm_gc_live_data_size_bytes 8.7626752E7
# HELP executor_completed_tasks_total The approximate total number of tasks that have
completed execution
# TYPE executor_completed_tasks_total counter
executor_completed_tasks_total{name="applicationTaskExecutor",} 0.0
executor_completed_tasks_total{name="taskScheduler",} 2.0
# HELP system_cpu_count The number of processors available to the Java virtual
machine
# TYPE system_cpu_count gauge
```

```
system_cpu_count 8.0
```

properties

The following endpoint returns property values on Entrust CAs.

```
https://{host}:8444/{server.servlet.context-path}/v1/certificate-authorities/{caId}/  
properties?fields={properties}
```

Where :

- `{host}` is the hostname or IP address of the CA Gateway host server.
- `{server.servlet.context-path}` is the value of the `server.servlet.context-path` parameter in the `application.yml` configuration file.
- `{caId}` is the Entrust Certificate Authority identifier.
- `{properties}` is a comma-separated list of the following property identifiers:
 - `defaultPolicyOIDs`
 - `encryptionPolicyOIDs`
 - `verificationPolicyOIDs`

For example, the following request checks all these properties on the Entrust Certificate Authority instance with the `CA3` identifier.

```
GET https://localhost:8444/cagw/v1/certificate-authorities/CA3/status?  
fields=defaultPolicyOIDs,encryptionPolicyOIDs,verificationPolicyOIDs
```

The response looks like the following.

```
{  
  "type": "CAPropertiesResponse",  
  "CAPropertiesInformation": {  
    "properties": {  
      "defaultPolicyOIDs": [  
        "1.1.1.1",  
        "2.2.2.2"  
      ],  
      "encryptionPolicyOIDs": [  
        "1.1.1.1"  
      ],  
      "verificationPolicyOIDs": [  
        "2.2.2.2"  
      ]  
    }  
  }  
}
```

status

The following endpoint returns the up or down status of a Certificate Authority.

```
https://{host}:8444/{server.servlet.context-path}/v1/certificate-authorities/{caId}/status
```

Where:

- `{host}` is the hostname or IP address of the CA Gateway host server.
- `{server.servlet.context-path}` is the value of the `server.servlet.context-path` parameter in the `application.yml` configuration file.
- `{caId}` is the Certificate Authority identifier.

For example, the following request checks the status of a Certificate Authority with the `CA3` identifier.

```
GET https://localhost:8444/cagw/v1/certificate-authorities/CA3/status
```

The response looks like the following.

```
{
  "type" : "CAStatusResponse",
  "status" : "UP",
}
```

swagger-ui

The following endpoint provides a Swagger UI for visualizing and interacting with the CA Gateway REST API. CA Gateway includes this UI to assist developers in API integrations.

```
https://{host}:8444/{server.servlet.context-path}/swagger-ui
```

Where:

- `{host}` is the hostname or IP address of the CA Gateway host server.
- `{server.servlet.context-path}` is the value of the `server.servlet.context-path` parameter in the `application.yml` configuration file.

✗ This UI is not for, nor will it be supported, in the production uses of CA Gateway. It is not a substitute for an administrator UI. We recommend using Entrust's Certificate Manager or an equivalent interface provided by another product.

To test CA Gateway with Swagger

1. In the `application.yml` file, configure a tenant, or an integrator.
2. Install the tenant or integrator credential in the browser.
3. Make sure that the certification chain of the CA Gateway TLS certificate is trusted.
4. Navigate to the URL of the Swagger UI. For example:

```
https://localhost:8444/cagw/swagger-ui
```

5. When prompted by the browser, select the credential of the tenant or integrator.
6. Use the Swagger options to generate curl commands. For example, the following command lists the CAs visible to the tenant or integrator.

```
curl --cert-type P12 --cert tenant.p12:mypassword -X GET "https://cid-cagw.dev.entrust.local/cagw/v1/certificate-authorities" -H "accept: application/json"
```

✗ When running curl commands, some Linux versions do not support authenticating with a P12 file.

v1

The following endpoint returns version information on CA Gateway.

```
https://{host}:8444/{server.servlet.context-path}/v1
```

Where:

- `{host}` is the hostname or IP address of the CA Gateway host server.
- `{server.servlet.context-path}` is the value of the `server.servlet.context-path` parameter in the `application.yml` configuration file.

i This endpoint is the main API entry point to invoke API capabilities.

CA Capabilities reference

The "Get CA Capabilities" endpoint of the CA Gateway API informs on the capabilities supported by each type of CA. The following sections give a complete reference of the returned values.

- [CA management capabilities](#)
- [Certificate enrollment capabilities](#)
- [Certificate management capabilities](#)
- [Certificate search capabilities](#)

CA management capabilities

The "Get CA Capabilities" endpoint returns the following values for each CA management capability.

- [CAStatus](#)
- [PermitsDefaultCA](#)
- [SupportsMultipleCAs](#)

CAStatus

Check whether the CA is up or down.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft ADCS	False

PermitsDefaultCA

The CA can be set as the default CA of CA Gateway.

CA	Returned value
Entrust Certificate Authority	False
ECS	False
Microsoft ADCS	False

SupportsMultipleCAs

The CA type supports multiple CAs of the same type.

CA	Returned value
Entrust Certificate Authority	False
ECS	False
Microsoft ADCS	False

Certificate enrollment capabilities

The "Get CA Capabilities" endpoint returns the following values for each enrollment capability.

- [CAGeneratedKey](#)
- [CAGeneratedKeyBackup](#)
- [ClientGeneratedKeyBackup](#)
- [EnrollmentByCSR](#)
- [ExtensionInCSR](#)
- [ExtensionInRequest](#)
- [KeyInRequest](#)
- [PKCS12Response](#)

- [SANInCSR](#)
- [SANInRequest](#)
- [SubjectNameInRequest](#)
- [ValidateProofOfPossession](#)
- [ValidityPeriodInRequest](#)
- [X509CertificateResponse](#)

CAGeneratedKey

Generate the key in the server and return the generated key in PKCS#12 form). Individual profiles within the CA can disable this capability.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft ADCS	True

CAGeneratedKeyBackup

Back up the server-generated key.

CA	Returned value
Entrust Certificate Authority	True
ECS	False
Microsoft ADCS	True

ClientGeneratedKeyBackup

Back up the key provided by the client during the request.

CA	Returned value
Entrust Certificate Authority	True
ECS	False
Microsoft ADCS	True

EnrollmentByCSR

Support certificate signing requests.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft AD CS	True

ExtensionInCSR

Process the extension request in the CSR.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft AD CS	True

ExtensionInRequest

Process the extension request in the enrollment request.

CA	Returned value
Entrust Certificate Authority	True
ECS	False
Microsoft AD CS	False

KeyInRequest

In the enrollment request, the client can add a key for the enrollment.

CA	Returned value
Entrust Certificate Authority	True
ECS	False
Microsoft ADCS	False

PKCS12Response

Return certificates and keys in PKCS#12 form.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft ADCS	True

SANInCSR

Process the Subject Alternative Names in the CSR.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft ADCS	True

SANInRequest

Process Subject Alternative Names in the enrollment request.

CA	Returned value
Entrust Certificate Authority	True
ECS	True

CA	Returned value
Microsoft ADCS	False

SubjectNameInRequest

Use Subject Name parameters of the CSR to construct the subject's DN of the supplied order.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft ADCS	False

ValidateProofOfPossession

Validate the proof of possession.

CA	Returned value
Entrust Certificate Authority	True
ECS	False
Microsoft ADCS	False

ValidityPeriodInRequest

Requests can supply a validity period.

CA	Returned value
Entrust Certificate Authority	True
ECS	False
Microsoft ADCS	False

X509CertificateResponse

Return certificates in X509 form.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft AD CS	True

Certificate management capabilities

The "Get CA Capabilities" endpoint returns the following values for each certificate management capability.

- [CertificateAction](#)
- [RevokeAction](#)
- [CertificateEvents](#)
- [Recover](#)
- [SubjectDNAction](#)

CertificateAction

List the lifecycle management actions supported by the issued certificates.

Action	SM	ECS	MS AD CS
HoldAction	✓		✓
UnholdAction	✓		✓
RevokeAction	✓	✓	✓
DeactivateAction		✓	
RenewAction		✓	
ReissueAction		✓	

RevokeAction

List the revocation reasons supported by the certificates.

Reason	SM	ECS	MS ADCS
unspecified	✓	✓	✓
keyCompromise	✓	✓	✓
cACompromise			✓
affiliationChanged	✓	✓	✓
superseded	✓	✓	✓
cessationOfOperation	✓	✓	✓
certificateHold	✓		✓
removeFromCRL (Unholds a certificate previously revoked with the certificateHold reason)			
privilegeWithdrawn			
cACompromise			

CertificateEvents

States if the CA supports the Certificates Events API.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft ADCS	True

Recover

States if the CA can recover certificates by DN.

CA	Returned value
Entrust Certificate Authority	Recover all certificates, recover the latest certificates.
ECS	True
Microsoft AD CS	Recover all certificates, recover the latest certificates.

SubjectDNAction

List the certificate actions by the subject's DN.

Actions	SM	ECS	MS AD CS
HoldAction	✓		✓
UnholdAction	✓		✓
RevokeAction	✓		✓
DeactivateAction	✓		
ReactivateAction	✓		

Certificate search capabilities

The "Get CA Capabilities" endpoint returns the following values for each search capability.

- [SearchBySerial](#)
- [SearchBySubjectDN](#)

SearchBySerial

Lookup certificates by serial number.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft AD CS	True

SearchBySubjectDN

Lookup certificates by the subject's DN.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft ADCS	True

13 Managing Log Forwarder

Cryptographic Security Platform provides the Log Forwarder solution for forwarding logs to a Splunk SIEM (Security Information and Event Management) server.

To configure and deploy the Log Forwarder solution

1. Open the following URL in a Web browser.

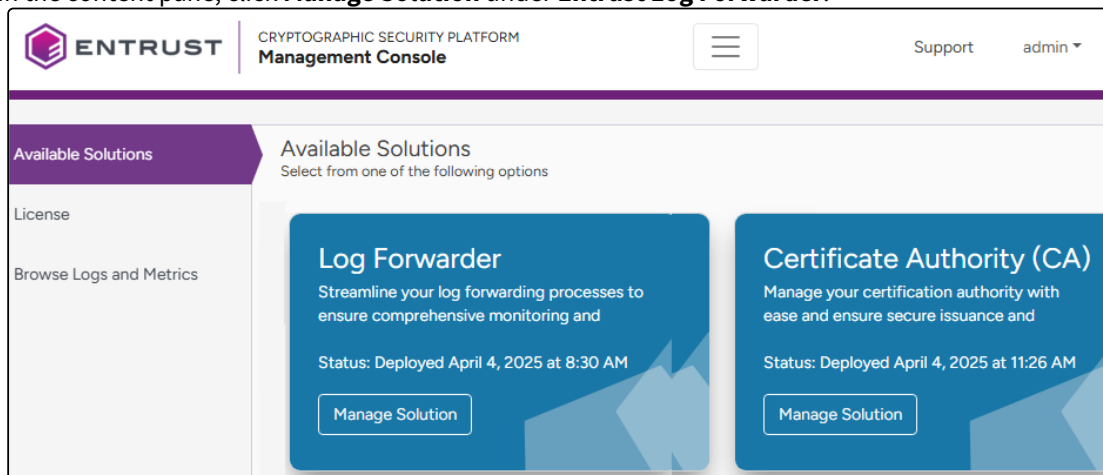
```
https://<machine>/management-console
```

Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

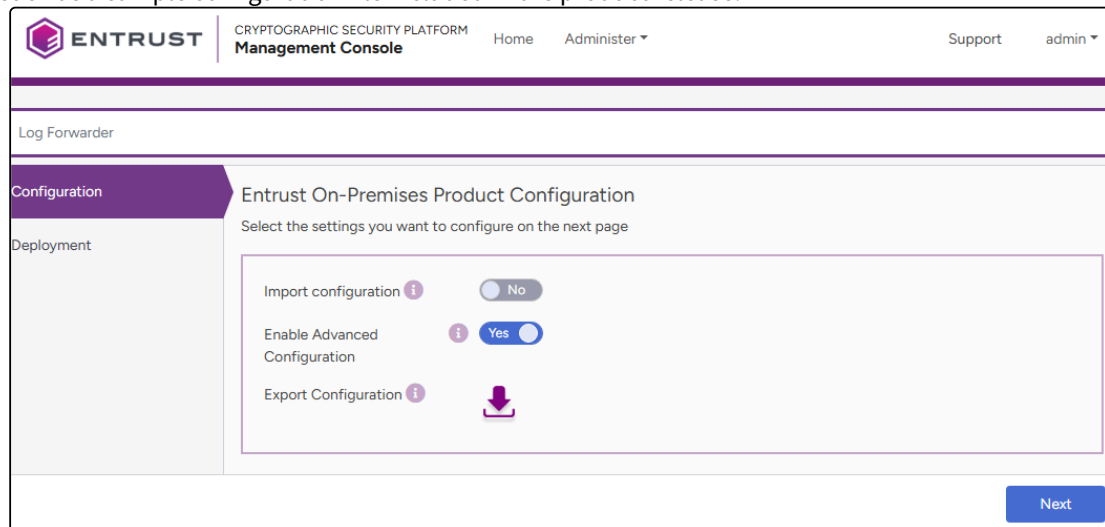
2. Log into the Management Console a user belonging to a role with Log Forwarder management permissions – for example, the initial `admin` administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

3. In the content pane, click **Manage Solution** under **Entrust Log Forwarder**.



4. Activate the **Import configuration** toggle switch if you want to import configuration settings from a file, such as a sample configuration file included in the product release.



5. Active the **Enable Advanced Configuration** if you want to configure the full set of configuration parameters supported by the solution.
 6. Click **Next**.
 7. Configure the solution settings described in the following sections.
 - [Log Server](#)
 - [TLS](#)
1. Click **Validate** to validate the configured settings.
 2. Correct any detected configuration error until the **Validate** option displays no warnings.
 3. Optionally, click the **Download** button to export the current configuration. You can later import this configuration with the already mentioned **Import configuration** toggle switch.
 4. Click **Submit** and wait while Cryptographic Security Platform uploads the configuration and any attached file, such as a P12 file with authentication credentials.
 5. Click **Deploy**.

Log Server

Select the SIEM server.

- [Type](#)
- [Host](#)
- [Port](#)
- [Token](#)

Type

The type of SIEM server. The current Cryptographic Security Platform release only supports selecting **Splunk**.

i As explained in [SIEM requirements](#), the current Cryptographic Security Platform release only supports the Splunk SIEM.

Mandatory: Yes


Host

The IP address or hostname of the external SIEM server.

Mandatory: Yes

Port

The port of the SIEM service.

 In the Splunk configuration, this port is the "HTTP Event Collector" port.

Mandatory: Yes

Token

A secret authentication token provided by the external SIEM service.

Mandatory: Yes

TLS

Configure the TLS security in communications with the external SIEM server.

- [Enabled](#)
- [Verify](#)
- [CA Certificate File](#)

Enabled

Check this checkbox to use TLS security in communications with the external SIEM server.

When no proxy server is configured, communications with the SIEM server use the following protocols.

Enabled	Log forwarder communication with the SIEM server
Checked	HTTPS
Unchecked	HTTP

After running the `clusterctl proxy set` command with the `protocol` parameter set to `http`, communications with the SIEM server use the following protocols.

Enabled	Log forwarder communication with the proxy	Proxy communication with the SIEM server
Checked	HTTP	HTTPS
Unchecked	HTTP	HTTP

After running the `clusterctl proxy set` command with the `protocol` parameter set to `https`, communications bypass the proxy because Log forwarder does not support HTTPS communications with a proxy.

Enabled	Log forwarder communication with the SIEM server
Checked	HTTPS
Unchecked	HTTP

Mandatory: No. When omitting this optional setting, TLS security is enabled by default.

Verify

Check this box to verify the TLS certificate of the external SIEM server.

Mandatory: No. When omitting this optional setting, the TLS certificate is not verified.

CA Certificate File

Click **Select Files** to import the CA certificate for validating the TLS certificate of the external SIEM server.

Mandatory: No. System certificates are used when omitting this optional setting.

14 Upgrading

See below for how to upgrade your current installation to CSP 1.0.0.

- [Upgrade requirements](#)
- [Upgrading from Entrust Deployment Manager 2.0.2](#)
- [Upgrading from PKI Hub 1.0.0](#)

Upgrade requirements

Your installation must meet the following requirements for upgrading to CSP 1.0.0.

- [Required platform version for upgrading](#)
- [Required solution versions for upgrading](#)
- [Required installation mode for upgrading](#)
- [Required files for upgrading](#)
- [Required license for upgrading](#)
- [Required machine for upgrading](#)
- [Required IP version for upgrading](#)

Required platform version for upgrading

You need one of the following installations.

Product	Version
PKI Hub	1.0.0
Entrust Deployment Manager	2.0.2

Required solution versions for upgrading

When upgrading from Entrust Deployment Manager 2.0.2, ensure the installed solutions have been upgraded to the following versions.

Solution	Version
CA Gateway	3.0.4
Timestamping Authority	2.1.1
Certificate Manager	4.0.4
Entrust Validation Authority	2.4.3
Certificate Enrollment Gateway	2.1.0

Required installation mode for upgrading

The platform being upgraded must have been installed (in one or several nodes) using the `prod-mode` mode described in [Installing CSP](#).

Required files for upgrading

You need the following files described in [Downloading the installation files](#).

File	Description
PKI Hub 1.1.0 for VMWare vSphere, Hyper-V and Nutanix	ISO installation image for Cryptographic Security Platform. You need this file to upgrade any installation, ISO-based or non-ISO-based.
EDM 2.0.x to PKI Hub upgrade tool	RPM package for the upgrade command-line tool.

Required license for upgrading

If your current installation is Entrust Deployment Manager 2.0.2, you need a CSP (Entrust Crypto Security Platform) license.

i When [Upgrading from Entrust Deployment Manager 2.0.2](#), you will use the license file path as argument of the `pki-hub-upgrade upgrade` command.

Required machine for upgrading

All the installation nodes must meet the [Machine requirements](#).

✗ This release adds [Machine requirements](#) to previous Entrust Deployment Manager or PKI Hub installations.

Required IP version for upgrading

As explained in [IP address requirements](#), Cryptographic Security Platform only supports IPv4 and disables IPv6 by default. Therefore, before upgrading, you must change all DNS server configurations from IPv6 to IPv4. See [Configuring the connection of an ISO installation](#) for how to perform this operation in ISO installations.

✗ The upgrade removes all IPv6 addresses from the `/etc/hosts` file.

Upgrading from Entrust Deployment Manager 2.0.2

See below for instructions on how to upgrade and Entrust Deployment Manager 2.0.2 installation to CSP 1.0.0.

i See the Entrust Deployment Manager 2.0.2 installation and administration guide for upgrading an Entrust Deployment Manager installation to 2.0.2.

To upgrade an Entrust Deployment Manager 2.0.2 node to CSP 1.0.0

1. Backup the installation state as explained in the Entrust Deployment Manager 2.0.2 guide.
2. Make sure your installation meets the [Upgrade requirements](#)
3. In all the installation nodes:
 - a. Use an SFTP client to copy the `pki-hub-upgrade.rpm` package file on the `/home/sysadmin` node folder.
 - b. Run the following command to install the package.

```
sudo dnf install pki-hub-upgrade.rpm --assumeyes
```

4. Run the `pki-hub-upgrade prepare` command sequentially in all nodes.
 - Follow the steps described in [Applying missing machine requirements](#) if the command prompt reports missing [Machine requirements](#) – for example.

```
$ sudo pki-hub-upgrade prepare
Checking node status done |||||||||||||||||||||||||||||||||||||||| 100 %
The following tasks have to be performed to complete the preparation of the
node:
- The node total disk size needs to be increased at least to 1 TiB.
- Follow the Entrust PKI Hub documentation on how to increase the disk
size for your platform.
- WARNING: this task may imply service outage in the node, depending
on your platform.
Once all the manual preparation tasks have been completed, re-execute the
'pki-hub-upgrade prepare' command.
```

- Follow the steps described in [Reinstalling Entrust Deployment Manager 2.0.2](#) if the command prompt requests a reinstallation – for example:

```
$ sudo pki-hub-upgrade prepare
Checking node status done |||||||||||||||||||||||||||||||||||||||| 100 %
The following tasks have to be performed to complete the preparation of the
node:
- The node needs to be reinstalled.
- Follow the Entrust PKI Hub documentation on how to reinstall an EDM
2.0.0-based node for upgrading to Entrust PKI Hub.
- WARNING: this task may imply service outage in the node, depending
on your platform.
Once all the manual preparation tasks have been completed, re-execute the
'pki-hub-upgrade prepare' command.
```

- No additional actions are required if the prompt confirms that the node is ready for an upgrade – for example:

```
$ sudo pki-hub-upgrade prepare
Checking node status done |||||||||||||||||||||||||||||||||||||||| 100 %
The node is ready to be upgraded to PKI Hub 1.1.0
```

- Perform the operations sequentially on each node:
 - Use an SFTP client to copy the CSP license file and the ISO image on the `/home/sysadmin` node folder.
 - Run the `pki-hub-upgrade upgrade` command.
 - Wait until the command is complete (which may take around two hours) before repeating the process in the next node.
- Reboot all nodes sequentially. Wait for 15 minutes before rebooting the next node.
- Back up the installation state as explained in section [Backing up](#) of this guide.

Applying missing machine requirements

The `pki-hub-upgrade prepare` command output may report missing Machine requirements:

- Insufficient size
- Missing auxiliary disk

For example:

[illegible]

In such cases, you must repeat the following steps on each installation node.

To apply missing machine requirements on a node

1. Stop the node.
2. Apply the missing [Machine requirements](#).
3. Start the node.
4. Wait 15 minutes.
5. Rerun the `pki-hub-upgrade prepare` command. If all requirements are met, the command will prompt an output like the following.

```
$ sudo pki-hub-upgrade prepare
Checking node status done |||||||||||||||||||||||||||||||||||||||| 100 %
The node is ready to be upgraded to PKI Hub 1.1.0
```

Reinstalling Entrust Deployment Manager 2.0.2

The [pki-hub-upgrade prepare](#) command output may request a reinstallation of Entrust Deployment Manager 2.0.2 – for example:

```
$ sudo pki-hub-upgrade prepare
Checking node status done |||||||||||||||||||||||||||||||||||||||| 100 %
The following tasks have to be performed to complete the preparation of the node:
- The node needs to be reinstalled.
  - Follow the Entrust PKI Hub documentation on how to reinstall an EDM 2.0.0-based
  node for upgrading to Entrust PKI Hub.
  - WARNING: this task may imply service outage in the node, depending on your
  platform.
Once all the manual preparation tasks have been completed, re-execute the 'pki-hub-
upgrade prepare' command.
```

Specifically, this situation occurs when:

- Entrust Deployment Manager 2.0.2 was installed using an ISO file.
- Entrust Deployment Manager 2.0.2 was upgraded from 2.0.0 at some point.

In this case, follow the steps below, depending on the number of nodes on your installation.

- [Reinstalling multi-node Entrust Deployment Manager 2.0.2 installations](#)
- [Reinstalling single-node Entrust Deployment Manager 2.0.2 on installations](#)

Reinstalling multi-node Entrust Deployment Manager 2.0.2 installations

This section explains how to reinstall Entrust Deployment Manager 2.0.2 when the following conditions are met.

- The [pki-hub-upgrade prepare](#) command prompts "The node needs to be reinstalled".
- Entrust Deployment Manager was installed using an ISO file.
- Entrust Deployment Manager was upgraded from 2.0.0 at some point.
- Entrust Deployment Manager runs on more than one node.

In this case, you must repeat the following steps sequentially on each node.

- [Getting information on the target node](#)
- [Removing the target node from the cluster](#)
- [Uninstalling Entrust Deployment Manager 2.0.2 on the target node](#)
- [Reinstalling Entrust Deployment Manager 2.0.2 on the target node](#)
- [Completing Entrust Deployment Manager 2.0.2 reinstall on the target node](#)



In the steps below, the "target node" is the node on which the Entrust Deployment Manager is being reinstalled.

Getting information on the target node

Run the [clusterctl node join-token](#) on the target node to get the joining token.

Get also system information on this node. As detailed in the following table, you need to save fewer settings when the node uses DHCP (Dynamic Host Configuration Protocol).

Setting	Command	DHCP	No-DHCP
The IP address of the node	Run <code>hostname -I</code> and copy the first listed IP address	✓	✓
The hostname of the node	Run <code>hostname</code>	✓	✓
The IP addresses of the DNS servers	Run <code>cat /etc/resolv.conf</code>	✗	✓
The IP address of the gateway	Run <code>route -n</code>	✗	✓
The IP addresses of the NTP servers	Run <code>chronyc sources -v</code>	✗	✓
The chrony config file	Copy the <code>/etc/chrony/chrony.conf</code> file	✓	✓

Removing the target node from the cluster

In any of the other cluster nodes, run the [pki-hub-upgrade remove-node](#) using the IP address previously obtained when [Getting information on the target node](#).

Run also the [clusterctl node join-token](#) command to get the node joining token of this node.

Uninstalling Entrust Deployment Manager 2.0.2 on the target node

Uninstall Entrust Deployment Manager 2.0.2 on the target node.

To uninstall Entrust Deployment Manager 2.0.2

1. Run the [clusterctl uninstall](#) command to uninstall Entrust Deployment Manager 2.0.2.
2. Remove the node hostname and IP address from the DNS server and load balancer.

Reinstalling Entrust Deployment Manager 2.0.2 on the target node

Reinstall Entrust Deployment Manager 2.0.2 on the target node.

i The below steps only apply to VMware platforms. Contact customer support to reinstall from ISO image on other platforms.

To reinstall Entrust Deployment Manager 2.0.2

1. Power off the Virtual Machine hosting the node.
2. Right-click on the machine name and select **Edit Settings**.
3. Select the **Virtual Hardware** tab.
4. Expand the **CD/DVD drive** section:
 - Select the installation ISO image for Entrust Deployment Manager 2.0.2.
 - Check the **Connect At Power On** box.

5. Select the **VM Options** tab.
6. Expand the **Boot Options** section:
 - If the machine firmware is configured to boot using the BIOS, set the **Boot Delay** to the maximum allowed value (for example, 10000 milliseconds).
 - If the machine firmware is configured to use UEFI, check the **Force EFI setup** box.
7. Click **OK** to save the settings.
8. Power on the virtual machine.
9. Click **Launch Web Console** to access the boot menu.
 - If the machine firmware is configured to boot using the BIOS, press **ESC** before the **Boot Delay** period expires, select the **CD-ROM Drive** option to boot from the ISO, and press **Enter**.
 - If the machine firmware is configured to use UEFI, select the **<EFI VMware Virtual SATA CDROM Drive (0.0)>** option and press **Enter**.
10. Wait while the installation completes.

Completing Entrust Deployment Manager 2.0.2 reinstall on the target node

Perform the below steps on the target node to complete the Entrust Deployment Manager 2.0.2 reinstall.

To complete Entrust Deployment Manager 2.0.2 reinstall

1. Restore the system information obtained when [Getting information on the target node](#).
2. Run the `clusterctl node add` command using the joining token obtained when [Removing the target node from the cluster](#).
3. Add the node IP address to the DNS server and the load balancer (if any).
4. Use an SFTP client to copy the `pki-hub-upgrade-1.1.0.rpm` package in the `/home/sysadmin` node directory.
5. Run the following command to install the upgrade package; you will need it to continue the upgrade process.

```
sudo dnf install pki-hub-upgrade.rpm --assumeyes
```


Reinstalling single-node Entrust Deployment Manager 2.0.2 on installations

This section explains how to reinstall Entrust Deployment Manager 2.0.2 when the following conditions are met.

- The `pki-hub-upgrade prepare` command prompts "The node needs to be reinstalled".
- Entrust Deployment Manager was installed using an ISO file.
- Entrust Deployment Manager was upgraded from 2.0.0 at some point.
- Entrust Deployment Manager runs on a single node.

In this case, you must repeat the following steps.

- [Scheduling the HSM service outage](#)
- [Getting system information on the original node](#)
- [Creating an auxiliary node](#)
- [Getting information on the auxiliary node](#)
- [Uninstalling Entrust Deployment Manager 2.0.2 on the original node](#)
- [Reinstalling Entrust Deployment Manager 2.0.2 on the original node](#)
- [Completing Entrust Deployment Manager 2.0.2 reinstall on the original node](#)
- [Removing the auxiliary node](#)

 In the steps below, the "original node" is the node on which the Entrust Deployment Manager is reinstalled. The "auxiliary node" is a disposable node created for reinstallation.

Scheduling the HSM service outage

During reinstallation, single-node deployments lose connectivity with the Hardware Security Module. Therefore, it is advisable to schedule the reinstallation procedure during a period of low workload for solutions that use an HSM.

- Timestamping Authority
- Validation Authority

Getting system information on the original node

Run the `clusterctl node join-token` on the original node to get the joining token.

Get also system information on this node. As detailed in the following table, you need to save fewer settings when the node uses DHCP (Dynamic Host Configuration Protocol).

Setting	Command	DHCP	No-DHCP
The IP address of the node	Run <code>hostname -I</code> and copy the first listed IP address	✓	✓
The hostname of the node	Run <code>hostname</code>	✓	✓
The IP addresses of the DNS servers	Run <code>cat /etc/resolv.conf</code>	✗	✓
The IP address of the gateway	Run <code>route -n</code>	✗	✓
The IP addresses of the NTP servers	Run <code>chronyc sources -v</code>	✗	✓
The chrony config file	Copy the <code>/etc/chrony/chrony.conf</code> file	✓	✓

Creating an auxiliary node

Create and configure an auxiliary node for the reinstall process.

To create and configure an auxiliary node

1. Create a new machine node with a hostname and IP address different from the ones assigned to the original node.
2. Install Entrust Deployment Manager 2.0.2 on this node, as explained in the Entrust Deployment Manager 2.0.2 product guide.
3. Run the `clusterctl node add` command using the joining token of the original node.
4. Add the node IP address to the DNS server and the load balancer (if any).
5. Use an SFTP client to copy the `pki-hub-upgrade-1.1.0.rpm` package in the `/home/sysadmin` node directory.
6. Run the following command to install the upgrade package.

```
sudo dnf install pki-hub-upgrade.rpm --assumeyes
```

7. Run the [pki-hub-upgrade remove-node](#) using the IP address obtained in [Getting node information](#).

Getting information on the auxiliary node

Run the [clusterctl node join-token](#) on the auxiliary node to get the joining token.

Uninstalling Entrust Deployment Manager 2.0.2 on the original node


Uninstall Entrust Deployment Manager 2.0.2 on the original node.

To uninstall Entrust Deployment Manager 2.0.2

1. Run the [clusterctl uninstall](#) command to uninstall Entrust Deployment Manager 2.0.2.
2. Remove the node hostname and IP address from the DNS server and load balancer.

Reinstalling Entrust Deployment Manager 2.0.2 on the original node

Reinstall Entrust Deployment Manager 2.0.2 on the original node.

 The below steps only apply to VMware platforms. Contact customer support to reinstall from ISO image on other platforms.

To reinstall Entrust Deployment Manager 2.0.2

1. Power off the Virtual Machine hosting the node.
2. Right-click on the machine name and select **Edit Settings**.
3. Select the **Virtual Hardware** tab.
4. Expand the **CD/DVD drive** section:
 - Select the installation ISO image for Entrust Deployment Manager 2.0.2.
 - Check the **Connect At Power On** box.
5. Select the **VM Options** tab.
6. Expand the **Boot Options** section:
 - If the machine firmware is configured to boot using the BIOS, set the **Boot Delay** to the maximum allowed value (for example, 10000 milliseconds).
 - If the machine firmware is configured to use UEFI, check the **Force EFI setup** box.
7. Click **OK** to save the settings.
8. Power on the virtual machine.
9. Click **Launch Web Console** to access the boot menu.
 - If the machine firmware is configured to boot using the BIOS, press **ESC** before the **Boot Delay** period expires, select the **CD-ROM Drive** option to boot from the ISO, and press **Enter**.
 - If the machine firmware is configured to use UEFI, select the **<EFI VMware Virtual SATA CDRom Drive (0.0)>** option and press **Enter**.
10. Wait while the installation completes.

Completing Entrust Deployment Manager 2.0.2 reinstall on the original node

Perform the below steps on the original node to complete the Entrust Deployment Manager 2.0.2 reinstall.

To complete Entrust Deployment Manager 2.0.2 reinstall

1. Restore the system information obtained when [Getting information on the original node](#).
2. Run the [clusterctl node add](#) command using the joining token obtained when [Getting information on the auxiliary node](#).
3. Add the node IP address to the DNS server and the load balancer (if any).

4. Use an SFTP client to copy the `pki-hub-upgrade-1.1.0.rpm` package in the `/home/sysadmin` node directory.
5. Run the following command to install the upgrade package.

```
sudo dnf install pki-hub-upgrade.rpm --assumeyes
```

6. Run the `pki-hub-upgrade remove-node` using the IP address obtained when [Getting information on the auxiliary node](#).

Removing the auxiliary node


Remove the auxiliary node after completing the upgrade process.

To remove the auxiliary node

1. Run the `clusterctl uninstall` command to uninstall Entrust Deployment Manager.
2. Remove the node hostname and IP address from the DNS and load balancer (if any).
3. Delete the Virtual Machine of the auxiliary node.

Upgrading from PKI Hub 1.0.0

See below for upgrading a PKI Hub 1.0.0 installation to CSP 1.0.0.

 During the upgrade process or while fixing a failed upgrade, you can only run the following commands (or equivalent Management Console operations): `clusterctl node info`, `clusterctl proxy clear`, `clusterctl proxy info`, `clusterctl proxy set`, `clusterctl uninstall`, `clusterctl version`.

To upgrade PKI Hub 1.0.0 to CSP 1.0.0

1. Backup the installation state as explained in the PKI Hub 1.0.0 guide.
2. Repeat the following steps on each PKI Hub node.
 - a. Use an SFTP client to copy the CSP 1.0.0 image file to the `/home/sysadmin` node folder.
 - b. Run the `clusterctl upgrade` command and wait until completion (around 2 hours).
3. Reboot each node sequentially, with at least 15 minutes before each reboot.
4. Back up the installation state as explained in [Backing up](#).

15 Administrating

Cryptographic Security Platform supports the administration operations described below.

- [Administrating nShield HSM integration](#)
- [Checking the etcd database size](#)
- [Checking the persistent volume disk usage](#)
- [Defragmenting the etcd database](#)
- [Managing the retention policies](#)
- [Recovering from disaster](#)
- [Restarting the nodes](#)
- [Updating DNS resolution](#)

See [Command reference](#) for the parameters required by each command.

Administrating nShield HSM integration

See below for the required steps when updating the integration with an Entrust nShield HSM (Hardware Security Module).

- [Applying nShield HSM configuration updates](#)
- [Integrating a nShield TVD](#)

Applying nShield HSM configuration updates

After updating the settings of an Entrust nShield HSM, perform the following steps in the solutions that use it.

- [Applying nShield HSM configuration updates to Certificate Authority](#)
- [Applying nShield HSM configuration updates to Validation Authority](#)
- [Applying nShield HSM configuration updates to Timestamping Authority](#)

Applying nShield HSM configuration updates to Certificate Authority

After updating the settings of an Entrust nShield HSM, perform the following steps to apply the changes in the Certificate Authority solution.

To apply Entrust nShield HSM configuration updates to Certificate Authority

1. Export the solution settings to a folder. You can either:
 - Run the [clusterctl solution config export](#) command.
 - Use the Management Console, as explained in [Backing up solution settings](#).
2. Replace the `kmdata.tar` file in the exported settings folder with the `kmdata.tar` file of your new HSM configuration.
3. Run the [clusterctl solution config import](#) command to import the modified configuration.
4. Redeploy the solution. You can either:
 - Run the [clusterctl solution deploy](#) command.
 - Use the Management Console.

Applying nShield HSM configuration updates to Validation Authority

After updating the settings of an Entrust nShield HSM, perform the following steps to apply the changes in the Validation Authority solution.

To apply Entrust nShield HSM configuration updates to Validation Authority

1. Run the `evactl export-nshield` command to export the nShield settings to a folder.
2. Replace the `kmdata.tar` file in the exported settings folder with the `kmdata.tar` file of your new HSM configuration.
3. Run the `evactl import-nshield` command to import the modified settings.
4. Redeploy the solution. You can either:
 - Run the `clusterctl solution deploy` command.
 - Run the Management Console.

Applying nShield HSM configuration updates to Timestamping Authority

After updating the settings of an Entrust nShield HSM, perform the following steps to apply the changes in the Timestamping Authority solution.

To apply Entrust nShield HSM configuration updates to Timestamping Authority

1. Run the `tsactl export-nshield` command to export the nShield settings to a folder.
2. Replace the `kmdata.tar` file in the exported settings folder with the `kmdata.tar` file of your new HSM configuration.
3. Run the `tsactl import-nshield` command to import the modified settings.
4. Redeploy the solution. You can either:
 - Run the `clusterctl solution deploy` command.
 - Run the Management Console.

Integrating a nShield TVD

After integrating an Entrust nShield Trusted Verification Device (TVD), redeploy all solutions using an Entrust nShield HSM. You can:

- Use the Management Console.
- Run the `clusterctl solution deploy` command.

Checking the etcd database size

See below for monitoring the size of the etcd database integrated into Cryptographic Security Platform.

To check the size of the etcd database

1. Browse to the **Etcd > etcd Status** dashboard.
2. Check the information in the **DB Info per Member** section: used space, need for defragmentation, available capacity, etc.
3. If the dashboard alerts that the cluster needs defragmentation, or the etcd used space is close to 100%, perform the operation described in [Defragmenting the etcd database](#).

Checking the persistent volume disk usage

To check the disk usage of the persistent volumes, you can either:

- Login to the Grafana portal, as explained in [Browsing logs with Grafana](#), and browse the **Node Exporter Full** dashboard.
- Run the `clusterctl volume info` command.

Defragmenting the etcd database

See below how to defragment the `etcd` database of one node. In multi-node installations, repeat the procedure sequentially in all the nodes.

⚠ Defragmenting a live etcd member blocks the system from reading and writing data while rebuilding states. This operation can take several seconds, during which the whole cluster node is unavailable.

To defragment the etcd database in one node

1. Get the current etcd revision.

```
rev=$(sudo ETCDCCTL_API=3 etcdctl --cert /var/lib/rancher/k3s/server/tls/etcd/
client.crt --key /var/lib/rancher/k3s/server/tls/etcd/client.key --cacert /var/
lib/rancher/k3s/server/tls/etcd/server-ca.crt endpoint status --write-
out="json" | egrep -o '"revision":[0-9]*' | egrep -o '[0-9].*')
```

2. Compact away all old `etcd` revisions.

```
sudo ETCDCCTL_API=3 etcdctl --cert /var/lib/rancher/k3s/server/tls/etcd/
client.crt --key /var/lib/rancher/k3s/server/tls/etcd/client.key --cacert /var/
lib/rancher/k3s/server/tls/etcd/server-ca.crt compact $rev
```

3. Defragment `etcd` on the node.

```
sudo ETCDCCTL_API=3 etcdctl --cert /var/lib/rancher/k3s/server/tls/etcd/
client.crt --key /var/lib/rancher/k3s/server/tls/etcd/client.key --cacert /var/
lib/rancher/k3s/server/tls/etcd/server-ca.crt defrag
```

4. Disarm the `etcd` database space alarm.

```
sudo ETCDCCTL_API=3 etcdctl --cert /var/lib/rancher/k3s/server/tls/etcd/
client.crt --key /var/lib/rancher/k3s/server/tls/etcd/client.key --cacert /var/
lib/rancher/k3s/server/tls/etcd/server-ca.crt alarm disarm
```

Managing the retention policies

The default retention policy for logs and metrics is the following.

Data	Days	Default storage	Record deletion
Logs	28	10 GiB	After 28 days or when reaching 75% of the storage

Data	Days	Default storage	Record deletion
Metrics	14	10 GiB	After 14 days or when reaching 80% of the storage

You can manage these retention settings with the following commands.

- [clusterctl retention config logs](#)
- [clusterctl retention config metrics](#)
- [clusterctl retention info](#)

Recovering from disaster

Perform the following steps to recover Cryptographic Security Platform and the deployed solutions after a system crash.

- [Recovering single-node installations](#)
- [Recovering multi-node installations with a quorum](#)
- [Recovering multi-node installations without a quorum](#)

 As explained in [Installing CSP](#), only `prod-mode` installations support disaster recovery.

Recovering single-node installations

When a single-node installation crashes, recover the Cryptographic Security Platform and the deployed solutions from a backup as explained in [Restoring the state](#).

Recovering multi-node installations with a quorum

When your multi-node installation retains the quorum described in [Required number of nodes](#), you must simply remove, restore and add the crashed nodes.

To recover a crashed node.

1. Mark the node as unschedulable.

```
sudo kubectl cordon <node-to-delete>
```

2. Drain the pods from the node to delete.

```
sudo kubectl drain <node-to-delete> --delete-emptydir-data --disable-eviction  
--force --ignore-daemonsets --timeout=600s
```

3. Delete the node from the cluster.

```
sudo kubectl delete node <node-to-delete> --timeout=600s
```

4. Restore the node and add it again to the cluster, as explained in [Adding nodes](#).

Recovering multi-node installations without a quorum

When your multi-node installation does not retain the quorum described in [Load balancing requirements](#), follow the steps below for recovery.

To recover a multi-node deployment without a quorum

1. Run `clusterctl uninstall` in all the nodes to uninstall Cryptographic Security Platform.
2. Recover the Cryptographic Security Platform and the deployed solutions from a backup as explained in [Restoring the state](#).

Restarting the nodes

Some Cryptographic Security Platform upgrades may require restarting the system. In prod-mode installations, restart the nodes:

- One by one.
- At least 15 minutes apart.

Otherwise, you might encounter system problems and risk losing the quorum described in [Required number of nodes](#).

After restarting a node, run the following command to force the start of the `chrony` service.

```
sudo systemctl restart chronyd.service
```

Updating DNS resolution

To update DNS resolution after installing Cryptographic Security Platform, repeat the following instructions on each node.

✗ As explained in [DNS requirements](#), Cryptographic Security Platform does not support accessing a DNS server through a proxy.

Platform	Instructions
VMware vSphere or Nutanix	See the Configuring the connection of an ISO installation section of this guide.
Amazon Web Services	Refer to the docs.aws.amazon.com product documentation.
Azure	Refer to the learn.microsoft.com/azure product documentation.

When completing the DNS update, run the following command to restart the `coredns` service.

```
sudo kubectl rollout restart deployment coredns -n kube-system
```

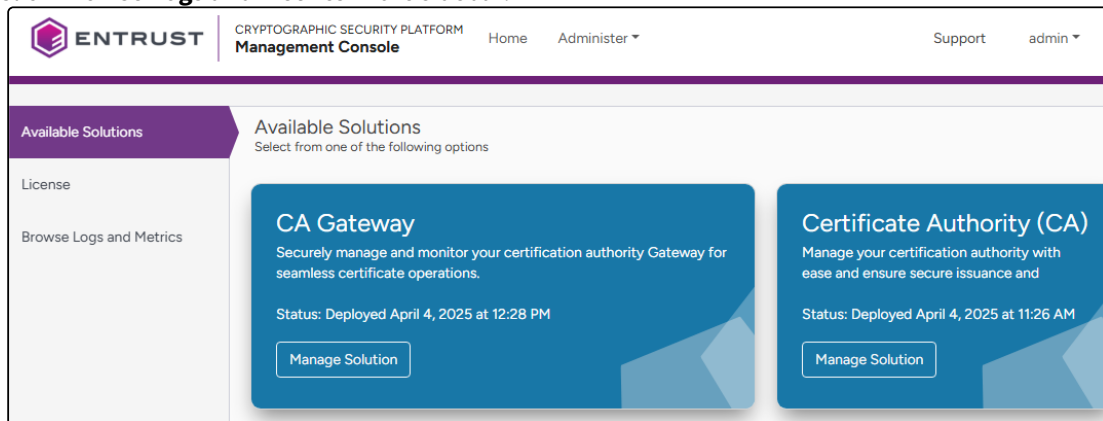

16 Browsing logs with Grafana

Cryptographic Security Platform provides a [Grafana](#) portal to browse logs and metrics on the internal services and the installed Entrust solutions.

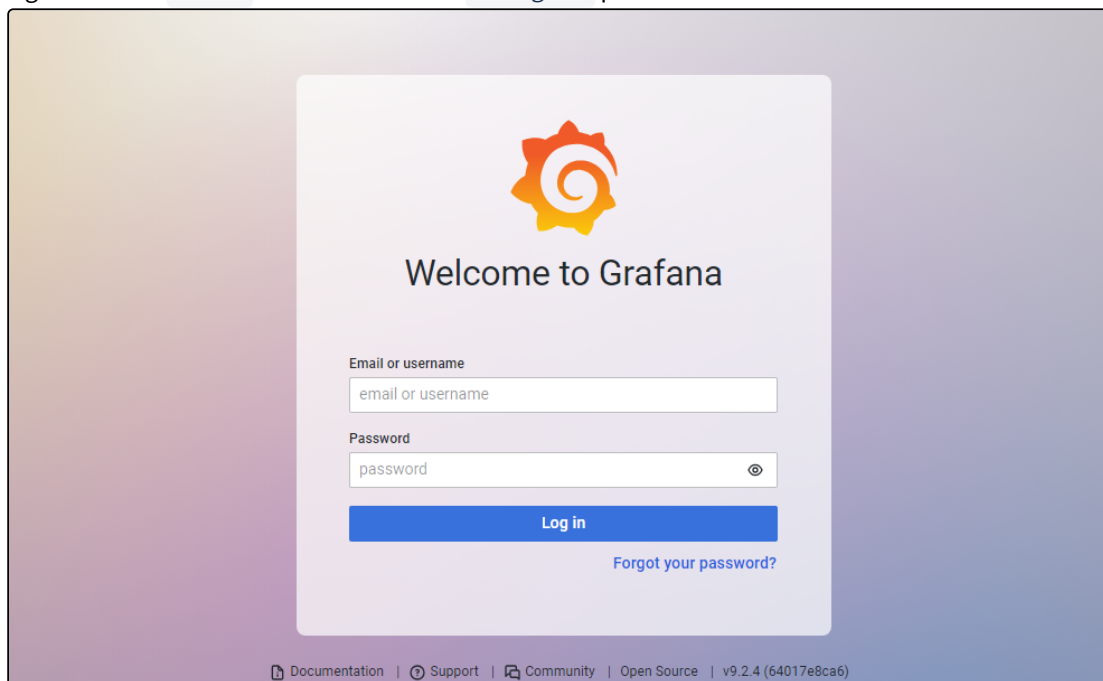
i See [Managing Log Forwarder](#) for how to forward logs to a Splunk SIEM (Security Information and Event Management) server.

To manage logs with Grafana

1. Login into the Management Console.
2. Click **Browse Logs and Metrics** in the sidebar.



3. Log in with the `admin` username and the `changeme` password.



4. Perform the following operations.
 - [Updating the Grafana initial administrator](#)
 - [Browsing and exporting logs with the Grafana Loki Dashboard](#)
 - [Browsing log file contents with Grafana](#)


Updating the Grafana initial administrator

Once you are logged in to Grafana with the default credentials of the initial administrator, you must perform one of the following operations.

- [Changing the password of the initial administrator](#)
- [Replacing the initial administrator](#)

For other user management operations, such as creating non-administrative users, see:

<https://grafana.com/docs/grafana/v9.2/administration/user-management>

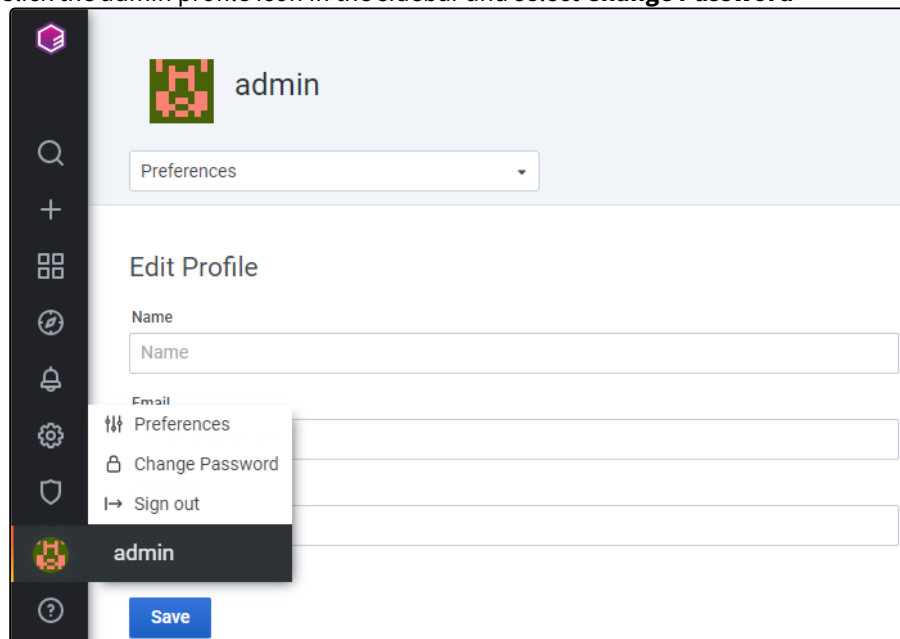
 The process described in [Backing up](#) does not include any Grafana configuration.

Changing the password of the initial administrator

You can keep the initial administrator by simply changing the default password.

To replace the password of the initial administrator

1. Log in to Grafana with the `admin` username and the `changeme` password.
2. Click the admin profile icon in the sidebar and select **Change Password**



3. Fill in the change password form and click **Save**.

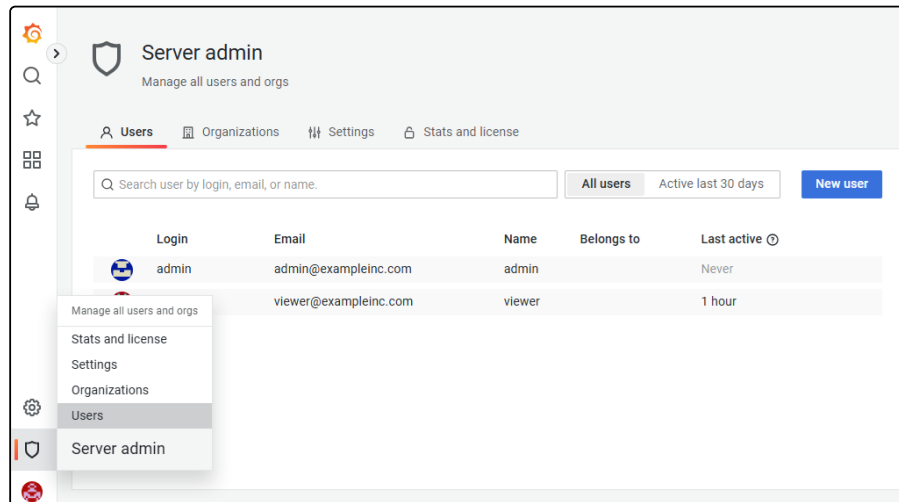
Replacing the initial administrator

See below for creating a new Grafana administrator that replaces the initial default one.

To replace the Grafana initial administrator

1. Log in to Grafana with the `admin` username and the `changeme` password.

- Click the shield icon in the sidebar and select **Users**.



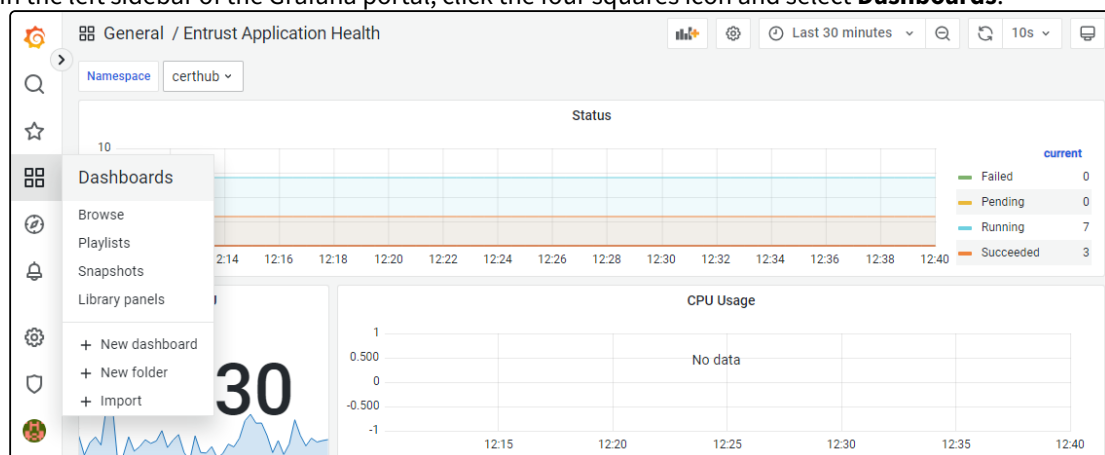
- Click **New**.
- Fill in the **New user** form and click **Create User**.
- In the user details view, click **Change** under **Permissions**.
- Set **Grafana Admin** to **Yes**.
- Click the shield icon in the sidebar and select **Users**.
- In the **Users** grid, click the name of the initial **admin** administrator.
- In the user details view, click either:
 - Delete user** to delete this initial administrator.
 - Disable user** to disable it.

Browsing and exporting logs with the Grafana Loki Dashboard

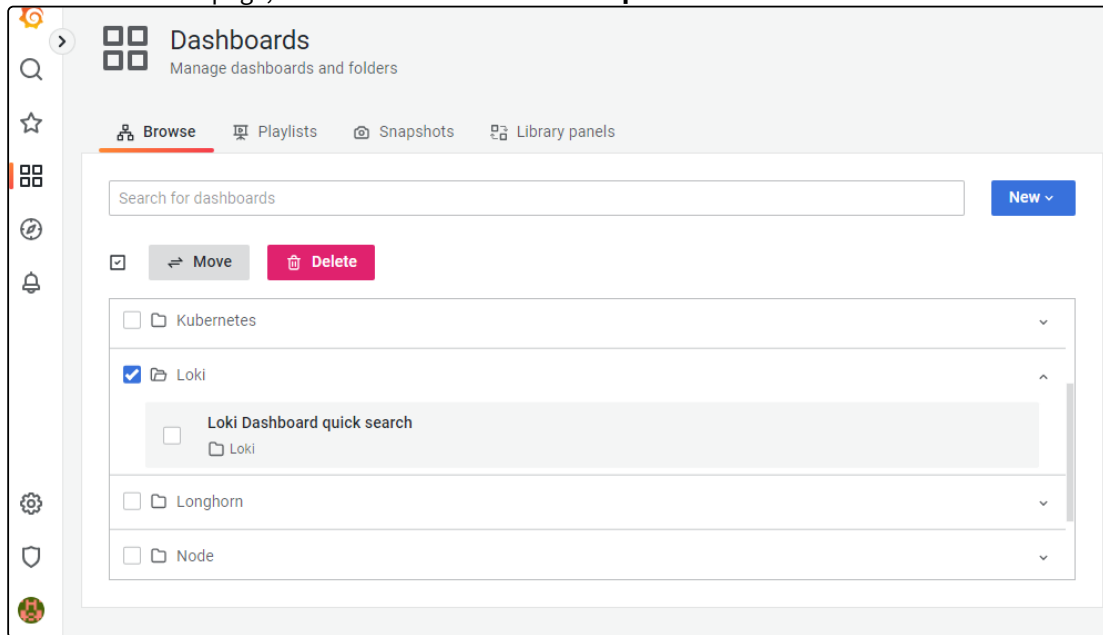
With the Grafana Loki Dashboard, users can browse and export logs of the Cryptographic Security Platform system and the deployed solutions.

To browse and export logs with the Grafana Loki Dashboard

- In the left sidebar of the Grafana portal, click the four squares icon and select **Dashboards**.

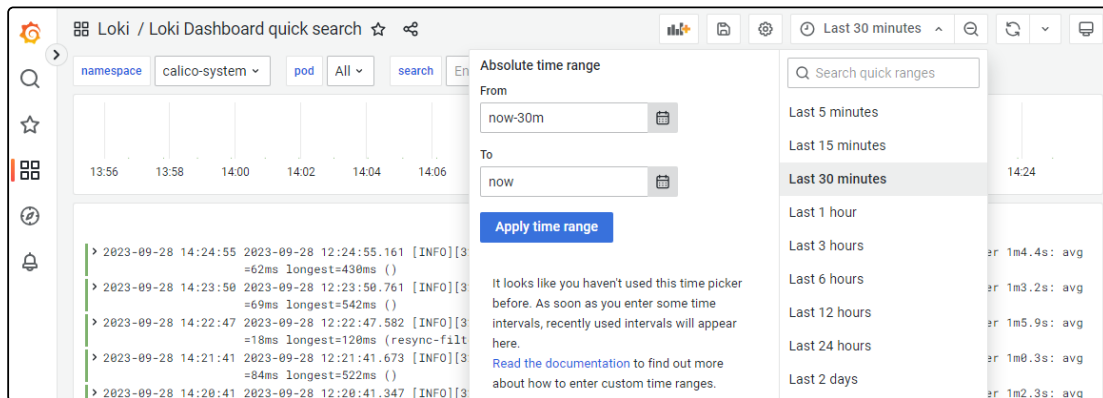


- In the **Dashboards** page, select **Loki > Loki Dashboard quick search**.

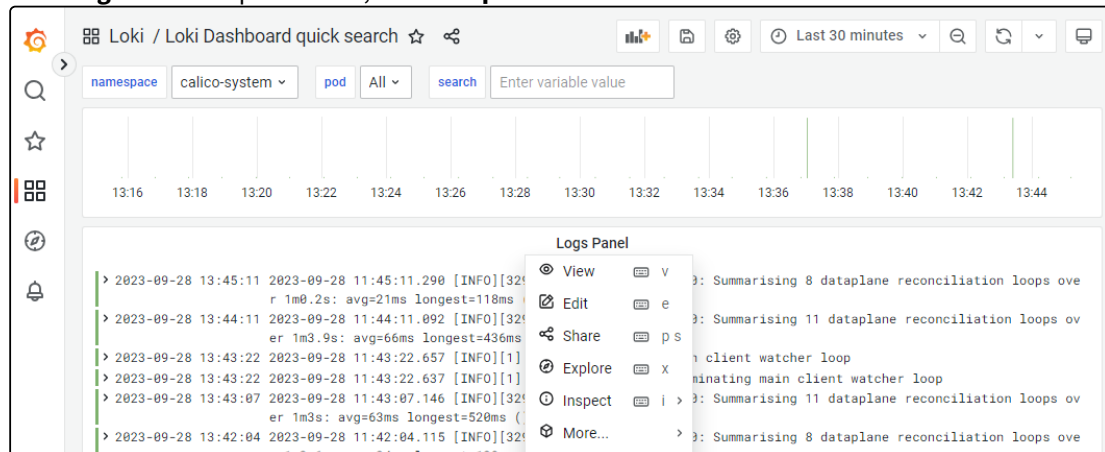


- Define a log query with the menu options.

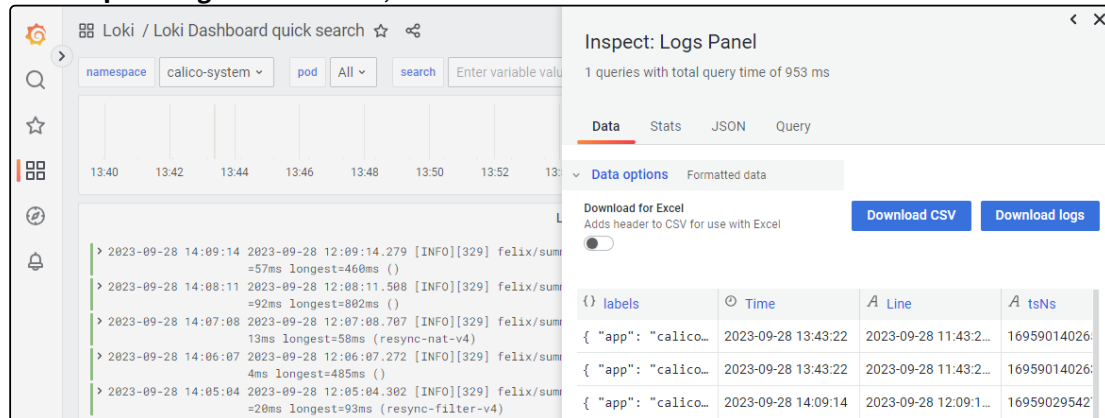
- namespace
- pod
- search
- Time range



4. In the **Logs Panel** drop-down list, select **Inspect**.



5. In the **Inspect: Logs Panel** sidebar, select the **Data** tab.



6. In the **Data** tab, click:

- **Download CSV** to download the logs into a CSV file.
- **Data options > Download for Excel** and **Download CSV** to download the logs into an Excel-compatible CSV file.
- **Download logs** to download the raw logs into a text file.

namespace

Click **namespace** in the top-right menu and select the namespace for querying logs.

Namespace	Monitored service
calico-system	The Calico networking service.
csf-docker-registry	The Docker registry.
longhorn-system	The Longhorn system.
istio-system	The Istio system.

Namespace	Monitored service
logging	The Log Forwarder solution.
csf-monitoring	The Prometheus service.
csf-logs	The Loki service.
kube-system	The K3s system.
cm	The Certificate Manager solution
pkihub-v<YYYYMMDDhhmm>	The Certificate Authority solution, version <YYYYMMDDhhmm> .
cagw	The CA Gateway solution.
ceg	The Certificate Enrollment Gateway solution.
tsa	The Entrust Timestamping Authority solution.
eva	The Validation Authority solution.
management-console	The web console for deploying and managing Entrust solutions.
tigera-operator	The Tigera Operator for deploying the Calico networking service.
auth-service	The authentication system for Cryptographic Security Platform administrators.
solution-manager	The service for managing the deployed Entrust solutions.

pod

Click **pod** in the top-right menu and select the running pods for which to browse logs.

search

Type a custom log query in the **search** search box.

Time range

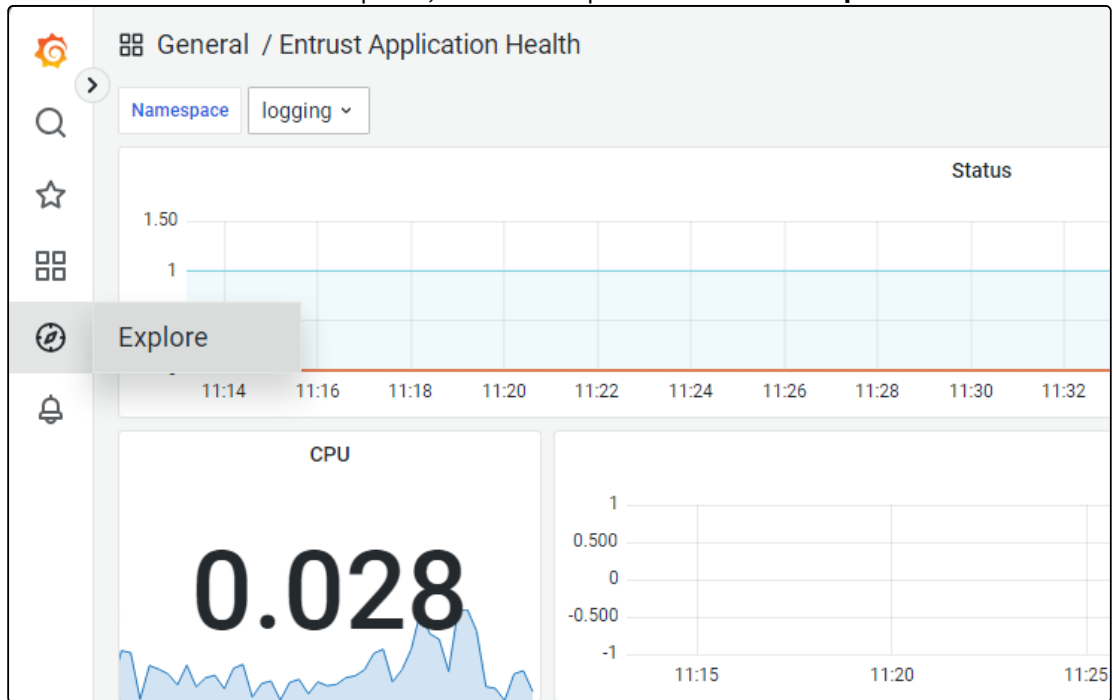
Click the clock icon in the top right menu and select the time range for querying logs.

Browsing log file contents with Grafana

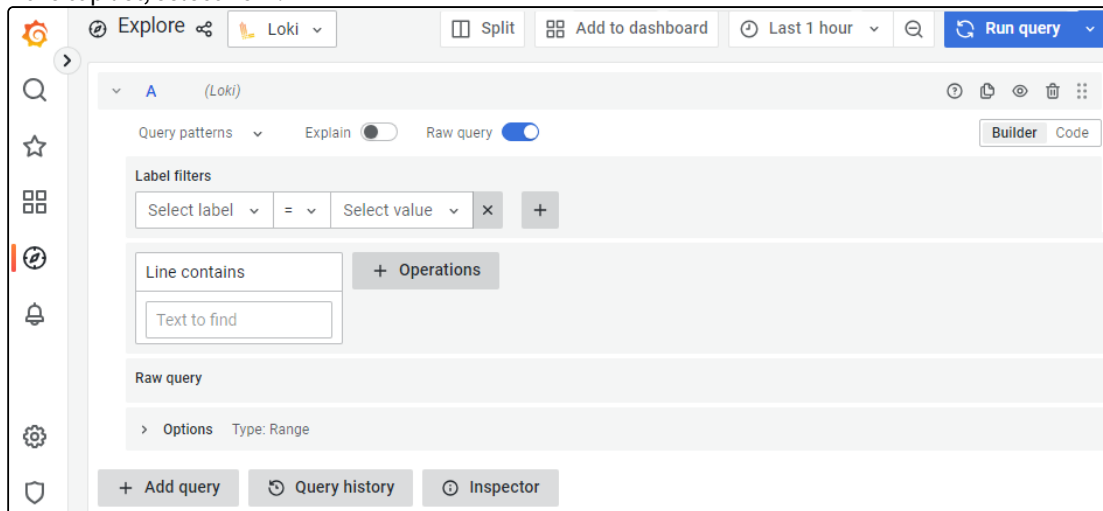
Grafana allows browsing operating system-level logs recorded in files.

To browse log files with Grafana

1. In the left sidebar of the Grafana portal, click the compass icon and select **Explore**.



2. In the top list, select **Loki**.



3. In the **Label filters** list, select **filename**.
4. In the **Select value** field, select a log file.
5. Click **+Operations** to filter the file contents.
6. Click **+Add query** to include additional filters – for example:
 - [Filtering Validation Authority logs](#)
 - [Filtering Timestamping Authority logs](#)
7. In the top-right corner, click **Run query** to display the selected contents.

Filtering Validation Authority logs

See below for how to filter Validation Authority in the Loki dashboard of Grafana.

- [Querying Validation Authority logs](#)
- [Querying OCSP request logs](#)
- [Auditing the executed evactl commands](#)

Querying Validation Authority logs

Add the following filters under **Label filters** to query Entrust Validation Authority logs.

Select label	Select value	Query output
namespace	eva	Entrust Validation Authority logs.
app	<service>	Logs for the <service> service.

Querying OCSP request logs

Add the following under **Label filters** to query logs on OCSP request processing.

Select label	Select value	Query output
namespace	eva	Entrust Validation Authority logs.
app	eva-ocspresponder	Logs for the OCSP responder service.

Use the **Line contains** fields to add filters like the following.

Line contains	Query output
SendRevocationStatusRequest	Logs for OCSP requests.
SendRevocationStatusRequest.Failed	Logs for failed OCSP requests.
<sn>	Logs for requests on the certificate with the <sn> serial number.
<dn>	Logs for requests on the certificate issued by a CA with the <dn> distinguished name.

Auditing the executed evactl commands

Add the following filters under **Label filters** to audit the execution of the `evactl` command line tool.

Select label	Select value	Query output
filename	var/log/entrust/eva/evactl.log	A record of all the executed <code>evactl</code> commands

Filtering Timestamping Authority logs

See below for how to filter Timestamping Authority logs in the Loki dashboard of Grafana.

- [Auditing the executed tsactl commands](#)
- [Checking the clock status](#)
- [Querying timestamping request logs](#)

Auditing the executed tsactl commands

Add the following filters under **Label filters** to audit the execution of the `tsactl` command line tool.

Select label	Select value	Query output
filename	/var/log/entrust/tsa/tsactl.log	A record of all the executed <code>tsactl</code> commands

Checking the clock status

Add the following filters under **Label filters** to query clock status service logs.

Select label	Select value	Query output
namespace	tsa	Timestamping Authority logs.
app	clockstatus	Logs of the clock status service.

Use the **Line contains** field to filter time checking logs.

Line contains	Query output
"GetClockData.	Logs for time checking operations.

Querying timestamping request logs

Add the following filters under **Label filters** to query timestamping request logs.

Select label	Select value	Query output
namespace	tsa	Timestamping Authority logs.
app	tsa	Logs of the timestamping service.

Use the **Line contains** fields to add filters like the following.

Line contains	Query output
"ProcessTimeStampRequest."	Logs for all timestamping requests.
"ProcessTimeStampRequest.Failed"	Logs for failed timestamping requests.
"endpoint": "<issuerID>"	Logs for timestamping requests received by the <issuerID> timestamp issuer, where <issuerID> is the value of the <i>Issuer ID</i> configuration value.

17 Backing up and restoring

See below for the backup and restore operations supported by Cryptographic Security Platform.

- [Backing up](#)
- [Restoring](#)

Backing up

See below for how to backup the state of Cryptographic Security Platform and all the deployed solutions.

- [Backing up the state](#)
- [Backing up solution settings](#)
- [Backing up databases](#)
- [Backing up the HSM](#)

Backing up the state

See below to back up the state of a Cryptographic Security Platform installation comprising one or several nodes.

- [Backing up the state of a single-node Cryptographic Security Platform installation](#)
- [Backing up the state of a multi-node Cryptographic Security Platform installation](#)

 As explained in [Installing CSP](#), only `prod-mode` installations support state backup and restore.

Backing up the state of a single-node Cryptographic Security Platform installation

When installed in a single node, follow the step below to back up the state of the Cryptographic Security Platform installation.

To back up the state of a single-node Cryptographic Security Platform installation

1. Run the `clusterctl backup create` command to generate a backup file – for example:

```
$ sudo clusterctl backup create --file /home/sysadmin/202341014.bkp --password 7Txsxu
```

1. If the deployed solutions use databases, back up the database contents as explained in [Backing up the database](#).
2. If the deployed solutions use an HSM (Hardware Security Module) to protect private keys, backup the device configuration as explained in [Backing up the HSM](#).
3. Move all the backup data from the Cryptographic Security Platform node to a secure location – for example, using an SFTP client.

Backing up the state of a multi-node Cryptographic Security Platform installation


When installed in several nodes, perform the step below in any node to back up the state of the Cryptographic Security Platform installation

To back up the state of a multi-node Cryptographic Security Platform installation

1. Run the `clusterctl backup create` command to generate a backup file – for example:

```
$ sudo clusterctl backup create --file /home/sysadmin/202341014.bkp --password 7Txsxu
```


2. Manually backup the following data.
 - The key and certificate for TLS
 - The registration credentials
 - The volume capacity policies configured with the [clusterctl volume capacity](#) command.
 - The retention policies configured with the [clusterctl retention config logs](#) and [clusterctl retention config metrics](#) commands.
 - The proxy settings are configured with the [clusterctl proxy set](#) command.
3. Follow the steps described in [Backing up solution settings](#) to back up the CA Gateway, Certificate Enrollment Gateway and Certificate Manager solutions.

 The settings of the other solutions are automatically included in the backup file generated with the [clusterctl backup create](#) command.

4. If the deployed solutions use databases, back up the database contents as explained in [Backing up the database](#).
5. If the deployed solutions use an HSM (Hardware Security Module) to protect private keys, backup the device configuration as explained in [Backing up the HSM](#).
6. Move all the backup data from the Cryptographic Security Platform node to a secure location – for example, using an SFTP client.

Backing up solution settings

In single-node Cryptographic Security Platform installations, the [clusterctl backup create](#) command, executed when [Backing up the state](#), already contains all solution settings. However, multi-node installations require manually exporting the settings of each deployed solution.

 Ensure you have sensitive data, such as passwords or PINs, which are not included in the backup file.

To back up the settings of a solution


1. Log into the Management Console.
2. Click **Manage Solution** under the solution name.
3. Click **Export Configuration** to download a zipped file containing the configuration settings and credential files, such as key stores.

Backing up databases

Follow the instructions of the DBMS vendor to back up the databases used by Entrust solutions.

Backing up the HSM

If the deployed solutions use an HSM (Hardware Security Module) to protect private keys, back up the device using the tools provided by the HSM vendor.

 If you previously ran the [clusterctl backup create](#) command, for example when [Backing up the Cryptographic Security Platform state](#), you do not need to back up HSM-protected keys. The backup file generated by the command includes these keys.

Restoring


See below for how to restore the state of Cryptographic Security Platform and all the deployed solutions.

- [Restoring the state](#)
- [Restoring solution settings](#)
- [Restoring databases](#)
- [Restoring the HSM](#)

Restoring the state

See below to restore the state of a Cryptographic Security Platform installation comprising one or several nodes.

- [Restoring the state of a single-node Cryptographic Security Platform installation](#)
- [Restoring the state of a multi-node Cryptographic Security Platform installation](#)

 As explained in [Installing CSP](#), only `prod-mode` installations support state backup and restore.

Restoring the state of a single-node Cryptographic Security Platform installation

See below to restore the Cryptographic Security Platform status when installed in a single node.

To restore a single-node Cryptographic Security Platform installation

1. Reproduce the Cryptographic Security Platform installation used for [Backing up the state](#). Specifically:
 - Install the same Cryptographic Security Platform version.
 - Set the node hostname and IP address as in the original installation.
2. If the deployed solutions use an HSM (Hardware Security Module) to protect private keys, restore the device configuration as explained in [Restoring the HSM](#).
3. If the solutions of the restored installation use databases, restore the database contents as explained in [Restoring databases](#).
4. Copy the file generated with the `clusterctl backup create` command when [Backing up the state](#).
5. Run the `clusterctl backup restore` command to restore the backup file.
6. Log into the Management Console and click **Deploy** for the CA Gateway solution (if deployed in the restored solution).

Restoring the state of a multi-node Cryptographic Security Platform installation

See below to restore the Cryptographic Security Platform status when installed in several nodes.

To restore a multi-node Cryptographic Security Platform installation

1. Reproduce the Cryptographic Security Platform installation used for [Backing up the state](#). Specifically:
 - Install the same Cryptographic Security Platform version.
 - Add the same number of nodes as in the original installation.
 - Set the node hostname and IP address as in the original installation.
2. If the deployed solutions use an HSM (Hardware Security Module) to protect private keys, restore the device configuration as explained in [Restoring the HSM](#).
3. If the solutions of the restored installation use databases, restore the database contents as explained in [Restoring databases](#).
4. Import the license as explained in [Setting or updating the license](#).
5. Run the `clusterctl certificate` command to install the TLS certificate and key backup.
6. Run the `clusterctl volume capacity` to restore the previous volume capacity policies.
7. Run `clusterctl retention config logs` to restore the previous log retention period.

8. Run `clusterctl retention config metrics` to restore the previous metric retention period.
9. Run the `clusterctl proxy set` to restore the previous proxy settings.
10. Follow the steps described in [Restoring solution settings](#) to restore and deploy the Gateway, Certificate Enrollment Gateway, and Certificate Manager solutions (if present in the restored installation).
11. In any installation node:
 - a. Copy the file generated with the `clusterctl backup create` command when [Backing up the state](#).
 - b. Run the `clusterctl backup restore` command to restore the backup file.
12. Log into the Management Console and click **Deploy** for the following solutions (if deployed in the restored platform).
 - Certificate Authority
 - Validation Authority
 - Timestamping Authority

Restoring solution settings

Follow the steps below to restore the settings of a solution.

To restore the settings of a solution


1. Extract the contents of the zipped backup file generated when [Backing up solution settings](#).
2. Log into the Management Console.
3. Click **Manage Solution** under the solution name.
4. Click **Import Configuration** and select the JSON configuration file included in the backup file.
5. Click **Next**.
6. Manually enter data not included in the imported configuration, such as passwords and credential files.
7. Click **Validate** to validate the configured settings.
8. Correct any detected configuration error until the **Validate** option displays no warnings.
9. Click **Submit** and wait while Cryptographic Security Platform uploads the configuration and any attached file, such as authentication credentials.
10. Click **Deploy**.

Restoring databases

Follow the instructions of the DBMS vendor to restore the databases used by Entrust solutions.

Restoring the HSM

If the deployed solutions use an HSM (Hardware Security Module) to protect private keys, restore the device using the tools provided by the HSM vendor.

 If you previously ran the `clusterctl backup restore` command, you do not need to restore HSM-protected keys. The backup file imported by the command includes these keys.

18 Uninstalling

To uninstall Cryptographic Security Platform and all the deployed Entrust solutions, run the `clusterctl uninstall` command in all the installation nodes – for example:

```
$ sudo clusterctl uninstall  
Warning: The cluster and the deployed applications are going to be uninstalled  
Are you sure you want to uninstall the cluster? [Y/n]: Y  
Uninstalling done |██████████████████████████████████████| 100 %
```

19 Command reference

See below for the commands supported by the Cryptographic Security Platform command-line tools.

✖ The commands described in the following sections require passwordless `sudo` permissions.

- `clusterctl backup create`
- `clusterctl backup restore`
- `clusterctl certificate`
- `clusterctl help`
- `clusterctl install`
- `clusterctl license import`
- `clusterctl node add`
- `clusterctl node info`
- `clusterctl node join-token`
- `clusterctl proxy clear`
- `clusterctl proxy info`
- `clusterctl proxy set`
- `clusterctl retention config logs`
- `clusterctl retention config metrics`
- `clusterctl retention info`
- `clusterctl solution config export`
- `clusterctl solution config import`
- `clusterctl solution deploy`
- `clusterctl solution info`
- `clusterctl solution secret set`
- `clusterctl solution upload`
- `clusterctl uninstall`
- `clusterctl upgrade`
- `clusterctl version`
- `clusterctl volume capacity`
- `clusterctl volume info`
- `evactl check all`
- `evactl check cert-source`
- `evactl check db`
- `evactl check hsm`
- `evactl create-csr`
- `evactl create-key`
- `evactl delete-key`
- `evactl enroll`
- `evactl export-nshield`
- `evactl import-nshield`
- `evactl import-p12`
- `evactl import-thales`
- `evactl list-certs`
- `evactl list-keys`
- `evactl load-oracle-wallet`
- `evactl reenroll`
- `evactl stop`
- `pki-hub-upgrade prepare`
- `pki-hub-upgrade remove-node`
- `pki-hub-upgrade upgrade`

- [tsactl check clock](#)
- [tsactl check hsm](#)
- [tsactl create-csr](#)
- [tsactl create-key](#)
- [tsactl delete-key](#)
- [tsactl export-nshield](#)
- [tsactl import-nshield](#)
- [tsactl import-thales](#)
- [tsactl list-keys](#)
- [tsactl stop](#)

clusterctl backup create

Executed when: [Backing up the state](#).

Saves the state of Cryptographic Security Platform and the installed Entrust solutions.


```
clusterctl backup create --file <file> [--password <pwd>]
```

See below for a description of each parameter.

- [-f, --file <file>](#)
- [-p, --password <pwd>](#)

For example:

```
$ sudo clusterctl backup create --path /home/sysadmin/edm20230307.bkp
Password:
Re-enter password:
Backing up config done |||||||||||||||||||||||||||||||||||||||| 100 %
```

 If an option value contains spaces or special characters, you must surround the entire value with quotation marks.

-f, --file <file>

Export the backup in `<file>`, where `<file>` is the full path of a file with the `.bkp` extension.

Mandatory: Yes.

-p, --password <pwd>

Protect the backup file with the `<pwd>` password.

Mandatory: No. When omitting this option, the command prompts for the password and password confirmation.

clusterctl backup restore

Executed when: [Restoring the state](#).

Restores the state of Cryptographic Security Platform.

```
clusterctl backup restore --file <file> [--password <pwd>]
```

See below for a description of each parameter.

- `-f, --file <file>`
- `-p, --password <pwd>`

For example:


```
$ sudo clusterctl backup restore --file /home/sysadmin/20241009.bkp
```

Specifically, this command:

1. Restores the state of Cryptographic Security Platform along with the deployed Entrust solutions.
2. In physical and VMware machines, enables `firewalld` and creates firewall rules for opening the [Required open ports](#).

The command raises an exception when executed in a node with:

- A different hostname than the backed-up node.
- Cryptographic Security Platform already installed.

 If an option value contains spaces or special characters, you must surround the entire value with quotation marks.

`-f, --file <file>`

Restore the `<file>` backup, where `<file>` is the path of a file generated with the `clusterctl backup create` command.

Mandatory: Yes.

`-p, --password <pwd>`

Open the backup file with the `<pwd>` password, where `<pwd>` is the password passed to the `clusterctl backup create` command when exporting the backup.

Mandatory: No. When omitting this option, the command prompts for the password.

clusterctl certificate

Executed when: [Replacing the default TLS certificate](#).

Installs the TLS certificate of Cryptographic Security Platform.

```
clusterctl certificate --cert <bundle> --key <key>
```

See below for a description of each parameter.

- `-c, --cert <bundle>`

- `-k, --key <key>`

For example:

```
$ sudo clusterctl certificate --cert /home/sysadmin/cert.pem --key /home/sysadmin/key.pem
```


If the Certificate Authority solution is already deployed, redeploy the solution to make the changes effective.

```
$ clusterctl solution deploy --solution-id pkihub
```

`-c, --cert <bundle>`

Load the TLS certificate and the certification chain from `<bundle>`, where `<bundle>` is the path of a plaintext file in the following PEM format.


```
-----BEGIN CERTIFICATE-----
<TLS Server cert in B64 encoding>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<CA Subordinate Cert in B64 encoding>
-----END CERTIFICATE-----
```

 The selected certificate must meet the requirements described in [Replacing the default TLS certificate](#).

Mandatory: Yes.

`-k, --key <key>`

Load the private key from `<key>`, where `<key>` is the path of a PEM file.

 Password-protected keys are not currently supported.

Mandatory: Yes.

clusterctl help

Prints help information on `clusterctl` subcommands. You can use any of the following syntaxes.

```
clusterctl help <subcommands>
```

```
clusterctl <subcommands> -h
```

```
clusterctl <subcommands> --help
```

Where `<subcommands>` is the list of subcommands. For example, the following command lines display identical help information on [clusterctl retention config logs](#).

```
clusterctl help retention config logs
```

```
clusterctl retention config logs -h
```

```
clusterctl retention config logs --help
```

clusterctl install

Executed when: [Installing CSP](#).

Installs Cryptographic Security Platform.

```
clusterctl install [--mode <mode>]
```

For example:

```
$ sudo clusterctl
Installing done |||||||||||||||||||||||||||||||||||||||| 100 %
```

Specifically, this command:

1. Validates the [Requirements](#).
2. Enables `firewalld` and creates firewall rules for opening the [Required open ports](#).
3. Installs Cryptographic Security Platform.
4. Generates a self-signed TLS certificate (that you can optionally replace during the product configuration).

--mode <mode>

Run the installation in `<mode>` mode. Where `<mode>` is either:

- demo-mode
- prod-mode

See the table below for a description of each mode.

Setting	demo-mode	prod-mode
Deployment type	Proof-of-concept deployments.	Production deployments.

Setting	demo-mode	prod-mode
Requirements	Does not need the disk performance requirements described in Machine requirements . Specifically, fsync latency is not an issue in this mode.	All the Requirements .
Supported number of nodes	One	One or more. See Required number of nodes for details.
Supported operations	You cannot perform the operations described in Joining nodes , Backing up the state , Recovering from disaster , or Restoring the state .	All
Supported updates	You cannot upgrade to a newer version or migrate to a multi-node installation.	All

Mandatory: No. This optional value defaults to `prod-mode`.

clusterctl license import

Executed when: [Setting or updating the license](#).

Sets or updates the Cryptographic Security Platform license.

```
clusterctl license import -f <license>
```

Where `<license>` is the path of the license file. For example:

```
$ sudo license import -f pkihub.lic
License imported
```

clusterctl node add

Executed when: [Joining nodes](#).

Adds a node to Cryptographic Security Platform.

```
clusterctl node add <node> <token>
```

See below for a description of each parameter.

- `<node>`
- `<token>`

For example:

```
$ sudo clusterctl node add 10.1.141.28  
4d22f2665fe0680bd3d6f479f176dc21367f41bca9e83864024dc83da0c7c86c  
Adding a node done ||||||||||||||||||||||||||||||||||||| 100 %  
Warning: The cluster only contains 2 nodes. Three nodes are required to achieve HA  
and an odd number of nodes is recommended
```

This command:

- Prints a warning when the cluster does not contain the [Required number of nodes](#).
- Enables `firewalld` and creates firewall rules for opening the [Required open ports](#).
- In case of execution error, rolls back all actions and reports the error cause.

As explained in [Joining nodes](#):

- Do not run this command simultaneously in different nodes of the same Cryptographic Security Platform deployment.
- Redeploy the deployed solutions (if any) to make the changes effective.

<node>

The IP address of a node already in the Cryptographic Security Platform cluster.

 In AWS and Azure cloud installations, use the private IP of the node.

Mandatory: Yes.

<token>

The joining token obtained when running the `clusterctl node join-token` command in the `<node>` node.

Mandatory: Yes.

clusterctl node info

Lists the nodes of Cryptographic Security Platform.

```
clusterctl node info
```

For example:

```
$ sudo clusterctl node info
```

NODE NAME	NODE IP	NODE AGE
myhost01.mydomain.com	10.1.141.50	5h57m
myhost02.mydomain.com	10.1.141.51	4h42m
myhost03.mydomain.com	10.1.141.52	4h11m

Where:

- `NODE NAME` is the node name.
- `NODE IP` is the node's IP.

- `NODE AGE` is the time during which the node has been in operation.

If Cryptographic Security Platform runs on less than 3 nodes, the information includes a warning message because HA requires at least 3 nodes (we recommend an odd number of nodes).

clusterctl node join-token


Executed when: [Joining nodes](#).

Prints the joining token for other nodes to join the cluster.

```
clusterctl node join-token
```

For example:

```
$ sudo clusterctl node join-token
NODE JOIN TOKEN
7dc820922681be2197736246ef32784a530186c3e58e07ac671768de690c3ca0
```

 You must run this command in a node already added to Cryptographic Security Platform.

clusterctl proxy clear


Executed when: [Configuring the proxy](#).

Clears the proxy configuration.

```
clusterctl proxy clear
```

For example:

```
$ sudo clusterctl proxy clear
The proxy configuration has been cleared
```

 Changes will be effective when deploying (or redeploying) the solution with Management Console or the [clusterctl solution deploy](#) command.

clusterctl proxy info

Executed when: [Configuring the proxy](#).

Prints the proxy configuration values set with the [clusterctl proxy set](#) command.

```
clusterctl proxy info
```

For example:

```
$ sudo clusterctl proxy info
Protocol:      https
Host:         myproxy
Port:         443
User:         bob
Password:      ****
TLS server cert: None
No proxy:     example.com,192.168.1.1,sub.domain.com
```

clusterctl proxy set

Executed when: [Configuring the proxy](#).

Configures the connection with the proxy server.


```
clusterctl proxy set --host <host> [--port <port>] [--protocol <protocol>] [--
certificate <cert>] [--user <user>] [--password <pwd>] [--no-proxy <no-proxy>]
```

See below for a description of each parameter.

- `--host <host>`
- `--port <port>`
- `--no-proxy <no-proxy>`
- `--user <user>, --password <pwd>`
- `--protocol <protocol>`
- `--certificate <cert>`

For example:

```
$ sudo clusterctl proxy set --host myproxy --user bob --password demo
The proxy configuration has been set
```

 Changes will be effective when deploying (or redeploying) the solution with Management Console or the [clusterctl solution deploy](#) command.

--host <host>

Select the `<host>` proxy, where `<host>` is an address in one of the following formats.

Address format	Limitations
IP address	None
Hostname	The <code>--protocol <protocol></code> option only supports the <code>https</code> value

Mandatory: Yes.

--port <port>


Select `<port>` as the proxy port number.

Mandatory: No. When omitted, this parameter defaults to 443.

--no-proxy <no-proxy>

Skip the proxy when connecting to the `<no-proxy>` sites, where `<no-proxy>` is a comma-separated list (without spaces) of domains or IP addresses. For example:

```
example.com,192.168.1.1,sub.domain.com
```

 The `<no-proxy>` list cannot include IP addresses in CIDR (Classless Inter-Domain Routing) format like `192.168.1.0/24`.

Mandatory: No.

--user <user>, --password <pwd>

Authenticate in the proxy with the `<user>` username and the `<pwd>` password.

Mandatory: No. See the following table for the actions performed when setting or omitting this parameter.

--user	--password	Action
<user>	<pwd>	Set <code><user></code> and <code><pwd></code> as proxy basic authentication credentials
<user>		Prompt for the password of the <code><user></code> user
	<pwd>	Throw an error
		Assume that the proxy requires no authentication

--protocol <protocol>

The protocol for accessing the proxy. See the table below for the supported values.


Value	Limitations
http	The <code>--host <host></code> option only supports IP addresses

Value	Limitations
https	None

Mandatory: No. This optional value defaults to `https`.

`--certificate <cert>`

Authenticate in the proxy with the `<cert>` certificate, where `<cert>` is the path of a plaintext file in PEM format.

 The certificate should include a SAN matching the host.

Mandatory: No. See the following table for the actions performed when setting or omitting this parameter.

<code>--protocol</code>	<code>--certificate</code>	Action
http	<code><cert></code>	Throw an error
http		Set an HTTP connection
https	<code><cert></code>	Set an HTTPS connection with the <code><cert></code> certificate
https		Set an HTTPS connection with the default certificate of the operating system

clusterctl retention config logs

Executed when: [Managing the retention policies](#).

Updates the log retention period.

```
clusterctl retention config logs --period <period> [-y]
```

See below for a description of each parameter.


- `--period <period>`
- `-y, --yes`

For example, to set a 15-days retention period.

```
$ sudo clusterctl retention config logs --period 15
Warning: The command execution will temporarily interrupt the selected service. This
might take several minutes
Are you sure you want to modify the retention values? [Y/n]: Y
Configuring logs retention period to 15 days... Done
```

--period <period>

Set the retention period to `<period>`, where `<period>` is a number of days.

 A `<period>` value lower than the current period deletes all logs older than `<period>`.

Mandatory: Yes.


-y, --yes

Skip the confirmation prompt.

clusterctl retention config metrics

Executed when: [Managing the retention policies](#).

Updates the metrics retention period, the metrics allocated space, or both.

 This command temporarily interrupts the metrics service.

```
clusterctl retention config metrics --period <period> --size <size> [-y]
```

See below for a description of each parameter.

- `--period <period>`
- `--size <size>`
- `-y, --yes`

For example, to update both the retention period and allocated space:

```
$ sudo clusterctl retention config metrics --period 15 --size 2
Warning: The command execution will temporarily interrupt the selected service. This
might take several minutes
Are you sure you want to modify the retention values? [Y/n]: Y
Configuring metrics retention period to 15 days... Done
Configuring metrics retention size to 2Gi... Done
```

To update only the retention size:

```
$ sudo clusterctl retention config metrics --size 2
```

```
Warning: The command execution will temporarily interrupt the selected service. This
might take several minutes
Are you sure you want to modify the retention values? [Y/n]: Y
Configuring metrics retention size to 2Gi... Done
```

✗ The `--period` and `--size` options are only mutually exclusive when set to 0. When set to a value greater than 0, you can pass both options or only one.

`--period <period>`

Set the retention period to `<period>`, where `<period>` is a number of days.

- A `<period>` value lower than the current period deletes all metrics older than `<period>`.
- A `<period>` value of 0 disables the retention period so the metrics retention is only limited by `<size>`.

Mandatory: No. When omitting this option, the retention period remains unchanged.

`--size <size>`

Allocate `<size>` for the metrics, there `<size>` is a number of Gi allocated for the metrics (float values supported).

- A `<size>` value lower than the current size deletes all metrics exceeding `<size>`.
- A `<size>` value of 0 disables the allocated space limit, so the metrics retention is only limited by `<period>`.

⚠ When updating the allocated size, run the `clusterctl volume capacity` command to update the Prometheus volume size accordingly.

Mandatory: No. When omitting this option, the metrics space remains unchanged.

`-y, --yes`

Skip the confirmation prompt.

clusterctl retention info

Executed when: [Managing the retention policies](#).

Prints the current retention settings.

```
clusterctl retention info
```

For example:

```
$ sudo clusterctl retention info
SERVICE    PERIOD  MAX SIZE
metrics     14d     1GB
```

logs	28d	N/A
------	-----	-----

Where:

- `SERVICE` is the service name: metrics or logs.
- `PERIOD` is the retention period for the logs or metrics.
- `MAX SIZE` is the maximum size allocated for the metrics.

See [clusterctl retention config logs](#) and [clusterctl retention config metrics](#) for updating these retention settings.

clusterctl solution config export

Exports the configuration of an installed Entrust solution.

```
clusterctl solution config export --solution-id <solution_id> --path <dir_path>
```

See below for a description of each parameter.

- `-i, --solution-id <solution_id>`
- `-f, --path <dir_path>`

For example:


```
$ sudo clusterctl solution config export --solution-id eva --path /home/sysadmin/eva/
config
Exporting the configuration files... Done
```

The command will raise an error if:

- The `<dir_path>` folder does not exist in the node where you run the command.
- The `<dir_path>` folder is not empty.
- The Entrust solution is not correctly registered and deployed.

`-i, --solution-id <solution_id>`

Export the configuration of the solution with the `<solution_id>` identifier.

 Run the [clusterctl solution info](#) command to get the identifiers of the installed Entrust solutions.

Mandatory: Yes.

`-f, --path <dir_path>`

Export the configuration in `<dir_path>`, where `<dir_path>` is the path of an empty folder in the execution node.

Mandatory: Yes.

clusterctl solution config import

Imports the configuration of an installed Entrust solution.

```
clusterctl solution config import --solution-id <solution_id> --path <dir_path>
```

See below for a description of each parameter.

- `-i, --solution-id <solution_id>`
- `-f, --path <dir_path>`

For example:

```
$ sudo clusterctl solution config import --solution-id eva --path /home/sysadmin/eva/
config
Importing the configuration files... Done
```

The command will raise an error if:

- The `<dir_path>` folder does not exist in the node where you run the command.
- The `<dir_path>` folder is empty.
- The Entrust solution is not correctly registered and deployed.

⚠ To make configuration changes effective, redeploy the solution with the [clusterctl solution deploy](#) command.

`-i, --solution-id <solution_id>`

Import the configuration of the solution with the `<solution_id>` identifier.

ℹ Run the [clusterctl solution info](#) command to get the identifiers of the installed Entrust solutions.

Mandatory: Yes.

`-f, --path <dir_path>`

Import all configuration files that are included in the folder with the `<dir_path>` path and have filenames matching the following regular expression.

```
^[a-zA-Z0-9/\\.\\-]{3,64}$
```

✗ The command removes from the solution any other configuration file. Therefore, always run the [clusterctl solution config import](#) command beforehand to ensure you have the complete set of configuration files.

Mandatory: Yes.


`clusterctl solution deploy`

Deploys an Entrust solution or redeploys an already deployed Entrust solution to make configuration changes effective.

```
clusterctl solution deploy --solution-id <solution_id>
```

-i,--solution-id <solution_id>

Deploy the solution with the `<solution_id>` identifier.

 Run the [clusterctl solution info](#) command to get the identifiers of the installed Entrust solutions.

Mandatory: Yes.

clusterctl solution info

Prints the main settings of each deployed Entrust solution.

```
clusterctl solution info
```

For example:

```
$ sudo clusterctl solution info
SOLUTION ID    DEPLOYED
ceg           1.4 at 2022-04-18T23:45:10.000Z (success)
cm            1.1 at 2022-07-11T10:49:31.000Z (success)
eva           1.0 at 2022-06-11T13:40:57.000Z
cagw          processing
```

See below for a description of each column.

- [SOLUTION ID](#)
- [DEPLOYED](#)

SOLUTION ID

The solution identifier. See the following table for these supported values.

Solution identifier	Solution
cagw	CA Gateway
cm	Certificate Manager
ceg	Certificate Enrollment Gateway
eva	Validation Authority

Solution identifier	Solution
Log Forwarder	Log Forwarder
pkihub-v<YYYYMMDDhhmm>	Certificate Authority, version <YYYYMMDDhhmm> .
tsa	Timestaping Authority

DEPLOYED

The date and status of the last deployment, in the following format.

```
<date> <status>
```

See the following table for the supported values.

Deployment status	<date>	<status>
Not deployed	—	Not deployed yet
In progress	The UTC date when the deployment started.	(deploying)
Successfully completed	The UTC date when the deployment ended.	(success)
Failed	The UTC date when the deployment started.	(failure)

clusterctl solution secret set

Sets the value of a secret.

```
clusterctl solution secret set --solution-id <solution_id> [--from-literal
<secret_id>=<secret_value> | --from-file <secret_id>=<secret_path>]
```

See below for a description of each parameter.

- `-i,--solution-id <solution_id>`
- `--from-literal <secret_id>=<secret_value>`
- `--from-file <secret_id>=<secret_path>`

For example:


```
$ sudo clusterctl solution secret set --solution-id ceg --from-literal password='S!B\*d$zDsb='
```

! If already deployed, redeploy the solution with the `clusterctl solution deploy` command to make changes effective.

`-i,--solution-id <solution_id>`

Set the secret in the solution with the `<solution_id>` identifier.

i Run the `clusterctl solution info` command to get the identifiers of the installed Entrust solutions.

Mandatory: Yes.

`--from-literal <secret_id>=<secret_value>`

Set the secret value from an inline value.

! This option is mutually exclusive with `--from-path`. When omitting both options, the command assumes the `--from-literal` option and prompts the user for `<secret_id>` and `<secret_value>`.

Parameter	Value	Format restrictions
<code><secret_id></code>	The identifier of the secret	3-128 characters in length, start with a letter, and contain only alphanumeric characters, underscores, and hyphens.
<code><secret_value></code>	The value of the secret	Cannot exceed 128KB. Must be enclosed in quotes to escape special characters (such as <code>\$</code> , <code>\</code> , <code>*</code> , <code>=</code> , and <code>!</code>) with a backslash (<code>\</code>) as in the above example.

Mandatory: No.

`--from-file <secret_id>=<secret_path>`

Set the secret value from a file.

! This option is mutually exclusive with `--from-literal`. When omitting both options, the command assumes the `--from-literal` option and prompts the user for `<secret_id>` and `<secret_value>`.

Parameter	Value	Format restrictions
<secret_id>	The identifier of the secret	3-128 characters in length, start with a letter, and contain only alphanumeric characters, underscores, and hyphens.
<secret_path>	The path of a file containing the Base64 encoding of the secret value	Cannot exceed 128KB. Must be enclosed in quotes to escape special characters (such as \$, \ , * , = , and !) with a backslash (\) as in the above example.

Mandatory: No.

clusterctl solution upload

✖ Execute this command only when instructed by customer support to apply solution hotfixes.

Uploads a solution to the solution manager endpoint.

```
clusterctl solution upload --solution-id <solution_id> --file <sln>
```

See below for a description of each parameter.


- -i, --solution-id <solution_id>
- -f, --file <sln>

For example:

```
$ sudo clusterctl solution upload -i cm -f /home/sysadmin/cm.sln  
Preparing done ||||||||||||||||||||||||||||||||||||||||| 100 %  
Uploading done ||||||||||||||||||||||||||||||||||||||||| 100 %  
Processing done |||||||||||||||||||||||||||||||||||||||| 100 %  
Certificate Manager: version 4.1 uploaded
```

-i, --solution-id <solution_id>

Upload the solution with the `<solution_id>` the solution identifier.

 Run the `clusterctl solution info` command to get the identifiers of the installed Entrust solutions.

Mandatory: Yes.

-f, --file <sln>

Upload the `<sln>` solution setup file, where `<sln>` is the path of the Entrust solution setup file with `sln` extension.

 Login to trustedcare.entrust.com for downloading this file.

Mandatory: Yes.

clusterctl uninstall

Uninstalls Cryptographic Security Platform along with all the deployed Entrust solutions.

```
clusterctl uninstall [-y]
```

When prompted, confirm the uninstall process.

```
$ sudo clusterctl uninstall
The cluster and the deployed solutions are going to be uninstalled
Are you sure you want to uninstall the cluster? [Y/n]:
```

-y, --yes

Skip the confirmation prompt.

clusterctl upgrade


Executed when: [Upgrading from PKI Hub 1.0.0](#).

Upgrades a PKI Hub 1.0.0 installation to CSP 1.0.0.

```
clusterctl upgrade --iso-path <iso>
```

For example:

```
$ clusterctl upgrade --iso-path /home/sysadmin/pki-hub-1.1.0.iso
```

 If the installation meets all [Upgrade requirements](#), the command takes around 2 hours to complete. Otherwise, the command throws an error.

-f, --iso-path <iso>

Apply the `<iso>` upgrade, where `<iso>` is the path of the ISO installation file for CSP 1.0.0.

Mandatory: Yes.

clusterctl version

Prints the Cryptographic Security Platform version.

```
clusterctl version
```

For example, after installing or upgrading Cryptographic Security Platform to version 1.1.0.

```
$ sudo clusterctl version
Cryptographic Security Platform release 1.1.0
Installation mode: prod-mode
```

When Cryptographic Security Platform is not installed, the command specifies "cluster not installed" in the installation mode.

```
$ sudo clusterctl version
Cryptographic Security Platform release 1.1.0
Installation mode: cluster not installed
```

clusterctl volume capacity

Sets the size capacity of a volume.

✖ This command temporarily interrupts the associated service for up to several minutes.

```
clusterctl volume capacity <pv> --size <size> [-y]
```

See below for a description of each parameter.

- `<pv>`
- `--size <size>`
- `-y, --yes`

When prompted, confirm the size modification – for example:

```
$ sudo clusterctl volume capacity storage-entitlements-service --size 2
Warning: The command execution will temporarily interrupt the service associated to
the Persistent Volume. This might take several minutes
Are you sure you want to modify the Persistent Volume capacity? [Y/n]: Y
Resizing the storage-entitlements-service Persistent Volume to 2Gi... Done
```

`<pv>`

Set the capacity of the `<pv>` persistent volume, where `<pv>` is one of the volume names listed by the [clusterctl volume info](#) command.

Mandatory: Yes.

--size <size>

Set the persistent volume size to `<size>`, where `<size>` is a number of Gi (float values supported).

- If this value does not exceed the current volume size, the command will throw an error message. Run the [clusterctl volume info](#) command to check the current volume sizes.
- When changing the size capacity of the Prometheus volume, run the [clusterctl retention config metrics](#) command to update the metrics retention accordingly.

Mandatory: Yes.

-y, --yes

Skip the confirmation prompt.

clusterctl volume info

Executed when: [Checking the persistent volume disk usage](#)

Prints information on the persistent volumes of Cryptographic Security Platform.

```
clusterctl volume info
```

For example:

```
$ sudo clusterctl volume info
NAME                                CAPACITY  USAGE    % USED
ceg-config-rwx-pvc                 93.0MB    1.0MB    1.08%
ceg-db-rwx-pvc                     976.0MB   1.0MB    0.20%
storage-auth-service-0             975.9MB   2.7MB    0.27%
storage-csf-grafana-0              3.9GB     18.7MB   0.47%
storage-csf-loki-0                 9.8GB     209.3MB  1.09%
storage-docker-registry            19.6GB    4.1GB    21.16%
storage-prometheus-prometheus-0    9.8GB     5.9GB    60.07%
storage-solution-manager-0         9.8GB     36.2MB   0.36%
```

evactl check all

Debugs all the components of the Validation Authority deployment.

```
evactl check all [-c <tls_ca_path>] [-i <cert_id>] [-l <level>] [-p <pin>] [-v
<vendor>] [-t <token>]
```

For example:

```
$ sudo evactl check all
Starting PKCS #11 Manager... Done
=====
CHECKING HSM
```

```

=====

Slot Id -> 0
Label -> pking203
Serial Number -> 1433959427612
Model -> LunaSA 7.2.0
Firmware Version -> 7.0.3
Configuration -> Luna User Partition With S0 (PED) Signing With
Cloning Mode
Slot Description -> Net Token Slot
FM HW Status -> FM Ready

Slot Id -> 1
Label -> pking202
Serial Number -> 1433964084224
Model -> LunaSA 7.2.0
Firmware Version -> 7.0.3
Configuration -> Luna User Partition With S0 (PED) Signing With
Cloning Mode
Slot Description -> Net Token Slot
FM HW Status -> FM Ready

Current Slot Id: 0

Passing HSM checks... Done

=====
CHECKING DB
=====
Starting Configurator... Done
Checking DB user privileges... Done
Checking DB tables... Done

=====
CHECKING CAGW
=====

CAID: intminions~subordinate
Checking CAGW is reachable... Done
Checking configured CA... Done

=====

Tests passed successfully

```

See below for a description of each parameter.

- -c <tls_ca_path>
- -i <cert_id>
- -l <level>
- -p <pin>
- -v <vendor>

- -t <token>

-c <tls_ca_path>


Validate the TLS server certificate of CA Gateway with <tls_ca_path>. Where <tls_ca_path> is the path of a CA file in PEM format.

Mandatory: No. When omitting this option, the command uses the CA configured in [CSP CA Gateway](#).

-i <cert_id>


Authenticate in CA Gateway with the <cert_id> certificate, where <cert_id> is the identifier of the certificate described in [CA Gateway for Validation Authority](#).

Mandatory: No. This optional parameter defaults to the latest client certificate imported with the [evactl import-p12](#) command.

 Run the [evactl list-certs](#) command to list the available certificates and the latest one imported.

-l <level>

Debug the nShield HSM with the <level> level, where <level> is a `CKNFAST_DEBUG` variable level. When not using a nShield HSM, the command ignores this option.

 See the nShield documentation for details on the `CKNFAST_DEBUG` configuration parameter.

Mandatory: No. This optional parameter defaults to 0.

-p <pin>

Authenticate in the HSM with the <pin> PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-v <vendor>

Use the <vendor> security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

✖ The command will raise an error if you omit this option and the configuration is not loaded.

-t <token>

Select the HSM token with the `<token>` label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

✖ The command will raise an error if you omit this option and the configuration is not loaded.

evactl check cert-source

Checks the certificate sources for every configured CA.

```
evactl check cert-source [-c <tls_ca_path>] [-i <cert_id>]
```

For example:

```
$ sudo evactl check cert-source
Starting Configurator...           Done

CAID: ca~subordinate
  Checking CAGW is reachable...    Done
  Checking configured CA...        Done

Tests passed successfully
```

See below for a description of each option.

- `-c <tls_ca_path>`
- `-i <cert_id>`

-c <tls_ca_path>


Validate the TLS server certificate of CA Gateway with `<tls_ca_path>`. Where `<tls_ca_path>` is the path of a CA file in PEM format.

Mandatory: No. When omitting this option, the command uses the CA configured in [CSP CA Gateway](#).

-i <cert_id>

Authenticate in CA Gateway with the <cert_id> certificate, where <cert_id> is the identifier of the certificate described in [CA Gateway for Validation Authority](#).

Mandatory: No. This optional parameter defaults to the latest client certificate imported with the [evactl import-p12](#) command.

 Run the [evactl list-certs](#) command to list the available certificates and the latest one imported.

evactl check db

Checks the database connectivity, required users, user privileges, and tables.

```
evactl check db
```

For example:

```
$ sudo evactl check db
Starting Configurator...           Done
Checking DB user privileges...     Done
Checking DB tables...              Done
```

evactl check hsm

Checks the HSM connectivity.

```
evactl check hsm [-l <level>] [-p <pin>] [-v <vendor>] [-t <token>]
```

For example:

```
$ sudo evactl check hsm
Starting PKCS #11 Manager...       Done

Slot Id ->                         0
Label ->                           pking203
Serial Number ->                   1433959427612
Model ->                           LunaSA 7.2.0
Firmware Version ->                7.0.3
Configuration ->                   Luna User Partition With SO (PED) Signing With
Cloning Mode
Slot Description ->                 Net Token Slot
FM HW Status ->                     FM Ready

Slot Id ->                         1
Label ->                           pking202
Serial Number ->                   1433964084224
```

```

Model -> LunaSA 7.2.0
Firmware Version -> 7.0.3
Configuration -> Luna User Partition With S0 (PED) Signing With
Cloning Mode
Slot Description -> Net Token Slot
FM HW Status -> FM Ready

Current Slot Id: 0

Passing HSM checks... Done

```

See below for a description of each option.

- `-l <level>`
- `-p <pin>`
- `-v <vendor>`
- `-t <token>`

`-l <level>`

Debug the nShield HSM with the `<level>` level, where `<level>` is a `CKNFAST_DEBUG` variable level. When not using a nShield HSM, the command ignores this option.



See the nShield documentation for details on the `CKNFAST_DEBUG` configuration parameter.

Mandatory: No. This optional parameter defaults to 0.

`-p <pin>`

Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

`-v <vendor>`

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.



It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

✗ The command will raise an error if you omit this option and the configuration is not loaded.

-t <token>

Select the HSM token with the <token> label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

✗ The command will raise an error if you omit this option and the configuration is not loaded.

evactl create-csr

Generates a new certificate signing request (CSR) for a key pair previously generated with the [evactl create-key](#) command.

```
evactl create-csr -k <key_id> [-s <subject>] [-o <csr>] [-p <pin>] [-t <token>] [-v <vendor>] [-y]
```

For example:


```
$ sudo evactl create-csr -k 7ce798c13a411bc1da4a9f983ed6d44fb4d7ed1a -s "CN=97357462, O=Entrust, C=ES"
Starting PKCS #11 resource... Done
Using token with label mytoken
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIBIDCBxQIBADAzMTEwLWYDVQQDEyg3Y2U30ThjMTNhNDExYmMxZGE0YTlmOTgz
...
9xMajw==
-----END CERTIFICATE REQUEST-----
```

See below for a description of each option.

- -k <key_id>
- -s <subject>
- -o <csr>
- -p <pin>
- -t <token>
- -v <vendor>
- -y

-k <key_id>


Select the key with the <key_id> identifier.

 Run the `evactl list-keys` command to get the key identifiers.

Mandatory: Yes.

-s <subject>

Use `<subject>` as the Subject of the certificate request. Where `<subject>` is a full Distinguished Name (DN) or Relative Distinguished Name (RDN).

 For Entrust Validation Authority to recognize the Subject, the DN attributes must be in capital letters.

For example:

```
CN=Example User,O=Example,C=US
```

```
CN=Example User
```

Mandatory: No. When omitting this option, the Subject in the generated certificate request defaults to the following:

```
CN=<key_id>
```

Where `<key_id>` is the key identifier.

-o <csr>

Save the certificate signing request (CSR) in a file with the `<csr>` path.

Mandatory: No. When omitting this option, the command prints the CSR to the standard output.

-p <pin>


Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-t <token>

Select the HSM token with the `<token>` label.


Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

 The command will raise an error if you omit this option and the configuration is not loaded.


-v <vendor>

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

 It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

 The command will raise an error if you omit this option and the configuration is not loaded.

-y

Skip the confirmation prompt.

evactl create-key

Generates the key pair and the [certificate signing request \(CSR\)](#) of the certificate for signing OCSP responses.

```
evactl create-key -k <key_type> [-s <subject>] [-o <csr>] [-p <pin>] [-t <token>] [-v <vendor>] [-y]
```

For example:

```
$ sudo evactl create-key -k RSA2048 -s "CN=97357462, O=Entrust, C=ES"
Starting PKCS #11 pod... Done
Using token with label mytoken
Created key with id 4a00a4617d1afd5ad626955132dd0d396a69ed24
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIICqDCCAQAQAwwMzExMC8GA1UEAxMoNGEwMGE0NjE3ZDFhZmQ1YWQ2MjY5NTUx
...
etTv+pac+nJKW8fw
-----END CERTIFICATE REQUEST-----
```

See below for a description of each option.

- `-k <key_type>`
- `-s <subject>`

- -o <csr>
- -p <pin>
- -t <token>
- -v <vendor>
- -y

-k <key_type>

Create a key of the <key_type> type, where <key_type> is one of the following.


- RSA2048
- RSA3072
- RSA4096
- ECDSAP256
- ECDSAP384
- ECDSAP521

Mandatory: Yes.

-s <subject>

Use <subject> as the Subject of the certificate request. Where <subject> is either:

- A full Distinguished Name (DN)
- A Relative Distinguished Name (RDN).

 The DN attributes must be in capital letters for the Subject to be recognized.

For example:

```
CN=Example User,O=Example,C=US
```

```
CN=Example User
```

Mandatory: No. When omitting this option, the Subject in the generated certificate request defaults to the following:

```
CN=<key_id>
```

Where <key_id> is the key identifier.

-o <csr>

Save the certificate signing request (CSR) in a file with the <csr> path.

Mandatory: No. When omitting this option, the command prints the CSR to the standard output.

-p <pin>

Authenticate in the HSM with the <pin> PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-t <token>

Select the HSM token with the <token> label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

✗ The command will raise an error if you omit this option and the configuration is not loaded.

-v <vendor>

Use the <vendor> security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

✗ The command will raise an error if you omit this option and the configuration is not loaded.

-y

Skip the confirmation prompt.

evactl delete-key

Deletes a key.

```
evactl delete-key -k <key-id> [-p <pin>] [-t <token>] [-v <vendor>] [-y]
```

For example:


```
$ sudo evactl delete-key -k c403e0abae421c73625666dcff26dacf184eddd4 -y
Starting PKCS #11 Manager... Done
Using token with label pking203
Deleted public key with id c403e0abae421c73625666dcff26dacf184eddd4
Deleted private key with id c403e0abae421c73625666dcff26dacf184eddd4
```

See below for a description of each option.

- `-k <key_id>`
- `-p <pin>`
- `-t <token>`
- `-v <vendor>`
- `-y`

`-k <key_id>`

Select the key with the `<key_id>` identifier.

 Run the `evactl list-keys` command to get the key identifiers.

Mandatory: Yes.

`-p <pin>`


Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

`-t <token>`

Select the HSM token with the `<token>` label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.


 The command will raise an error if you omit this option and the configuration is not loaded.

`-v <vendor>`


Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.

Vendor	Security module
thales	Thales HSM. See HSM requirements for the supported models.

 It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

 The command will raise an error if you omit this option and the configuration is not loaded.

-y

Skip the confirmation prompt.

evactl enroll

```
evactl enroll -a <auth_code> -r <ref_number> -u <url> -l <ca_label> [-c
<tls_ca_path>]
```

For example:

```
$ sudo evactl enroll -r 12473209 -a KNII-F4UH-8VX3 -u https://
mycagateway.example.com:9443 -l my_issuing_ca
```

See below for a description of each option.

-a <auth_code>

Authenticate in the End Entity Enrollment server of CA Gateway with the <auth_code> authorization code.

Mandatory: Yes.

-c <tls_ca_path>

Validate the TLS server certificate of CA Gateway with <tls_ca_path> . Where <tls_ca_path> is the path of a CA file in PEM format.

Mandatory: No. When omitting this option, the command uses the CA configured in [CSP CA Gateway](#).

-l <ca_label>

Use the <ca_label> CA, where <ca_label> is the label of a CA in the End Entity Enrollment server of CA Gateway.

Mandatory: Yes.

-r <ref_number>

Authenticate in the End Entity Enrollment server of CA Gateway with the `<ref_number>` reference_number.

Mandatory: Yes.

-u <url>

Select the End Entity Enrollment server of CA Gateway exposed in the `<url>` URL.

Mandatory: Yes.

evactl export-nshield

Saves a copy of the nShield Security World keys and configuration currently loaded in Validation Authority. You can later import it with [evactl import-nshield](#), even in a different deployment of Validation Authority.

```
evactl export-nshield -f <kmdata_dir> [-t]
```

For example:

```
$ sudo evactl export-nshield -f /opt/nfast/copy-kmdata
```

See below for a description of each option.

- `-f <kmdata_dir>`
- `-t`

-f <kmdata_dir>

Save the configuration in the `<kmdata_dir>` folder.

Mandatory: Yes.

-t

Save the configuration in the following compressed file.

```
<kmdata_dir>/kmdata.tar.gz
```

Mandatory. No. When omitting this option, the command does not compress the configuration in the `<kmdata_dir>` folder.

evactl import-nshield

Imports the nShield Security World configuration so Entrust Validation Authority can use the keys managed by the nShield HSM.


```
evactl import-nshield -f <kmdata> [-y]
```

For example:

```
$ sudo evactl import-nshield -f ./kmdata
```

See below for a description of each option.

- `-f <kmdata>`
- `-y`

 Changes will be effective when deploying (or redeploying) the solution with Management Console or the `clusterctl solution deploy` command.

`-f <kmdata>`

Import the `<kmdata>` configuration, where `<kmdata>` is one of the following.

- The path of the nShield `kmdata` folder.
- The path of a backup folder generated with the `evactl export-nshield` command.
- The path of a `tar.gz` backup file generated with the `evactl export-nshield` command.

 See [Loading the HSM configuration](#) for considerations on this configuration.

Mandatory: Yes.

`-y`

Skip the confirmation prompt.

evactl import-p12

Sets the PKCS #12 described in [CA Gateway for Validation Authority](#).


```
evactl import-p12 -f <p12> [-p <pwd>]
```

For example:

```
$ sudo evactl import-p12 -f eva-cagw.p12 -p password
Starting Configurator...           Done
Importing P12...                   Done
```

See below for a description of each option.

- `-f <p12>`
- `-p <pwd>`

 Changes will be effective when deploying (or redeploying) the solution with Management Console or the `clusterctl solution deploy` command.

-f <p12>

The path of the PKCS #12 file containing the key and the certificate for authenticating in CA Gateway.

Mandatory: Yes.

-p <pwd>

The password of the PKCS #12.

Mandatory: No. When omitting this option, the command prompts for the password.

evactl import-thales

Imports the configuration of a Thales HSM. Use the following syntax to import this configuration from a ZIP file.

```
evactl import-thales -d <package_path> [-y]
```

Use the following syntax to import this configuration from a Chrystoki file.


```
evactl import-thales -c <cert_dir> -k <chrystoki> [-y]
```

For example:

```
$ sudo evactl import-thales -c ./eva-thales-config/cert -k ./eva-thales-config/Chrystoki.conf -y
Saving Thales configuration... Done
Warning: EVA is already deployed! To apply the changes, EVA needs to be redeployed using the evactl deploy command.
```

See below for a description of each option.

- **-c <cert_dir>**
- **-d <package_path>**
- **-k <chrystoki>**
- **-y, --yes**

 Changes will be effective when deploying (or redeploying) the solution with Management Console or the `clusterctl solution deploy` command.

-c <cert_dir>

Import the client and server certificates for the Luna Network or DPoD authentication. Where `<cert_dir>` is the path of a `cert` directory with the following contents.

```

└─cert
  └─client
      <clientKey>.pem
      <clientCert>.pem
  └─server
      <caCert>.pem

```

See below for a description of each field.


Value	Description
<clientKey>	The file name of a PEM file containing the client's private key.
<clientCert>	The file name of a PEM file containing the client's certificate.
<caCert>	The file name of a PEM file containing the CA certificate for validating the server's certificate.

After running the command, verify the `Chrystoki.conf` file includes the following configuration.

```

ClientPrivKeyFile = /usr/safenet/lunaclient/cert/client/<clientKey>.pem;
ClientCertFile = /usr/safenet/lunaclient/cert/client/<clientCert>.pem;
ServerCAFile = /usr/safenet/lunaclient/cert/server/<caCert>.pem;

```

 Do not modify any other path in the `Chrystoki.conf` file.

Mandatory: Yes.

-d <package_path>

Use the `<package_path>` DPoD configuration package, where `<package_path>` is the path of the ZIP package file.

Mandatory: Yes.

-k <chrystoki>

Import the `<chrystoki>` configuration of the Luna Network or DPoD client, where `<chrystoki>` is the path of the `Chrystoky.conf` file.

Mandatory: Yes.

-y, --yes

Skip the confirmation prompt.


```
Vt6tXSZmHkI1rZ1uEJweBWlGp8MHHU6Rot0mZFZ0ourxihmRcD3siDHXu6hADp54wHjGDET7V2WVPMKvcVAW
e+TgzAJcVpYBw07fj4kqER2Uml0T0PfjRtdTC9swxl30aC+UfmleAoBrSjWB+O6lw60bp5oL1gPgIUD9R5fZ
osqPNbVfS5gs6/
Vo5BqfFcGIGMxVTAGMBAAGjggFSMIIBTjAMBGNVHRMBAf8EAjAAMB0GA1UdDgQWBBSk2b3+ZE3ZyIe4bTi3ph
Adv6jB0zAfBgNVHSMEGDAWgBQ4XuxK8LobB2x+dGs0jaqQo0BHWzBLBggrBgEFBQcBAQQ/
MD0wOwYIKwYBBQUHMAAGGL2h0dHA6Ly9vY3NwLmRldi5wa2lodWlUy29tL29jc3AvZW50cnVzdC9pbmRjYWd3M
EYGA1UdHwQ/
MD0wO6A5oDeGNWh0dHA6Ly9jcmwuZGV2LnBraWh1Yi5jb20vY3JsL2VudHJ1c3QvaW50Y2Fndy9jcmwuY3JsM
EQGA1UdEQ9MDuGOWlkcDovL2ludGNhZ3dpZHAVMDc3NjJlYzUzN2NhYmFiZjUwZGI1Mjc4M2E3Y2YzNTQ3YT
NiZjJiMzA0BgNVHQ8BAf8EBAMCB4AwEwYDVR0lBAwwCgYIKwYBBQUHAWIwDQYJKoZIhvcNAQELBQADggEBAFy
o2+QcxN4gN8XxhnErYQ3ET9kk5hrXUa+RGGcTLiegiNKX/
fxlG0V51QglvP4rFd12bnYCMqSQulq0H08m0E3U7wmKZem40Ml0Ifjp94RyDHaMnp0Wv9e4C6I6Q6nv4CX6nr
9TDmpIKG32c0kKu7veSZaLDBVA/Wg+W2ox6yf3W8PbPpUbf6Ld6UC/
gu0hzBMLqw8H+lq4WQs9KWcFFF5+XMm4y1Q38HIL0b0DBVpei0Q0no41mc9+7w/
0W3ix+DDcuLIJEMaKg0ynXujl9Ga0wfm7qZdC+eJ1z0N3m2HBVfZWFEWaKZ8lm2ZqkuZNzCyKJ430qgP2X2WF
axav+c=",
  "SN": "31:5A:FC:C9:6E:FE:18:20:42:6B:79:72:44:14:AD:DE",
  "DN": "subject=O = intcagwidp, OU = CAGW, serialNumber =
07762ec537cababf50db52783a7cf3547a3bf2b3"
}
]
```

evactl list-keys

Lists the keys in the PKCS #11 token.

```
evactl list-keys [-p <pin>] [-t <token>] [-v <vendor>]
```

For example:

```
$ sudo evactl list-keys
Starting PKCS #11 Manager... Done
Using token with label pking203
Public Key Object; RSA 2048 bits
  Label:      305ecd78340acc3d906be370a01e7884
  ID:         03b1dac1e383b8d3adea5a6a2c6200bde58ffb40
  Usage:      verify

Private Key Object; RSA 2048 bits
  Label:      F
  ID:         0f
  Usage:      sign, unwrap

Public Key Object; RSA 2048 bits
  Label:      F
  ID:         0f
  Usage:      verify, wrap

Private Key Object; RSA 2048 bits
  Label:      webserver-root1
```

```
ID:      103d6c94ea10b98ab37186cc1c4977eb
Usage:    sign
```

See below for a description of each option.

- `-p <pin>`
- `-t <token>`
- `-v <vendor>`

`-p <pin>`

Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

`-t <token>`

Select the HSM token with the `<token>` label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

✗ The command will raise an error if you omit this option and the configuration is not loaded.

`-v <vendor>`

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

✗ The command will raise an error if you omit this option and the configuration is not loaded.


evactl load-oracle-wallet

Loads the Oracle wallet for validating the TLS server certificate of an Oracle DBMS. Overwrites the wallet previously loaded.

```
evactl load-oracle-wallet -f <wallet-folder> [-y]
```


For example:

```
sudo evactl load-oracle-wallet -f ./oracle-wallet
Loading Oracle Wallet... Done
```

 If the **Driver** value selected in **Database** is not **oracle**, skip this command and select the certificate with the **SSL validation certificate** parameter instead.

-f <wallet-folder>

Load the the **<wallet-folder>** Oracle Wallet containing the certificate. Where **<wallet-folder>** is the path of the Oracle Wallet folder.

 See the Oracle documentation for how to generate an Oracle Wallet with the **orapki** command-line tool.

Mandatory: Yes.

-y

Skip the confirmation prompt.

evactl reenroll

Issues a new certificate for authenticating in CA Gateway (see [evactl enroll](#) for how to generate the first certificate).

```
evactl reenroll -l <ca_label> -u <url> [-c <tls_ca_path>] [-i <cert-id>]
```

For example:

```
$ sudo evactl reenroll -u https://mycagateway.example.com:9443/.well-known/est/
intcagwidp/simplereenroll -l intcagwidp
```

See below for a description of each option.

- **-c <tls_ca_path>**
- **-i <cert_id>**
- **-l <ca_label>**
- **-u <url>**

✖ Run this command before the current certificate expires.

-c <tls_ca_path>

Validate the TLS server certificate of CA Gateway with <tls_ca_path>. Where <tls_ca_path> is the path of a CA file in PEM format.

Mandatory: No. When omitting this option, the command uses the CA configured in [CSP CA Gateway](#).

-i <cert_id>

Authenticate in CA Gateway with the <cert_id> certificate, where <cert_id> is the identifier of the certificate described in [CA Gateway for Validation Authority](#).

Mandatory: No. This optional parameter defaults to the latest client certificate imported with the [evactl import-p12](#) command.

i Run the [evactl list-certs](#) command to list the available certificates and the latest one imported.

-l <ca_label>

Use the <ca_label> CA, where <ca_label> is the label of a CA in the End Entity Enrollment server of CA Gateway.

Mandatory: Yes.

-u <url>

Select the End Entity Enrollment server of CA Gateway exposed in the <url> URL.

Mandatory: Yes.

evactl stop

Stops a deployed Validation Authority.

```
evactl stop
```

For example:

```
$ sudo evactl stop
Stopping Virtual Services... Done
Stopping Services... Done
Stopping Deployments... Done
Stopping Stateful Sets... Done
Stopping Pods... Done
```

i To restart Validation Authority, use the Management Console, or run the [clusterctl solution deploy](#) command with the `eva` solution identifier.

pki-hub-upgrade prepare

Executed when: [Upgrading from Entrust Deployment Manager 2.0.2](#)

Prepares a node for upgrading and reports any missing requirements.

```
pki-hub-upgrade prepare
```

The command will take around 5 minutes to complete and then prompt the following messages.

- [The node needs to be reinstalled](#)
- [The node total disk size needs to be increased](#)
- [A new additional disk is required](#)
- [The node is ready to be upgraded](#)

The node needs to be reinstalled

the command will prompt the following message when [Reinstalling Entrust Deployment Manager 2.0.2](#) is needed.

```
$ sudo pki-hub-upgrade prepare
Checking node status done |||||||||||||||||||||||||||||||||||||||| 100 %
The following tasks have to be performed to complete the preparation of the node:
- The node needs to be reinstalled.
  - Follow the Entrust PKI Hub documentation on how to reinstall an EDM 2.0.0-based
    node for upgrading to Entrust PKI Hub.
  - WARNING: this task may imply service outage in the node, depending on your
    platform.
Once all the manual preparation tasks have been completed, re-execute the 'pki-hub-
upgrade prepare' command.
```

The node total disk size needs to be increased

The command will prompt the following when the size of the primary disk does not meet one described in [Machine requirements](#).

```
$ sudo pki-hub-upgrade prepare
Checking node status done |||||||||||||||||||||||||||||||||||||||| 100 %
The following tasks have to be performed to complete the preparation of the node:
  - The node total disk size needs to be increased at least to 1 TiB.
    - Follow the Entrust PKI Hub documentation on how to increase the disk size for
      your platform.
    - WARNING: this task may imply service outage in the node, depending on your
      platform.
Once all the manual preparation tasks have been completed, re-execute the 'pki-hub-
upgrade prepare' command.
```

See [Applying missing machine requirements](#) for how to fix this issue.

A new additional disk is required

The command will prompt the following when the secondary disk is missing or does not meet the one described in [Machine requirements](#).

```
$ sudo pki-hub-upgrade prepare
Checking node status done |||||||||||||||||||||||||||||||||||||||| 100 %
The following tasks have to be performed to complete the preparation of the node:
  - A new additional disk of at least 15 Gb is required" .
  - Follow the Entrust PKI Hub documentation on how to add an additional disk for
your platform.
  - WARNING: this task may imply service outage in the node, depending on your
platform.
Once all the manual preparation tasks have been completed, re-execute the 'pki-hub-
upgrade prepare' command.
```

See [Applying missing machine requirements](#) for how to fix this issue.

The node is ready to be upgraded

The command will prompt the following when all the upgrade requirements are met. You can then continue the process described in [Upgrading from Entrust Deployment Manager 2.0.2](#).

```
$ sudo pki-hub-upgrade prepare
Checking node status  done |||||||||||||||||||||||||||||||||||||||| 100 %
The node is ready to be upgraded to PKI Hub 1.1.0
```

pki-hub-upgrade remove-node


Executed when: Upgrading from Entrust Deployment Manager 2.0.2

Removes a node from the cluster.

```
pki-hub-upgrade remove-node --node <node> [-y]
```


See below for a description of each parameter.

- `<node>`
- `-y, --yes`

 The command will take around 20 minutes to complete.

`<node>`

The IP address or identifier of a node in the Cryptographic Security Platform cluster. Run the [clusterctl node info](#) to list all the cluster nodes.

 The `<node>` value cannot correspond to the node where the command is executed.

Mandatory: Yes.

`-y, --yes`

Skip the confirmation prompt.

pki-hub-upgrade upgrade

Executed when: [Upgrading from Entrust Deployment Manager 2.0.2](#)

Removes a node from the cluster.

```
pki-hub-upgrade upgrade --iso-path <iso-path> --license-path <license-path>
```

See below for a description of each parameter.

- `<iso-path>`
- `<license-path>`

`<iso-path>`

The path of the image file for CSP 1.0.0. See [Downloading the installation files](#) for how to download this file.

Mandatory: Yes.

`<license-path>`

The path of the license file for CSP 1.0.0.

Mandatory: Yes.

tsactl check clock

Checks the host connection with the time source.

```
tsactl check clock
```

For example:

```
$ sudo tsactl check clock
Starting Pod... Done
Checking clock status... Done
```

tsactl check hsm

Checks the HSM connectivity.

```
tsactl check hsm [-l <level>] [-p <pin>] [-t <token>] [-v <vendor>]
```

For example:

```
$ sudo tsactl check hsm
Obtaining loaded secrets and configuration... Done
Starting PKCS #11 Manager... Done

Slot Id -> 0
Label -> pking203
Serial Number -> 1433959427612
Model -> LunaSA 7.2.1
Firmware Version -> 7.0.3
Configuration -> Luna User Partition With S0 (PED) Signing With
Cloning Mode
Slot Description -> Net Token Slot
FM HW Status -> FM Ready

Slot Id -> 1
Label -> pking202
Serial Number -> 1433964084224
Model -> LunaSA 7.2.1
Firmware Version -> 7.0.3
Configuration -> Luna User Partition With S0 (PED) Signing With
Cloning Mode
Slot Description -> Net Token Slot
FM HW Status -> FM Ready

Current Slot Id: 0

Passing HSM checks... Done
```

See below for a description of each option.

- [-l <level>](#)
- [-p <pin>](#)

- -t <token>
- -v <vendor>

-l <level>

Debug the nShield HSM with the <level> level, where <level> is a `CKNFAST_DEBUG` variable level. When not using an nShield HSM, the command ignores this option.



See the nShield documentation for details on the `CKNFAST_DEBUG` configuration parameter.

Mandatory: No. This optional parameter defaults to 0.

-p <pin>

Authenticate in the HSM with the <pin> PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-t <token>

Select the HSM token with the <token> label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.



The command will raise an error if you omit this option and the configuration is not loaded.

-v <vendor>

Check an HSM of the <vendor> vendor, where <vendor> is either:

- nshield
- thales

Mandatory : When omitting this option, the command assumes the value of the **Vendor** configuration parameter and throws an error if not set.

tsactl create-csr

Generates a new certificate signing request (CSR) for a key pair previously generated with the `tsactl create-key` command.

```
tsactl create-csr -k <key_id> [-s <subject>] [-o <csr>] [-p <pin>] [-t <token>] [-v <vendor>] [-y]
```

For example:


```
$ sudo tsactl create-csr -k 7ce798c13a411bc1da4a9f983ed6d44fb4d7ed1a -s "CN=97357462,  
O=Entrust, C=ES"  
Obtaining loaded secrets and configuration... Done  
Starting PKCS #11 Manager... Done  
Using token with label mytoken  
CSR:  
-----BEGIN CERTIFICATE REQUEST-----  
MIIBIDCBxQIBADAzMTEwLWYDVQQDEyg3Y2U30ThjMTNhNDExYmMxZGE0YTlmOTgz  
...  
9xMajw==  
-----END CERTIFICATE REQUEST-----
```

See below for a description of each option.

- `-k <key_id>`
- `-s <subject>`
- `-o <csr>`
- `-p <pin>`
- `-t <token>`
- `-v <vendor>`
- `-y`

`-k <key_id>`


Select the key with the `<key_id>` identifier.

 Run the `tsactl list-keys` command to get the key identifiers.

Mandatory: Yes.

`-s <subject>`

Use `<subject>` as the Subject of the certificate request. Where `<subject>` is a full Distinguished Name (DN) or Relative Distinguished Name (RDN).

 The DN attributes must be in capital letters for the Timestamping Authority solution to recognize the Subject.

For example:

```
CN=Example User,O=Example,C=US
```

```
CN=Example User
```

Mandatory: No. When omitting this option, the Subject in the generated certificate request defaults to the following:


```
CN=<key_id>
```

Where `<key_id>` is the key identifier.

-o <csr>

Save the certificate signing request (CSR) in a file with the `<csr>` path.

Mandatory: No. When omitting this option, the command prints the CSR to the standard output.

-p <pin>

Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-t <token>

Select the HSM token with the `<token>` label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

✗ The command will raise an error if you omit this option and the configuration is not loaded.

-v <vendor>

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

✗ The command will raise an error if you omit this option and the configuration is not loaded.

-y

Skip the confirmation prompt.

tsactl create-key

Generates the key pair and the certificate signing request (CSR) of the certificate for signing TST responses.

```
tsactl create-key -k <key_type> [-s <subject>] [-o <csr>] [-p <pin>] [-t <token>] [-v  
<vendor>] [-y]
```

For example:

```
$ sudo tsactl create-key -k RSA2048 -s "CN=97357462, O=Entrust, C=ES"  
Obtaining loaded secrets and configuration... Done  
Starting PKCS #11 Manager... Done  
Using token with label mytoken  
Created key with id 4a00a4617d1afd5ad626955132dd0d396a69ed24  
CSR:  
-----BEGIN CERTIFICATE REQUEST-----  
MIICqDCCAQAQAwMzExMC8GA1UEAxMoNGEwMGE0NjE3ZDFhZmQ1YWQ2MjY5NTUx  
...  
etTv+pac+nJKW8fw  
-----END CERTIFICATE REQUEST-----
```

See below for a description of each option.

- -k <key_type>
- -s <subject>
- -o <csr>
- -p <pin>
- -t <token>
- -v <vendor>
- -y

-k <key_type>

Create a key of the <key_type> type, where <key_type> is one of the following.


- RSA2048
- RSA3072
- RSA4096
- ECDSAP256
- ECDSAP384
- ECDSAP521

Mandatory: Yes.

-s <subject>

Use <subject> as the Subject of the certificate request. Where <subject> is either:

- A full Distinguished Name (DN)
- A Relative Distinguished Name (RDN).

 The DN attributes must be in capital letters for the Subject to be recognized.

For example:

```
CN=Example User,O=Example,C=US
```

```
CN=Example User
```

Mandatory: No. When omitting this option, the Subject in the generated certificate request defaults to the following:

```
CN=<key_id>
```

Where `<key_id>` is the key identifier.

-o <csr>

Save the certificate signing request (CSR) in a file with the `<csr>` path.

Mandatory: No. When omitting this option, the command prints the CSR to the standard output.

-p <pin>


Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-t <token>

Select the HSM token with the `<token>` label.


Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

 The command will raise an error if you omit this option and the configuration is not loaded.


-v <vendor>

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

 It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

 The command will raise an error if you omit this option and the configuration is not loaded.

-y

Skip the confirmation prompt.

tsactl delete-key

Deletes a key.

```
tsactl delete-key -k <key-id> [-p <pin>] [-t <token>] [-v <vendor>] [-y]
```

For example:


```
$ sudo tsactl delete-key -k c403e0abae421c73625666dcff26dacf184eddd4 -y
Obtaining loaded secrets and configuration... Done
Starting PKCS #11 Manager... Done
Using token with label pking203
Deleted public key with id c403e0abae421c73625666dcff26dacf184eddd4
Deleted private key with id c403e0abae421c73625666dcff26dacf184eddd4
```

See below for a description of each option.

- -k <key_id>
- -p <pin>
- -t <token>
- -v <vendor>
- -y

-k <key_id>

Select the key with the <key_id> identifier.

 Run the `tsactl list-keys` command to get the key identifiers.

Mandatory: Yes.

-p <pin>


Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-t <token>

Select the HSM token with the `<token>` label.


Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

 The command will raise an error if you omit this option and the configuration is not loaded.


-v <vendor>

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

 It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

 The command will raise an error if you omit this option and the configuration is not loaded.

-y

Skip the confirmation prompt.

tsactl export-nshield

Saves a copy of the nShield Security World keys and configuration currently loaded in TSA. You can later import it with [tsactl import-nshield](#), even in a different deployment of TSA.

```
tsactl export-nshield -o <output-directory> [-t]
```

For example:

```
$ sudo tsactl export-nshield -o /opt/nfast/copy-kmdata
```

See below for a description of each option.

- [-o <output-directory>](#)
- [-t](#)

-o <output-directory>

Save the configuration in the [<output-directory>](#) folder.

Mandatory: Yes.

-t

Save the configuration in the following compressed file.

```
<output-directory>/kmdata.tar.gz
```

Mandatory. No. When omitting this option, the command does not compress the configuration in the [<output-directory>](#) folder.

tsactl import-nshield

Imports the nShield Security World configuration so the Timestamping Authority solution can use the keys managed by the nShield HSM.


```
tsactl import-nshield -f <kmdata> [-y]
```

For example:

```
$ sudo tsactl import-nshield -f ./kmdata
```

See below for a description of each option.


- [-f <kmdata>](#)
- [-y, --yes](#)

 Changes will be effective when deploying (or redeploying) the solution with Management Console or the `clusterctl solution deploy` command.

`-f <kmdata>`

Import the `<kmdata>` configuration, where `<kmdata>` is one of the following.

- The path of the nShield `kmdata` folder.
- The path of a backup folder generated with the `tsactl export-nshield` command.
- The path of a `tar.gz` backup file generated with the `tsactl export-nshield` command.

 See [Loading the HSM configuration](#) for considerations on this configuration.

Mandatory: Yes.

`-y, --yes`

Skip the confirmation prompt.

`tsactl import-thales`

Imports the configuration of a Thales HSM. Use the following syntax to import this configuration from a ZIP file.

```
tsactl import-thales -d <package_path> [-y]
```

Use the following syntax to import this configuration from a Chrystoki file.


```
tsactl import-thales -c <cert_dir> -k <chrystoki> [-y]
```

For example:

```
$ sudo tsactl import-thales -c ./tsa-thales-config/cert -k ./tsa-thales-config/Chrystoki.conf -y
Saving Thales configuration... Done
Warning: tsa is already deployed! To apply the changes, tsa needs to be redeployed using the tsactl deploy command.
```

See below for a description of each option.

- `-c <cert_dir>`
- `-d <package_path>`
- `-k <chrystoki>`
- `-y, --yes`

 Changes will be effective when deploying (or redeploying) the solution with Management Console or the `clusterctl solution deploy` command.

-c <cert_dir>

Import the client and server certificates for the Luna Network or DPoD authentication. Where `<cert_dir>` is the path of a `cert` directory with the following contents.

```

└─cert
   └─client
      <clientKey>.pem
      <clientCert>.pem
   └─server
      <caCert>.pem

```

See below for a description of each field.


Value	Description
<clientKey>	The file name of a PEM file containing the client's private key.
<clientCert>	The file name of a PEM file containing the client's certificate.
<caCert>	The file name of a PEM file containing the CA certificate for validating the server's certificate.

After running the command, verify the `Chrystoki.conf` file includes the following configuration.

```

ClientPrivKeyFile = /usr/safenet/lunaclient/cert/client/<clientKey>.pem;
ClientCertFile = /usr/safenet/lunaclient/cert/client/<clientCert>.pem;
ServerCAFile = /usr/safenet/lunaclient/cert/server/<caCert>.pem;

```

 Do not modify any other path in the `Chrystoki.conf` file.

Mandatory: Yes.

-d <package_path>

Use the `<package_path>` DPoD configuration package, where `<package_path>` is the path of the ZIP package file.

Mandatory: Yes.

-k <chrystoki>

Import the `<chrystoki>` configuration of the Luna Network or DPoD client, where `<chrystoki>` is the path of the `Chrystoky.conf` file.

Mandatory: Yes.

-y, --yes

Skip the confirmation prompt.

tsactl list-keys

Lists the keys in the PKCS #11 token.

```
tsactl list-keys [-p <pin>] [-t <token>] [-v <vendor>]
```

For example:

```
$ sudo tsactl list-keys
Obtaining loaded secrets and configuration... Done
Starting PKCS #11 Manager... Done
Using token with label pking203
Public Key Object; RSA 2048 bits
  Label:      305ecd78340acc3d906be370a01e7884
  ID:         03b1dac1e383b8d3adea5a6a2c6200bde58ffb40
  Usage:      verify

Private Key Object; RSA 2048 bits
  Label:      F
  ID:         0f
  Usage:      sign, unwrap

Public Key Object; RSA 2048 bits
  Label:      F
  ID:         0f
  Usage:      verify, wrap

Private Key Object; RSA 2048 bits
  Label:      webserver-root1
  ID:         103d6c94ea10b98ab37186cc1c4977eb
  Usage:      sign
```

See below for a description of each option.

- -p <pin>
- -t <token>
- -v <vendor>

-p <pin>

Authenticate in the HSM with the <pin> PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-t <token>

Select the HSM token with the `<token>` label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

✗ The command will raise an error if you omit this option and the configuration is not loaded.

-v <vendor>

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

✗ The command will raise an error if you omit this option and the configuration is not loaded.


tsactl stop

Stops a deployed Timestamping Authority solution.

```
tsactl stop
```

For example:

```
$ sudo tsactl stop
Stopping Virtual Services...      Done
Stopping Services...             Done
Stopping Deployments...          Done
Stopping Stateful Sets...        Done
Stopping Pods...                 Done
```


 To restart Timestamping Authority, redeploy the solution as explained in [Configuring and deploying Timestamping Authority](#).


20 CIS benchmarks




























The Cryptographic Security Platform third-party software is hardened to meet the following recommendations.

- [Linux CIS benchmarks](#)
- [Password policy CIS benchmarks](#)
- [Kubernetes CIS benchmarks](#)

Linux CIS benchmarks

The Cryptographic Security Platform operating system is hardened to meet most of the "CIS Red Hat Enterprise Linux 8 Benchmark v1.0.0" recommendations for the "Level 1—Server" profile. Specifically, this operating system meets all recommendations except those marked  in the following table.

 The **ISO**, **Raw**, and **VHD** columns refer to the available file formats for [Installing the image](#).

CIS recommendation	Description	ISO	Raw	VHD
1.1.2.1	Ensure <code>/tmp</code> is a separate partition			
1.1.2.2	Ensure <code>nodev</code> option set on <code>/tmp</code> partition			
1.1.2.3	Ensure <code>noexec</code> option set on <code>/tmp</code> partition			
1.1.2.4	Ensure <code>nosuid</code> option set on <code>/tmp</code> partition			
1.1.3.2	Ensure <code>nodev</code> option set on <code>/var</code> partition			
1.1.3.3	Ensure <code>noexec</code> option set on <code>/var</code> partition			
1.1.3.4	Ensure <code>nosuid</code> option set on <code>/var</code> partition			
1.1.4.2	Ensure <code>nodev</code> option set on <code>/var/tmp</code> partition			
1.1.4.3	Ensure <code>noexec</code> option set on <code>/var/tmp</code> partition			

CIS recommendation	Description	ISO	Raw	VHD
1.1.4.4	Ensure <code>nosuid</code> option set on <code>/var/tmp</code> partition	✓	✗	✗
1.1.5.2	Ensure <code>nodev</code> option set on <code>/var/log</code> partition	✓	✗	✗
1.1.5.3	Ensure <code>noexec</code> option set on <code>/var/log</code> partition	✓	✗	✗
1.1.5.4	Ensure <code>nosuid</code> option set on <code>/var/log</code> partition	✓	✗	✗
1.1.6.2	Ensure <code>nodev</code> option set on <code>/var/log/audit</code> partition	✓	✗	✗
1.1.6.3	Ensure <code>noexec</code> option set on <code>/var/log/audit</code> partition	✓	✗	✗
1.1.6.4	Ensure <code>nosuid</code> option set on <code>/var/log/audit</code> partition	✓	✗	✗
1.1.7.2	Ensure <code>nodev</code> option set on <code>/home</code> partition	✓	✗	✗
1.1.7.3	Ensure <code>nosuid</code> option set on <code>/home</code> partition	✓	✗	✗
1.3.1	Ensure AIDE is installed	✗	✗	✗
1.3.2	Ensure filesystem integrity is regularly checked	✗	✗	✗
1.4.1	Ensure bootloader password is set	✓	✗	✗
1.6.1.6	Ensure no unconfined services exist	✗	✗	✗
3.2.1	Ensure IP forwarding is disabled	✗	✗	✗

CIS recommendation	Description	ISO	Raw	VHD
3.3.1	Ensure source routed packets are not accepted	✗	✗	✗
3.3.2	Ensure ICMP redirects are not accepted	✗	✗	✗
3.3.9	Ensure IPv6 router advertisements are not accepted	✗	✗	✗
3.4.1.5	Ensure <code>firewalld</code> default zone is set	✓	✗	✗
3.4.3.3.3	Ensure ip6tables firewall rules exist for all open ports	✗	✗	✗
5.5.1	Ensure password creation requirements are configured - minlen	✗	✗	✗
6.1.2	Ensure sticky bit is set on all world-writable directories	✗	✗	✗
6.1.11	Ensure no world writable files exist	✗	✗	✗
6.1.12	Ensure no unowned files or directories exist	✗	✗	✗
6.1.13	Ensure no ungrouped files or directories exist	✗	✗	✗

Password policy CIS benchmarks

On the first login, you will be asked to replace the initial password of the Cryptographic Security Platform administrator.

Name	Initial password
sysadmin	changeme

As per the 5.5.1 benchmark of the "CIS Red Hat Enterprise Linux 8 Benchmark v1.0.0" recommendations for the "Level 1 - Server" profile, the new password:


- Must consist of at least 16 characters.
- Cannot be based on a dictionary word.
- Must contain at least one uppercase character.







- Must contain at least one lowercase character.
- Must contain at least one digit.
- Must contain at least one special character (for example, punctuation).

Once set, Cryptographic Security Platform user passwords have the following settings.

Setting	Value
Password validity	365 days
Grace period before disabling the user account after password expiry	30 days
Minimum time between password changes	7 days
Shell session inactivity timeout	900 seconds

Kubernetes CIS benchmarks

The Cryptographic Security Platform K3s (Lightweight Kubernetes) meets most of the "CIS Kubernetes Benchmark v1.6.0" recommendations for the "Level 2—Master Node and Level 2—Worker Node" profile. Specifically, it meets all the recommendations marked  in the following table.

CIS recommendation	Description	Compliance
1.1.1	Ensure that the API server pod specification file permissions are set to 644 or more restrictive	
1.1.2	Ensure that the API server pod specification file ownership is set to root:root	
1.1.3	Ensure that the controller manager pod specification file permissions are set to 644 or more restrictive	
1.1.4	Ensure that the controller manager pod specification file ownership is set to root:root	
1.1.5	Ensure that the scheduler pod specification file permissions are set to 644 or more restrictive	
1.1.6	Ensure that the scheduler pod specification file ownership is set to root:root	

CIS recommendation	Description	Compliance
1.1.7	Ensure that the etcd pod specification file permissions are set to 644 or more restrictive	✓
1.1.8	Ensure that the etcd pod specification file ownership is set to root:root	✓
1.1.9	Ensure that the Container Network Interface file permissions are set to 644 or more restrictive	✓
1.1.10	Ensure that the Container Network Interface file ownership is set to root:root	✓
1.1.11	Ensure that the etcd data directory permissions are set to 700 or more restrictive if etcd is used	✓
1.1.12	Ensure that the etcd data directory ownership is set to etcd:etcd if etcd is used	✓
1.1.13	Ensure that the admin.kubeconfig file permissions are set to 644 or more restrictive	✓
1.1.14	Ensure that the admin.kubeconfig file ownership is set to root:root	✓
1.1.15	Ensure that the scheduler.kubeconfig file permissions are set to 644 or more restrictive	✓
1.1.16	Ensure that the scheduler.kubeconfig file ownership is set to root:root	✓
1.1.17	Ensure that the cloud-controller.kubeconfig file permissions are set to 644 or more restrictive	✓
1.1.18	Ensure that the /var/lib/rancher/k3s/server/cred/cloud-controller.kubeconfig file ownership is set to root:root	✓
1.1.19	Ensure that the Kubernetes PKI directory and file ownership is set to root:root	✓

CIS recommendation	Description	Compliance
1.1.20	Ensure that the Kubernetes PKI certificate file permissions are set to 644 or more restrictive	✓
1.1.21	Ensure that the Kubernetes PKI key file permissions are set to 600	✓
1.2.1	Ensure that the --anonymous-auth argument is set to false	✓
1.2.2	Ensure that the --basic-auth-file argument is not set	✓
1.2.3	Ensure that the --token-auth-file parameter is not set	✓
1.2.4	Ensure that the --kubelet-https argument is set to true	✓
1.2.5	Ensure that the --kubelet-client-certificate and --kubelet-client-key arguments are set as appropriate	✓
1.2.6	Ensure that the --kubelet-certificate-authority argument is set as appropriate	✓
1.2.7	Ensure that the --authorization-mode argument is not set to AlwaysAllow	✓
1.2.8	Ensure that the --authorization-mode argument includes Node	✓
1.2.9	Ensure that the --authorization-mode argument includes RBAC	✓
1.2.10	Ensure that the admission control plugin EventRateLimit is set	✗
1.2.11	Ensure that the admission control plugin AlwaysAdmit is not set	✓
1.2.12	Ensure that the admission control plugin AlwaysPullImages is set	✗

CIS recommendation	Description	Compliance
1.2.13	Ensure that the admission control plugin SecurityContextDeny is set if PodSecurityPolicy is not used	✓
1.2.14	Ensure that the admission control plugin ServiceAccount is set	✗
1.2.15	Ensure that the admission control plugin NamespaceLifecycle is set	✓
1.2.16	Ensure that the admission control plugin PodSecurityPolicy is set	✓
1.2.17	Ensure that the admission control plugin NodeRestriction is set	✓
1.2.18	Ensure that the --insecure-bind-address argument is not set	✓
1.2.19	Ensure that the --insecure-port argument is set to 0	✗
1.2.20	Ensure that the --secure-port argument is not set to 0	✓
1.2.21	Ensure that the --profiling argument is set to false	✓
1.2.22	Ensure that the --audit-log-path argument is set	✓
1.2.23	Ensure that the --audit-log-maxage argument is set to 30 or as appropriate	✓
1.2.24	Ensure that the --audit-log-maxbackup argument is set to 10 or as appropriate	✓
1.2.25	Ensure that the --audit-log-maxsize argument is set to 100 or as appropriate	✓
1.2.26	Ensure that the --request-timeout argument is set as appropriate	✓






CIS recommendation	Description	Compliance
1.2.27	Ensure that the --service-account-lookup argument is set to true	✗
1.2.28	Ensure that the --service-account-key-file argument is set as appropriate	✓
1.2.29	Ensure that the --etcd-certfile and --etcd-keyfile arguments are set as appropriate	✓
1.2.30	Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate	✓
1.2.31	Ensure that the --client-ca-file argument is set as appropriate	✓
1.2.32	Ensure that the --etcd-cafile argument is set as appropriate	✓
1.2.33	Ensure that the --encryption-provider-config argument is set as appropriate	✓
1.2.34	Ensure that encryption providers are appropriately configured	✗
1.2.35	Ensure that the API Server only makes use of Strong Cryptographic Ciphers	✓
1.3.1	Ensure that the --terminated-pod-gc-threshold argument is set as appropriate	✗
1.3.2	Ensure that the --profiling argument is set to false	✓
1.3.3	Ensure that the --use-service-account-credentials argument is set to true	✓
1.3.4	Ensure that the --service-account-private-key-file argument is set as appropriate	✓
1.3.5	Ensure that the --root-ca-file argument is set as appropriate	✓

CIS recommendation	Description	Compliance
1.3.6	Ensure that the RotateKubeletServerCertificate argument is set to true	✓
1.3.7	Ensure that the --bind-address argument is set to 127.0.0.1	✓
1.4.1	Ensure that the --profiling argument is set to false	✓
1.4.2	Ensure that the --bind-address argument is set to 127.0.0.1	✓
2.1	Ensure that the --cert-file and --key-file arguments are set as appropriate if use etcd as database	✓
2.2	Ensure that the --client-cert-auth argument is set to true	✓
2.3	Ensure that the --auto-tls argument is not set to true	✓
2.4	Ensure that the --peer-cert-file and --peer-key-file arguments are set as appropriate	✓
2.5	Ensure that the --peer-client-cert-auth argument is set to true	✓
2.6	Ensure that the --peer-auto-tls argument is not set to true	✓
2.7	Ensure that a unique Certificate Authority is used for etcd	✓
3.1.1	Client certificate authentication should not be used for users	✗
3.2.1	Ensure that a minimal audit policy is created	✗
3.2.2	Ensure that the audit policy covers key security concerns	✗

CIS recommendation	Description	Compliance
4.1.1	Ensure that the kubelet service file permissions are set to 644 or more restrictive	✓
4.1.2	Ensure that the kubelet service file ownership is set to root:root	✓
4.1.3	If proxy kubeproxy.kubeconfig file exists ensure permissions are set to 644 or more restrictive	✓
4.1.4	Ensure that the proxy kubeconfig file ownership is set to root:root	✓
4.1.5	Ensure that the --kubeconfig kubelet.conf file permissions are set to 644 or more restrictive	✓
4.1.6	Ensure that the --kubeconfig kubelet.conf file ownership is set to root:root	✓
4.1.7	Ensure that the certificate authorities file permissions are set to 644 or more restrictive	✓
4.1.8	Ensure that the client certificate authorities file ownership is set to root:root	✓
4.1.9	Ensure that the kubelet --config configuration file has permissions set to 644 or more restrictive	✓
4.1.10	Ensure that the kubelet --config configuration file ownership is set to root:root	✓
4.2.1	Ensure that the anonymous-auth argument is set to false	✓
4.2.2	Ensure that the --authorization-mode argument is not set to AlwaysAllow	✓
4.2.3	Ensure that the --client-ca-file argument is set as appropriate	✓
4.2.4	Ensure that the --read-only-port argument is set to 0	✓

CIS recommendation	Description	Compliance
4.2.5	Ensure that the --streaming-connection-idle-timeout argument is not set to 0	✗
4.2.6	Ensure that the --protect-kernel-defaults argument is set to true	✓
4.2.7	Ensure that the --make-iptables-util-chains argument is set to true	✗
4.2.8	Ensure that the --hostname-override argument is not set	✓
4.2.9	Ensure that the --event-qps argument is set to 0 or a level which ensures appropriate event capture	✗
4.2.10	Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate	✓
4.2.11	Ensure that the --rotate-certificates argument is not set to false	✓
4.2.12	Verify that the RotateKubeletServerCertificate argument is set to true	✓
4.2.13	Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers	✗
5.1.1	Ensure that the cluster-admin role is only used where required	✓
5.1.2	Minimize access to secrets	✓
5.1.3	Minimize wildcard use in Roles and ClusterRoles	✓
5.1.4	Minimize access to create pods	✓
5.1.5	Ensure that default service accounts are not actively used.	✗

CIS recommendation	Description	Compliance
5.1.6	Ensure that Service Account Tokens are only mounted where necessary	✗
5.2.1	Minimize the admission of privileged containers	✓
5.2.2	Minimize the admission of containers wishing to share the host process ID namespace	✓
5.2.3	Minimize the admission of containers wishing to share the host IPC namespace	✓
5.2.4	Minimize the admission of containers wishing to share the host network namespace	✓
5.2.5	Minimize the admission of containers with allowPrivilegeEscalation	✓
5.2.6	Minimize the admission of root containers	✓
5.2.7	Minimize the admission of containers with the NET_RAW capability	✓
5.2.8	Minimize the admission of containers with added capabilities	✓
5.2.9	Minimize the admission of containers with capabilities assigned	✓
5.3.1	Ensure that the CNI in use supports Network Policies	✓
5.3.2	Ensure that all Namespaces have Network Policies defined	✗
5.4.1	Prefer using secrets as files over secrets as environment variables	✓
5.4.2	Consider external secret storage	✗

CIS recommendation	Description	Compliance
5.5.1	Configure Image Provenance using ImagePolicyWebhook admission controller	
5.7.1	Create administrative boundaries between resources using namespaces	
5.7.2	Ensure that the seccomp profile is set to docker/default in your pod definitions	
5.7.3	Apply Security Context to Your Pods and Containers	
5.7.4	The default namespace should not be used	

21 Troubleshooting and technical assistance

See below for how to troubleshoot issues, generate reports and obtain technical assistance.

- [Troubleshooting Certificate Enrollment Gateway](#)
- [Troubleshooting Validation Authority](#)
- [Troubleshooting Timestamping Authority](#)
- [Generating technical assistance reports](#)

Troubleshooting Certificate Enrollment Gateway

See below for how to troubleshoot the main Certificate Enrollment Gateway issues.

Google ChromeOS integration errors

If errors occur during the [Google ChromeOS integration use case](#), check the Certificate Enrollment Gateway logs (as explained in [Browsing logs with Grafana](#)) and the Google Cloud Certificate Connector logs.

To browse Google Cloud Certificate Connector logs

1. Log into the Domain-joined Windows server hosting the Google Cloud Certificate Connector.
2. Select **Start > Windows Administrative Tools > Event Viewer** to open the Event Viewer.
3. Analyze events from **GoogleCloudCertificateConnector**.

Troubleshooting Validation Authority

See below for how to troubleshoot the main Validation Authority issues.

- [Connectivity issues](#)
- [Error: Another instance of evactl is running](#)

Connectivity issues

As explained in [CSP Validation Authority overview](#), Validation Authority connects to:

- A database.
- An HSM.
- A certificate status source (CA Gateway instance or CRL server).

To check the connection with these components, run the [evactl check all](#) command.

Error: Another instance of evactl is running

When trying to create or delete a key, you can encounter the following error.

```
Error: Another instance of evactl is running create-key or delete-key
```

When trying to enroll, reenroll or import a PKCS #12, you can encounter the following error.

```
Error: Another instance of evactl is running enroll, reenroll or import-p12
```

In both cases:

1. Make sure that there is no other instance of the `evactl` command line tool performing any of those operations.
2. Re-run the command with the `FORCE_MUTEX_OPERATION` environment variable set to 1. For example:

```
sudo FORCE_MUTEX_OPERATION=1 evactl create-key RSA2048
```

✗ Running a command with `FORCE_MUTEX_OPERATION` set to 1 can override the changes made by another `evactl` running instance.

Troubleshooting Timestamping Authority

See below for how to troubleshoot the main Timestamping Authority issues.

- [Connectivity issues](#)
- [Error: Another instance of tsactl is running](#)

Connectivity issues

As explained in [Timestamping Authority overview](#), the Timestamping Authority connects with:

- The system clock service (which is provided by the `chrony` connection to an NTP server).
- An HSM

To check the connection with these components, run the `tsactl check clock` and `tsactl check hsm` commands.

Error: Another instance of tsactl is running

You can encounter the following error when creating or deleting a key.

```
Error: Another instance of tsactl is running create-key or delete-key
```

In that case:

1. Ensure there is no other instance of `tsactl` performing any of those operations.
2. Re-run the command with the `FORCE_MUTEX_OPERATION` environment variable set to 1. For example:

```
sudo FORCE_MUTEX_OPERATION=1 ./tsactl create-key -k RSA2048
```

✗ Running a command with `FORCE_MUTEX_OPERATION` set to 1 can override the changes made by another `tsactl` running instance.

Generating technical assistance reports

To contact customer support, email the following information to support@entrust.com.

- Your contact information
- A description of the problem
- The conditions under which the error occurred
- The troubleshooting activities already performed

Attach to this email a diagnostic report file for each installation node.

- [Report file generation](#)
- [Report file path](#)

Report file generation

On each installation node, run the following command to generate a diagnostic report.

```
sudo diagnostic-report.sh [--password <pwd>] [--logs-since <hours>]
```

For example:

```
$ sudo diagnostic-report.sh
Gathering system information. This process could take a few minutes...
Packaging the report...

Randomly generated password:
^zuD,h|o`3!>q

Success. This file is meant for incidence analysis at the Support department's
request.
The file resulting from this execution must be sent to the aforementioned department.
```

See below for the supported options.

Option	Description	Mandatory
-p, --password <pwd>	Encrypt the generated diagnostics file with the <code><pwd></code> password.	No, When omitting this option, the script ciphers the file with a random password containing 13 OWAS special characters and prints the password in the execution console.
-s, --logs-since <hours>	Collect the logs generated in the last <code><hour></code> hours, where <code><hour></code> is an integer greater than 0.	No. When omitted, this value defaults to 48 hours.
--fast	Perform a fast diagnostic report.	No. Do not use this option unless customer support indicates it.

Option	Description	Mandatory
--disk-perf	Generate a disk performance report.	No. Do not use this option unless customer support indicates it.
--no-host	Skip host reports.	No. Do not use this option unless customer support indicates it.
-v, --version	Show the version of the report generation tool.	No.
-h, --help	Show help information on the report generation tool.	No.

Report file path

The report generation tool generates a file with the following path.

```
<dir>/diagnostic-report-<YYYY-MM-MM>T<hh-mm-ss>Z-<hostname>.edg
```

See the table below for each field.

Field	Value
<dir>	The directory on which the tool is executed.
<YYYY-MM-MM>	The file generation date.
<hh-mm-ss>	The file generation time.
<hostname>	The hostname of the node on which the tool is executed.

22 Licensing

See below for the Cryptographic Security Platform licenses.

- [Customer license](#)
- [Third-party license acknowledgments](#)

Customer license

This section defines the licensing terms and permitted uses of the Entrust Cryptographic Security Platform (CSP).

- [Authorized Use](#)
- [License Packages](#)
- [Deployment](#)
- [Plugins](#)
- [External Dependencies](#)
- [Trade Compliance](#)
- [Standard Compliance Packs Limitations](#)
- [Support and Record-Keeping](#)

Authorized Use

In this Licensing section, the term “Customer” means an Entrust customer who has purchased one or more CSP licenses, or an individual authorized by that customer to access components or features of the CSP (“Users”).

CSP is licensed for internal Customer use (i.e. use for the Customer’s own business purposes); however, the Customer is permitted to provide digital certificates, keys or secrets to Users who are outside of the Customer’s organization solely to enable resource access between the Customer and that User. Customer may also grant access to Users who are employees of external contractors, but only to the extent that such Users are using CSP on Customer’s behalf in the operation or management of the Customer’s business and Customer’s own cryptographic assets.

Except as may be otherwise specified in an express license agreement signed by Entrust, neither Customer nor any User may use CSP to set up or provide its own cryptographic management, analysis or reporting service for other companies (e.g. provision of CSP functionality as a “Managed Service Provider” or “Systems Integrator”).

License Packages

CSP has three licensing packages (Standard, Pro, and Enterprise), each of which includes different product functionalities/features, as well as volumes of included certificates, standard objects, enhanced objects, and third-party objects. The table below shows what is included, depending on whether Customer has purchased a Standard, Pro, or Enterprise license package.

Packages	Standard	Pro	Enterprise
Cryptographic Security Platform <ul style="list-style-type: none"> • CSP Compliance Manager • CSP Public Key Infrastructure • CSP Key & Secrets Management 	✓	✓	✓
Enhanced PKI Services <ul style="list-style-type: none"> • CSP Certificate Enrollment Gateway • CSP CA Gateway • CSP Timestamping • CSP Validation Authority 		✓	✓
CSP Certificate Manager (Discovery)		✓	✓
CSP Certificate Manager (Control)			✓
Certificates	50	200	A custom amount as specified in an Entrust-issued quote
Vault Appliances	2	8	A custom amount as specified in an Entrust-issued quote
Compliance Manager Appliances	2	2	A custom amount as specified in an Entrust-issued quote
Standard Compliance Pack for Keys & Secrets	1	4	A custom amount as specified in an Entrust-issued quote
Standard Compliance Pack for Certificates	1	4	A custom amount as specified in an Entrust-issued quote
Third-Party Objects Under Compliance	250	1000	A custom amount as specified in an Entrust-issued quote
KMIP Objects	83	333	A custom amount as specified in an Entrust-issued quote

Packages	Standard	Pro	Enterprise
Cloud Keys	83	333	A custom amount as specified in an Entrust-issued quote
Secrets	84	334	A custom amount as specified in an Entrust-issued quote
Application Security Keys	16	66	A custom amount as specified in an Entrust-issued quote
TDE Databases	16	66	A custom amount as specified in an Entrust-issued quote
Virtual Machines	18	68	A custom amount as specified in an Entrust-issued quote

The Customer will receive one or more license keys (“licenses”) to enable CSP features and the associated volumes of certificates, standard objects, enhanced objects, and third-party objects based on what the Customer has purchased. These licenses are subject to the following terms:

- Once a digital certificate is issued, it is deemed consumed.
- Once a standard or enhanced object is created, it is deemed consumed.
- Once a third-party object is created, it is deemed consumed.
- 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 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.

Each CSP license specifies a deployment type, which is categorized either as production or test. If not explicitly specified, the license is considered production.

- Production licenses allow CSP to be used in a production environment to issue and manage trusted digital certificates for Users.
- Test licenses must be used exclusively in a non-production (test) environment to develop, integrate, and verify configuration changes before promoting them to production.

Each CSP license entitles Customer to deploy:

- one cluster of CSP Compliance Manager appliances; and
- multiple clusters of CSP Key & Secrets Management, CSP PKI, and (for Pro and Enterprise licenses) CSP Certificate Manager.

Plugins

CSP CA Gateway functionality can be extended, through plugins, to connect to additional CA types. The Customer is permitted to run plugins. These plugins may be:

- Developed by Entrust (sold separately), or
- Developed by the Customer or a third party, under a valid CSP CA Gateway SDK License, and recognized by Entrust (via digital signing).

Plugins are out-of-scope for the product warranty and Entrust support for CSP.

External Dependencies

CSP licenses do not include any embedded and/or internal databases and Hardware Security Modules (HSM). These components are external dependencies that must be provided, installed, and configured separately by the Customer prior to the operation of the CSP software.

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 are provided to assist organizations in reviewing their cryptographic keys, secrets, and certificates against industry standards and best practices. While the Standard Compliance Packs will assist 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. It is Customer's sole responsibility to validate all requirements and manage compliance of 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 their activities). Entrust disclaims any liability arising from Customer's reliance on the Standard Compliance Packs.

Support and Record-Keeping

To ensure Entrust Customer Support is equipped to assist with issues reported, the Customer is expected to maintain reasonable records of the CSP deployment details including:

- The production instances in use.
- The environment(s) (on-premises or cloud) where those instances reside.

Third-party license acknowledgments

See below the license acknowledgments for the third-party software included in Cryptographic Security Platform.

- This software is based in part on the work of the FreeType Team.
- This software is based in part on the work of the Independent JPEG Group
- This product includes software developed by The XFree86 Project, Inc (<https://www.xfree86.org>) and its contributors.
- This product includes software developed by Henry Spencer.
- The configuration files in <https://github.com/grafana/helm-charts> have been modified by Entrust for product customization purposes.
- The configuration files in <https://github.com/grafana/loki> have been modified by Entrust for product customization purposes.
- The configuration files in <https://github.com/prometheus-community/helm-charts> have been modified by Entrust for product customization purposes.
- The configuration files in <https://github.com/longhorn/charts> have been modified by Entrust for product customization purposes.

23 Certificate profiles reference


Entrust provides the following set of certificate profiles for authorities and end-entities.

- [Basic authority certificate profiles](#)
- [External subordinate CA certificate profiles](#)
- [Subscriber certificate profiles](#)

Basic authority certificate profiles

Entrust provides the following basic profiles for root Certificate Authorities, issuing Certificate Authorities, and Validation Authorities (OCSP).

- basic-ca-root
- basic-ca-subord
- basic-ocsp

 These profiles are not exposed nor configurable. External root CAs are not covered by this profile.


See below a description of these profiles.

- [Key and signature algorithms](#)
- [Certificate fields](#)
- [Certificate critical extensions](#)
- [Certificate non-critical extensions](#)

Key and signature algorithms

All authority basic profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

Certificate fields

The authority basic profiles set the following certificate fields.

Field	basic-ca-root	basic-ca-subord	basic-ocsp
Issuer	Self-signed	Customer's online root CA	Customer's online root/ issuing CA
Subject	No constraint	No constraint	No constraint
Validity period	Less than or equal to 20 years	Less than or equal to 10 years. The subordinate expiry cannot exceed the root validity.	30 days

Certificate critical extensions

The authority basic profiles set the following certificate critical extensions.

Extension	basic-ca-root	basic-ca-subord	basic-ocsp
Basic Constraints	cA=True	cA=True, pathLenConstraint=0	cA = False
Extended Key Usage	Never present	Never present	OCSP Signing
Key Usage	digitalSignature, keyCertSign, cRLSign	digitalSignature, keyCertSign, cRLSign	digitalSignature, keyCertSign, cRLSign

Certificate non-critical extensions

The authority basic profiles set the following non-critical certificate extensions.

Extension	basic-ca-root	basic-ca-subord	basic-ocsp
AIA	Never present	Supplied when the customer enables OCSP on CA creation	Always present
Authority Key Identifier	Never present	Matches subjectKeyIdentifier of the signing certificate	Matches subjectKeyIdentifier of the signing certificate

Extension	basic-ca-root	basic-ca-subord	basic-ocsp
CRL Distribution Points	Never present (not applicable)	Always present	Always present
OCSP	Never present	Never present	No check
Subject Key Identifier	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

External subordinate CA certificate profiles

Entrust root Certificate Authorities support the following external subordinate Certificate Authority certificate profiles.

Profile set	Profiles
Azure Firewall Intermediate CA certificate profiles	azure-firewall-ca-subord
TLS Proxy CA certificate profiles	tlsproxy-ca-subord

Azure Firewall Intermediate CA certificate profiles

The Azure Firewall Intermediate CA service provides a `azure-firewall-ca-subord` profile for root Certificate Authorities.

- [Azure Firewall Subordinate CA signing use cases](#)
- [Azure Firewall Subordinate CA request extensions](#)
- [Azure Firewall Subordinate CA certificate fields](#)
- [Azure Firewall Subordinate CA certificate extensions](#)
- [Azure Firewall Subordinate CA algorithm constraints](#)
- [Azure Firewall Subordinate CA distinguished names](#)

Azure Firewall Subordinate CA signing use cases


The `azure-firewall-ca-subord` profile supports the following use cases.

- ECS Enterprise UI
- CA Gateway API

Azure Firewall Subordinate CA request extensions

The `azure-firewall-ca-subord` profile supports the following non-critical extensions in request.

Extension name	Extension OID
Certificate Policies	2.5.29.32

 Follow the [Microsoft Azure Intermediate requirements](#) to generate the CSR before requesting the CA certificate from PKIaaS.

Azure Firewall Subordinate CA certificate fields

The `azure-firewall-ca-subord` profile sets the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint
Validity period	Defaults to 1 year if not specified.

Azure Firewall Subordinate CA certificate extensions

The `azure-firewall-ca-subord` profile sets the following certificate extensions.


Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA=True, pathLenConstraint=1
CRL Distribution Points	No	Always present
Key Usage	Yes	Certificate Signing, CRL Signing, Digital Signature
Subject Alternative Name	No	No constraints

Extension	Critical	Value
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

Azure Firewall Subordinate CA algorithm constraints

The `azure-firewall-ca-subord` profile supports the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

Azure Firewall Subordinate CA distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6

Alias	OID
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3

Alias	OID
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

TLS Proxy CA certificate profiles

The TLS Proxy CA service provides provides a `tlsproxy-ca-subord` certificate profile for root Certificate Authorities.

- [TLS Proxy CA use cases](#)
- [TLS Proxy CA request extensions](#)
- [TLS Proxy CA certificate fields](#)
- [TLS Proxy CA certificate extensions](#)
- [TLS Proxy CA algorithm constraints](#)
- [TLS Proxy CA distinguished names](#)

i Each external subordinate CA issued by a PKIaaS root CA only consumes one PKIaaS Certificate license. Entrust does not charge for certificates issued by external subordinate CAs because those certificates are considered external and not using the PKIaaS infrastructure.

TLS Proxy CA use cases

The `tlsproxy-ca-subord` profile supports the following use cases.

- ECS Enterprise UI
- CA Gateway API

TLS Proxy CA request extensions

The `tlsproxy-ca-subord` profile supports the following non-critical extensions in request.

Extension name	Extension OID
CertificatePolicies	2.5.29.32

TLS Proxy CA certificate fields

The `tlsproxy-ca-subord` profile sets the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint
Validity period	Defaults to 1 year if not specified.

TLS Proxy CA certificate extensions

The `tlsproxy-ca-subord` profile sets the following certificate extensions.


Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA=True, pathLenConstraint=0
CRL Distribution Points	No	Always present
Extended Key Usage	No	TLS server authentication (1.3.6.1.5.5.7.3.1), TLS client authentication (1.3.6.1.5.5.7.3.2)

Extension	Critical	Value
Key Usage	Yes	Certificate Signing, CRL Signing, Digital Signature
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

TLS Proxy CA algorithm constraints

The `tlsproxy-ca-subord` profile supports the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

TLS Proxy CA distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4

Alias	OID
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1

Alias	OID
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

Subscriber certificate profiles

Entrust provides the following certificate policies for end-entity subscribers

Profile set	Profiles
EST certificate profiles	est-digital-signature est-digital-signature-key-encipherment est-key-encipherment est-non-repudiation
Mobile device certificate profile	mobile-device-p12-digital-signature-client-authentication

Profile set	Profiles
CMPv2 certificate profiles	cmp-digital-signature cmp-digital-signature-key-encipherment cmp-key-encipherment cmp-non-repudiation
V2G certificate profiles	v2g-supply-equipment v2g-user-identity
SCEP certificate profiles	scep-digital-signature scep-digital-signature-key-encipherment scep-key-encipherment scep-non-repudiation
Active Directory (WSTEP) certificate profiles	wstep-digital-signature wstep-digital-signature-key-encipherment wstep-key-encipherment wstep-non-repudiation wstep-non-repudiation-key-encipherment
Intune certificate profiles	intune-digital-signature intune-digital-signature-key-encipherment intune-digital-signature-key-encipherment-clientauth intune-key-encipherment intune-non-repudiation
MDMWS certificate profiles	mdmws-digital-signature mdmws-digital-signature-key-encipherment mdmws-digital-signature-key-encipherment-clientauth mdmws-key-encipherment mdmws-non-repudiation mdmws-p12-digital-signature mdmws-p12-digital-signature-key-encipherment mdmws-p12-digital-signature-key-encipherment-clientauth mdmws-p12-key-encipherment mdmws-p12-non-repudiation
Private SSL (ACMEv2) certificate profiles	privatessl-tls-client privatessl-tls-client-server privatessl-tls-client-server-data-encipherment privatessl-tls-client-server-supply-san privatessl-tls-server privatessl-tls-server-supply-san
Multiuse certificate profiles	multiuse-p12-client

Profile set	Profiles
	multiuse-p12-client-server multiuse-p12-custom multiuse-p12-key-data-encipherment-non-repudiation-client multiuse-p12-key-data-encipherment-non-repudiation-client-server multiuse-p12-key-encipherment-client multiuse-p12-key-encipherment-client-server multiuse-p12-key-encipherment-custom multiuse-p12-key-encipherment-non-repudiation-client multiuse-p12-key-encipherment-non-repudiation-client-server multiuse-p12-key-encipherment-non-repudiation-custom multiuse-p12-key-encipherment-non-repudiation-server multiuse-p12-key-encipherment-server multiuse-p12-non-repudiation-client multiuse-p12-non-repudiation-client-server multiuse-p12-non-repudiation-custom multiuse-p12-non-repudiation-server multiuse-p12-server
Smartcard certificate profiles	smartcard-card-authentication smartcard-digital-signature smartcard-domain-controller smartcard-key-management smartcard-piv-authentication smartcard-piv-content-signing
Code signing certificate profile	codesigning-digital-signature
S_MIME certificate profiles	smime-digital-signature-key-encipherment smime-key-encipherment smime-non-repudiation

Active Directory (WSTEP) certificate profiles

Entrust provides the following Active Directory (WSTEP) certificate profiles.

- wstep-digital-signature
- wstep-digital-signature-key-encipherment

- wstep-key-encipherment
- wstep-non-repudiation
- wstep-non-repudiation-key-encipherment

These profiles support the following features.

- [WSTEP use cases](#)
- [WSTEP key usages](#)
- [WSTEP request extensions](#)
- [WSTEP certificate fields](#)
- [WSTEP certificate extensions](#)
- [WSTEP algorithm constraints](#)
- [WSTEP distinguished names](#)

WSTEP use cases

All WSTEP profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API
- Entrust-hosted Enrollment Gateway
- On-prem Enrollment Gateway

WSTEP key usages

See below the Key Usage extension values supported by each WSTEP profile.

Profile	Key Usage
wstep-digital-signature	Digital Signature
wstep-digital-signature-key-encipherment	Digital Signature, Key Encipherment
wstep-key-encipherment	Key Encipherment
wstep-non-repudiation	Digital Signature, Non-Repudiation
wstep-non-repudiation-key-encipherment	Digital Signature, Non-Repudiation, Key Encipherment

WSTEP request extensions

All WSTEP profiles support the following non-critical extensions in request.

Extension name	Extension OID
Certificate Policies	2.5.29.32

Extension name	Extension OID
Extended Key Usage	2.5.29.37
Application Policies	1.3.6.1.4.1.311.21.10
Smime Capabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

WSTEP certificate fields

All WSTEP profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

WSTEP certificate extensions

All WSTEP profiles set the following certificate extensions.


Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False

Extension	Critical	Value
CRL Distribution Points	No	Always present
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

WSTEP algorithm constraints

All WSTEP profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

WSTEP distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4

Alias	OID
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1

Alias	OID
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

CMPv2 certificate profiles

Entrust provides the following CMPv2 certificate profiles.

- cmp-digital-signature
- cmp-digital-signature-key-encipherment
- cmp-key-encipherment
- cmp-non-repudiation

These profiles support the following features.

- [CMPv2 use cases](#)
- [CMPv2 key usages](#)
- [CMPv2 request extensions](#)
- [CMPv2 certificate fields](#)
- [CMPv2 certificate extensions](#)
- [CMPv2 algorithm constraints](#)

- [CMPv2 distinguished names](#)

CMPv2 use cases

All CMPv2 profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

CMPv2 key usages

See below the Key Usage extension values supported by each CMPv2 profile.

Profile	Key Usage
cmp-digital-signature	Digital Signature
cmp-digital-signature-key-encipherment	Digital Signature, Key Encipherment
cmp-key-encipherment	Key Encipherment
cmp-non-repudiation	Digital Signature, Non-Repudiation

CMPv2 request extensions

All CMPv2 profiles support the following non-critical extensions in request.

Extension name	Extension OID
Certificate Policies	2.5.29.32
Extended Key Usage	2.5.29.37
Application Policies	1.3.6.1.4.1.311.21.10
Smime Capabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

CMPv2 certificate fields

All CMPv2 profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

CMPv2 certificate extensions


All CMPv2 profiles set the following certificate extension.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Extended Key Usage	No	No constraints
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

CMPv2 algorithm constraints

All CMPv2 profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

CMPv2 distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10

Alias	OID
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5

Alias	OID
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

Code signing certificate profile

Entrust provides the `codesigning-digital-signature` certificate profile for code signing.

- [Code signing use cases](#)
- [Code signing certificate fields](#)
- [Code signing certificate extensions](#)
- [Code signing algorithm constraints](#)
- [Code signing distinguished names](#)

Code signing use cases

The `codesigning-digital-signature` profile supports the following use cases.

- ECS Enterprise UI
- CA Gateway API

Code signing certificate fields

The `codesigning-digital-signature` profile sets the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA
Validity period	Less than or equal to the expiry of the issuing CA. Default to 1 year if not specified in the request.

Field	Value
Subject	No constraint

Code signing certificate extensions

The `codesigning-digital-signature` profile sets the following certificate extensions.


Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Extended Key Usage	No	Code Signing (1.3.6.1.5.5.7.3.3)
Key Usage	Yes	Digital Signature
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

Code signing algorithm constraints

The `codesigning-digital-signature` profile supports the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512

Key algorithm	Signature algorithm
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

Code signing distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15

Alias	OID
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2

Alias	OID
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

eSIM certificate profiles

Entrust provides the following certificate profiles for eSIM end-entity users.

- esim-delivery-auth
- esim-delivery-binding
- esim-delivery-tls-server
- esim-discovery-auth
- esim-discovery-tls-server

These profiles support the following features.

- [eSIM use cases](#)
- [eSIM key usages and certificate policies](#)
- [eSIM certificate fields](#)
- [eSIM certificate extensions](#)
- [eSIM algorithm constraints](#)
- [eSIM distinguished names](#)

eSIM use cases

All eSIM end-entity profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

eSIM key usages and certificate policies

See below the Key Usage, Extended Key Usage (EKU), and Certificate Policy extension values supported by each eSIM profile.

Profile	Key Usage	Extended Key Usage	Certificate Policy
esim-delivery-auth	Digital Signature	—	id-rspRole-dp-auth (2.23.146.1.2.1.4)
esim-delivery-binding	Digital Signature	—	id-rspRole-dp-pb (2.23.146.1.2.1.5)

Profile	Key Usage	Extended Key Usage	Certificate Policy
esim-delivery-tls-server	Digital Signature	TLS server authentication (1.3.6.1.5.5.7.3.1)	id-rspRole-dp-tls (2.23.146.1.2.1.3)
esim-discovery-auth	Digital Signature	—	id-rspRole-ds-auth (2.23.146.1.2.1.7)
esim-discovery-tls-server	Digital Signature	TLS server authentication (1.3.6.1.5.5.7.3.1)	id-rspRole-ds-tls (2.23.146.1.2.1.6)

eSIM certificate fields

All eSIM profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 3 years if not specified in the request.

eSIM certificate extensions

All eSIM profiles set the following certificate extensions.


Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA=False
CRL Distribution Points	No	Always present
Subject Alternative Name	No	No constraints

Extension	Critical	Value
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

eSIM algorithm constraints

All eSIM profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

eSIM distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6

Alias	OID
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3

Alias	OID
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

EST certificate profiles

Entrust provides the following EST (Enrollment over Secure Transport) certificate profiles.

- est-digital-signature
- est-digital-signature-key-encipherment
- est-key-encipherment
- est-non-repudiation

These profiles support the following features.

- [EST signing use cases](#)
- [EST key usages](#)
- [EST request extensions](#)
- [EST certificate fields](#)
- [EST certificate extensions](#)
- [EST algorithm constraints](#)
- [EST signing distinguished names](#)

EST signing use cases

All EST profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

EST key usages

See below the Key Usage extension values each EST profile supports.

Profile	Key Usage
est-digital-signature	Digital Signature
est-digital-signature-key-encipherment	Digital Signature, Key Encipherment
est-key-encipherment	Key Encipherment
est-non-repudiation	Digital Signature, Non-Repudiation

EST request extensions

All EST profiles support the following non-critical extensions in request.

Extension name	Extension OID
Certificate Policies	2.5.29.32
Extended Key Usage	2.5.29.37
Application Policies	1.3.6.1.4.1.311.21.10
Smime Capabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

EST certificate fields

All EST profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

EST certificate extensions

All EST profiles set the following certificate extension values.


Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Extended Key Usage	No	No constraints
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

EST algorithm constraints

All EST profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384

Key algorithm	Signature algorithm
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

EST signing distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12

Alias	OID
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13

Alias	OID
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

Intune certificate profiles

Entrust provides the following Intune certificate profiles.

- intune-digital-signature
- intune-digital-signature-key-encipherment
- intune-digital-signature-key-encipherment-clientauth
- intune-key-encipherment
- intune-non-repudiation

These profiles support the following features.

- [Intune use cases](#)
- [Intune key usages](#)
- [Intune request extensions](#)
- [Intune certificate fields](#)
- [Intune certificate extensions](#)
- [Intune algorithm constraints](#)
- [Intune distinguished names](#)

Intune use cases

All Intune profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API
- Entrust-hosted Enrollment Gateway
- On-prem Enrollment Gateway

Intune key usages

See below the Key Usage and Extended Key Usage (EKU) extension values supported by each [Intune](#) profile.

Profile	Key Usage	Extended Key Usage	Allows Extended Key Usage in request
intune-digital-signature	Digital Signature	—	✓
intune-digital-signature-key-encipherment	Digital Signature, Key Encipherment	—	✓
intune-digital-signature-key-encipherment-clientauth	Digital Signature, Key Encipherment	TLS client authentication (1.3.6.1.5.5.7.3.2)	✗
intune-key-encipherment	Key Encipherment	—	✓
intune-non-repudiation	Digital Signature, Non-Repudiation	—	✓

Intune request extensions

All Intune profiles support the following non-critical extensions in request.

Extension name	Extension OID
Certificate Policies	2.5.29.32
Application Policies	1.3.6.1.4.1.311.21.10
Smime Capabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

Intune certificate fields

All Intune profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.

Field	Value
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

Intune certificate extensions

All Intune profiles set the following certificate extensions.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

Intune algorithm constraints

All Intune profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption

Key algorithm	Signature algorithm
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

i NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

Intune distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17

Alias	OID
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3

Alias	OID
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

MDMWS certificate profiles

Entrust provides the following MDMWS (Mobile Device Management Web Service) certificate profiles.

- mdmws-digital-signature
- mdmws-digital-signature-key-encipherment
- mdmws-digital-signature-key-encipherment-clientauth
- mdmws-key-encipherment
- mdmws-non-repudiation
- mdmws-p12-digital-signature
- mdmws-p12-digital-signature-key-encipherment
- mdmws-p12-digital-signature-key-encipherment-clientauth
- mdmws-p12-key-encipherment
- mdmws-p12-non-repudiation

These profiles support the following features.

- [MDMWS use cases](#)
- [MDMWS issuance modes and key usages](#)
- [MDMWS request extensions](#)
- [MDMWS certificate fields](#)
- [MDMWS certificate extensions](#)
- [MDMWS algorithm constraints](#)
- [MDMWS distinguished names](#)

MDMWS use cases

All MDMWS profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API
- Entrust-hosted Enrollment Gateway
- On-prem Enrollment Gateway

MDMWS issuance modes and key usages

MDMWS profiles support the following issuance modes:

- Issue the certificate from a CSR.
- Issue the certificate and an [RSA2048 private key](#) in a P12 file.

See below the issuance mode, Key Usage, and Extended Key Usage (EKU) values each MDMWSprofile supports.

Profile	CSR	P12	Key Usage	Extended Key Usage	Allows Extended Key Usage in request
mdmws-digital-signature	✓	✗	Digital Signature	No constraints	✓
mdmws-digital-signature-key-encipherment	✓	✗	Digital Signature, Key Encipherment	No constraints	✓
mdmws-digital-signature-key-encipherment-clientauth	✓	✗	Digital Signature, Key Encipherment	TLS client authentication (1.3.6.1.5.5.7.3.2)	✗
mdmws-key-encipherment	✓	✗	Key Encipherment	No constraints	✓
mdmws-non-repudiation	✓	✗	Digital Signature, Non-Repudiation	No constraints	✓
mdmws-p12-digital-signature	✓	✓	Digital Signature	No constraints	✓
mdmws-p12-digital-signature-key-encipherment	✓	✓	Digital Signature, Key Encipherment	No constraints	✓
mdmws-p12-digital-signature-key-encipherment-clientauth	✓	✓	Digital Signature, Key Encipherment	TLS client authentication (1.3.6.1.5.5.7.3.2)	✗
mdmws-p12-key-encipherment	✓	✓	Key Encipherment	No constraints	✓
mdmws-p12-non-repudiation	✓	✓	Digital Signature, Non-Repudiation	No constraints	✓

MDMWS request extensions

All MDMWS profiles support the following non-critical extensions in request.

Extension name	Extension OID
Certificate Policies	2.5.29.32
Application Policies	1.3.6.1.4.1.311.21.10
Smime Capabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

MDMWS certificate fields

All MDMWS profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

MDMWS certificate extensions

All MDMWS profiles set the following certificate extension values.


Extension	OID
CertificatePolicies	2.5.29.32
ApplicationPolicies	1.3.6.1.4.1.311.21.10
SmimeCapabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7

Extension	OID
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

MDMWS algorithm constraints

All MDMWS profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

MDMWS distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6

Alias	OID
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3

Alias	OID
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

Mobile device certificate profile

Entrust provides the `mobile-device-p12-digital-signature-client-authentication` certificate profile for mobile devices.

- [Mobile device use cases](#)
- [Mobile device certificate issuance mode](#)
- [Mobile device certificate fields](#)
- [Mobile device certificate extensions](#)
- [Mobile device algorithm constraints](#)
- [Mobile distinguished names](#)

Mobile device use cases

The `mobile-device-p12-digital-signature-client-authentication` profile supports the following use cases.

- ECS Enterprise UI
- CA Gateway API

Mobile device certificate issuance mode

The `mobile-device-p12-digital-signature-client-authentication` profile supports the following issuance modes:

- Issue the certificate from a CSR.
- Issue the certificate and an RSA2048 private key in a P12 file.

Mobile device certificate fields

The `mobile-device-p12-digital-signature-client-authentication` profile sets the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA
Validity period	Less than or equal to subordinate expiry of the issuing CA. Default to 1 year if not specified in the request.
Subject	No constraint

Mobile device certificate extensions

The `mobile-device-p12-digital-signature-client-authentication` profile sets the following certificate extensions.


Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Extended Key Usage	No	TLS client authentication (1.3.6.1.5.5.7.3.2)
Key Usage	Yes	Digital Signature
Subject Alternative Name	No	No constraints

Extension	Critical	Value
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

Mobile device algorithm constraints

The `mobile-device-p12-digital-signature-client-authentication` profile supports the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

Mobile distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5

Alias	OID
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2

Alias	OID
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

Multiuse certificate profiles

Entrust provides the following multiuse profiles.

- multiuse-p12-client
- multiuse-p12-client-server
- multiuse-p12-custom
- multiuse-p12-key-data-encipherment-non-repudiation-client
- multiuse-p12-key-data-encipherment-non-repudiation-client-server
- multiuse-p12-key-encipherment-client
- multiuse-p12-key-encipherment-client-server
- multiuse-p12-key-encipherment-custom
- multiuse-p12-key-encipherment-non-repudiation-client
- multiuse-p12-key-encipherment-non-repudiation-client-server
- multiuse-p12-key-encipherment-non-repudiation-custom
- multiuse-p12-key-encipherment-non-repudiation-server
- multiuse-p12-key-encipherment-server
- multiuse-p12-non-repudiation-client

- multiuse-p12-non-repudiation-client-server
- multiuse-p12-non-repudiation-custom
- multiuse-p12-non-repudiation-server
- multiuse-p12-server

These profiles support the following features.

- [Multiuse use cases](#)
- [Multiuse issuance modes](#)
- [Multiuse key usages](#)
- [Multiuse request extensions](#)
- [Multiuse certificate fields](#)
- [Multiuse certificate extensions](#)
- [Multiuse algorithm constraints](#)
- [Multiuse distinguished names](#)

Multiuse use cases

All multiuse profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

Multiuse issuance modes

All multiuse profiles support the following issuance modes:

- Issue the certificate from a CSR.
- Issue the certificate and an RSA2048 private key in a P12 file.

Multiuse key usages

See below the Key Usage and Extended Key Usage (EKU) extension values each multiuse profile supports.

Profile Name	Key Usage	Extended Key Usage	Allows Extended Key Usage in request
multiuse-p12-client	Digital Signature, Key Agreement	TLS client Authentication (1.3.6.1.5.5.7.3.2)	✗
multiuse-p12-client-server	Digital Signature, Key Agreement	TLS client Authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)	✗
multiuse-p12-custom	Digital Signature, Key Agreement	No constraints	✓

Profile Name	Key Usage	Extended Key Usage	Allows Extended Key Usage in request
multiuse-p12-key-data-encipherment-non-repudiation-client	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment	TLS client Authentication (1.3.6.1.5.5.7.3.2)	✗
multiuse-p12-key-data-encipherment-non-repudiation-client-server	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment	TLS client Authentication (1.3.6.1.5.5.7.3.2)	✗
multiuse-p12-key-encipherment-client	Digital Signature, Key Agreement, Key Encipherment	TLS client Authentication (1.3.6.1.5.5.7.3.2)	✗
multiuse-p12-key-encipherment-client-server	Digital Signature, Key Agreement, Key Encipherment	TLS client Authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)	✗
multiuse-p12-key-encipherment-custom	Digital Signature, Key Agreement, Key Encipherment	No constraints	✓
multiuse-p12-key-encipherment-non-repudiation-client	Digital Signature, Key Agreement, Key Encipherment, Non-Repudiation	TLS client Authentication (1.3.6.1.5.5.7.3.2)	✗
multiuse-p12-key-encipherment-non-repudiation-client-server	Digital Signature, Key Agreement, Key Encipherment, Non-Repudiation	TLS client Authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)	✗
multiuse-p12-key-encipherment-non-repudiation-custom	Digital Signature, Key Agreement, Key Encipherment, Non-Repudiation	No constraints	✓

Profile Name	Key Usage	Extended Key Usage	Allows Extended Key Usage in request
multiuse-p12-key-encipherment-non-repudiation-server	Digital Signature, Key Agreement, Key Encipherment, Non-Repudiation	TLS server authentication (1.3.6.1.5.5.7.3.1)	✗
multiuse-p12-key-encipherment-server	Digital Signature, Key Agreement, Key Encipherment	TLS server authentication (1.3.6.1.5.5.7.3.1)	✗
multiuse-p12-non-repudiation-client	Digital Signature, Key Agreement, Non-Repudiation	TLS client Authentication (1.3.6.1.5.5.7.3.2)	✗
multiuse-p12-non-repudiation-client-server	Digital Signature, Key Agreement, Non-Repudiation	TLS client Authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)	✗
multiuse-p12-non-repudiation-custom	Digital Signature, Key Agreement, Non-Repudiation	No constraints	✓
multiuse-p12-non-repudiation-server	Digital Signature, Key Agreement, Non-Repudiation	TLS server authentication (1.3.6.1.5.5.7.3.1)	✗
multiuse-p12-server	Digital Signature, Key Agreement	TLS server authentication (1.3.6.1.5.5.7.3.1)	✗

Multiuse request extensions

All multiuse profiles support the following non-critical extensions in request.

Extension	OID
ApplicationPolicies	1.3.6.1.4.1.311.21.10
CertificatePolicies	2.5.29.32

Multiuse certificate fields

All multiuse profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

Multiuse certificate extensions


All multiuse profiles set the following certificate extensions.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Key Usage	Yes	Digital Signature, Key Encipherment
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

Multiuse algorithm constraints

All multiuse profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

Multiuse distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10

Alias	OID
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5

Alias	OID
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

Private SSL (ACMEv2) certificate profiles

Entrust provides the following Private SSL (ACMEv2) certificate profiles.

- `privatessl-tls-client`
- `privatessl-tls-client-server`
- `privatessl-tls-client-server-data-encipherment`
- `privatessl-tls-client-server-supply-san`
- `privatessl-tls-server`
- `privatessl-tls-server-supply-san`

These profiles support the following features.

- [Private SSL use cases](#)
- [Private SSL key usages](#)
- [Private SSL fill_san_dns_with_cn](#)
- [Private SSL request extensions](#)
- [Private SSL certificate fields](#)
- [Private SSL certificate extensions](#)
- [Private SSL algorithm constraints](#)
- [Private SSL distinguished names](#)

Private SSL use cases

All private SSL profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

Private SSL key usages

See below the Key Usage and Extended Key Usage (EKU) extension values each private SSL profile supports.

Profile	Key Usage	Extended Key Usage
privatessl-tls-client	Digital Signature	TLS client authentication (1.3.6.1.5.5.7.3.2)
privatessl-tls-client-server	Digital Signature	TLS client authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)
privatessl-tls-client-server-data-encipherment	Digital Signature, Data Encipherment	TLS client authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)
privatessl-tls-client-server-supply-san	Digital Signature	TLS client authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)
privatessl-tls-server	Digital Signature	TLS server authentication (1.3.6.1.5.5.7.3.1)
privatessl-tls-server-supply-san	Digital Signature	TLS server authentication (1.3.6.1.5.5.7.3.1)

Private SSL fill_san_dns_with_cn

When the `fill_san_dns_with_cn` parameter is `True`, the profile copies in the `SubjectAltname` extension all the `CN` fields:

- included in the `Subject` extension, and
- not already in the `SubjectAltname` extension (to avoid duplicated entries).

See below the value of this parameter in each profile.

Profile	fill_san_dns_with_cn
privatessl-tls-client	False
privatessl-tls-client-server	False
privatessl-tls-client-server-data-encipherment	False

Profile	fill_san_dns_with_cn
privatessl-tls-client-server-supply-san	True
privatessl-tls-server	False
privatessl-tls-server-supply-san	True

Private SSL request extensions

All private SSL profiles support the following non-critical extensions in request.

Extension Name	Extension OID
Application Policies	1.3.6.1.4.1.311.21.10
Certificate Policies	2.5.29.32

Private SSL certificate fields

All Private SSL profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

Private SSL certificate extensions

All private SSL profiles set the following certificate extensions.


Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate

Extension	Critical	Value
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

Private SSL algorithm constraints

All private SSL profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

Private SSL distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3

Alias	OID
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8

Alias	OID
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

S/MIME Secure Email certificate profiles

Entrust provides the following S/MIME Secure Email certificate profiles.

- smime-digital-signature-key-encipherment
- smime-key-encipherment
- smime-non-repudiation

These profiles support the following features.

- [S/MIME use cases](#)
- [S/MIME key usages](#)
- [S/MIME certificate fields](#)
- [S/MIME certificate extensions](#)

- [S/MIME algorithm constraints](#)
- [S/MIME distinguished names](#)

S/MIME use cases

All S/MIME Secure Email profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

S/MIME key usages

See below the Key Usage and Extended Key Usage (EKU) extension values each profile supports.

Profile	Key Usage	Extended Key Usage
smime-digital-signature-key-encipherment	Digital Signature, Key Encipherment	TLS client authentication (1.3.6.1.5.5.7.3.2) Email Protection (1.3.6.1.5.5.7.3.4)
smime-key-encipherment	Key Encipherment	Email Protection (1.3.6.1.5.5.7.3.4)
smime-non-repudiation	Digital Signature, Non-Repudiation	Email Protection (1.3.6.1.5.5.7.3.4)

S/MIME certificate fields

All S/MIME Secure Email profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

S/MIME certificate extensions

All S/MIME Secure Email profiles set the following certificate extensions.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

S/MIME algorithm constraints

All S/MIME Secure Email profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

i NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

S/MIME distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1

Alias	OID
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

SCEP certificate profiles

Entrust provides the following SCEP (Simple Certificate Enrollment Protocol) certificate profiles.

- scep-digital-signature
- scep-digital-signature-key-encipherment
- scep-key-encipherment
- scep-non-repudiation

These profiles support the following features.

- [SCEP use cases](#)
- [SCEP key usages](#)
- [SCEP request extensions](#)
- [SCEP certificate fields](#)
- [SCEP certificate extensions](#)
- [SCEP algorithm constraints](#)
- [SCEP distinguished names](#)

SCEP use cases

All SCEP profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

SCEP key usages

See below the Key Usage extension values each profile supports.

Profile	Key Usage
scep-digital-signature	Digital Signature
scep-digital-signature-key-encipherment	Digital Signature, Key Encipherment
scep-key-encipherment	Key Encipherment
scep-non-repudiation	Digital Signature, Non-Repudiation

SCEP request extensions

All SCEP profiles support the following non-critical extensions in request.

Extension name	Extension OID
Certificate Policies	2.5.29.32
Extended Key Usage	2.5.29.37
Application Policies	1.3.6.1.4.1.311.21.10
Smime Capabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7

Extension name	Extension OID
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

SCEP certificate fields

All SCEP profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

SCEP certificate extensions


All SCEP profiles set the following certificate extensions.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA=False
CRL Distribution Points	No	Always present
Extended Key Usage	No	No constraints
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

SCEP algorithm constraints

All SCEP profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

SCEP distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9

Alias	OID
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4

Alias	OID
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

Smartcard certificate profiles

Entrust provides the following smartcard certificate profiles.

- smartcard-card-authentication
- smartcard-digital-signature
- smartcard-domain-controller
- smartcard-key-management
- smartcard-piv-authentication
- smartcard-piv-content-signing

These profiles support the following features.

- [Smartcard use cases](#)
- [Smartcard key usages and request extensions](#)
- [Smartcard certificate fields](#)
- [Smartcard certificate extensions](#)
- [Smartcard algorithm constraints](#)
- [Smartcard distinguished names](#)

Smartcard use cases

All smartcard profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

Smartcard key usages and request extensions

See below the Key Usage and Extended Key Usage (EKU) extension values each smartcard profile supports.

Profile	Key Usage	Extended Key Usage	Allowed in request
smartcard-card-authentication	Digital Signature	No constraints	PIV Interim Indicator (2.16.840.1.101.3.6.9.1) Security ID (1.3.6.1.4.1.311.25.2)
smartcard-digital-signature	Digital Signature, Non-Repudiation	No constraints	PIV Interim Indicator (2.16.840.1.101.3.6.9.1) Security ID (1.3.6.1.4.1.311.25.2)
smartcard-domain-controller	Digital Signature, Key Encipherment	TLS server authentication (1.3.6.1.5.5.7.3.1) TLS client authentication (1.3.6.1.5.5.7.3.2)	—
smartcard-key-management	Key Encipherment	No constraints	PIV Interim Indicator (2.16.840.1.101.3.6.9.1) Security ID (1.3.6.1.4.1.311.25.2)
smartcard-piv-authentication	Digital Signature	Any Extended Key Usage (2.5.29.37.0) Microsoft Smart Card Login (1.3.6.1.4.1.311.20.2.2) TLS client authentication (1.3.6.1.5.5.7.3.2)	PIV Interim Indicator (2.16.840.1.101.3.6.9.1) Security ID (1.3.6.1.4.1.311.25.2)
smartcard-piv-content-signing	Digital Signature, Non-Repudiation	No constraints	—

Smartcard certificate fields

All smartcard profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.

Field	Value
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

Smartcard certificate extensions

All smartcard profiles set the following certificate extensions.


Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

Smartcard algorithm constraints

All smartcard profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption

Key algorithm	Signature algorithm
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

Smartcard distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42

Alias	OID
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4

Alias	OID
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

V2G certificate profiles

Entrust provides the following V2G (Vehicle-to-Grid) certificate profiles

- v2g-supply-equipment
- v2g-user-identity

These profiles support the following features.

- [V2G use cases](#)
- [V2G key usages and validity periods](#)
- [V2G certificate fields](#)
- [V2G certificate extensions](#)
- [V2G algorithm constraints](#)
- [V2G distinguished names](#)

V2G use cases

All V2G profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

V2G key usages and validity periods

See below the Key Usage, Extended Key Usage (EKU), and certificate validity period each profile supports.

Profile	Key Usage	Extended Key Usage	Validity period
v2g-supply-equipment	Digital Signature, Key Agreement	TLS server authentication (1.3.6.1.5.5.7.3.1)	1 year
v2g-user-identity	Digital Signature, Non-Repudiation	—	2 year

V2G certificate fields

All V2G profiles set the following certificate fields.

Field	Value
Issuer	The customer's subordinate issuing-CA
Subject	No constraint

V2G certificate extensions

All V2G profiles set the following certificate extensions.


Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

V2G algorithm constraints

All V2G profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption

Key algorithm	Signature algorithm
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

 NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

V2G distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17

Alias	OID
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3

Alias	OID
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

24 Integration report

This section provides a complete integration report for Cryptographic Security Platform.

- [Base installation integration report](#)
- [Certificate Authority integration report](#)
- [CSP Certificate Manager integration report](#)
- [CSP CA Gateway integration report](#)
- [CSP Enrollment Services integration report](#)
- [CSP Validation Authority integration report](#)
- [CSP Timestamping Authority integration report](#)

Base installation integration report

Regardless of deployed solutions, all Cryptographic Security Platform installations share the following integration report.

- [Cryptographic Security Platform versions](#)
- [Infrastructures supported by Cryptographic Security Platform](#)
- [Browsers supported by Cryptographic Security Platform](#)
- [SIEM supported by Cryptographic Security Platform](#)
- [Cryptographic Security Platform upgrade](#)
- [Cryptographic Security Platform internationalization](#)

Cryptographic Security Platform versions

Cryptographic Security Platform has the following versions.

Version	Date	Description
1.0.0	May 2025	First commercial release

Infrastructures supported by Cryptographic Security Platform

You can install Cryptographic Security Platform on the following platform infrastructures.

- Amazon Web Services (AWS)
- Microsoft Azure
- Microsoft Hyper-V
- Nutanix
- VMware vSphere

See the Cryptographic Security Platform guide for the required installation steps.

Browsers supported by Cryptographic Security Platform

PKI Hub provides web portals such as the Management Console, Grafana, and the Certificate Hub administration console. These portals support the following web browsers.


Browser	Supported versions
Apple Safari	5 or higher
Google Chrome	8 or higher
Microsoft Edge	The stable versions listed by Microsoft in https://learn.microsoft.com/en-us/deployedge/microsoft-edge-support-lifecycle
Mozilla Firefox	9 or higher

Browser compatibility is quite high, so most versions operate without issue. If there is an issue, we will address it using the latest browser version available for the operating system.

SIEM supported by Cryptographic Security Platform

Cryptographic Security Platform can forward the system logs to the following Security Information and Event Management (SIEM) servers.

- Splunk Enterprise
- Splunk Cloud


 Cryptographic Security Platform allows ingesting system records through the HTTP Event Collector (HEC) interface.

Cryptographic Security Platform upgrade

This product release does not support upgrades from prior releases.

Cryptographic Security Platform internationalization

Cryptographic Security Platform is released in English.

 As explained in the user guide, you must set the system locale `en_US.UTF-8` during installation.

Certificate Authority integration report

CSP Certificate Authority is a robust, private-trust CA solution designed for enterprises aiming to establish and maintain a secure, scalable, and efficient Public Key Infrastructure (PKI). Built-in with a 2-tier PKI hierarchy, this on-premises CA provides seamless certificate issuance and management, ensuring full control over your organization's cryptographic ecosystem.

When deployed on Cryptographic Security Platform, this Entrust solution adds the following to the [Base installation integration report](#).

- [CSP Certificate Authority releases](#)
- [Hardware secure modules supported by CSP Certificate Authority](#)

- [Entrust products compatible with CSP Certificate Authority](#)
- [Databases supported by CSP Certificate Authority](#)

CSP Certificate Authority releases

CSP Certificate Authority has the following releases.

Version	Installation	Upgrade Method
1.0	First commercial release.	—

Hardware secure modules supported by CSP Certificate Authority

When integrating a Hardware Security Module (HSM):

- You do not need to install the client drivers because the solution already includes this software. However, these client drivers cannot be updated.
- You can only use 1/N card sets. A card set of, for example, 2/5 cards is not supported.
- Changing the settings of an Entrust nShield HSM requires the steps described in [Administrating nShield HSM integration](#).

See the following table for supported versions.

Hardware	Client driver	Firmware
Entrust NShield Connect XC	13.6.3	12.60.15 & 12.60.2
Entrust NShield 5c	13.6.3	13.2.4

Entrust products compatible with CSP Certificate Authority

CSP Certificate Authority 2.1.0 is compatible with the following Entrust products.

Entrust product	Version	Product integration report
CA Gateway (embedded)	3.0.3	CSP CA Gateway integration report
CSP Certificate Manager	4.0.3	CSP Certificate Manager integration report
CSP Enrollment Services	2.1.0	CSP Enrollment Services integration report

Databases supported by CSP Certificate Authority

CSP Certificate Authority is tested with the following external databases.

Database vendor	Version
PostgreSQL	15.6

CSP Certificate Manager integration report

Entrust CSP Certificate Manager allows you to view and manage certificates across your enterprise, regardless of the issuer.

 CSP Certificate Manager uses Entrust CSP CA Gateway as the underlying CA interface.

When deployed on Cryptographic Security Platform, this Entrust solution adds the following to the [Base installation integration report](#).

- [Entrust products compatible with CSP Certificate Manager](#)
- [Platforms supported by CSP Certificate Manager](#)
- [Databases supported by CSP Certificate Manager](#)
- [Web browsers supported by CSP Certificate Manager](#)
- [Plugins supported by CSP Certificate Manager](#)
- [Standards supported by CSP Certificate Manager](#)


Entrust products compatible with CSP Certificate Manager

CSP Certificate Manager is compatible with the following Entrust products.

- CSP CA Gateway 2.8.20
- CSP Certificate Manager Discovery Scanner 2.1.0
- IDaaS (Identity as a Service) for multi-factor login.

Platforms supported by CSP Certificate Manager

In addition to Cryptographic Security Platform, CSP Certificate Manager supports standalone installations on Kubernetes 1.25. We expect it to operate on all supported Kubernetes and Kubernetes variants, such as RedHat OpenShift and Rancher OS.

 Only upgrades from older releases support Kubernetes. New deployments only support Entrust Cryptographic Security Platform.

Databases supported by CSP Certificate Manager


The external CSP Certificate Manager database must be hosted on the following Database Management System (DBMS).

DBMS	Version
PostgreSQL	15 or higher

Web browsers supported by CSP Certificate Manager

The CSP Certificate Manager user console is tested with the latest version of the following web browsers.

Web Browser	Windows	Mac OS
Chrome	✓	✓
Firefox	✓	✓
Microsoft Edge	✓	✗
Safari	✗	✓

 Browser compatibility is quite high, so most versions operate without issue. If there is an issue, we will address it with the latest browser version available for the operating system.

Plugins supported by CSP Certificate Manager

CSP Certificate Manager supports the following plugins.

Plugin	Version	Support Notes
KMIP KMS	2.0	Works for any KMS supported by a KMIP 2.0 protocol
F5 BIG IP	F5 iControl REST API version 15.1	Also compatible with newer F5 BIG-IP versions.

Standards supported by CSP Certificate Manager

CSP Certificate Manager supports the following standards.

Standard	Version	Supported by external IdP providers	Notes
OpenID Connect (OIDC)	1.0	✓	OIDC 1.0 is a layer on top of OAuth 2.0; versioning gets confusing.
Lightweight Directory Access Protocol (LDAP)	v3	✓	Includes AD.

CSP CA Gateway integration report

CSP CA Gateway is a lightweight, container-based module implementing a CA-agnostic Certificate Lifecycle and Policy Management API. Using CSP CA Gateway, your applications can implement certificate issuance, renewal, and revocation actions across all your Entrust-supported Certification Authorities (CAs). CSP CA Gateway provides policy retrieval capabilities that applications can use to customize API and user-facing dialogs to ensure that certificate actions conform to organizational policies.

- i** CSP CA Gateway supports easy upgrades using container technology. We maintain backward compatibility on the API so you can upgrade CSP CA Gateway without worrying that consuming applications will encounter API problems. We release CSP CA Gateway quarterly to make new features available.

When deployed on Cryptographic Security Platform, this Entrust solution adds the following to the [Base installation integration report](#).

- [Products compatible with CSP CA Gateway](#)
- [Platforms supported by CSP CA Gateway](#)

Products compatible with CSP CA Gateway

CSP CA Gateway supports the following products.

- [Certificate Authorities compatible with CSP CA Gateway](#)
- [Other Entrust products compatible with CSP CA Gateway](#)
- [HSM compatible with CSP CA Gateway](#)
- [Open-source plugins compatible with CSP CA Gateway](#)

Certificate Authorities compatible with CSP CA Gateway

CSP CA Gateway is compatible with the following Certificate Authorities.

Product	Version	Support Notes
Entrust Certificate Authority (ECA)	10.1.1, 10.2	All capabilities are supported.
	8.3	The Events API is not supported
		Storing ECA 8.3 RA credentials in nCipher or Luna HSM is not supported
Entrust Certificate Services	Service	TLS certificates are supported
Entrust PKIaaS	Service	CSRs must be provided on enrollment. PKIaaS support added in CSP CA Gateway 2.1

Product	Version	Support Notes
Microsoft Active Directory Certificate Authority	2019, 2016, 2012 R2	CSRs must be provided on enrollment
AWS ACM CA		CA Plugin for cert operations

Other Entrust products compatible with CSP CA Gateway

CSP CA Gateway is also compatible with the following Entrust products.

Product	Version
nCipher Security World	12.50.11
Entrust Deployment Manager	2.0.2
Entrust Validation Authority	2.4.0

HSM compatible with CSP CA Gateway

CSP CA Gateway is compatible with the following HSM (Hardware Security Module).

Product	Version
nCipher Security World	12.50.11

Open-source plugins compatible with CSP CA Gateway

CSP CA Gateway is compatible with the following open-source plugins.

 Support is limited to CSP CA Gateway interoperation with the plugin.

Product	Version	Support Notes
Entrust CSP CA Gateway Vault Client	N/A	This is an Entrust open-source client for Hashicorp Vault that may be obtained from https://github.com/EntrustCorporation/CSP-CA-Gateway-vault-plugin


Platforms supported by CSP CA Gateway

In addition to Cryptographic Security Platform, CSP CA Gateway is distributed and operates as a Docker container. Our objective in leveraging Docker is to allow customers to utilize the broad array of Docker capabilities, features, and plug-in drivers. Entrust will make reasonable efforts to support our CSP CA Gateway product on the customer's chosen Docker deployment.

Platform	Version	Notes
Docker	18.9+	Operation as a Docker container is supported on all OS platforms supporting Docker.
Podman	4.7.1	—

CSP Enrollment Services integration report

CSP Enrollment Services automate user and device enrollment based on Entrust's next-generation microservice framework; the CEG provides a modular enrollment service supporting a wide range of industrial standards enrollment protocols listed in this document under Supported Enrollment Protocols. The combination of policy and automation eliminates outages due to manual renewal errors. IT operations, auditors, security policy enforcement, and management can be confident with the CSP Enrollment Services. Control your devices enterprise-wide through a centralized policy, automating your certificates from enrollment to retirement.

 CSP Enrollment Services integrates with Entrust CSP CA Gateway to provide certificate enrollment capabilities.

When deployed on Cryptographic Security Platform, this Entrust solution adds the following to the [Base installation integration report](#).

- [CSP Enrollment Services localization](#)
- [Enrollment protocols supported by CSP Enrollment Services](#)
- [Entrust products compatible with CSP Enrollment Services](#)

CSP Enrollment Services localization

The current CSP Enrollment Services release only supports English localization.

Enrollment protocols supported by CSP Enrollment Services

See below for details on the CSP Enrollment Services support for enrollment protocols.

- [CSP Enrollment Services support for ACME v2](#)
- [CSP Enrollment Services support for CMPv2](#)
- [CSP Enrollment Services support for EST](#)
- [CSP Enrollment Services support for Intune](#)
- [CSP Enrollment Services support for MDM](#)
- [CSP Enrollment Services support for MS-WSTEP](#)
- [CSP Enrollment Services support for SCEP](#)

CSP Enrollment Services support for ACME v2

See below for details on the CSP Enrollment Services support for ACME (Automatic Certificate Management Environment) v2.

- [ACME v2 version supported by CSP Enrollment Services](#)
- [ACME v2 clients tested with CSP Enrollment Services](#)
- [Load balancer support for ACME v2 enrollment with CSP Enrollment Services](#)

ACME v2 version supported by CSP Enrollment Services

CSP Enrollment Services supports the ACME v2 version described in:

<https://datatracker.ietf.org/doc/html/rfc8555>

ACME v2 clients tested with CSP Enrollment Services

The CSP Enrollment Services support for ACME v2 has been tested with the following clients.

- Win-ACME
- Certbot
- acme.sh
- Cert-Manager.io1.6 and v1.7

Load balancer support for ACME v2 enrollment with CSP Enrollment Services

ACME v2 enrollment with CSP Enrollment Services supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✓
3	✓
4	✓
7	✗

CSP Enrollment Services support for CMPv2

See below for details on the CSP Enrollment Services support for CMP (Certificate Management Protocol) v2.

- [CMPv2 version supported by CSP Enrollment Services](#)
- [CSP CA Gateway version for CMPv2 enrollment with CSP Enrollment Services](#)
- [Load balancer support for CMPv2 enrollment with CSP Enrollment Services](#)

CMPv2 version supported by CSP Enrollment Services

CSP Enrollment Services supports PKIX CMPv2 ([RFC 4210](#) and [RFC 6712](#)) for:

- LTE (4G/5G)
- VPN

CSP CA Gateway version for CMPv2 enrollment with CSP Enrollment Services

The CSP Enrollment Services support of CMPv2 is tested with CSP CA Gateway 3.0.3.

Load balancer support for CMPv2 enrollment with CSP Enrollment Services

CMPv2 enrollment with CSP Enrollment Services supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✓
3	✓
4	✓
7	✓

CSP Enrollment Services support for EST

See below for details on the CSP Enrollment Services support for EST (Enrollment over Secure Transport).

- [EST version supported by CSP Enrollment Services](#)
- [EST clients tested with CSP Enrollment Services](#)
- [Load balancer support for EST enrollment with CSP Enrollment Services](#)

EST version supported by CSP Enrollment Services

CSP Enrollment Services supports the EST standard described in:

<https://datatracker.ietf.org/doc/html/rfc7030>

EST clients tested with CSP Enrollment Services

The CSP Enrollment Services support for EST has been tested with the following clients.

Client	URL	Comments
LibEST 3.2.0	https://github.com/deviance/libest/tree/feature/opensslv3-compat	Requires compiling Uriparser-0.9.8 (https://github.com/uriparser/uriparser) before compiling and building LibEST.
GlobalSign EST client 1.0.6	https://github.com/globalsign/est	—

Load balancer support for EST enrollment with CSP Enrollment Services

EST enrollment with CSP Enrollment Services supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✓
3	✓
4	✓
7	✓

CSP Enrollment Services support for Intune

See below for details on the CSP Enrollment Services support for Microsoft Intune.

- [Intune versions supported by CSP Enrollment Services](#)
- [Load balancer support for Intune enrollment with CSP Enrollment Services](#)

Intune versions supported by CSP Enrollment Services

CSP Enrollment Services supports the Microsoft Intune versions listed at:

<https://docs.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers>

Load balancer support for Intune enrollment with CSP Enrollment Services

Intune enrollment with CSP Enrollment Services supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✓
3	✓
4	✓
7	✓

CSP Enrollment Services support for MDM

See below for details on the CSP Enrollment Services support for MDM (Mobile Device Management).

- [MDM version supported by CSP Enrollment Services](#)
- [MDM clients tested with CSP Enrollment Services](#)
- [Load balancer support for MDM enrollment with CSP Enrollment Services](#)

MDM version supported by CSP Enrollment Services

CSP Enrollment Services supports the following version of the MDM protocol.

- v8
- v9
- v11

MDM clients tested with CSP Enrollment Services

The CSP Enrollment Services support for MDM enrollment has been tested with the following clients.

- VMware Workspace One (Formally AirWatch)
- JAMF Pro
- MobileIron

Other MDM vendors leveraging Entrust MDMWS APIs should work out of the box.

Load balancer support for MDM enrollment with CSP Enrollment Services

MDM enrollment with CSP Enrollment Services supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✓
3	✓
4	✓
7	✓

CSP Enrollment Services support for MS-WSTEP

See below for details on the CSP Enrollment Services support for MS-WSTEP.

- [MS-WSTEP version supported by CSP Enrollment Services](#)
- [MS-WSTEP requests supported by CSP Enrollment Services](#)
- [MS-WSTEP domain enrollments supported by CSP Enrollment Services](#)
- [Windows products supported for MS-WSTEP enrollment with CSP Enrollment Services](#)
- [Load balancer support for MS-WSTEP enrollment with CSP Enrollment Services](#)

MS-WSTEP version supported by CSP Enrollment Services

CSP Enrollment Services supports the 12.0+ version of the MS-WSTEP protocol described at:

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-wstep/4766a85d-0d18-4fa1-a51f-e5cb98b752ea

MS-WSTEP requests supported by CSP Enrollment Services


CSP Enrollment Services supports the following MS-WSTEP types.

Request type	Supported
New	✓
Renewal	✓
Enroll On Behalf Of	✗
Key Archival	✗
Key Attestation	✗

MS-WSTEP domain enrollments supported by CSP Enrollment Services

CSP Enrollment Services supports the following MS-WSTEP domain enrollments.

- Domain and Sub-domain enrollments
- Read-Only Domain Controllers,
- Multiple Domains in the same Active Directory Forest and across trust-established forests.
- Cross Forest support across established trusts between the forests.

 Non-domain enrollments are not supported.

Windows products supported for MS-WSTEP enrollment with CSP Enrollment Services

The CSP Enrollment Services support for MS-WSTEP enrollment has been tested in the following Windows products.

Windows product	Version
Windows Domain Schema	2012 R2+ or later, the latest cipher support required.
Windows Server	2019 (IIS10 required for Certificate Enrollment Policy service)
Windows endpoints	10+, 2012 R2+

Load balancer support for MS-WSTEP enrollment with CSP Enrollment Services

MS-WSTEP enrollment with CSP Enrollment Services supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✓

Load balancing layer	Supported
3	✓
4	✓
7	✗

CSP Enrollment Services support for SCEP

See below for details on the CSP Enrollment Services support for SCEP (Simple Certificate Enrollment Protocol).

- [SCEP versions supported by CSP Enrollment Services](#)
- [Load balancer support for SCEP enrollment with CSP Enrollment Services](#)

SCEP versions supported by CSP Enrollment Services

CSP Enrollment Services supports the SCEP protocol described in;

<https://datatracker.ietf.org/doc/html/draft-nourse-scep-23>

Load balancer support for SCEP enrollment with CSP Enrollment Services

SCEP enrollment with CSP Enrollment Services supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✓
3	✓
4	✓
7	✓

Entrust products compatible with CSP Enrollment Services

CSP Enrollment Services is compatible with the following Entrust products.

- [Entrust CSP CA Gateway](#)
- [Entrust Certificate Authority](#)
- [Entrust PKI as a Service](#)
- [Entrust Managed PKI](#)
- [Entrust Certificate Services](#)
- [Microsoft Certificate Services](#)

Entrust CSP CA Gateway

CSP Enrollment Services is compatible with the following CSP CA Gateway versions:

- 2.8.1+
- 3.0.3

CSP CA Gateway integration supports the following protocols.

- WSTEP
- ACMEv2
- Intune-SCEP
- SCEP
- MDMWS
- EST
- CMPv2 (CAGW 3.0.3)

At the time of this publication, CSP CA Gateway supports:

- Entrust PKI as a Service (PKIaaS)
- Entrust Managed PKI Service (mPKI)
- Entrust Certificate Solutions Service (ECS)
- Entrust Authority Security Manager
- Microsoft ADCS 2019 and 2016

Entrust Certificate Authority

Through Entrust CSP CA Gateway, CSP Enrollment Services is compatible with the following versions of Entrust Certificate Authority (formerly Entrust Authority Security Manager).

- 8.3.30
- 10.0+
- 10.1.1
- 10.2.0+

Integration with Entrust Certificate Authority supports the following protocols:

- WSTEP
- ACMEv2
- Intune-SCEP
- SCEP
- MDMWS
- EST
- CMPv2 (10.0.30+ ECA 10.1.1 and 10.2, with CSP CA Gateway v3.0.3)

Entrust PKI as a Service

Through Entrust CSP CA Gateway, CSP Enrollment Services integrates with Entrust PKI as a Service (PKIaaS) to support the following protocols.

- WSTEP
- ACMEv2
- Intune-SCEP
- SCEP
- MDMWS
- EST

Entrust Managed PKI

Through Entrust CSP CA Gateway, CSP Enrollment Services integrates with the Entrust Managed PKI to support the following protocols.

- WSTEP
- ACMEv2
- Intune-SCEP
- SCEP
- MDMWS
- EST
- CMPv2 (10.0.30+ ECA 10.1.1 and 10.2, with CSP CA Gateway v3.0.3)

Entrust Certificate Services

Through Entrust CSP CA Gateway, CSP Enrollment Services integrates with the Entrust Certificate Services (ECS) to support the ACMEv2 protocol.

Microsoft Certificate Services

Through Entrust CSP CA Gateway, CSP Enrollment Services integrates with Windows 2016 and 2019 Microsoft Certificate Services to support the ACMEv2 protocol.

CSP Validation Authority integration report

CSP Validation Authority is an on-premises solution for checking the validity status of issued certificates before their expiration date. When deployed on Cryptographic Security Platform, this Entrust solution adds the following to the [Base installation integration report](#).

- [CSP Validation Authority releases](#)
- [Hardware secure modules supported by CSP Validation Authority](#)
- [Databases supported by CSP Validation Authority](#)

CSP Validation Authority releases

CSP Validation Authority has the following releases.

Version	Installation	Upgrade Method
2.3.0	First commercial release.	—
2.3.1	Bug-fixing release	Please refer to the user guide.

Hardware secure modules supported by CSP Validation Authority

When integrating a Hardware Security Module (HSM):

- You do not need to install the client drivers because the solution already includes this software. However, these client drivers cannot be updated.
- You cannot use HSMs from different providers simultaneously, meaning that nShield and Thales HSMs cannot coexist within the same deployment.

- You can only use 1/N card sets. A card set of, for example, 2/5 cards is not supported.
- Changing the settings of an Entrust nShield HSM requires the steps described in [Administrating nShield HSM integration](#).

See the following table for supported versions.

Hardware	Client driver	Firmware
Entrust NShield Connect XC	13.6.3	12.60.15 & 12.60.2
Entrust NShield 5c	13.6.3	13.2.4
Thales Luna HSM 7	10.7.0	7.7.1-20

Databases supported by CSP Validation Authority

CSP Validation Authority is tested with the following external databases.

Database vendor	Version
PostgreSQL	15
Oracle	21.3.0-xe
Microsoft SQL Server	2019-CU15-ubuntu-20.04
	2022-CU13-ubuntu-22.04

CSP Timestamping Authority integration report

CSP Timestamping Authority is an on-premises timestamping solution based on [RFC 3161](#) that guarantees that data, including documents or code, exists at a given time through the generation of digitally signed timestamps. Specifically:

- Proof of the time when a digital signature was applied or validated.
- Prevents code rejection, ensuring that the signature is valid when signing.
- Enables digital signature verification after the certificate used for the signature is revoked or expired.

When deployed on Cryptographic Security Platform, this Entrust solution adds the following to the [Base installation integration report](#).

- [CSP Timestamping Authority releases](#)
- [Hardware security modules supported with CSP Timestamping Authority](#)

CSP Timestamping Authority releases

CSP Timestamping Authority releases has the following releases.

Version	Installation	Upgrade
2.0.0	First commercial release.	—
2.1.0	Bug fixing release.	Please refer to the user guide.

Hardware security modules supported with CSP Timestamping Authority

When integrating a Hardware Security Module (HSM):

- You do not need to install the client drivers because the solution already includes this software. However, these client drivers cannot be updated.
- You cannot use HSMs from different providers simultaneously, meaning that nShield and Thales HSMs cannot coexist within the same deployment.
- You can only use 1/N card sets. A card set of, for example, 2/5 cards is not supported.
- Changing the settings of an Entrust nShield HSM requires the steps described in [Administering nShield HSM integration](#).

See the following table for supported versions.

Hardware	Client driver	Firmware
Entrust nShield Connect XC	13.6.3	12.60.15 & 12.60.2
Entrust nShield 5c	13.6.3	13.2.4
Thales Luna HSM 7	10.7.0	7.7.1-20