



ENTRUST

Cryptographic Security Platform 1.1.0

Installation and administration guide

Document issue: 1.0
Issue date: August 14, 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	14
	CA Gateway release notes	15
	Certificate Authority release notes	16
	Certificate Manager release notes.....	18
	Certificate Enrollment Gateway release notes	22
	Timestamping Authority release notes.....	24
	Validation Authority release notes	25
	Log Forwarder release notes	26
4	Requirements.....	28
	Required number of nodes	28
	Machine requirements.....	28
	Network requirements.....	29
	Software requirements.....	35
	HSM requirements	39
5	Starting up CSP	40
	Downloading the installation files	40
	Verifying the downloaded files.....	41
	Installing the image	42
	Installing CSP	103

Joining nodes	105
Replacing the default TLS certificate	105
Configuring the proxy	106
Changing the keyboard layout	106
Changing the operating system timezone	107
Configuring time synchronization.....	107
Manually starting starting the chrony service	107
Configuring an nShield HSM	108
6 Starting up the Management Console	110
Replacing the initial admin password.....	110
Setting or updating the license	111
Creating Management Console roles	111
Creating Management Console users	113
Integrating Identity providers	115
7 Managing CA Gateway	124
CA Gateway architecture	124
Obtaining the Gateway server certificate	125
Integrating Certificate Authorities with CA Gateway	129
Configuring and deploying CA Gateway	157
Issuing public trust certificates with CA Gateway	206
Administrating CA Gateway	208
CA Gateway endpoints.....	208
CA Capabilities reference.....	216
8 Managing Certificate Authority	225
Configuring and deploying Certificate Authority	225
Creating Certificate Authority tenants	230
Managing organizations	230
Managing Certificate Authority instances.....	236
Issuing certificates with Certificate Authority instances.....	255
Changing the HSM vendor	258

9	Managing Certificate Enrollment Gateway	260
	Certificate Enrollment Gateway overview	260
	Preparing to deploy Certificate Enrollment Gateway	260
	Issuing TLS certificates for Certificate Enrollment Gateway	300
	Configuring and deploying Certificate Enrollment Gateway	307
	Enrollment URLs for Certificate Enrollment Gateway	330
	Integrating Certificate Enrollment Gateway	335
10	Managing Certificate Manager	523
	Certificate Manager architecture	523
	Configuring and deploying Certificate Manager	524
	Using Certificate Manager	528
	Certificate Manager API	714
	Certificate Manager error reference	714
	Migrating Certificate Manager database to an external host	735
11	Managing Timestamping Authority	738
	Timestamping Authority overview	738
	Loading the HSM configuration on Timestamping Authority	738
	Configuring Entrust Certificate Authority for Timestamping Authority	738
	Generating a timestamping certificate and key pair	740
	Configuring and deploying Timestamping Authority	743
	Testing the timestamping service	750
12	Managing Validation Authority	752
	Validation Authority overview	752
	Loading the HSM configuration on Validation Authority	753
	Initializing the Validation Authority database	753
	Configuring a certificate information source for CSP Validation Authority	755
	Generating a VA certificate and key pair	757
	Configuring Entrust Certificate Authority for CSP Validation Authority	760
	Configuring and deploying Entrust Validation Authority	762
	Testing the OCSP Responder	779

13 Managing Log Forwarder	781
Log Server	782
TLS	784
14 Upgrading	786
Upgrade requirements	786
Upgrade process	786
Supported commands during the upgrade	787
15 Administrating	788
Administrating nShield HSM integration	788
Checking the etcd database size	789
Checking the node health	789
Checking the persistent volume disk usage	790
Defragmenting the etcd database	790
Managing the retention policies	791
Recovering from disaster	791
Restarting the nodes	792
Updating DNS resolution	792
16 Browsing logs with Grafana	794
Updating the Grafana initial administrator	794
Browsing and exporting logs with the Grafana Loki Dashboard	796
Browsing log file contents with Grafana	798
17 Backing up and restoring	802
Backing up	802
Restoring	803
18 Uninstalling	806
19 Command reference	807
clusterctl backup create	808
clusterctl backup restore	809
clusterctl certificate	809
clusterctl help	811

clusterctl install	811
clusterctl license import	812
clusterctl node add	813
clusterctl node info	813
clusterctl node join-token	814
clusterctl proxy clear	814
clusterctl proxy info	815
clusterctl proxy set.....	815
clusterctl retention config logs	818
clusterctl retention config metrics.....	818
clusterctl retention info	820
clusterctl solution config export	820
clusterctl solution config import.....	821
clusterctl solution deploy	822
clusterctl solution info	822
clusterctl solution secret set	823
clusterctl solution upload.....	825
clusterctl uninstall	826
clusterctl upgrade	826
clusterctl version.....	827
clusterctl volume capacity	827
clusterctl volume info	828
evactl check all.....	828
evactl check cert-source	831
evactl check db.....	832
evactl check hsm	832
evactl create-csr	834
evactl create-key	836
evactl delete-key	839
evactl enroll.....	840
evactl export-nshield	841

evactl import-nshield.....	842
evactl import-p12.....	842
evactl import-thales.....	843
evactl list-certs	845
evactl list-keys.....	846
evactl load-oracle-wallet.....	848
evactl reenroll	848
evactl stop	849
pki-hub-upgrade prepare	850
pki-hub-upgrade remove-node.....	851
pki-hub-upgrade upgrade	852
tsactl check clock	852
tsactl check hsm.....	853
tsactl create-csr.....	854
tsactl create-key.....	857
tsactl delete-key.....	859
tsactl export-nshield	861
tsactl import-nshield	861
clusterctl node user create	862
clusterctl node user delete	863
clusterctl node user info	864
clusterctl node user modify.....	865
tsactl import-thales	867
tsactl list-keys.....	869
tsactl stop	871
20 CIS benchmarks	872
Linux CIS benchmarks	872
Password policy CIS benchmarks	874
Kubernetes CIS benchmarks	875
21 Troubleshooting and technical assistance.....	883
Troubleshooting Certificate Enrollment Gateway	883

Troubleshooting Validation Authority	883
Troubleshooting Timestamping Authority	884
Generating technical assistance reports	884
22 Licensing.....	887
Customer license.....	887
Third-party license acknowledgments	890
23 Certificate profiles reference	891
Basic authority certificate profiles	891
Intermediate authority certificate profile.....	893
External subordinate CA certificate profiles.....	895
Subscriber certificate profiles	903
24 Post-quantum key types.....	972
Pure post-quantum algorithms.....	972
Explicit composite algorithms.....	1062
25 Integration report	1097
Base installation integration report.....	1097
CSP CA Gateway integration report	1099
CSP Certificate Authority integration report	1099
CSP Certificate Enrollment Gateway integration report.....	1100
CSP Certificate Manager integration report	1108
CSP Timestamping Authority integration report	1109
CSP Validation Authority integration report.....	1110

1 About this guide

This guide describes installing and managing the Entrust Cryptographic Security Platform (CSP) 1.1.0.

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

Revision information

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

Issue	Date	Section	Changes
1.0	July 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

This feature 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

This feature 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

This feature facilitates certificate lifecycle management and automation. It includes:

- **Discovery** capability to find and discover certificates across diverse platforms.
- An optional add-on, **Control** capability to automate the management of those certificates.

CSP Keys and Secrets Management

This feature 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:**

- **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.
- **DB TDE Keys:** Transparent Data Encryption (TDE) protected databases, including Oracle, MS SQL, MariaDB, and Open-source PostgreSQL, ensuring data-at-rest encryption.
- **VM Encryption Keys:** 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 1.1.0 is the first commercial release of Cryptographic Security Platform.

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

Platform release notes

See below the release notes for the base installation of Cryptographic Security Platform 1.1.0.

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

Platform new features

Cryptographic Security Platform 1.1.0 adds the following new features to the base installation.

- [Thales Luna client driver update \(ATEAM-17147\)](#)
- [Entrust nShield client driver update \(ATEAM-18429\)](#)
- [Grafana upgrade \(EDM-12811\)](#)
- [EntrustOS component update \(EDM-17549\)](#)
- [User management \(EDM-17593\)](#)

Thales Luna client driver update (ATEAM-17147)

This release updates the built-in client driver for the Thales Luna hardware cryptographic module (HSM).

 See [HSM requirements](#) for the list of supported HSM client drivers.

Entrust nShield client driver update (ATEAM-18429)

This release updates the built-in client driver for the Entrust nShield hardware cryptographic module (HSM).

 See [HSM requirements](#) for the list of supported HSM client drivers.

Grafana upgrade (EDM-12811)

This release upgrades the Grafana portal to version 12.0.1.

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

EntrustOS component update (EDM-17549)

This release updates third-party components of the EntrustOS operating system.

 See [Third-party license acknowledgments](#) for some of the third-party components in the EntrustOS operating system.

User management (EDM-17593)

This release adds the following commands for creating and managing system users.

- [clusterctl node user create](#)
- [clusterctl node user delete](#)
- [clusterctl node user info](#)
- [clusterctl node user modify](#)

Platform known issues

The base installation of Cryptographic Security Platform 1.1.0 has the following known issues.

- [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 1.1.0 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

See below the Management Console release notes for Cryptographic Security Platform 1.1.0.

- [Management Console known issues](#)

Management Console known issues

This release has the following Management Console 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.

CA Gateway release notes

See below the CA Gateway release notes for Cryptographic Security Platform 1.1.0.

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

CA Gateway new features

This release adds the following features to CA Gateway.

- [Sectigo CA support \(ATEAM-18339\)](#)
- [Profile selection on request \(ATEAM-18358\)](#)
- [Multiple KeyUsage on request \(ATEAM-18374\)](#)

Sectigo CA support (ATEAM-18339)

This release adds support for integrating Sectigo certificate authorities with CA Gateway.

 See [Integrating a Sectigo CA](#) for details on how to integrate a Sectigo CA.

Profile selection on request (ATEAM-18358)

This release adds support for selecting the user role of certificates issued by an Entrust Security Manager certificate authority.

 See in [Security Manager Profile Properties](#) how to select the profile using the **User type** setting.

Multiple KeyUsage on request (ATEAM-18374)

This release adds support for a plaintext comma-separated list of KeyUsage values on enrollment requests.

CA Gateway fixed bugs

This release fixes the following CA Gateway bugs.

- [Error when revoking certificates without Subject \(ATEAM-11625\)](#)
- [Unspecified validation error \(ATEAM-17472\)](#)

Error when revoking certificates without Subject (ATEAM-11625)

CA Gateway returns an error when trying to revoke a certificate with an empty Subject field.

Unspecified validation error (ATEAM-17472)

When entering a malformed value in the [Choose a key name](#) field, the Management Console displays a generic "Please match the requested format" breadcrumb message without indicating the source of the error.

Bug fixing: explicitly indicate that the CA key value must include only lowercase letters, numbers, and dashes ("-").

CA Gateway known issues

CA Gateway for Cryptographic Security Platform 1.1.0 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 Authority release notes

See below the Certificate Authority release notes for Cryptographic Security Platform 1.1.0.

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

Certificate Authority new features

This release adds the following new feature to Certificate Authority.

Support for 3-tier PKIs (ATEAM-18489)

This release adds support for creating 3-tier Public Key Infrastructure (PKI) hierarchies.

Certificate Authority fixed bugs

This release fixes the following Certificate Authority bugs.

- [HSM configuration requires an RFS server \(ATEAM-17470\)](#)
- [Image error \(ATEAM-18520\)](#)

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.

Bug resolution: add new configuration options under [HSM](#).

Image error (ATEAM-18520)

Cryptographic Security Platform installations with the Certificate Authority solution deployed throw the following error.

```
kubelet Failed to pull image \"localhost:300000/pkihub/init-attila:v202503271109\":  
rpc error: code = NotFound desc = failed to pull and unpack image
```

Certificate Authority known issues

This release has the following Certificate Authority 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 \(ATEAM-17445\)](#)
- [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.

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.

Certificate Manager release notes

See below the Certificate Manager release notes for Cryptographic Security Platform 1.1.0.

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

Certificate Manager new features

This release adds the following Certificate Manager features.

- [Fingerprint of the destination keys displayed on creation \(ATEAM-3217\)](#)
- [Header row added to empty reports \(ATEAM-17510\)](#)
- [Key Manager selection separated from Destinations \(ATEAM-18208\)](#)
- [High availability support \(ATEAM-18346\)](#)
- [Profile ID column added to the certificates grid \(ATEAM-18472\)](#)
- [New option to close all messages \(ATEAM-18474\)](#)
- [Column sorting improved usability \(ATEAM-18475\)](#)

Fingerprint of the destination keys displayed on creation (ATEAM-3217)

When you click the **Verify** button, the destination creation form displays the fingerprint of the destination SSH key, allowing you to verify it before adding the destination.

Header row added to empty reports (ATEAM-17510)

Certificate reports without records include a row header to ensure they are not confused with failed reports.

Key Manager selection separated from Destinations (ATEAM-18208)

Key Management Systems are no longer included in the **Destinations** list. They are now included in an independent list, allowing users to select both a Key Management System and a destination.

High availability support (ATEAM-18346)

On multinode installations, each pod runs with two replicas to ensure high availability.

Profile ID column added to the certificates grid (ATEAM-18472)

The new **Profile ID** column on the **Certificates** page displays the name of each certificate profile and supports filtering and sorting.

New option to close all messages (ATEAM-18474)

A new **Close all messages** button allows closing all the toasts in the breadcrumb area.

Column sorting improved usability (ATEAM-18475)

The headers of console grids (for certificates, sources, destinations, etc.) better indicate which columns support sorting. Specifically, sortable headers display a "This column is sortable" message when the mouse hovers over them.

Certificate Manager fixed bugs

This release fixes the following Certificate Manager bugs.

- [Matching tags not sorted \(ATEAM-18116\)](#)
- [Missing keyboard accessibility options \(ATEAM-18302\)](#)
- [Mandatory fields not validated \(ATEAM-18315\)](#)
- [No charts displayed on widgets \(ATEAM-18328\)](#)
- [Shared partitions not supported on path \(ATEAM-18348\)](#)
- [Certificate autorenewal cannot be disabled \(ATEAM-18470\)](#)
- [Multiple DNS in SAN not supported \(ATEAM-18674\)](#)
- [Authentication error in the user console \(ATEAM-18726\)](#)

Matching tags not sorted (ATEAM-18116)

When typing a tag name, the **Authorized Tag** field does not display a sorted list of the matching tags.

Missing keyboard accessibility options (ATEAM-18302)

The user cannot select a **Destination** using the keyboard accessibility options instead of the mouse.

Mandatory fields not validated (ATEAM-18315)

The generated public enrollment forms do not validate the mandatory fields.

No charts displayed on widgets (ATEAM-18328)

The widgets of the **Certificates** page display the "NaN%" string instead of a chart.

 Click >> **Show Insights** on the **Certificates** page to display the widgets.

Shared partitions not supported on path (ATEAM-18348)

Destinations of the **F5-BIG-IP-Destination-Plugin** type do not support shared partitions on the path.

Certificate autorenewal cannot be disabled (ATEAM-18470)

When creating a certificate, the wizard does not display the renewal options if `key_client_generated` is set to `true` in the selected profile.

Multiple DNS in SAN not supported (ATEAM-18674)

When requesting a certificate using a public enrollment form, the SAN (Subject Alternative Names) field only supports one DNS value.

Authentication error in the user console (ATEAM-18726)

After deploying Certificate Manager, the user may be unable to log in to the user console due to an authentication error.

Certificate Manager known issues

This release has the following Certificate Manager 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 \(ATEAM-16039\)](#)
- [Wildcard certificates not recorded \(ATEAM-16436\)](#)
- [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 \(ATEAM-16930\)](#)
- [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 \(ATEAM-17030\)](#)

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.

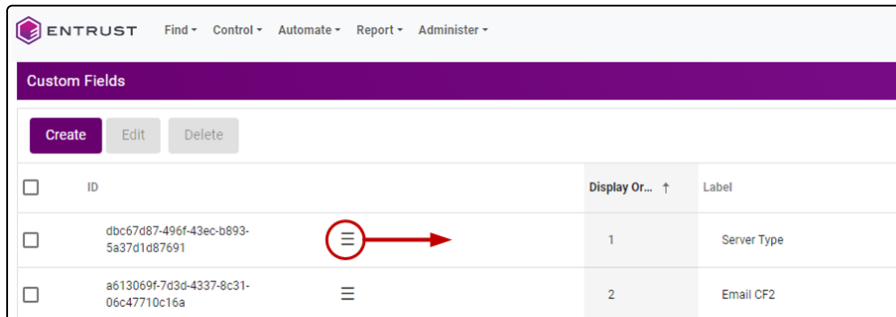
Issues when changing the display order of custom fields (ATEAM-15463)

In the **Custom Fields** page of the web console, 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.

Wildcard certificates not recorded (ATEAM-16436)

The application does not record wildcard certificates successfully scanned by the Discovery Scanner.

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

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 **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.

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 using 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 using 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 Enrollment Gateway release notes

See below the Certificate Enrollment Gateway release notes for Cryptographic Security Platform 1.1.0.

- [Certificate Enrollment Gateway known issues](#)

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 (ECSPR-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.

Timestamping Authority release notes

See below the Timestamping Authority release notes for Cryptographic Security Platform 1.1.0.

- [Timestamping Authority known issues](#)

 As explained in [Platform new features](#), this release updates the HSM client software.

Timestamping Authority known issues

This release has the following Timestamping Authority known issues.

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

Large kmdata files not supported (ATEAM-16338)

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

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.

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.

Validation Authority release notes

See below the Validation Authority release notes for Cryptographic Security Platform 1.1.0.

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

 As explained in [Platform new features](#), this release updates the HSM client software.

Validation Authority new features

This release adds the following Validation Authority features.

- [Support for signed OCSP requests \(ATEAM-17356\)](#)
- [Support for ECDSA-SHA384 \(ATEAM-18218\)](#)

Support for signed OCSP requests (ATEAM-17356)

This release adds support for accepting and validating signed OCSP requests.

Support for ECDSA-SHA384 (ATEAM-18218)

This release adds ECDSA-SHA384 as a supported hash algorithm for signing OCSP responses.

 See [OCSP Responder](#) for the list of supported hash algorithms.

Validation Authority fixed bugs

This release fixes the following Validation Authority bug.

Error when importing the CA certificate (ATEAM-18600)

Validation Authority throws an error when importing the certificate of the CA that issues the validated certificates.

Validation Authority known issues

This release has the following Validation Authority known issues.

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

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.

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 `evactl 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.

evactl logs not forwarded to Splunk (EDM-13275)

When integrated with a Splunk server, Cryptographic Security Platform does not forward logs recording `evactl` 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.

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
```

Log Forwarder release notes

See below the Log Forwarder release notes for Cryptographic Security Platform 1.1.0.

- [Log Forwarder new features](#)

Log Forwarder new features

This release adds the following Log Forwarder features.

- [Fluentbit upgrade \(EDM-14965\)](#)
- [Syslog support \(EDM-16732\)](#)

Fluentbit upgrade (EDM-14965)

This release upgrades to 4.0.2 the Fluentbit version of the Log Forwarder solution.

 See <https://fluentbit.io/announcements/v4.0.2> for details on the Fluentbit 4.0.2 release.

Syslog support (EDM-16732)

This release adds support for forwarding logs to a Syslog-compatible SIEM (Security Information and Event Management) server.

 See [SIEM requirements](#) for the list of supported SIEM servers.

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, a 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 https://etcd.io/docs/v3.4/metrics/#disk , 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.

When configuring the load balancer:

- Check the node health with `curl` as explained in [Checking the node health](#).
- Use sticky web connections to prevent issues in node switching.

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 Cryptographic Security Platform administrator	SSH

Target Port	Protocol	Source	Target service
443	TCP/ HTTPS	The IP of the Grafana and Management Console users	Grafana and the Management Console
15021	HTTP	The IP of the Cryptographic Security Platform administrator	Health endpoint (see Checking the node health)

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
30000	TCP	localhost	localhost
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

i 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)

Target Port	Protocol	Source	Target Service
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

Subnet	Reserved use
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.

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

Certificate Authority requirements

Entrust CA is currently the only issuing Certificate Authority supported by CSP Validation Authority.

Compliance Manager requirements

Cryptographic Security Platform 1.1.0 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 TLS certificate](#)
- [Database names](#)

✗ Certificate Authority and Certificate Manager cannot share the same database.

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+	✗
Certificate Manager	✗	15+	✗
Validation Authority	21.3.0	14.3 or 15.10	2019 CU15
			2022 CU13
Certificate Enrollment Gateway	✗	15+	2019+
			2022+

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 the DBMS documentation for the DBMS requirements on each platform. In the case of PostgreSQL, we recommend downloading the official Docker image:

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

If you are not using this Docker image, make sure to install the `pg_trgm` extension by running this command.

```
sudo dnf install postgresql15-contrib
```

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 TLS certificate

In TLS-protected connections with the database, the TLS 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](#)
- [Syslog](#)

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

Splunk

Cryptographic Security Platform can forward logs to the following Splunk services.

- Splunk Enterprise
- Splunk Cloud

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

Syslog

Cryptographic Security Platform can forward logs to Syslog-compatible services like Datadog.

 As explained in [Log Server](#), Cryptographic Security Platform supports the [RFC 5424](#) and [RFC3164](#) implementations of this protocol.

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	Windows	Mac O
Apple Safari	5 or higher	5 or higher
Google Chrome	8 or higher	8 or higher
Microsoft Edge	The stable versions listed by Microsoft in https://learn.microsoft.com/en-us/deployedge/microsoft-edge-support-lifecycle	Not supported
Mozilla Firefox	9 or higher	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)

See the following table for supported versions.

Hardware	Client driver	Firmware	CA	TSA	VA
Entrust nShield Connect XC	13.7.3 (FIPS 140-2 Level 3 mode supported)	12.60.15 & 12.60.2	✓	✓	✓
Entrust nShield 5c	13.7.3	13.2.4	✓	✓	✓
Thales Luna HSM 7	10.7.0	7.7.1-20	✗	✓	✓

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](#).

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 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 1.1.0 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 a Cryptographic Security Platform virtual machine on Hyper-V](#)
 - [Configuring the boot mode on Microsoft Hyper-V](#)
 - [Starting a Cryptographic Security Platform machine on Hyper-V](#)
3. Configure the image installation as explained in [Configuring a Cryptographic Security Platform ISO image installation](#).

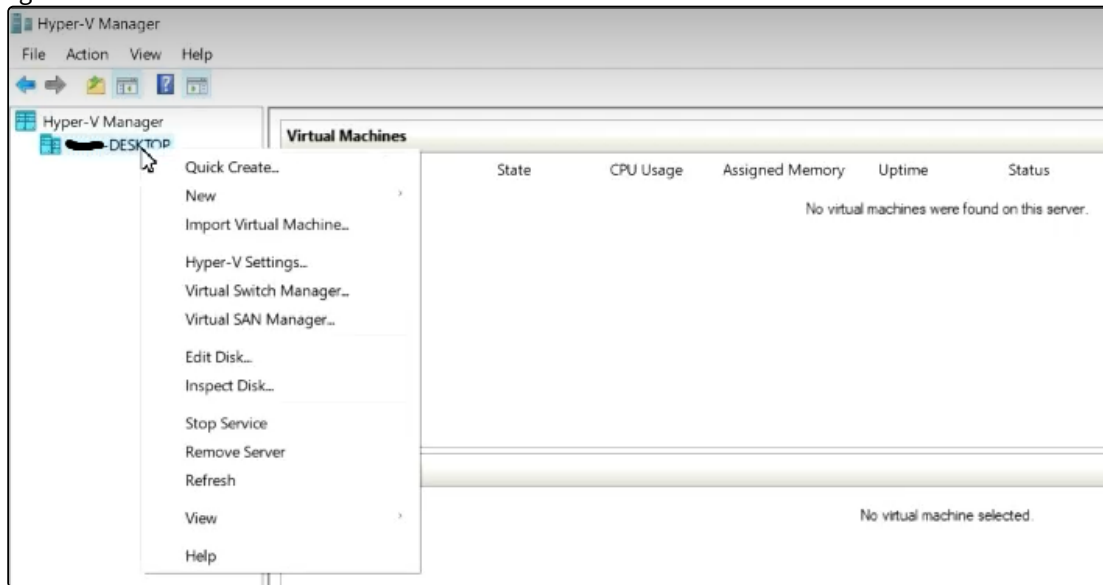
Creating a virtual machine on Hyper-V

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

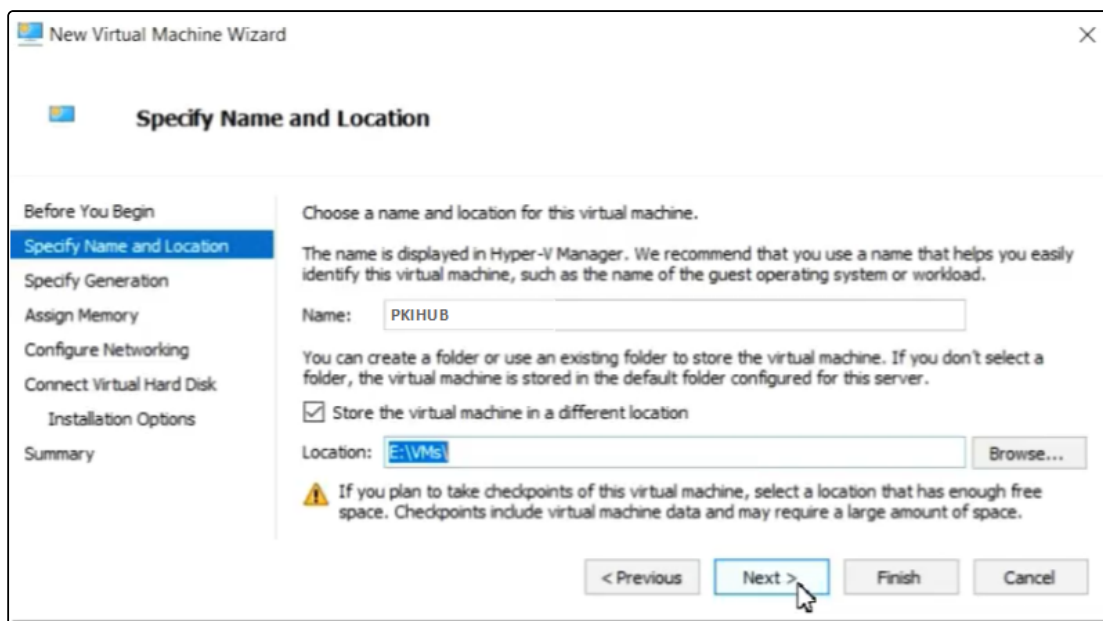
1. Open the **Hyper-V Manager** console.

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

Field	Root disk	etcd disk
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

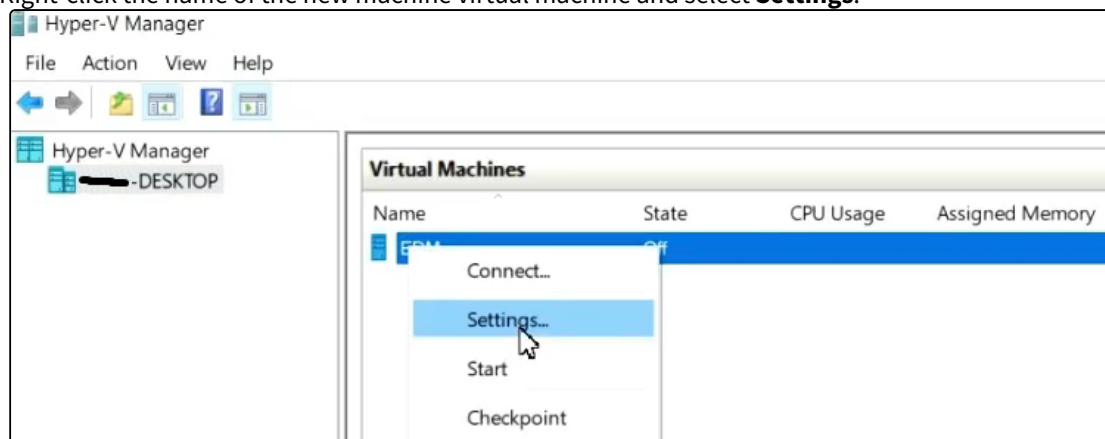
Review the selected settings and click **Finish** to complete the virtual machine creation.

Configuring a Cryptographic Security Platform virtual machine on Hyper-V

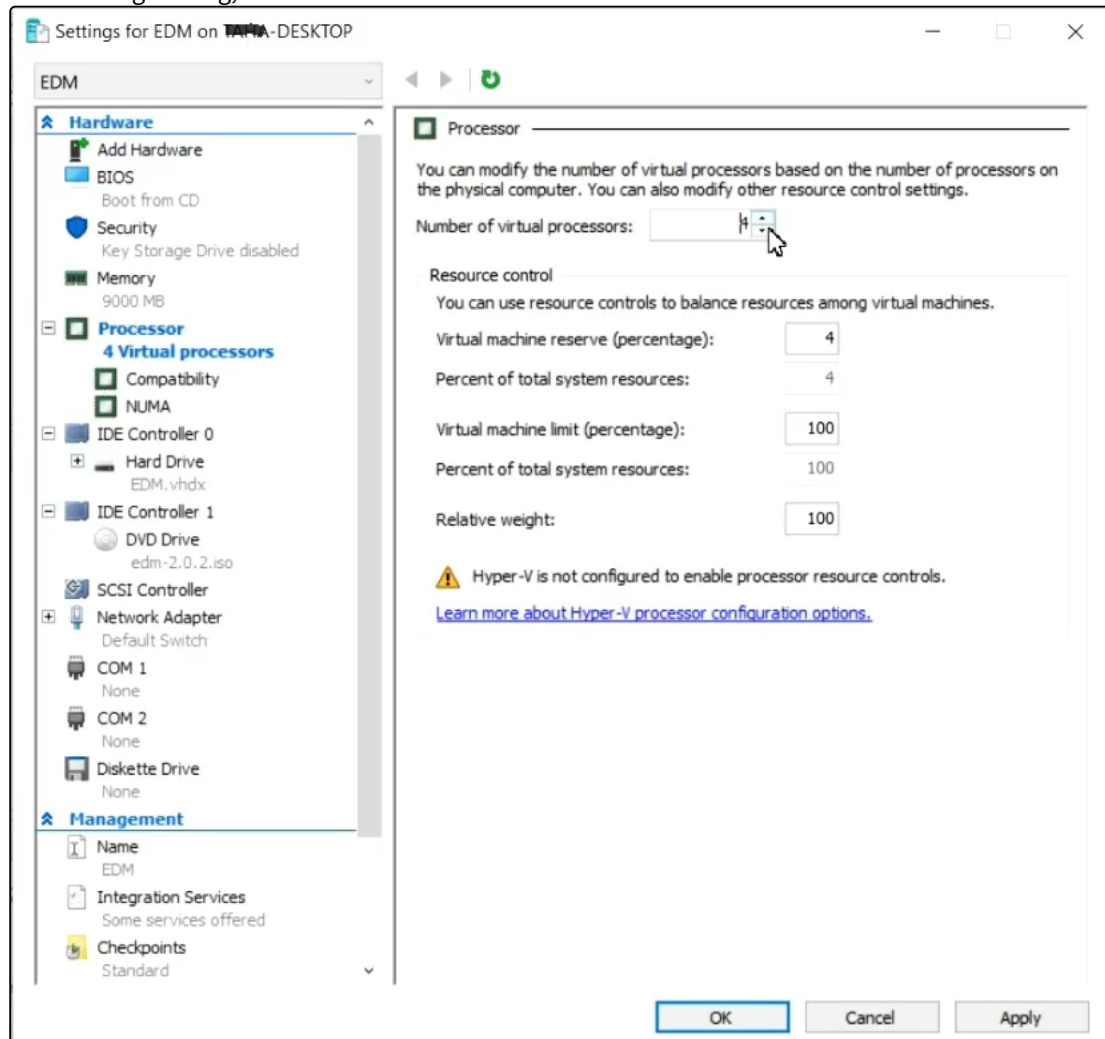
Once created, complete the new Cryptographic Security Platform virtual machine as follows.

To configure a 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

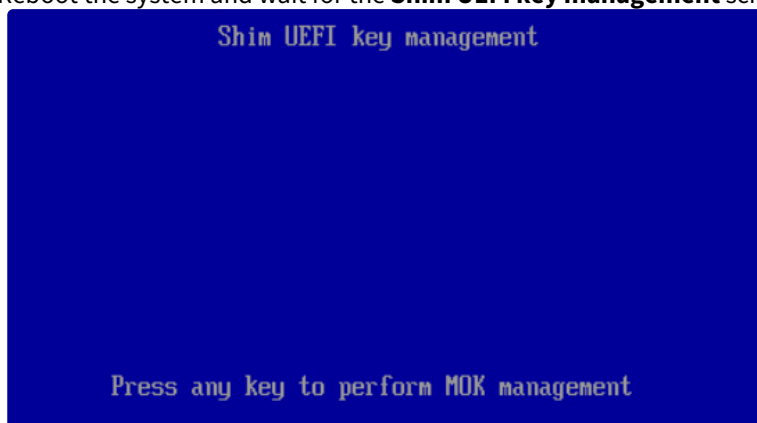
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

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

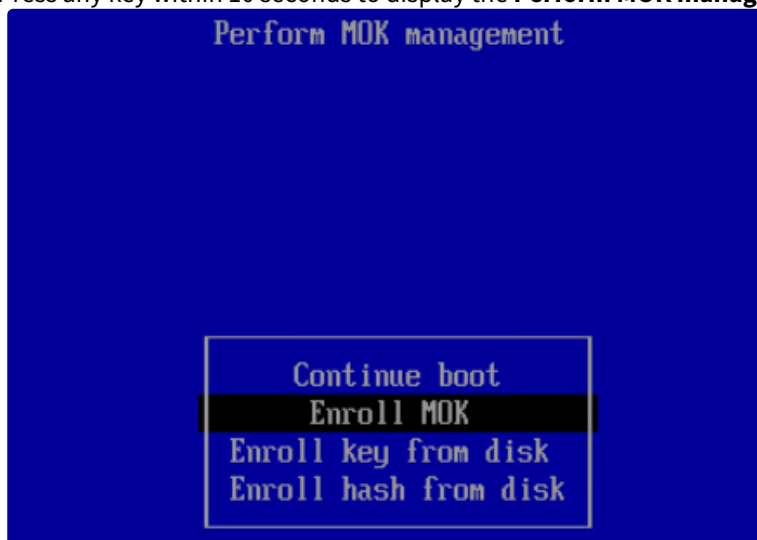
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

 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.

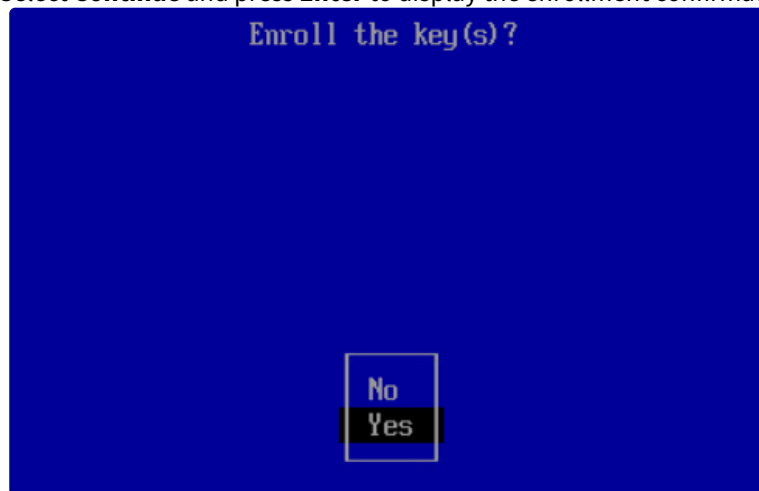


9. Select **View key 0** and press **Enter** to display the key information.

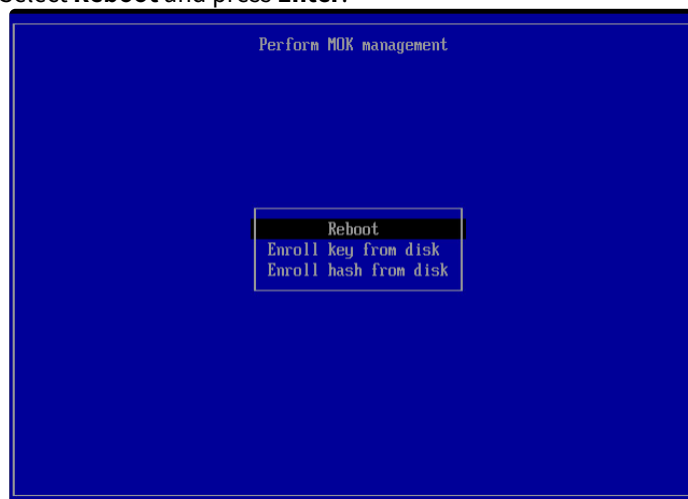


10. Check that the serial number is `0xe9d471cfb4fe136c`.
11. Check that the SHA1 fingerprint is `e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7`.
12. Press **ESC** to return to the **Enroll MOK** dialog.

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**.



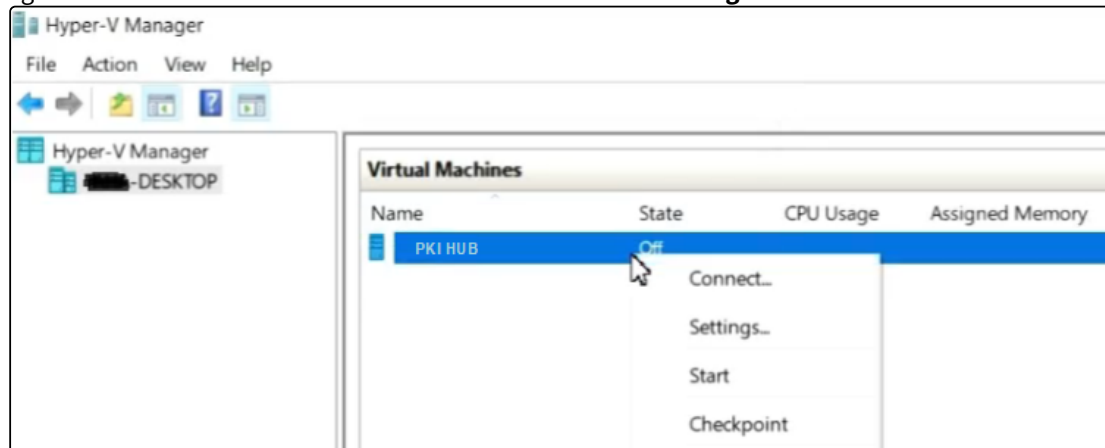
Starting a Cryptographic Security Platform machine on Hyper-V

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

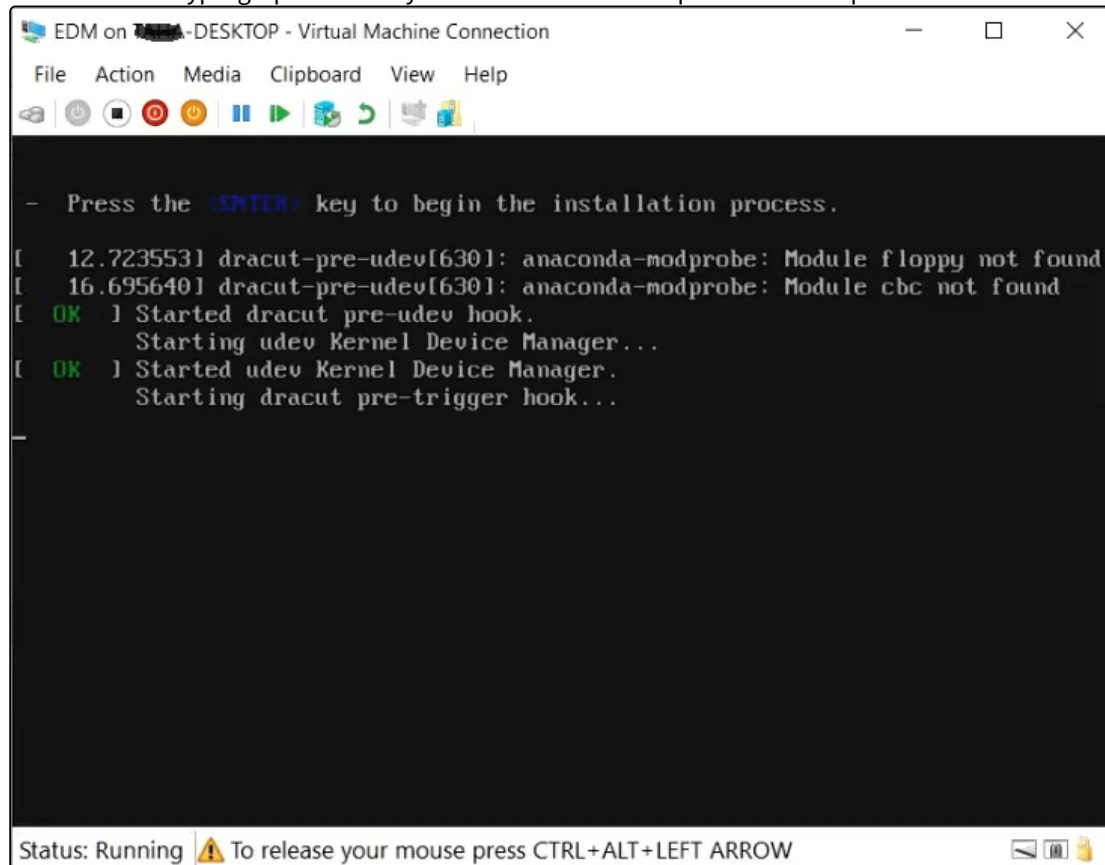
To start a Cryptographic Security Platform virtual machine on Hyper-V

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

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



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



- Login 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](#).

Installing the Cryptographic Security Platform ISO image on Nutanix

See below for installing and configuring a 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 a 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](#)

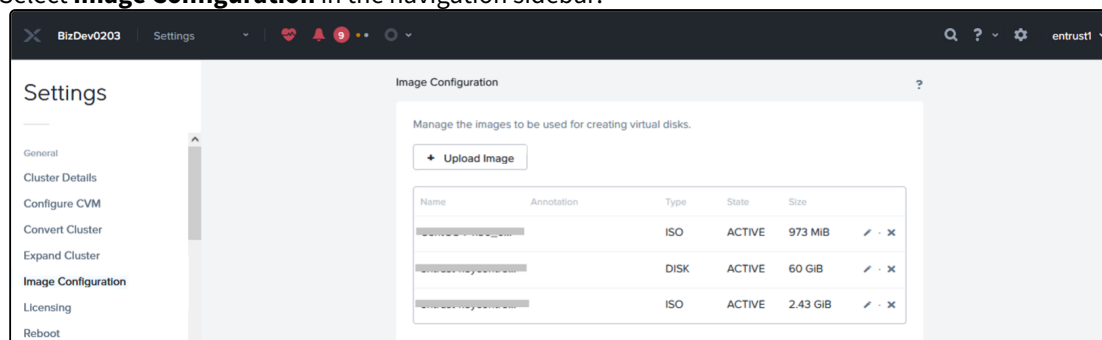
i As explained in [Creating a cluster of Cryptographic Security Platform virtual machines with Nutanix Prism Central](#), uploading the image to Nutanix Prism Central allows you to create a cluster of Cryptographic Security Platform machines.

Uploading the Cryptographic Security Platform ISO image with Nutanix Prism Element

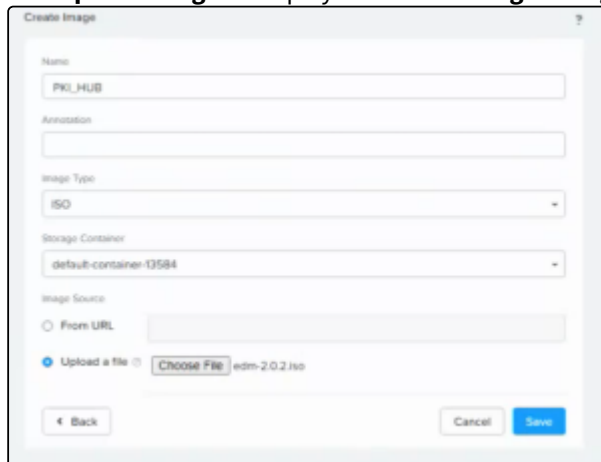
Follow the steps below to upload the Cryptographic Security Platform ISO image using the Nutanix Prism Element portal.

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	Image Type	State	Size	Actions
cryptosecure-iso	ISO	ACTIVE	340 KiB	✎ ✖ ✕
cryptosecure-disk	DISK	ACTIVE	16 GiB	✎ ✖ ✕
cryptosecure-disk	DISK	ACTIVE	16 GiB	✎ ✖ ✕
cryptosecure-disk	DISK	ACTIVE	60 GiB	✎ ✖ ✕
cryptosecure-disk	DISK	ACTIVE	81 GiB	✎ ✖ ✕
cryptosecure-disk	DISK	ACTIVE	81 GiB	✎ ✖ ✕
cryptosecure-disk	DISK	INACTIVE	-	✎ ✖ ✕
PKI_HUB	ISO	ACTIVE	5.36 GiB	✎ ✖ ✕
cryptosecure-disk	DISK	ACTIVE	100 GiB	✎ ✖ ✕
cryptosecure-disk	DISK	ACTIVE	100 GiB	✎ ✖ ✕

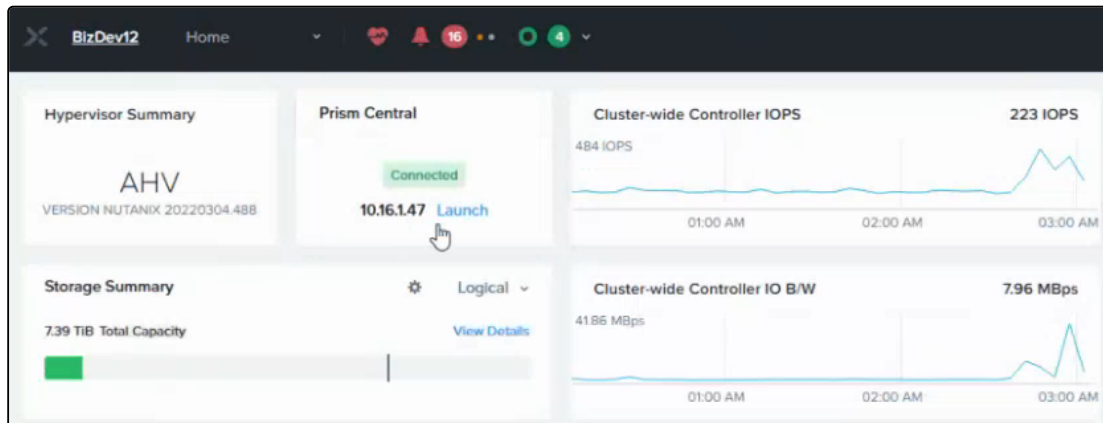
Uploading the Cryptographic Security Platform image file with Nutanix Prism Central

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

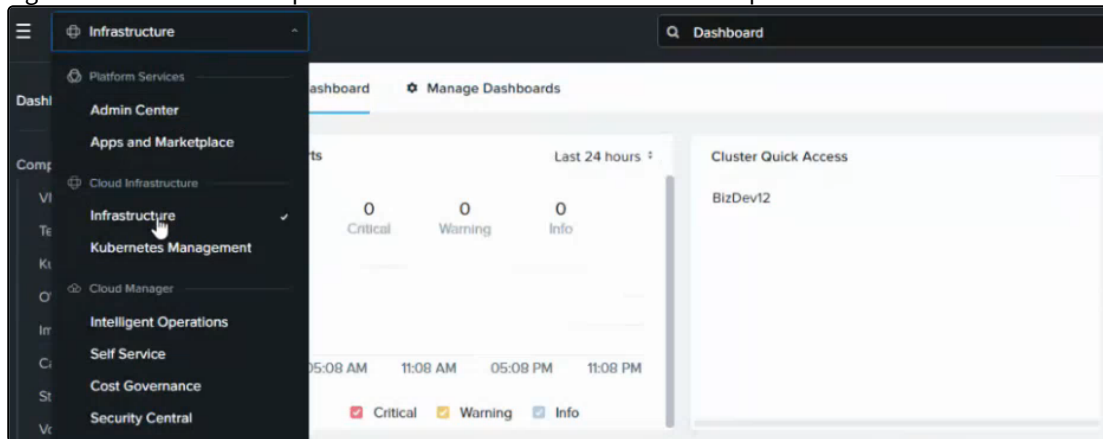
To upload the Entrust Cryptographic Security Platform image file with Nutanix Prism Central

- Log into your Nutanix Prism element web portal.

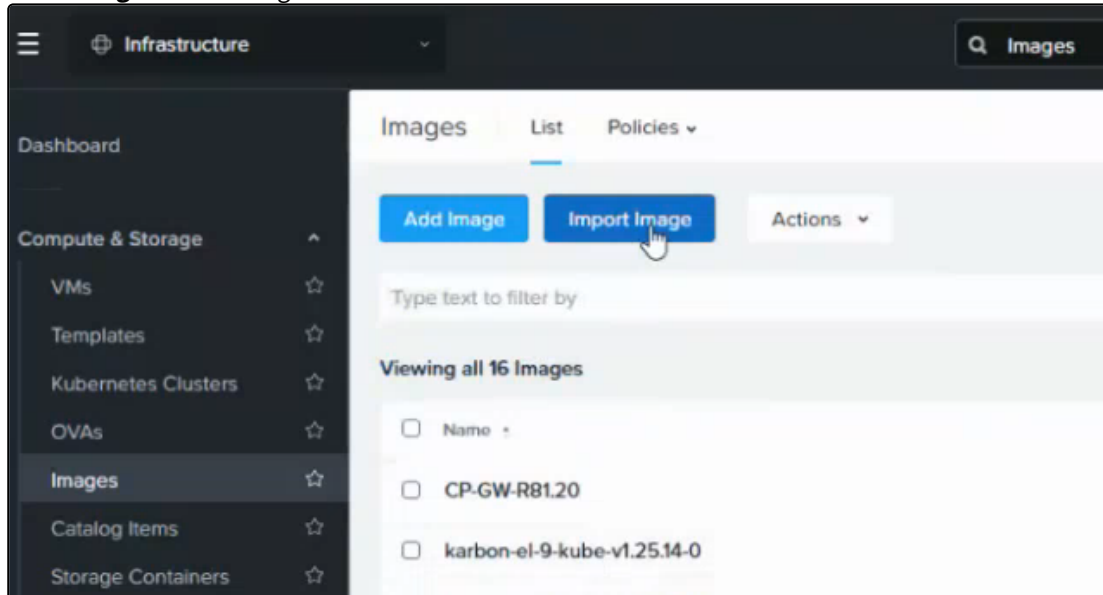
- Click **Launch** under **Prism Central**.



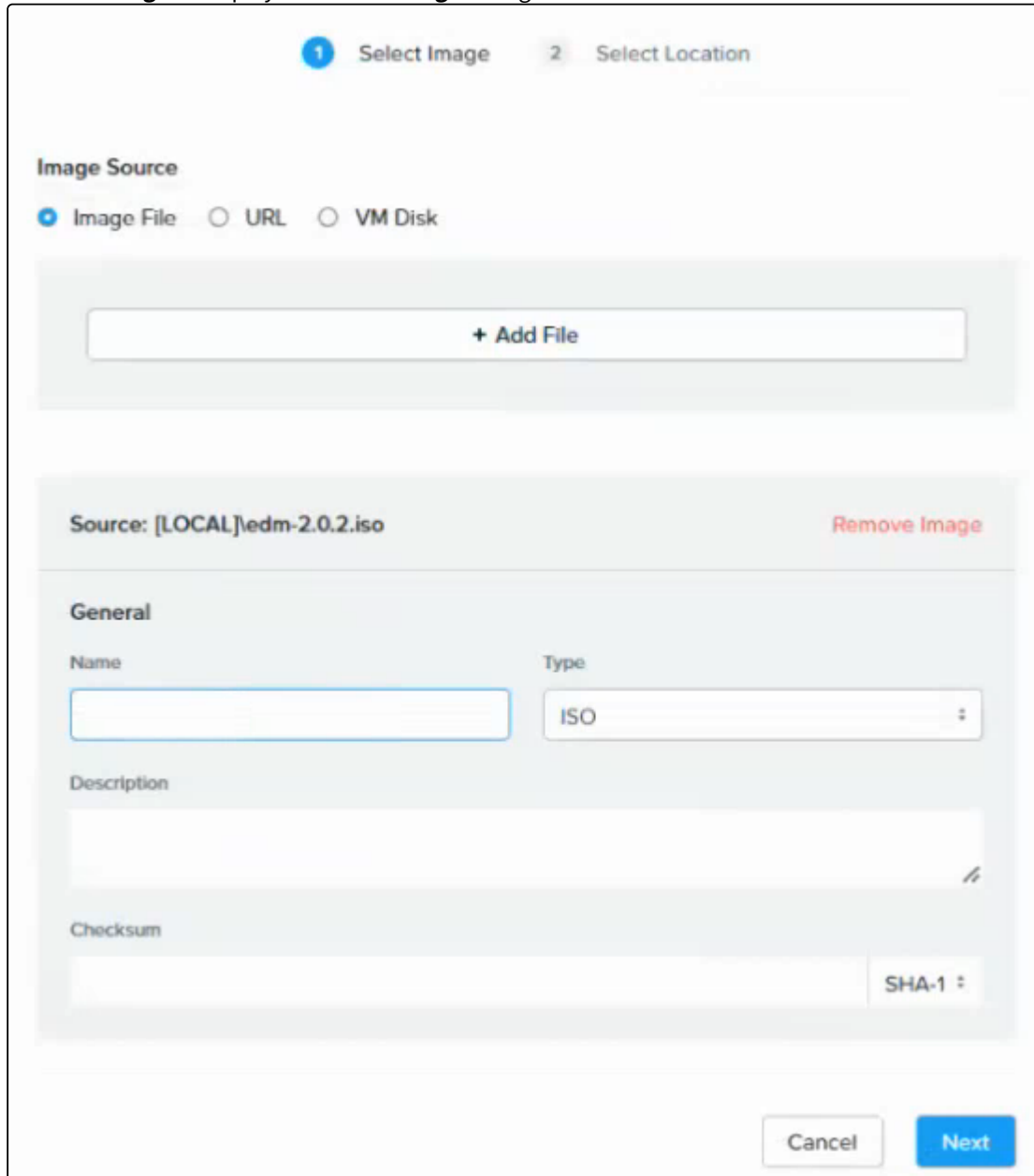
- Log into the Prism Central portal and select **Infrastructure** in the top-left menu.



- 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

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

General

Name

Type

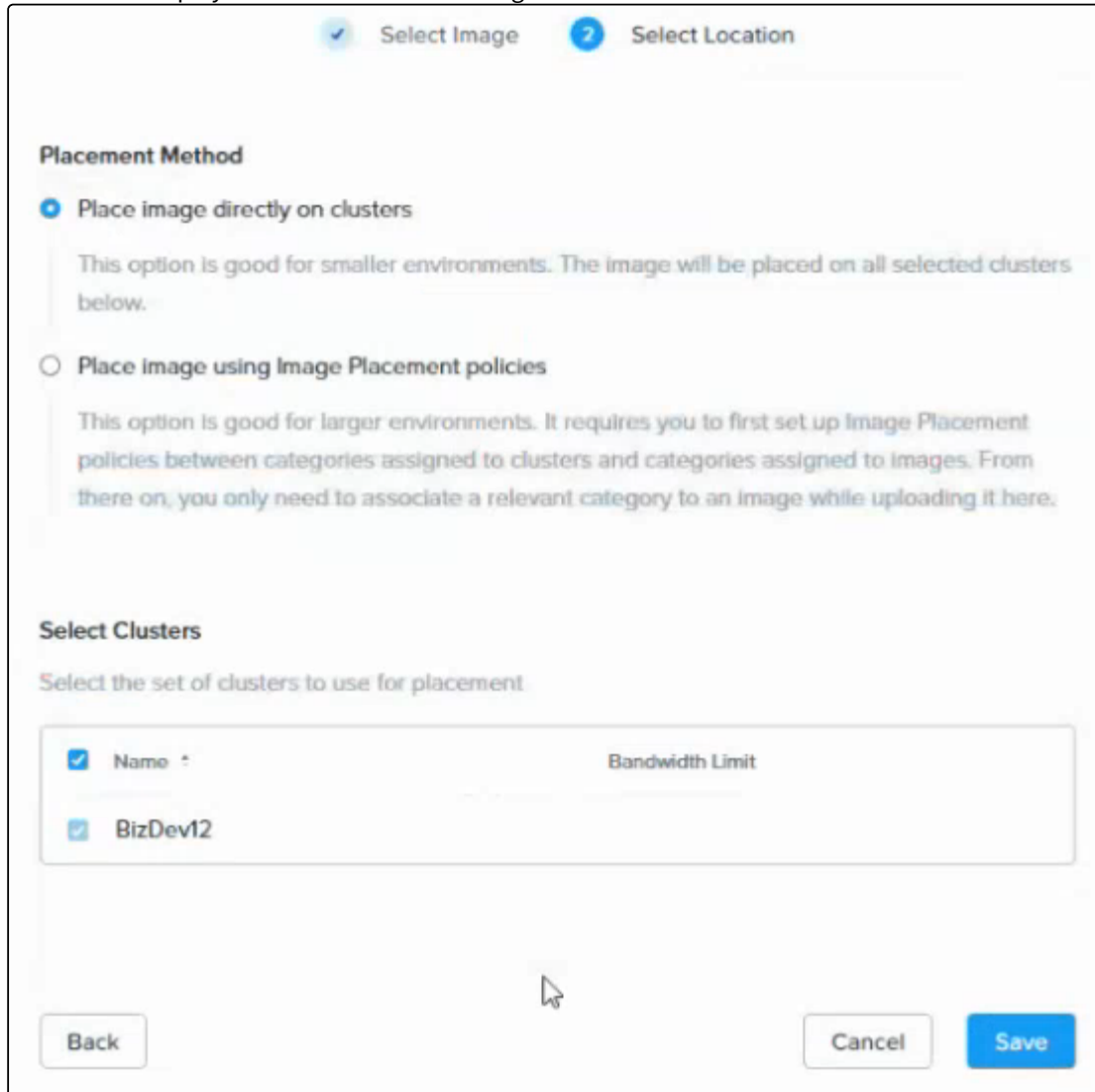
Description

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.

☒ Name	Bandwidth Limit
☒ 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.

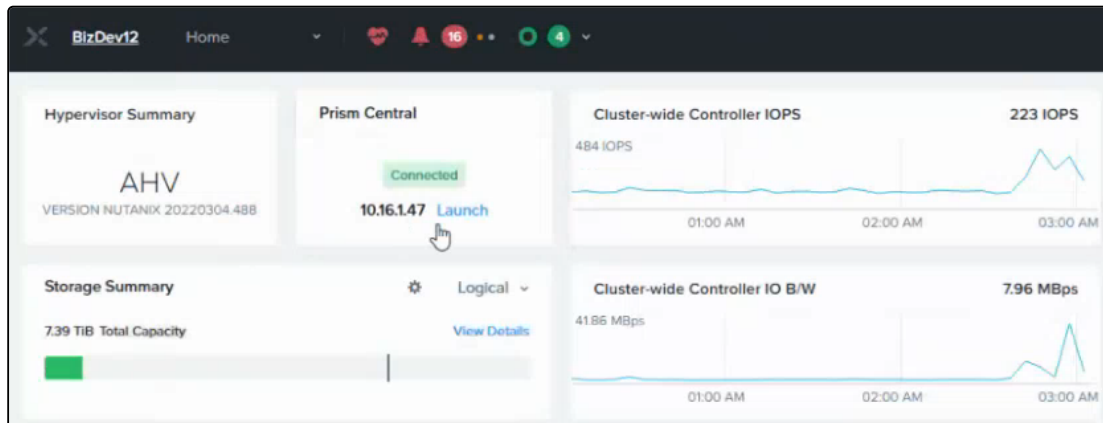
Importing the Cryptographic Security Platform image to Nutanix Prism Central

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.

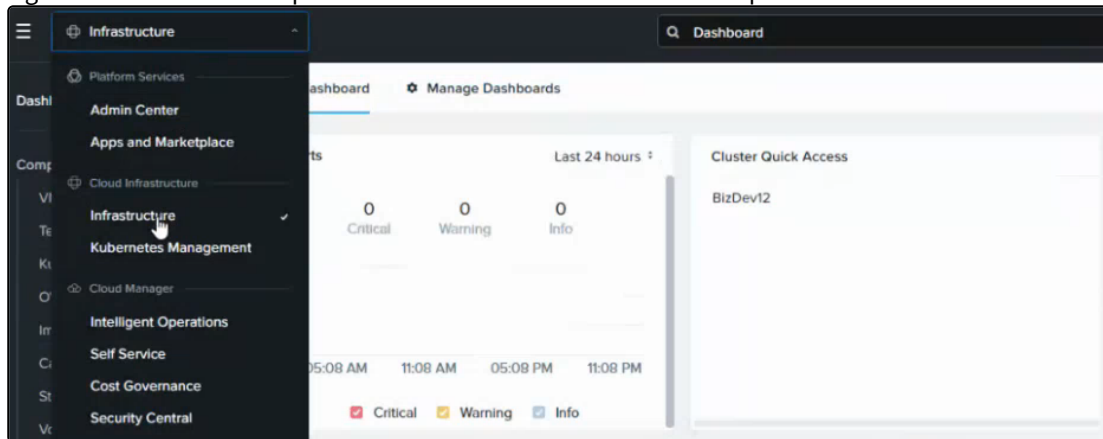
To import the Entrust Cryptographic Security Platform image from Nutanix Prism Element to Nutanix Prism Central

1. Log into your Nutanix Prism element web portal.

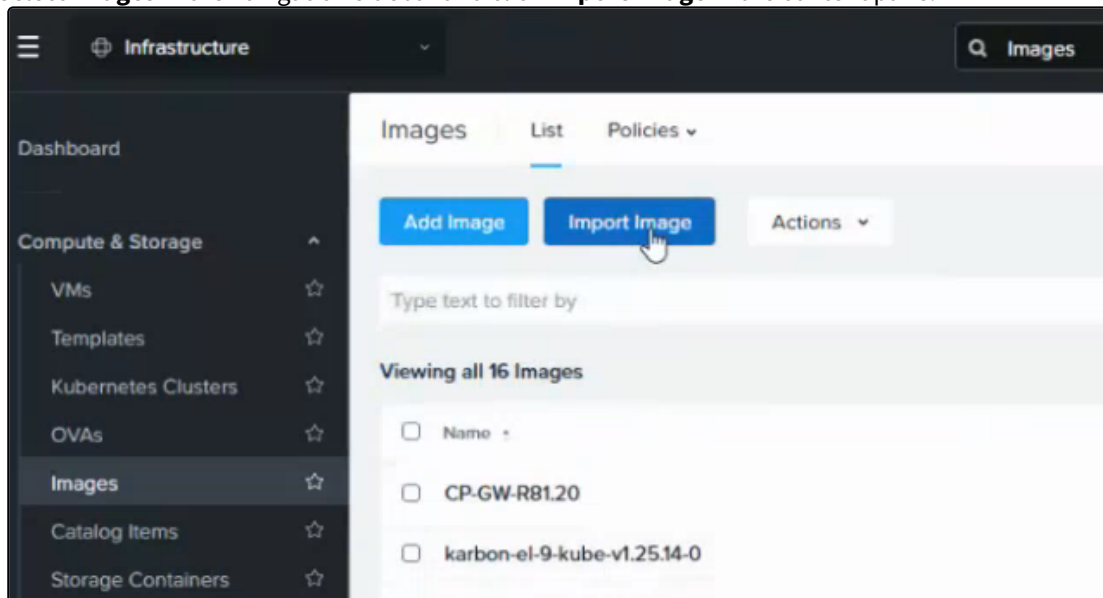
- Click **Launch** under **Prism Central**.



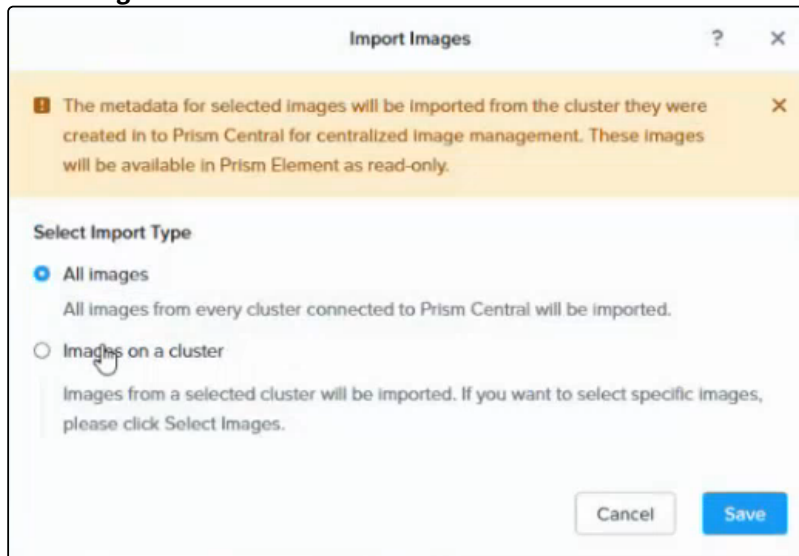
- Log into the Prism Central portal and select **Infrastructure** in the top-left menu.



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



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



Import Images

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.

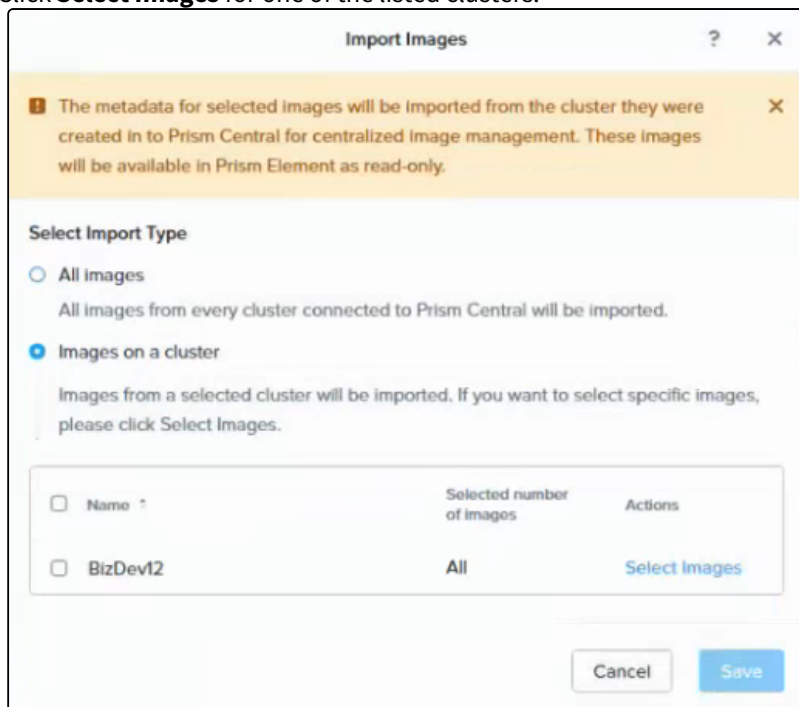
Select Import Type

☒ 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

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.

Select Import Type

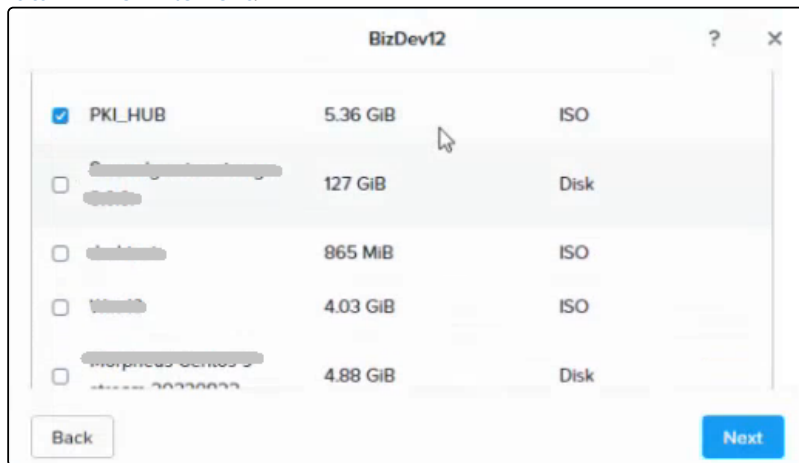
☐ All images
All images from every cluster connected to Prism Central will be imported.

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

☐	Name	Selected number of images	Actions
☐	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 a Cryptographic Security Platform virtual machine on Nutanix

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

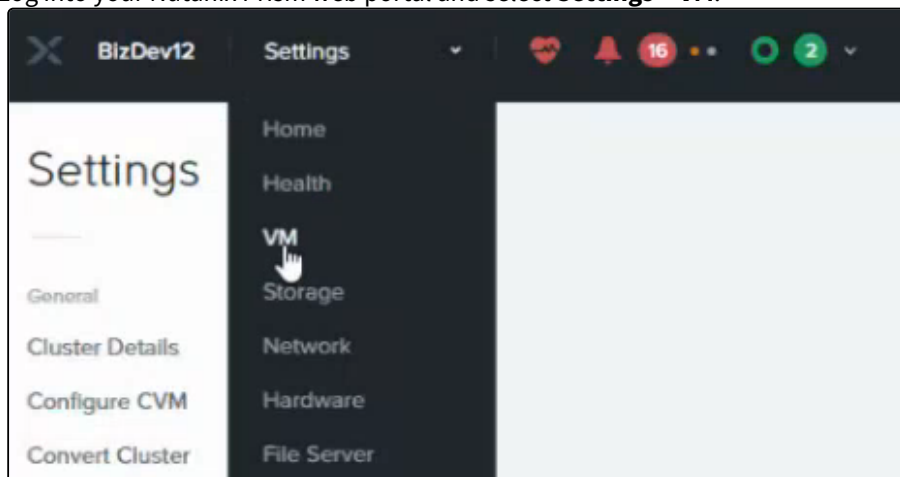
- [Creating a Cryptographic Security Platform virtual machine with Nutanix Prism Element](#)
- [Creating a cluster of Cryptographic Security Platform virtual machines with Nutanix Prism Central](#)

Creating a Cryptographic Security Platform virtual machine with Nutanix Prism Element

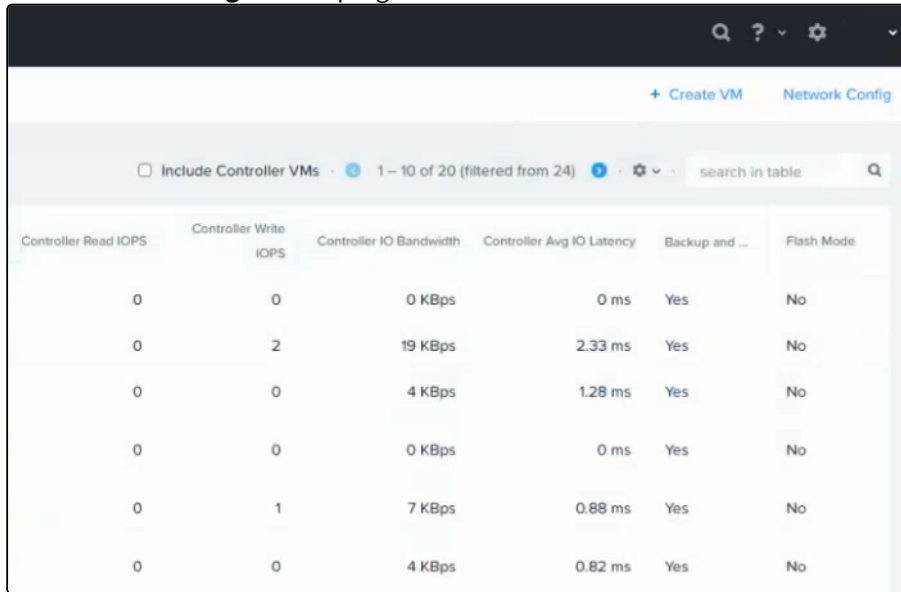
Follow the steps below to deploy the Cryptographic Security Platform image as a virtual image with the Nutanix Prism Element portal.

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

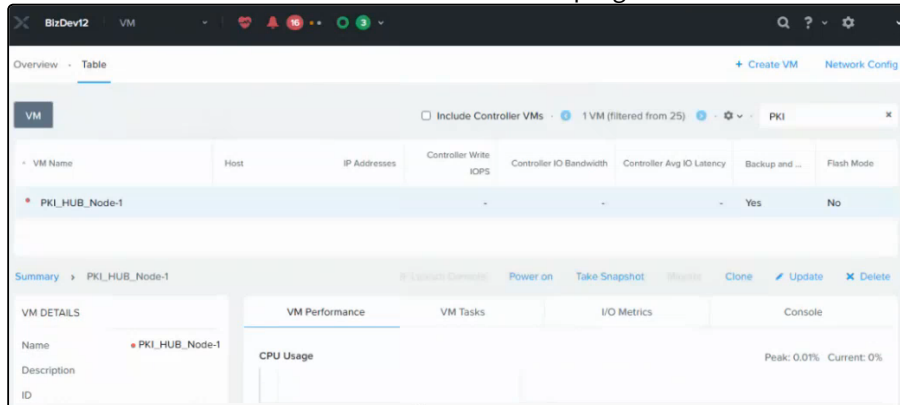
Compute Details

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.
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 .

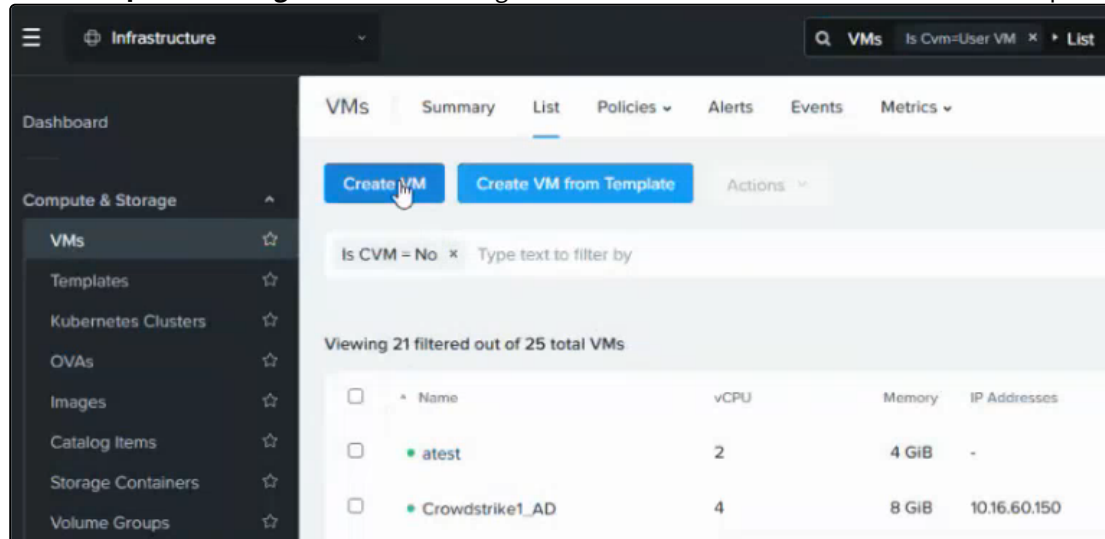
Click **+ Set Affinity** to select the host that will run the virtual machine.

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.
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

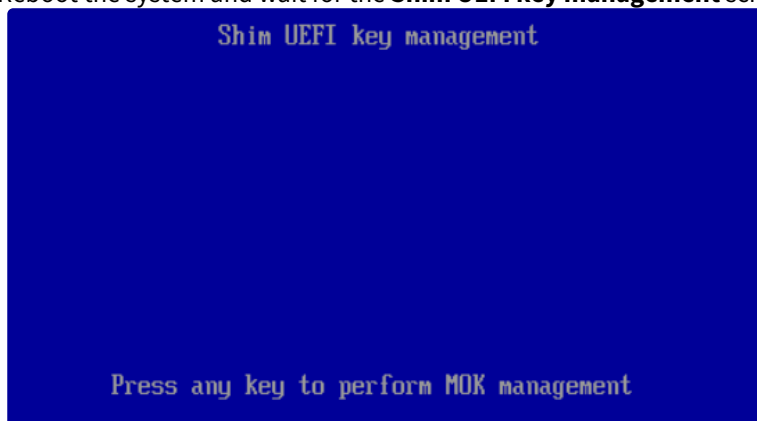
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

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

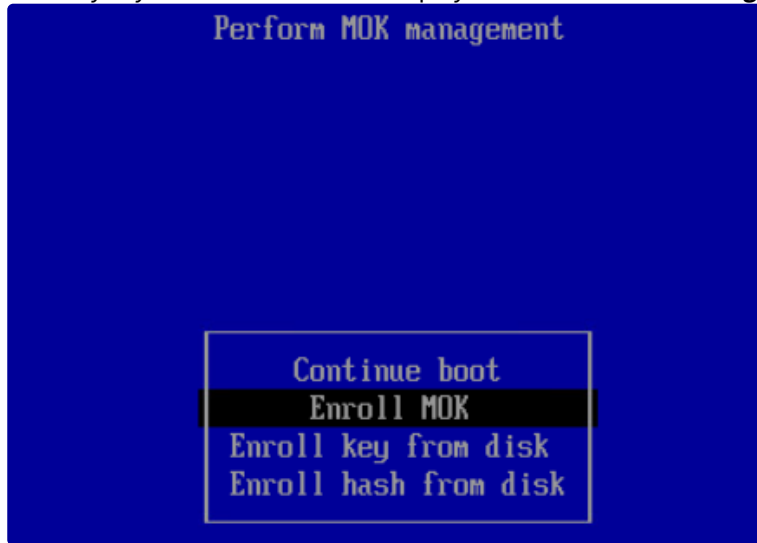
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

 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.



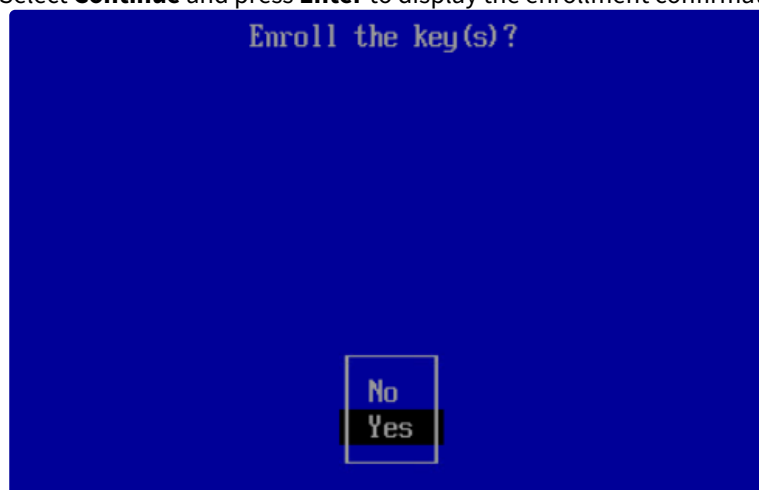
8. Select **Enroll MOK** and press **Enter** to display the **Enroll MOK** dialog.



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

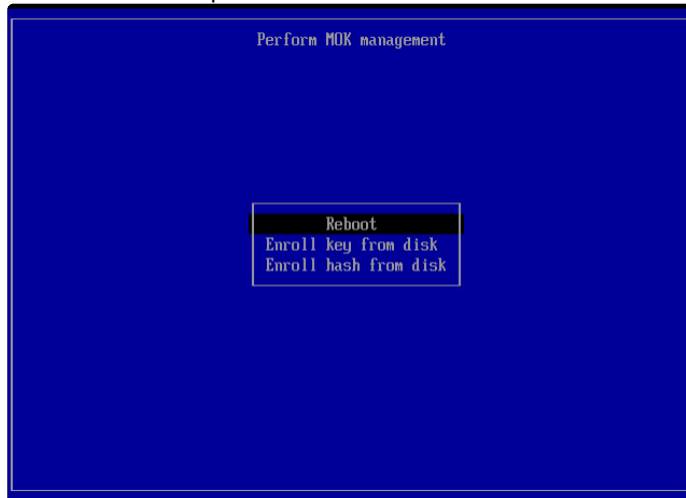


10. Check that the serial number is 0xe9d471cfb4fe136c .
11. Check that the SHA1 fingerprint is e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7 .
12. Press ESC to return to the **Enroll MOK** dialog.
13. Select **Continue** and press **Enter** to display the enrollment confirmation dialog.



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

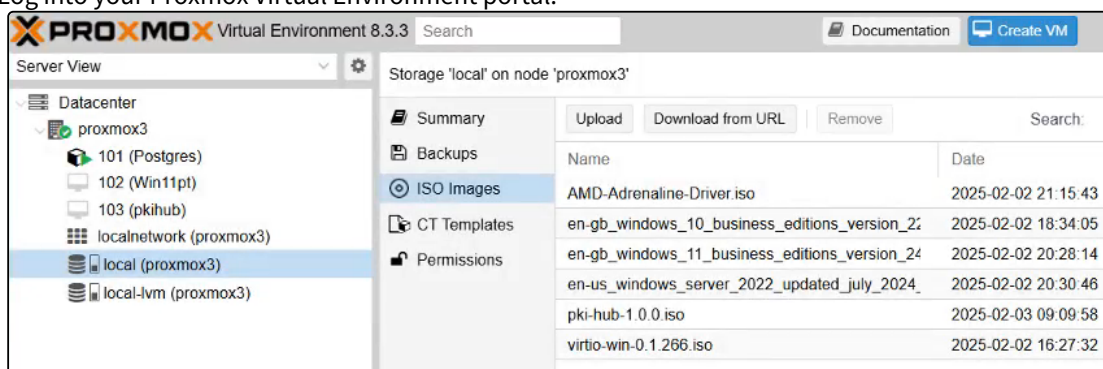
1. Download the ISO image, as explained in [Downloading the installation files](#).
2. Follow the below steps.
 - [Creating an virtual machine on Proxmox](#)
 - [Configuring the boot mode on Promox](#)
 - [Logging into Cryptographic Security Platform on Proxmox](#)
3. Configure the image installation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

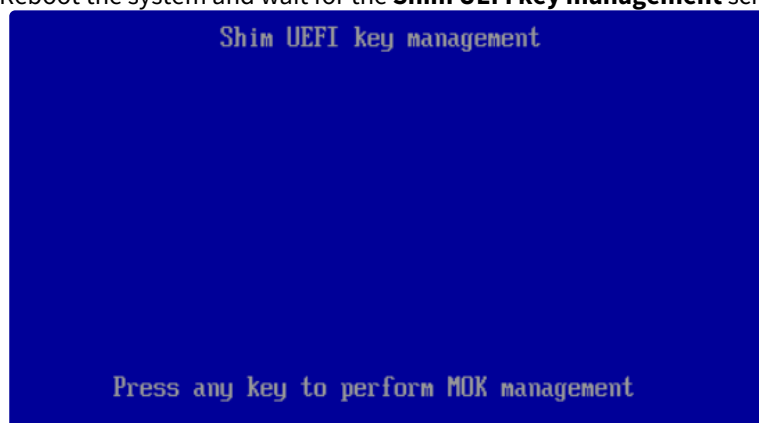
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

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

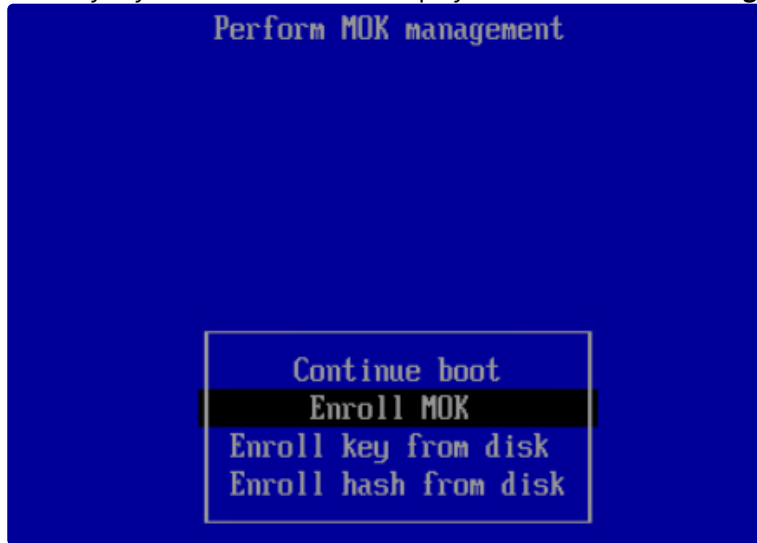
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

 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.



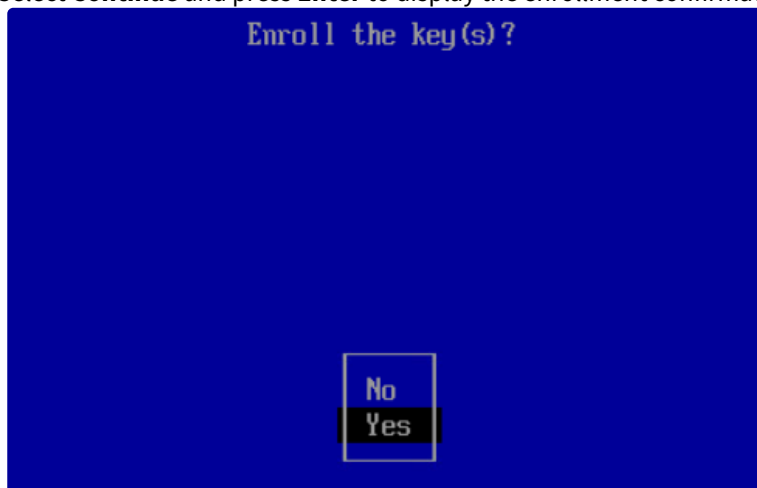
8. Select **Enroll MOK** and press **Enter** to display the **Enroll MOK** dialog.



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

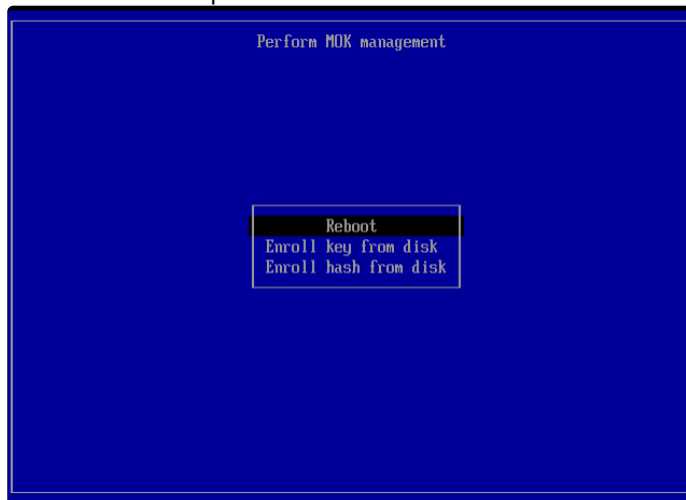


10. Check that the serial number is 0xe9d471cfb4fe136c .
11. Check that the SHA1 fingerprint is e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7 .
12. Press ESC to return to the **Enroll MOK** dialog.
13. Select **Continue** and press **Enter** to display the enrollment confirmation dialog.



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 a 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](#).

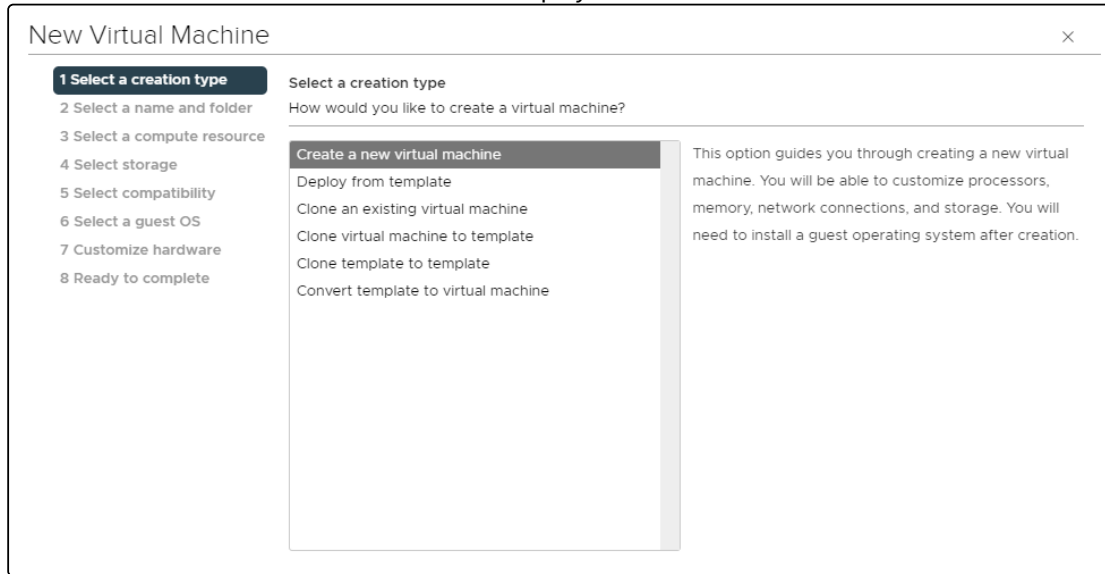
Creating a Entrust Cryptographic Security Platform virtual machine on VMware vSphere

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

To create a 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 .
Memory	Select the RAM size recommended in Machine requirements .

Field	Value
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

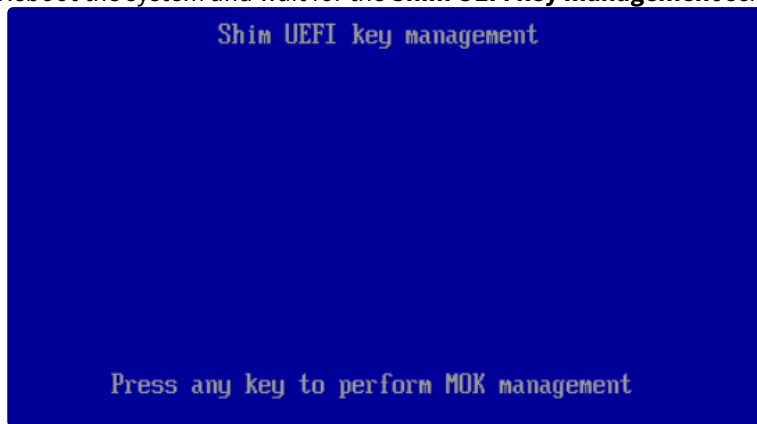
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

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

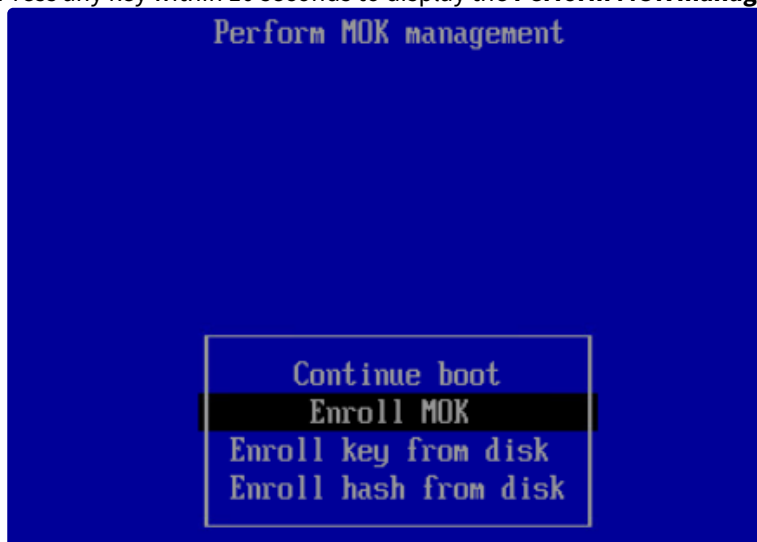
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

 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.

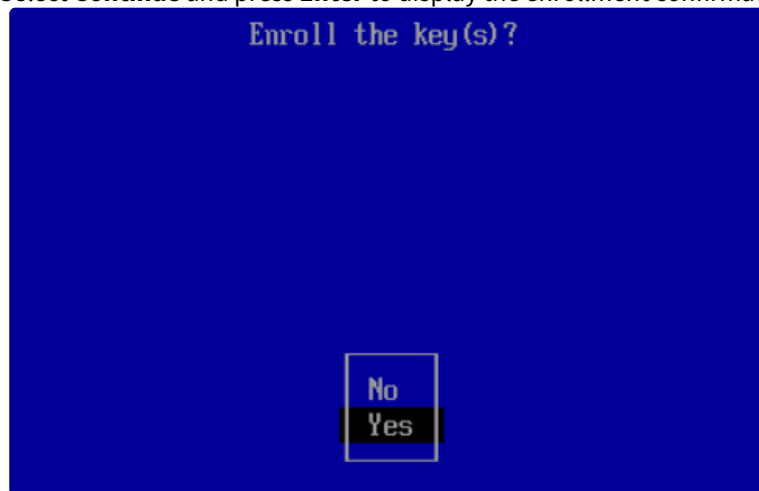


9. Select **View key 0** and press **Enter** to display the key information.

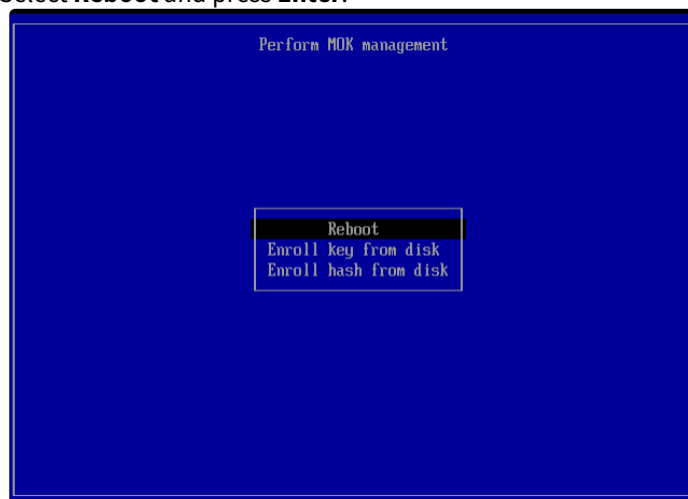


10. Check that the serial number is `0xe9d471cfb4fe136c`.
11. Check that the SHA1 fingerprint is `e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7`.
12. Press **ESC** to return to the **Enroll MOK** dialog.

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.

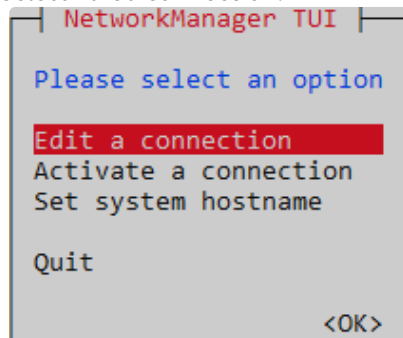
✗ After running the `clusterctl install` or `clusterctl node add` commands you cannot change the IP address or hostname of a node.

To configure the connection of a Cryptographic Security Platform ISO installation

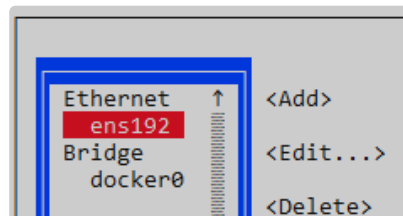
1. Log in to the machine locally as the `sysadmin` user.
2. Run the `nmtui` tool with `sudo` permissions.

```
sudo nmtui
```

3. Type the password of the `sysadmin` user.
4. Select **Edit a connection**.



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



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

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

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

```
192.168.100.4/24
```

11. In the **Gateway** field, enter the IP address of the default gateway for your network connection.
12. 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.

13. 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.

14. Select **&ltOK>** and press **Enter**.
15. Select **&ltBack>** and press **Enter**.
16. 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.

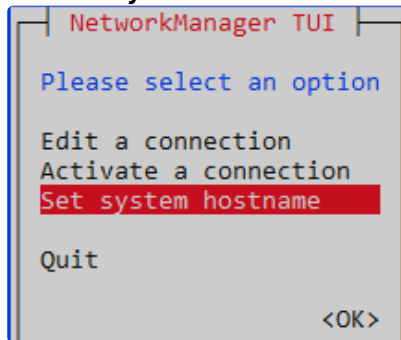
To configure the hostname

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

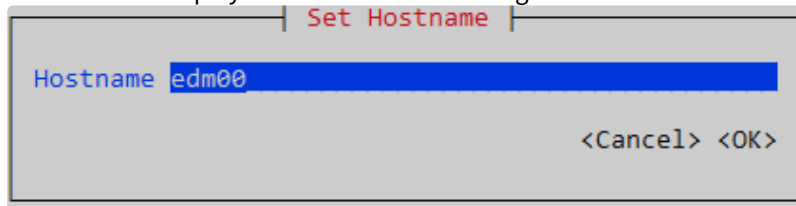
```
sudo nmtui
```

3. Type the password of the `sysadmin` user.

4. Select **Set system hostname**.



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



6. 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.
7. Select **<OK>** and press **Enter**.
8. Press **Enter** to confirm the hostname change.
9. Select **Quit** and press **Enter**.
10. 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

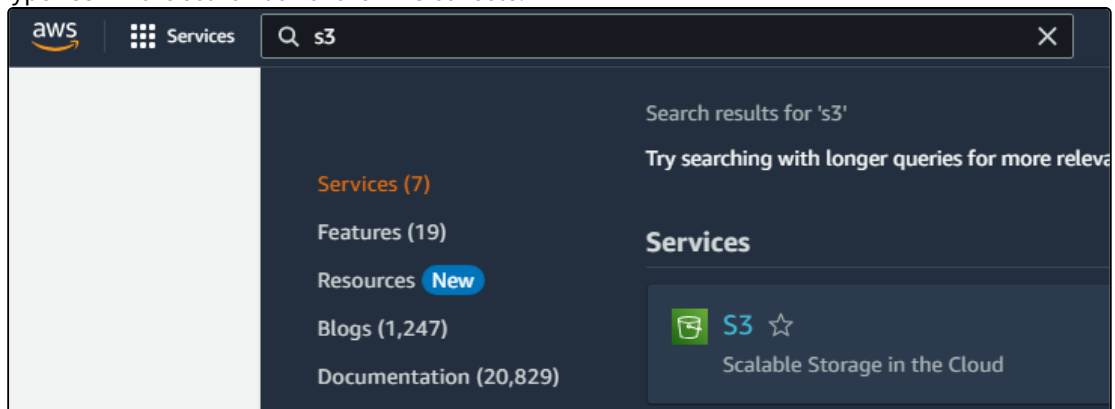
1. Download the Cryptographic Security Platform RAW image as explained in [Downloading the installation files](#).
2. Log into <https://console.aws.amazon.com> as a user with permission to:
 - Create and manage S3 buckets, roles, policies, snapshots, images, and EC2 instances.
 - Run AWS CLI commands 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

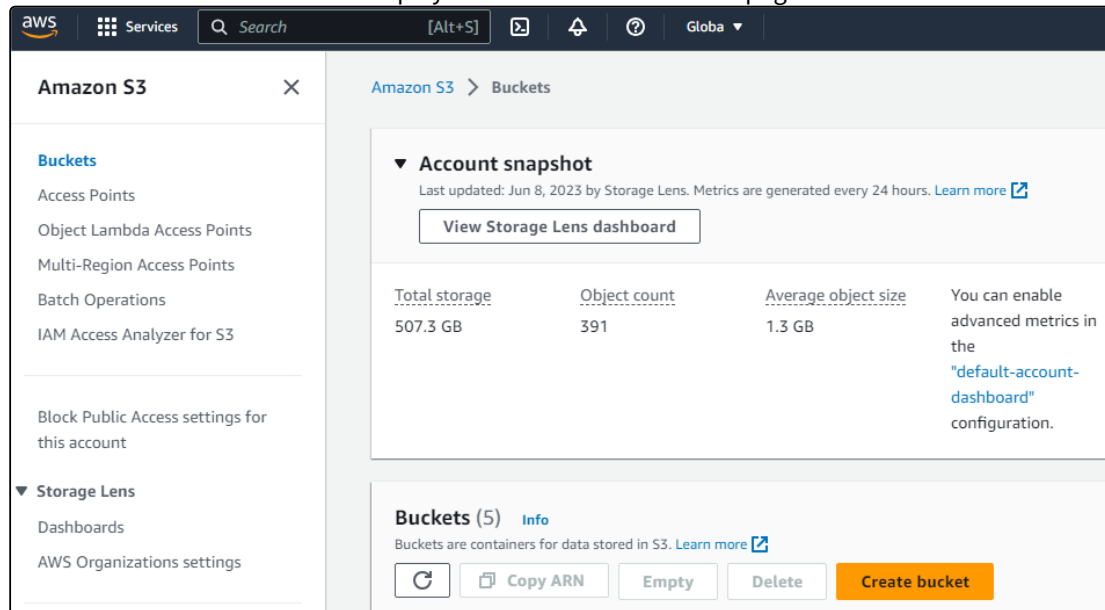
If you don't have an S3 bucket, create a new one as explained below.

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.

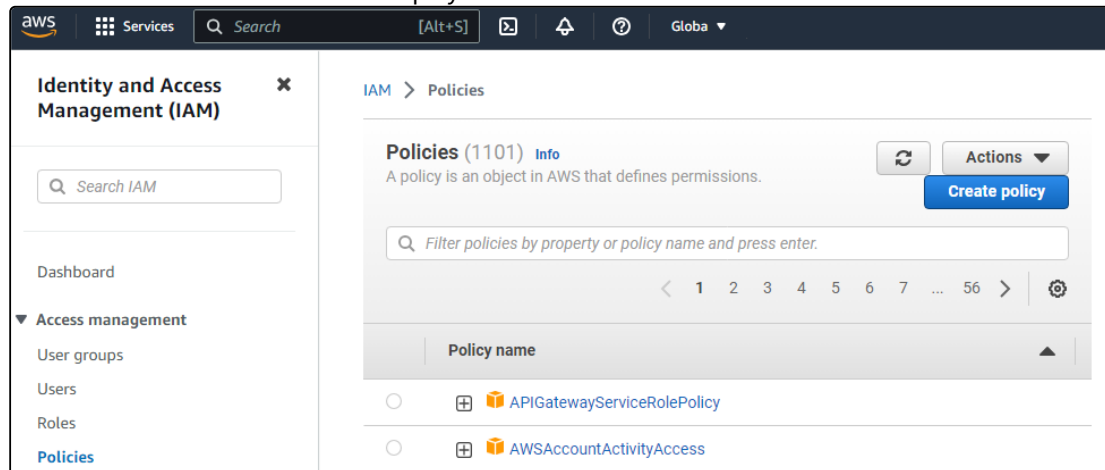
- [Creating a new IAM policy](#)
- [Updating an existing IAM policy](#)

Creating a new IAM policy

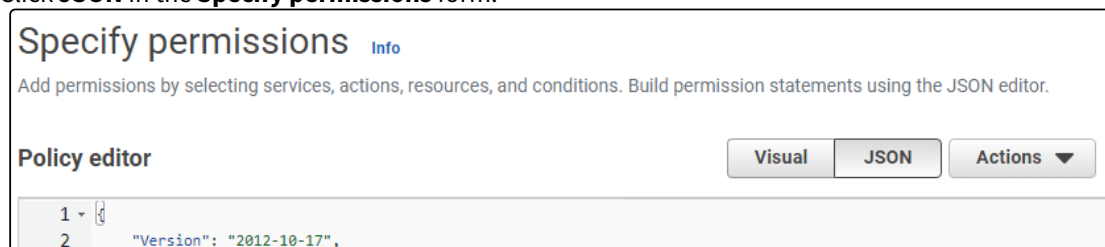
See below for creating an IAM policy granting permission to the S3 bucket.

To create an IAM policy

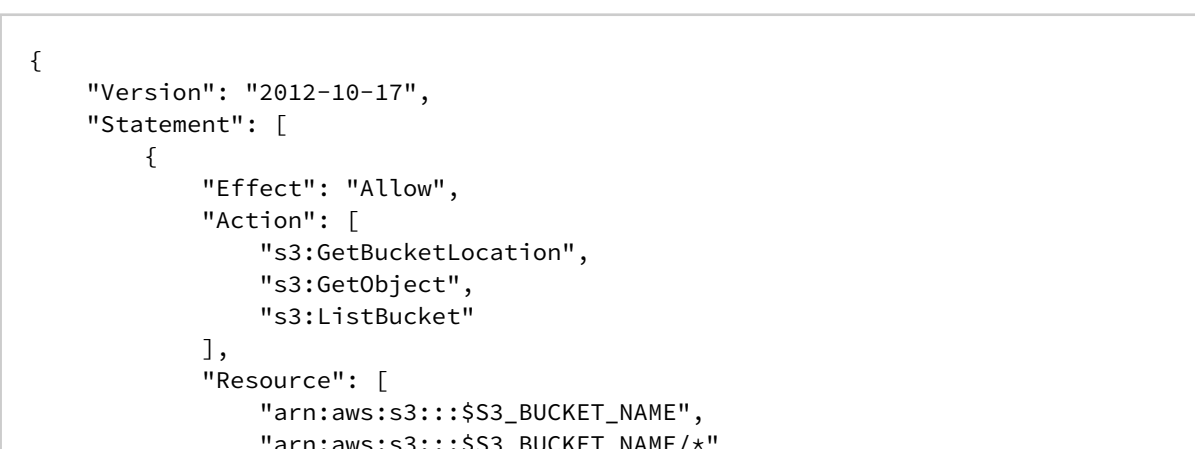
1. Type "IAM" in the search box of the AWS console.
2. Select **IAM** in the search results to display the IAM dashboard.



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.




```

    ],
    {
      "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**.

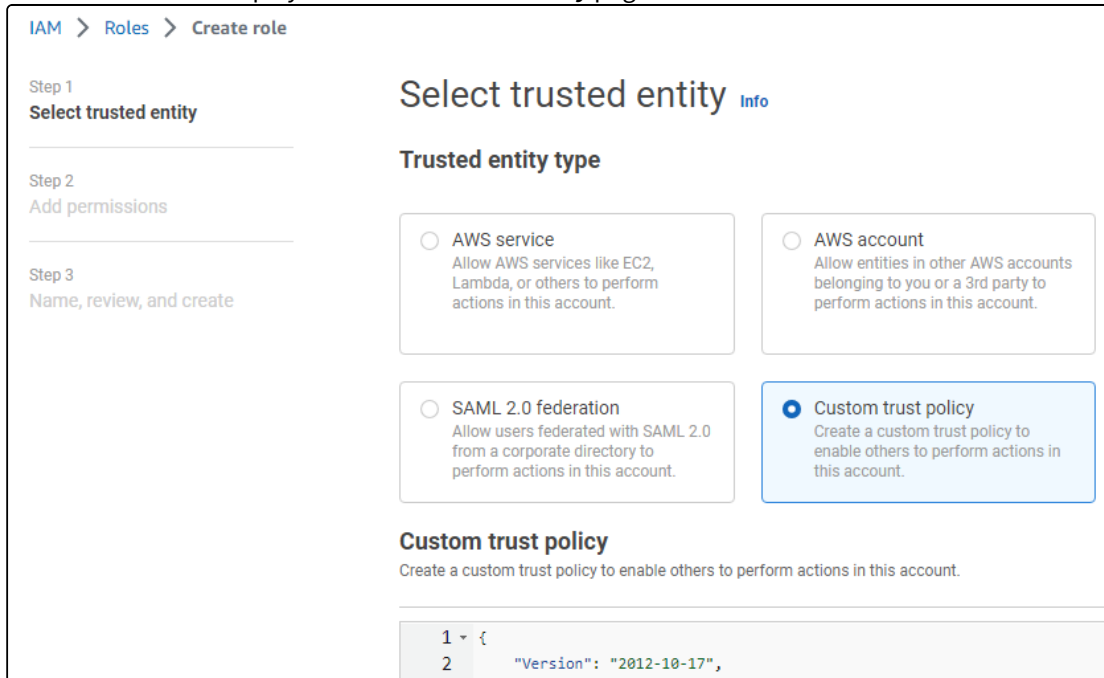
Creating an IAM role

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 content area has a breadcrumb 'IAM > Roles > Create role' and a title 'Select trusted entity' with an 'Info' link. Below the title, there are two sections: 'Trusted entity type' and 'Custom trust policy'. Under 'Trusted entity type', there are four radio button options: 'AWS service' (Allow AWS services like EC2, Lambda, or others to perform actions in this account.), 'AWS account' (Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.), 'SAML 2.0 federation' (Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.), and 'Custom trust policy' (Create a custom trust policy to enable others to perform actions in this account.). The 'Custom trust policy' option is selected. Below this, the 'Custom trust policy' section has a description 'Create a custom trust policy to enable others to perform actions in this account.' and a text area containing a JSON snippet: '1 {', '2', and '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:

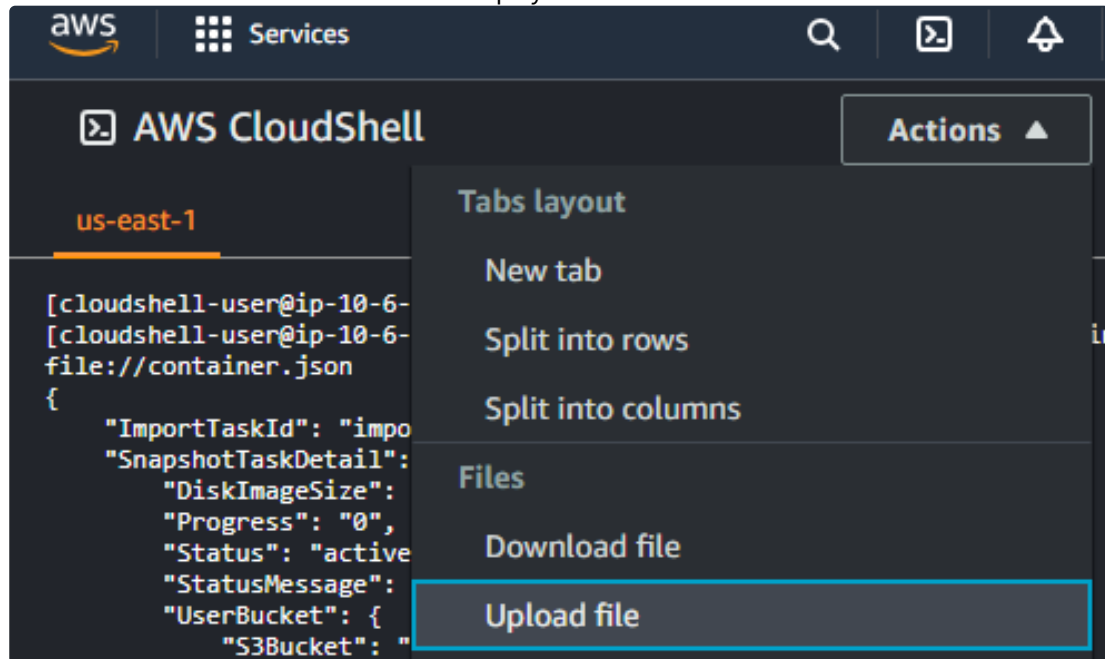
<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>

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](#).

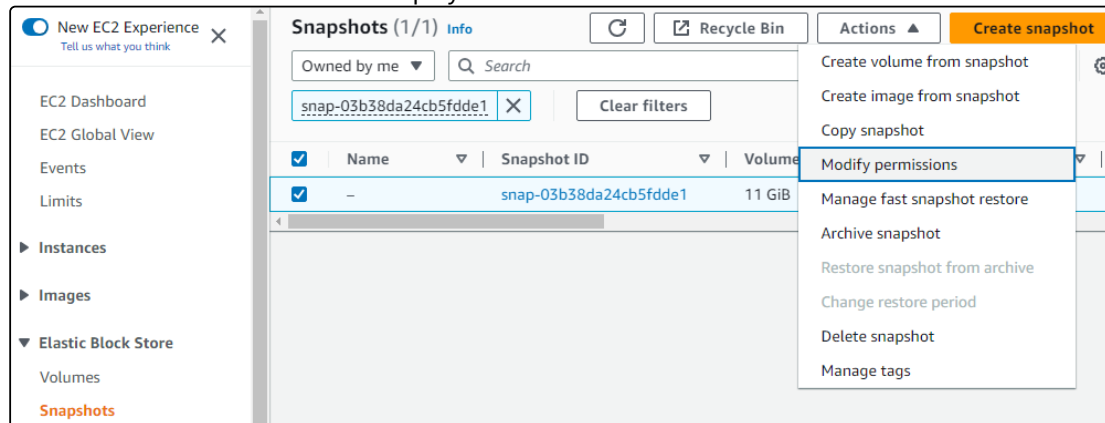
Creating an AMI from the snapshot

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	etcd 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.

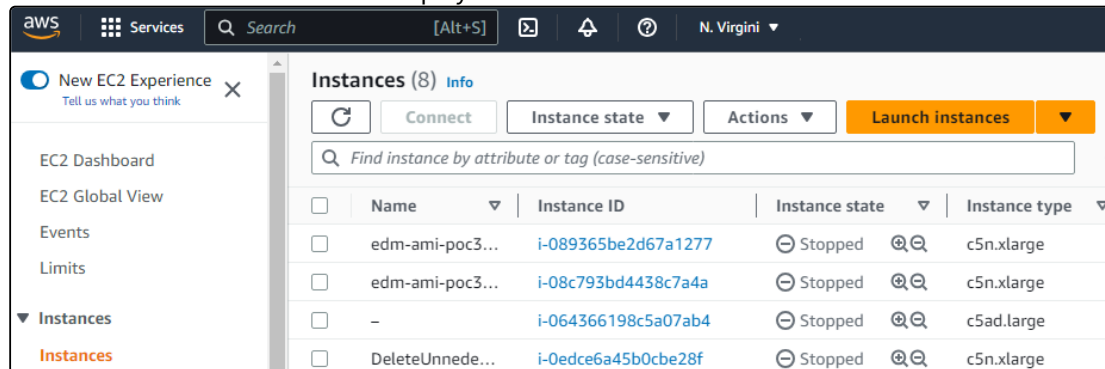
Creating the EC2 instance

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](#).

 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 `sysadmin` username 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.

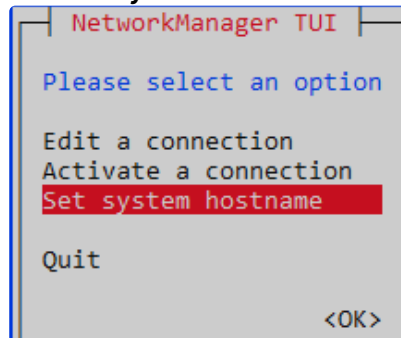
To configure the hostname

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

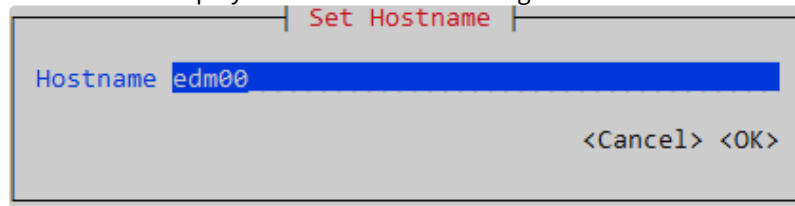
```
sudo nmtui
```

3. Type the password of the `sysadmin` user.

4. Select **Set system hostname**.



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



6. 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.
7. Select **<OK>** and press **Enter**.
8. Press **Enter** to confirm the hostname change.
9. Select **Quit** and press **Enter**.
10. 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

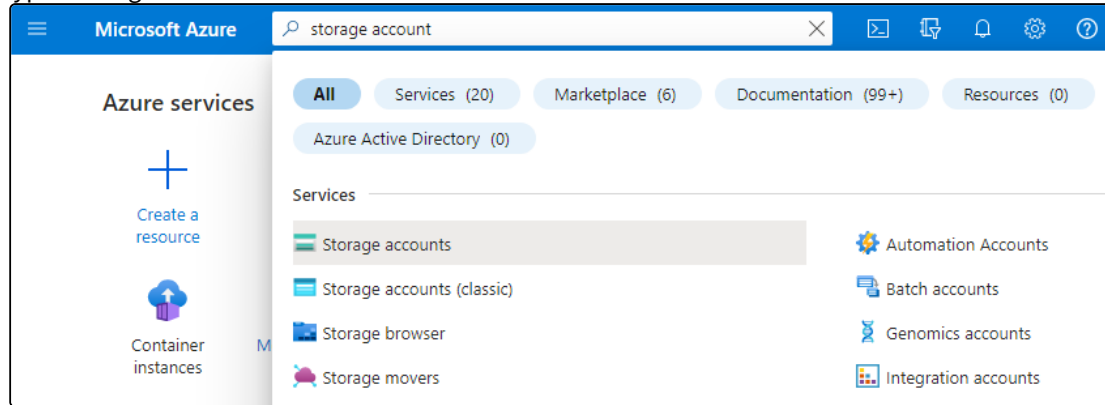
1. Download the Cryptographic Security Platform VHD image as explained in [Downloading the installation files](#).
2. Log into <https://portal.azure.com> as a user with permission to create and manage storage accounts, images, network rules, SSH keys, and virtual machines.
3. Perform the steps described 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.

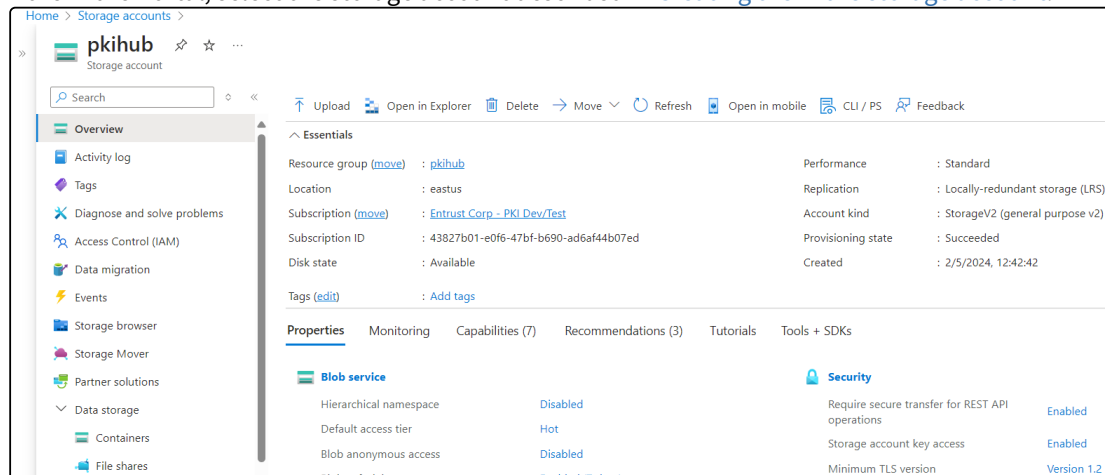
Uploading the VHD image file to Azure

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

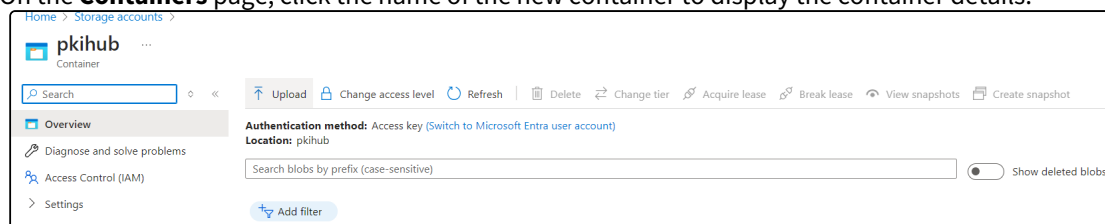
See [Downloading the installation files](#) for how to obtain this file.

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 .
Username	Type the azureuser name.
SSH public key source	Select the key described in Creating the SSH key for Azure .
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`

 Do not modify the `azureuser` administrator name in this command.

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 `sysadmin` username 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.

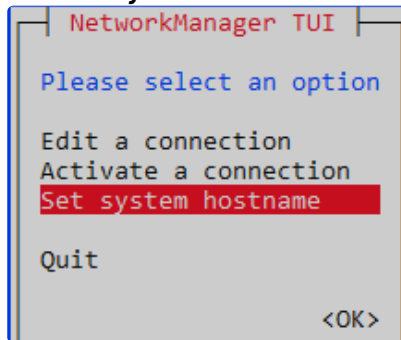
To configure the hostname

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

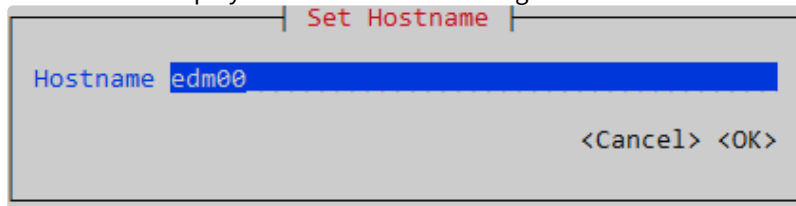
```
sudo nmtui
```

3. Type the password of the `sysadmin` user.

4. Select **Set system hostname**.



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



6. 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.
7. Select **<OK>** and press **Enter**.
8. Press **Enter** to confirm the hostname change.
9. Select **Quit** and press **Enter**.
10. 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

Generate the Cryptographic Security Platform TLS key pair using one of the following algorithms.

- RSA 2048 bits
- RSA 3072 bits
- RSA 4096 bits
- ECDSA curve NIST P-256

Issuing the TLS certificate

Issue the Cryptographic Security Platform TLS certificate using your corporate PKI.

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](#)

i 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 indicated values.

Section	Parameter	Mandatory value	Comment
server_remotecomms	impath_addr	0.0.0.0	You can omit this parameter, as the mandatory value is also the default value

Section	Parameter	Mandatory value	Comment
	impath_port	9004	You can omit this parameter, as the mandatory value is also the default value
server_remotecomms_ipv6	impath_addr	—	You can skip this parameter, as it is not evaluated when disabling IPv6
	impath_port	0	This value disables IPv6, as it is not supported

Therefore, the only mandatory contents in this file are the following.

```
[server_remotecomms_ipv6]
impath_port=0
```

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 a 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/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 in to the web Management Console and replace the initial password of the `admin` user.

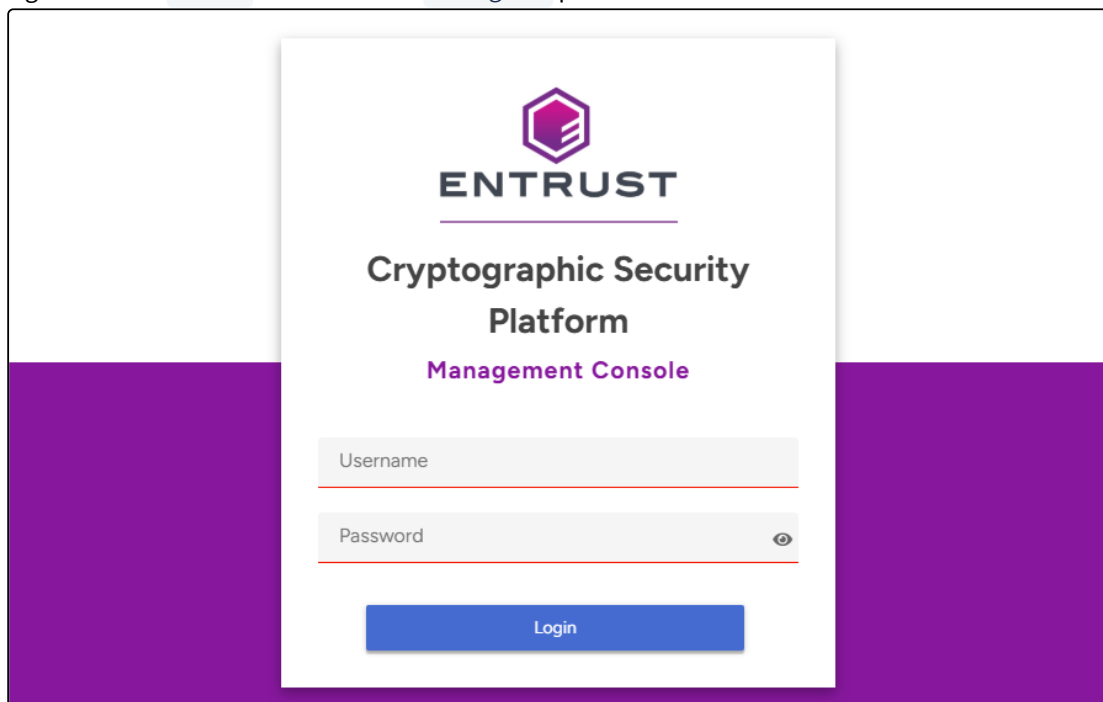
To replace the initial admin password

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 to enter and confirm a password meeting the requirements described in [Internal password](#).
4. 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.

 Every update of the license file requires redeploying the licensed solutions to be effective. Refer to the section dedicated to each solution for instructions on deploying it using the management console.

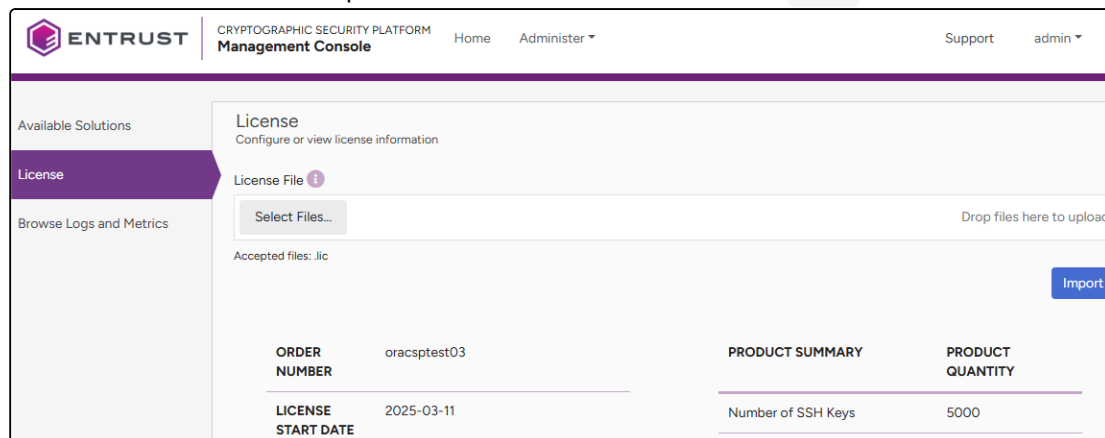
To set or update the license

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.

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

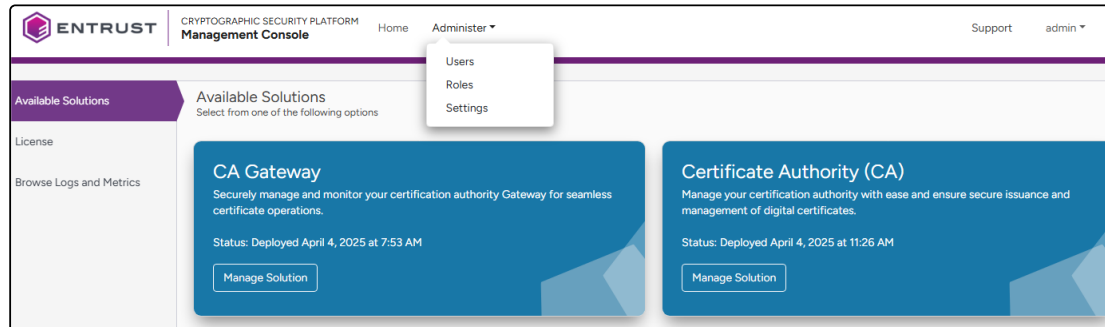
To create a Management Console role

1. Open the following URL in a Web browser.

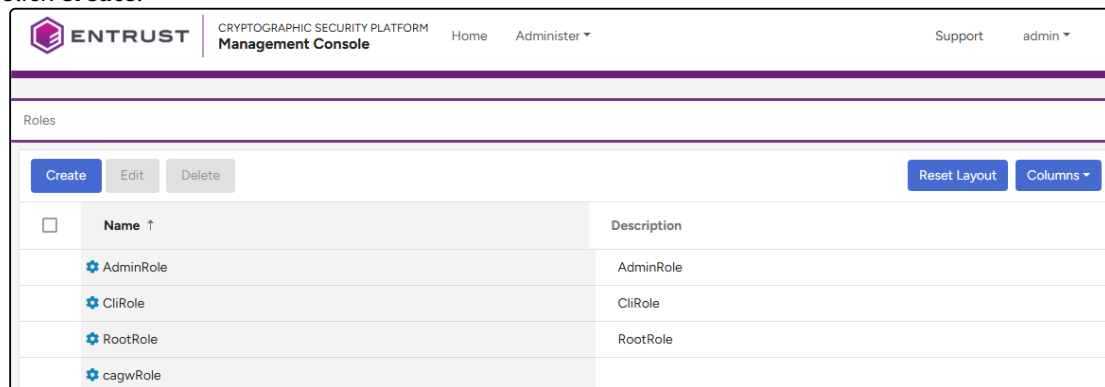
```
https://<machine>/management-console
```

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

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



- Click **Create**.



- Complete the following fields in the **Create** form.
 - [Name](#)
 - [Description](#)
 - [Permissions](#)
- 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
	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

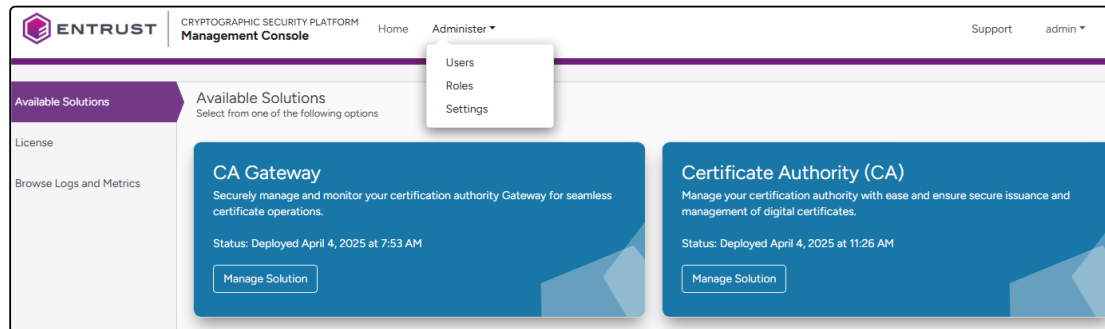
1. Open the following URL in a Web browser.

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

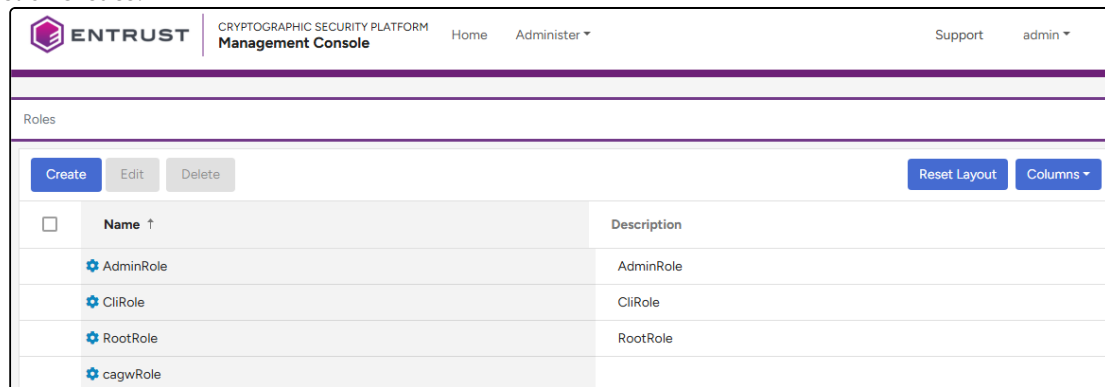
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

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

A password meeting the requirements described [Internal password](#).

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.

i 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

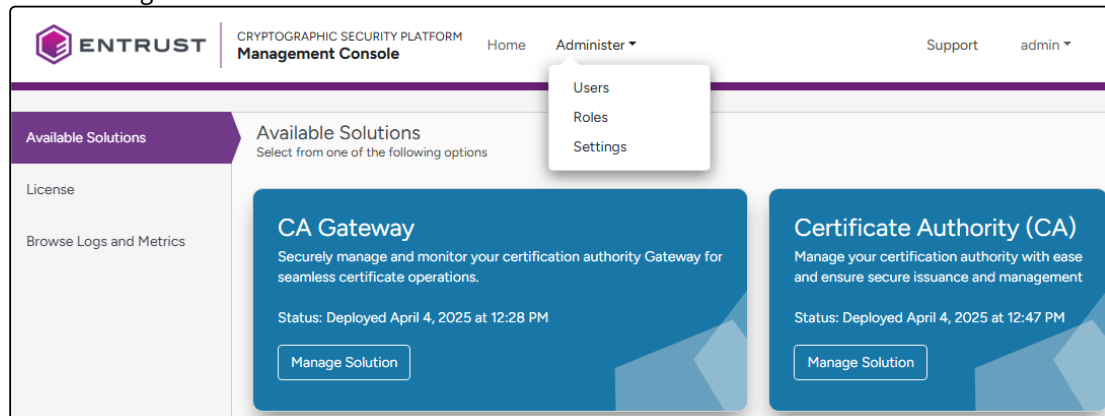
1. Open the following URL in a Web browser.

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

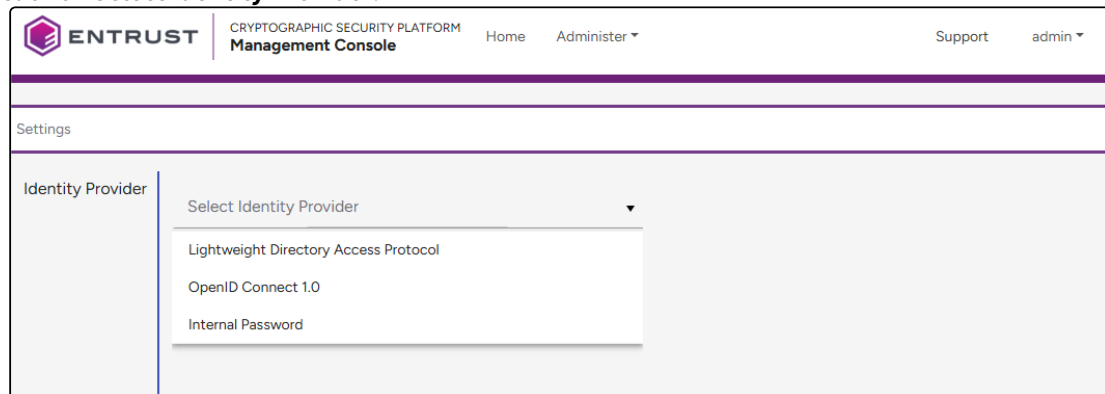
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

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 them 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 <code>profile</code> 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 console-registered administrators.

- [Password content policy](#)
- [Password history policy](#)
- [Account lockout policy](#)

Click the **Force Password Change** button if you want all the administrators to change their passwords at the next login.

Password content policy

Passwords managed by the **Internal password** authentication mechanism must meet the following content requirements.

Requirement	Value
Lenght	8 or more characters
Complexity	A zxcvbn score of 3 or more

Password history policy

The **Internal password** mechanism sets the password history to 1, meaning the new password cannot match the current or previous password.

Account logout policy

Following 5 failed password attempts, the **Internal password** mechanism locks the user account for 15 minutes. After this period, the user's retry counter is reset to zero.

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 CA Gateway

See below for configuring, deploying, and administering the CA Gateway solution.

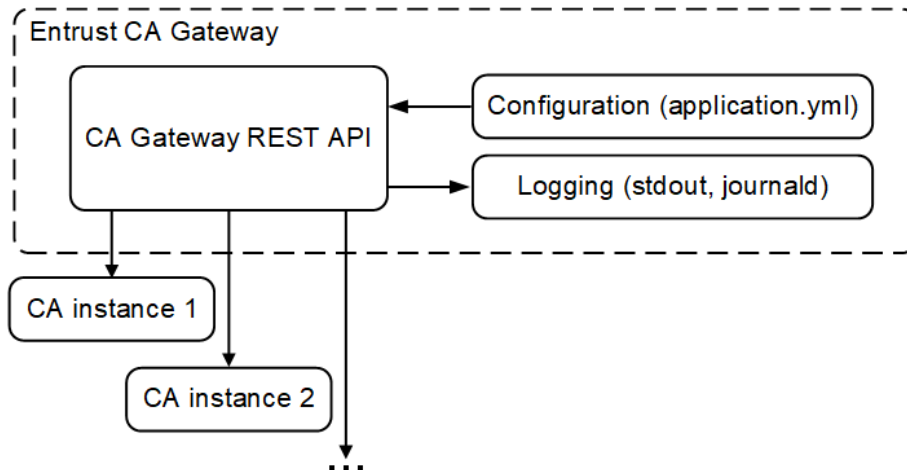
✗ As explained in [Starting up CSP](#), do not perform system operations other than those described in this guide. Specifically, the user and group identifiers 1339 are reserved for CA Gateway images, so the host server should not use them.

- [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](#)
- [Administering CA Gateway](#)
- [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](#)

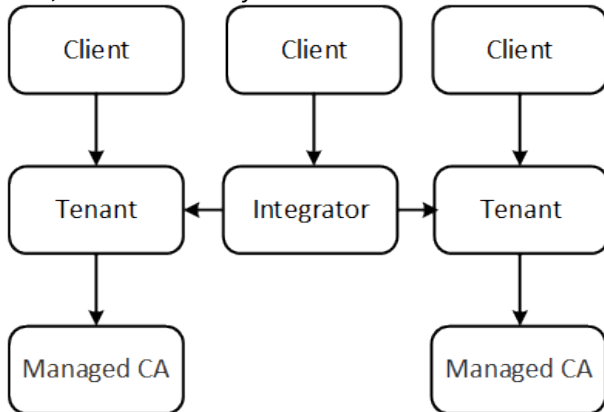
ℹ CA-specific plugins communicate with the underlying CAs through mutually authenticated TLS.

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.
-keystore	The full path of the Java keystore file. If not present, the keystore is created.

Option	Value
-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](#)

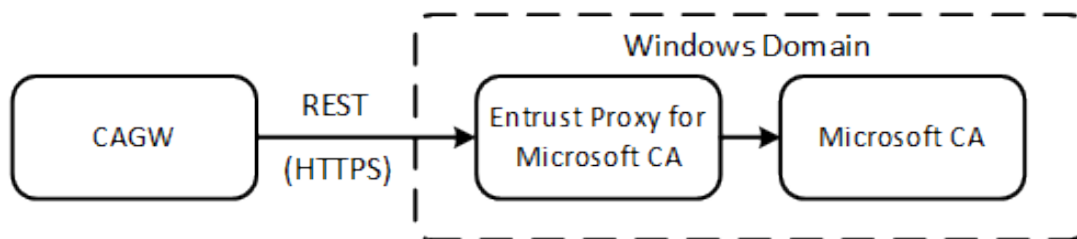
Integrating Certificate Authorities with CA Gateway

The sections below explain how to integrate CA Gateway with Certificate Authorities of different providers.

- [Integrating a Microsoft CA](#)
- [Integrating an ECS CA](#)
- [Integrating an Entrust Certificate Authority](#)
- [Integrating a Sectigo CA](#)

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.

- 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.
-dnaname	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

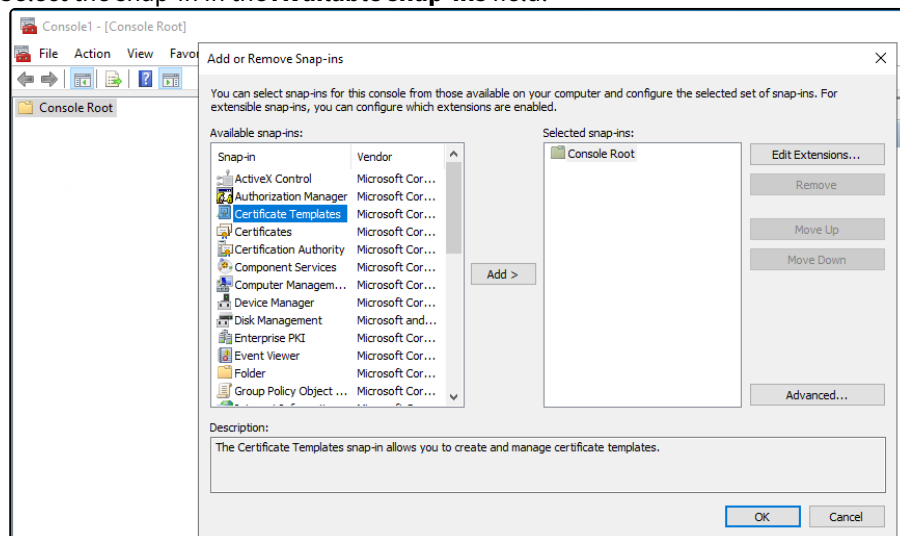
Run the Microsoft Management Console and add the following snap-ins.

- 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**.

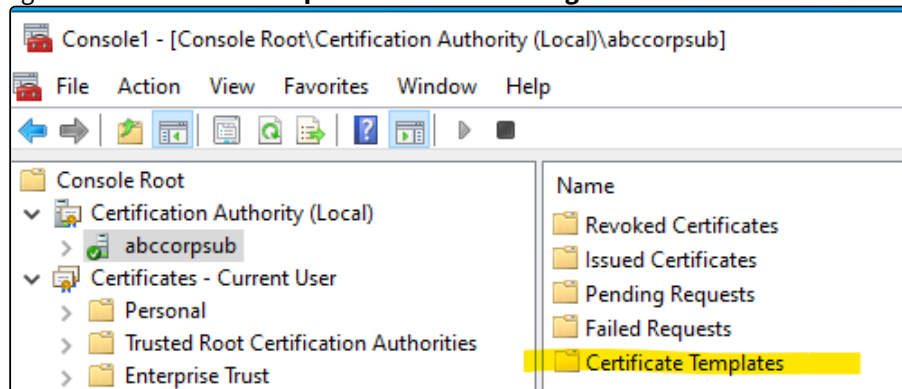
Creating a client authentication template for Microsoft CA

Create an authentication template for enabling client authentication in Microsoft CA.

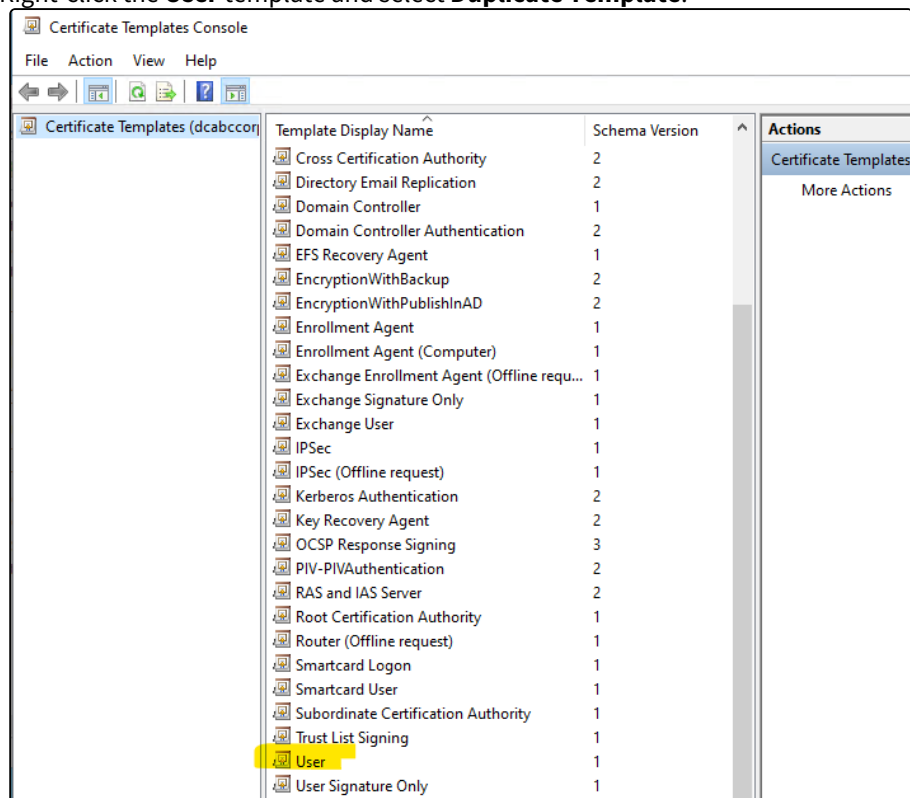
To create a client authentication template for Microsoft CA

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**.

- Right-click **Certificate Templates** and select **Manage**.



- Right-click the **User** template and select **Duplicate Template**.



- In the **General** tab of the **Properties of New Template** dialog, set **Template display name** to **Client Authentication**.
- In the **Subject Name** tab, enable **Supply in the request**.
- In the **Extensions** tab, edit **Application Policies** to remove **Encrypting File System** and **Secure Email**.
- Go to **Certificate Authority**.
- Right-click **Certificate Templates** and select **New >Certificate Template to Issue**.
- 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**.

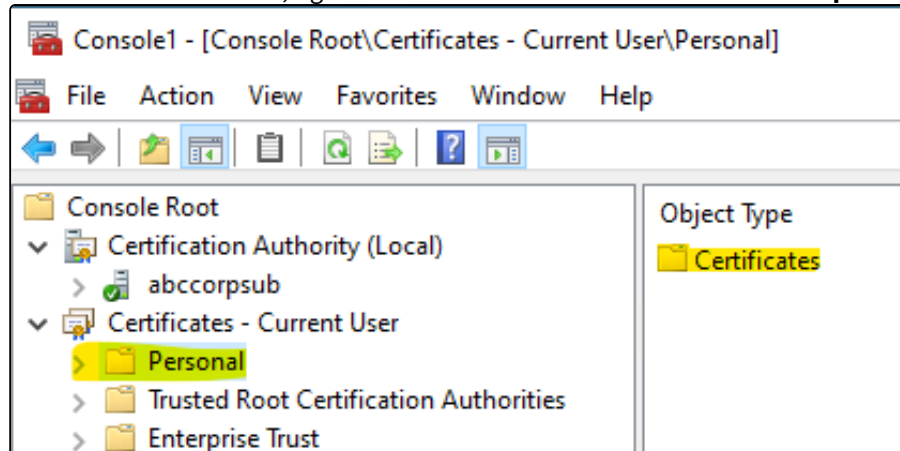
Creating an enrollment certificate for the CA Administrator

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

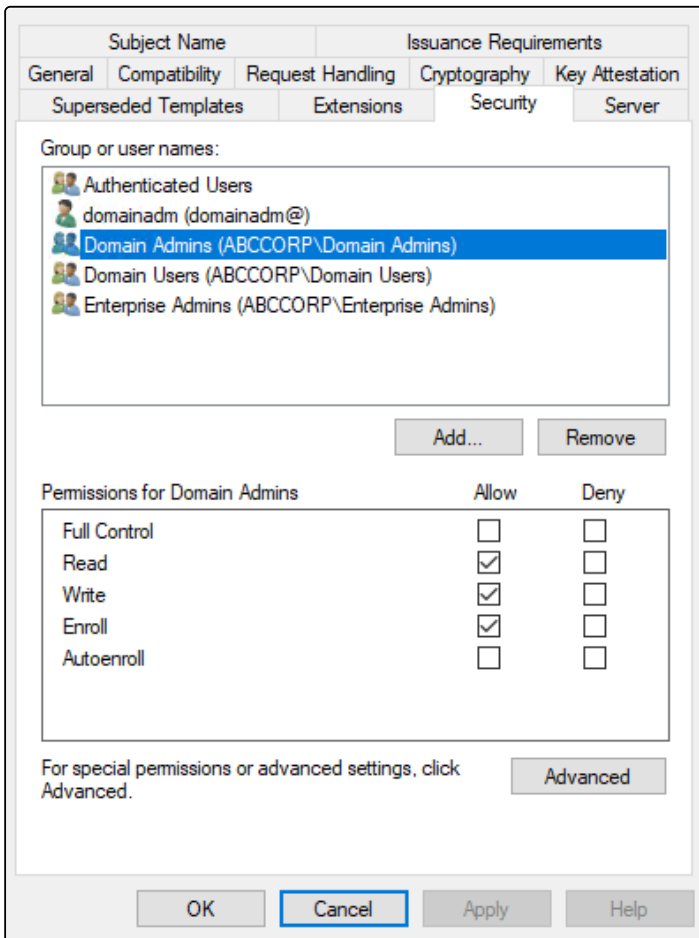
Security

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	☐	☐
Read	☒	☐
Write	☒	☐
Enroll	☒	☐
Autoenroll	☐	☐

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.

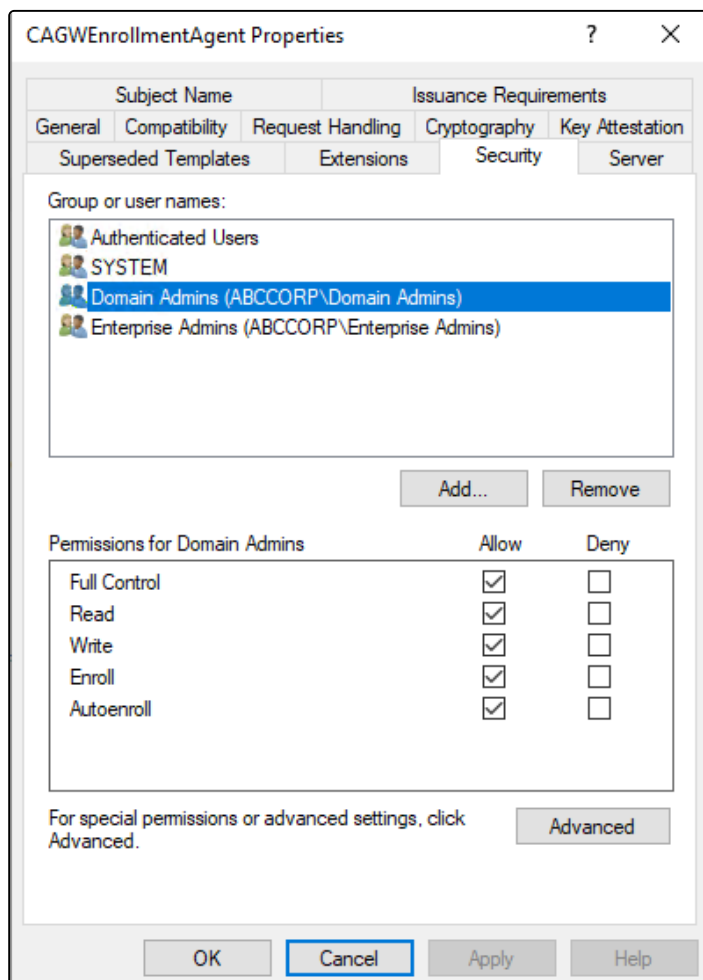
Parameter	Value
This number of authorized signatures	1
Policy type required in signature	Application policy
Application Policy	Certificate Request Agent

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:



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.

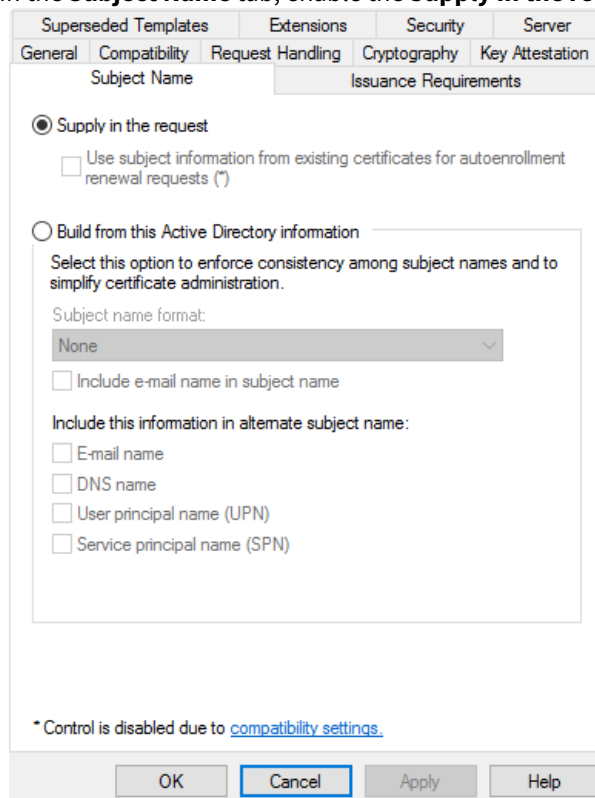
 See the integration guides of the supported HSM for the required operations.

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.



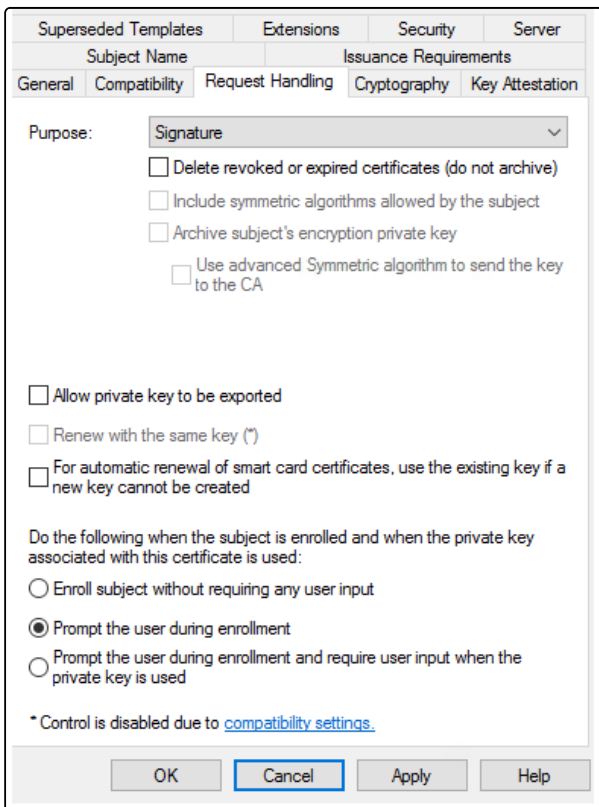
The screenshot shows the 'Subject Name' tab of the 'Certificate Template Properties' dialog. The 'Request Handling' tab is selected. Under 'Subject Name', the 'Supply in the request' radio button is selected. Below it, there is a checkbox for 'Use subject information from existing certificates for autoenrollment renewal requests (*)'. The 'Build from this Active Directory information' section is also visible, with a dropdown for 'Subject name format' set to 'None'. At the bottom, there is a note: '* Control is disabled due to [compatibility settings](#)'.

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

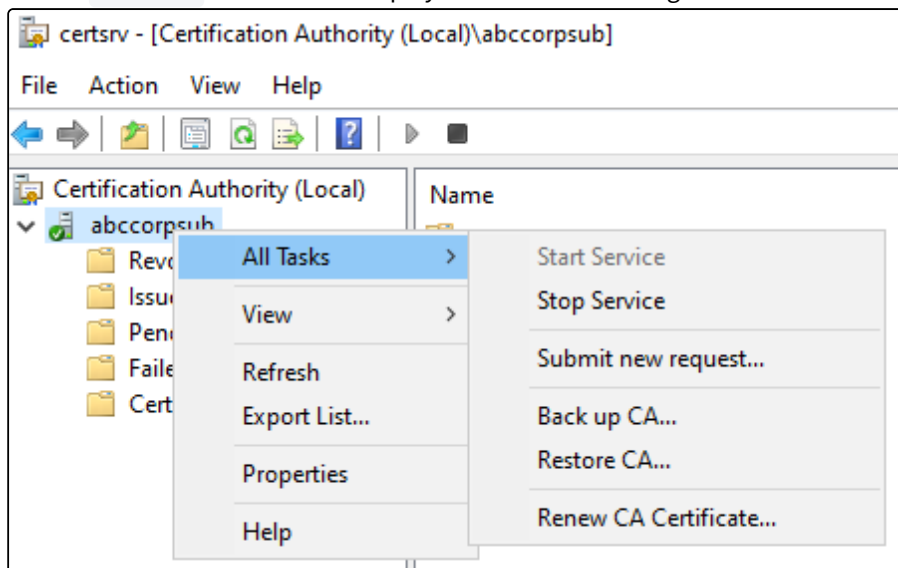
1. Log into the Windows machine hosting the Microsoft CA server.
2. Run the `regedit` command to open the Registry Editor.
3. Select the following registry key (`<CA_CN>` is the Common Name of the Microsoft CA).

```
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 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	View
	Administer at least one group
License Information	View
Roles	View
	Administer at least one role
Searchbases	View
	Administer at least one search base
Security Policy	Force CRLs
	View User Policy
	View Security Policy
	Export Certificate Specification
User Templates	Administer at least one template
User - General	View

Permission category	Permissions
	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 the 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 .

Field	Value
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).

Integrating a Sectigo CA

This section explains how to configure CA Gateway to integrate a Sectigo public CA.

- [Setting Sectigo permissions for API login](#)
- [Creating the Sectigo SSL credentials trust store](#)
- [Creating a Sectigo client key store](#)

Setting Sectigo permissions for API login

You need a Sectigo user with the following minimum privileges.

- [SSL certificate privileges](#)
- [Domain validation](#)

 See [com.Sectigo](https://com.sectigo) for how to set the Sectigo user in the CA Gateway configuration.

SSL certificate privileges

Assign at least the following SSL certificate privileges.

- Request SSL certificates
- Revoke SSL certificates
- Renew SSL certificates
- Manage SSL certificate requests
- Replace SSL certificates
- Manage SSL certificates

Domain validation

Future CA Gateway releases will require at least the following domain validation privileges.

- Manage domain validations
- Manage domains
- Approve domain delegation

Creating the Sectigo SSL credentials trust store

You need a credentials trust store for SSL communication with the Sectigo API.

 See [com.Sectigo](#) for how to set this trust store in the CA Gateway configuration.

To create the trust store for authenticating in the Sectigo API

1. Open a browser to the following URL.

```
https://cert-manager.com/customer/customer-uri>
```

Where `<customer-uri>` matches the `customer-uri` value you will configure on the [com.Sectigo](#) settings.

2. Click the lock icon beside the URL in the address bar and export the certificate chain.
3. Create a trust store containing the exported certificates. For example, use the `openssl pkcs12` command to create a PKCS #12 type trust store.

Creating a Sectigo client key store

As explained in [com.Sectigo](#), you can optionally select a key store as authentication mode for the Sectigo login. See below for instructions on how to create this key store.

- [Creating the enrollment form](#)
- [Adding a person](#)
- [Issuing the client certificate](#)
- [Creating an administrator](#)

 We recommend omitting this section and selecting a password instead when configuring the [com.Sectigo](#) settings.

Creating the enrollment form

Create an enrollment form for the client certificate.

1. Log in to the Sectigo portal using your browser.
2. Go to **Enrollment > Enrollment Forms**.
3. Click the **+** icon to create a new form.
4. In the **Name** field, enter a name for the enrollment form. For example:

```
myOrganization - Client certificate
```

5. In the **Type** list, select **Client certificate self-enrollment**.
6. In the **Configuration** tab, enable **Secret ID**.
7. Generate the **Enrollment Endpoint URL**.

Adding a person

Add a person to the Sectigo configuration.

1. Navigate to **Persons**.
2. Click the **+** icon.
3. Complete the **Add New Person** fields. Specifically:
 - Provide a secret.
 - Select the same email address you will later use for the administrator.

Issuing the client certificate

Issue a client certificate to authenticate in the Sectigo API.

1. Open the newly created enrollment form in a new browser tab.
2. Issue a certificate using the same secret and email address configured for the newly created person.
3. Download the PKCS #12 file.

Creating an administrator

Create a user with administrator privileges in Sectigo.

1. Navigate to **Settings > Admins**.
2. Click the **+** icon.
3. In the **Add Admin Type** dialog, select **Standard**.
4. Complete the **Add New Admin** fields. Specifically:
5. Use the same email address configured for the newly created person.
6. In the **Authentication** tab, select the newly issued certificate.

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 an SSH session in any of the Cryptographic Security Platform nodes.
2. Run the following command.

```
sudo /opt/entrust/ctr -a /run/k3s/containerd/containerd.sock image tag --force
docker.io/pkihub/alpine:3.21.3 localhost:30000/pkihub/init-
attila:v202503271109
```

3. Open the following URL in a Web browser.

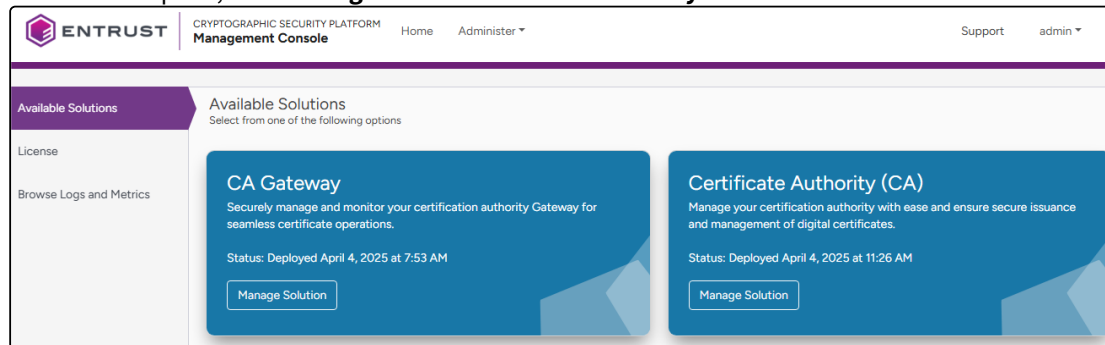
```
https://<machine>/management-console
```

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

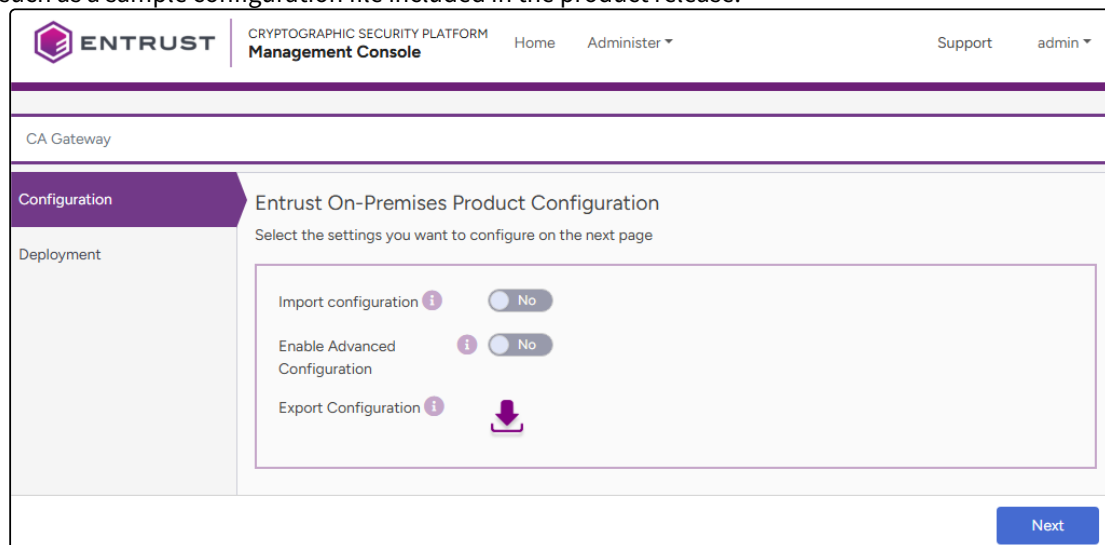
4. Log into the Management Console a user belonging to a role with CA Gateway management permissions – for example, the initial **admin** administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

5. 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.

- [SSL](#)
- [Key Alias](#)
- [Key Store](#)
- [Key Store Password](#)
- [Key Store Type](#)
- [Trust Store Type](#)
- [Trust Store](#)
- [Trust Store Password](#)

SSL

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
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

<setting>	Value	Default
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".
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.

 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: <code>google-min-responses + non-google-min-responses</code>

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 bits.

Minimum ECC Keysize

The minimum size for all authority ECC (elliptic curve) keys, as a number of bits.

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. See below for the supported characters and limitations.

Character	Limitation
Numbers	None
Letters	Does not support mixed case; all letters must either be uppercase or lowercase.
Dashes	Does not support mixed types; all dashes must either be hyphens ("-") or underscores ("_").

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 the following table for the supported values.

Connector Name	CA
com.entrust.ECS	Entrust Certificate Services
com.entrust.MicrosoftCA	Microsoft Certification Authority
com.entrust.SecurityManager	Entrust Security Manager
com.Sectigo	Sectigo CA

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.

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.

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).

i 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	✓

Setting	Value	Mandatory
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.

i 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.

com.Sectigo

To integrate a Sectigo Certificate Authority, select this connector and configure the following settings.

- [Sectigo settings](#)
- [Authentication settings](#)
- [SSL settings](#)

- [Enrollment settings](#)
- [Proxy settings](#)

Sectigo settings

Configure the following mandatory Sectigo settings.

Setting	Value
Customer URI	The customer identifier provided by Sectigo
Organization ID	The organization identifier provided by Sectigo
URL	The URL of the Sectigo API

Authentication settings

To authenticate in Sectigo with a password, enter the following values.

Setting	Value
Login Userid	A Sectigo login name for a user with the privileges described in Setting Sectigo permissions for API login
Login Password	The password of the selected Sectigo login name

To authenticate with the client store created in [Creating a Sectigo client key store](#), click **+ Sectigo CA Properties** and manually enter the following key-value pairs.

Key	Value
client-cert-key-store	The path of the client trust store described in Creating a Sectigo client key store
client-cert-key-alias	The alias of the client key in the client trust store
client-cert-key-store-password	The password of the client trust store
client-cert-key-store-type	The type of client trust store. Supported values are <code>JKS</code> and <code>PKCS12</code> .

SSL settings

Configure the following mandatory SSL settings to connect with the Sectigo API.

Setting	Value
SSL Truststore File	The path of the trust store described in Creating the Sectigo SSL credentials trust store
ssl-trust-store-password	The password of the trust store
SSL Truststore Type	The type of CA Gateway trust store. Supported values are <code>JKS</code> and <code>PKCS12</code> .

Enrollment settings

The following settings control the enrollment requests.

Key	Value	Default
enroll-back-off-timer	The starting back-off period for certificate retrieval	2 sec
enroll-max-back-off-timer	The maximum back-off period before the next certificate retrieval attempt	32 sec
enroll-max-attempts	The maximum number of certificate retrieval attempts	5

After submitting an enrollment, CA Gateway waits for the following period.

```
min(enroll-back-off-timer^attempt, enroll-max-back-off-timer)
```

Where the `attempt` value:

1. Starts at 1 on the first enrollment attempt.
2. Is increased by 1 after each retrieval attempt, until reaching the `enroll-max-attempts` value.

CA Gateway responds with the following HTTP codes to the client enrollment requests.

Code	Description
HTTP 200	The certificate has been retrieved on time
HTTP 202	The request has been processed, but CA Gateway has exceeded the <code>enroll-max-attempts</code> period
HTTP 404	Any other failure

When receiving a HTTP 202 response, you can:

1. Look up the certificate using the `{caId}` Certificate Authority identifier and the `{dn}` Distinguished Name.

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

2. Ascertain the serial number from the response.
3. Look up the certificate using the `{sn}` serial number.

```
/v1/certificate-authorities/{caId}/certificates/{sn}
```

Proxy settings

Configure the following settings if traffic to the CA server passes through a proxy.

i The proxy configured using these settings is part of your corporate infrastructure; it is not an Entrust product.

setting	Value
proxy-host-name	The hostname of the proxy for accessing the CA server.
proxy-port	The port for accessing the proxy
proxy-username	The username for authenticating in the proxy (if required)
proxy-password	The password for authenticating in the proxy (if required)

Enable CA Profile Sync

`true` to enable profile synchronization with the following Certificate Authorities.

- [Entrust Certificate Authority](#)
- [Sectigo CA profiles](#)

`false` otherwise.

Mandatory: No. This optional value defaults to `false`.

Entrust Certificate Authority

To synchronize profiles with an Entrust Certificate Authority, CA Gateway:

- Mirrors any eligible certificate types and definitions defined in the 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 **Enable niche certificate types** under [com.entrust.SecurityManager](#).

Sectigo CA profiles

To synchronize profiles with a Sectigo CA, CA Gateway follows the steps described in [Sectigo CA profile properties](#).

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](#)
- [Microsoft CA Profile Properties](#)
- [Sectigo CA profile properties](#)
- [Security Manager Profile Properties](#)

Choose a key name

Type a unique identifier for the profile. See below for the supported characters and limitations.

Character	Limitation
Numbers	None
Letters	Does not support mixed case; all letters must either be uppercase or lowercase.
Dashes	Does not support mixed types; all dashes must either be hyphens ("-") or underscores ("_").

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`.

Sectigo CA profile properties

To set the Sectigo-specific profile properties:

1. Type in the **Certificate Type** field the identifier of a profile configured in Sectigo.
2. Activate the [Enable CA Profile Sync](#) setting.
3. Make an API call to the `/v1/certificate-authorities/{caId}/profiles` endpoint.

CA Gateway will merge the profile configuration set in the Management Console with profiles configured at Sectigo. For example:

```
{
  "message": {
    "message": "Profiles retrieved successfully.",
    "details": []
  },
  "profiles": [
    {
      "id": "sectigo-profile-1",
      "name": "static-profileA-local",
      "properties": {
        "cert_type": "60515"
      },
      "protocols": [],
      "requestedProperties": [],
      "subjectAltNameRequirements": [],
      "subjectVariableRequirements": []
    },
    {
      "id": "60515",
      "name": "profileA",
      "properties": {
        "cert_type": "60515",
        "description": "",
        "key_type": "{\"EC\": [\"P-256\", \"P-384\", \"P-521\"], \"RSA\": [\"2048\", \"3072\", \"4096\", \"8192\"]}",
        "terms": "[30]",
        "use-secondary-org-name": "false"
      },
      "protocols": [],
      "requestedProperties": [],
      "subjectAltNameRequirements": [],

```

```
    "subjectVariableRequirements": []
  },
  {
    "id": "63999",
    "name": "Sectigo Enterprise Pro - Multi-Domain (OV)",
    "properties": {
      "cert_type": "63999",
      "description": "",
      "key_type": "{\"EC\": [\"P-256\", \"P-384\"], \"RSA\": [\"2048\", \"4096\", \"8192\"]}",
      "terms": "[47, 200, 365, 397]",
      "use-secondary-org-name": "false"
    },
    "protocols": [],
    "requestedProperties": [],
    "subjectAltNameRequirements": [],
    "subjectVariableRequirements": []
  },
  {
    "id": "64442",
    "name": "test",
    "properties": {
      "cert_type": "64442",
      "description": "asdfsadf",
      "key_type": "{\"EC\": [\"P-256\", \"P-384\", \"P-521\"], \"RSA\": [\"2048\", \"3072\", \"4096\", \"8192\"]}",
      "terms": "[30]",
      "use-secondary-org-name": "false"
    },
    "protocols": [],
    "requestedProperties": [],
    "subjectAltNameRequirements": [],
    "subjectVariableRequirements": []
  }
],
"type": "ProfilesResponse"
}
```

See below for the main parameters in this configuration.

- [key-types](#)
- [terms](#)

i In this API response, some parameter names include underscores for backwards compatibility, and key type values are escaped because they contain embedded JSON code.

key-types

A list of supported key types for the issued certificate. For example

```
"key_types": "{\"EC\": [\"P-256\", \"P-384\"], \"RSA\": [\"2048\", \"4096\", \"8192\"]}"
```

As described in the table below, the requested validity (if any) must be included on this list.

Request type	Requested key type	Key type for the issued certificate
PKCS #10	Included in the <code>key-types</code> list	As selected in the request
	Not included in the <code>key-types</code> list	Error
PKCS #12	—	The first in the <code>key-types</code> list, if key-type is not available, uses default.

Mandatory: No, this optional value defaults to a list containing a single RSA 2048 key type.

terms

A list of supported certificate validity periods, in days. For example

```
terms": "[47, 200, 365, 397]"
```

As described in the table below, the requested validity (if any) must be included on this list.

Request type	Requested validity	Validity of the issued certificate
PKCS #10	Included in the <code>terms</code> list	As selected in the request
	Not included in the <code>terms</code> list	Error
	None	The first in the <code>term</code> list, if term list not available, uses default.
PKCS #12	—	The first in the <code>term</code> list, if term list not available, uses default.

Mandatory: No, this optional value defaults to a list containing a single 30-day period.

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.

Value	Action
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 user type to apply 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.	✓

Setting	Value	Mandatory
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	✓	✓	✗	✗	✗

Permission	integ rator	policy- override- tenant	policy- constrained- tenant	read-only- integrator	read- only- tenant
External public keys (no CSR)	✓	✓	✗	✗	✗
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](#)
- [ping](#)
- [prometheus](#)

Checking the health of a CA

CA Gateway provides the [status](#) endpoint to check the health of a Certificate Authority.

CA Gateway endpoints

CA Gateway provides the following endpoints.

- [docs](#)
- [health](#)
- [ping](#)

- [prometheus](#)
- [properties](#)
- [status](#)
- [swagger-ui](#)
- [v1](#)
- [v1/certificate-authorities/{cald}/certificate-events](#)
- [v1/certificate-authorities/{cald}/properties](#)
- [v1/certificate-authorities/{cald}/status](#)

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 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 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://cicd-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.

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

The following endpoint returns a list of events in the certificates issued by the CA with the `{caId}` identifier.

```
https://<HOST>:<CAGW_HOST_PORT>/<server.servlet.context-path>/v1/certificate-authorities/{caId}/certificate-events
```

This endpoint returns the following values.

- `events`
- `nextPageIndex`
- `hasMore`

events

A list of events on the issued certificates. For example, certificate revocation.

i The endpoint retrieves 0 events for days without events.

nextPageIndex

An index to track which day and which event should be collected next.

- This index depends on the value assigned to the `default-query-page-size` configuration parameter.
- After the first query to the endpoint, all subsequent queries must include this index.

hasMore

A flag indicating if the endpoint has more results to return.

Value	Description
true	The endpoint can return more events from the last <code>nextPageIndex</code> till today
false	All events have been collected, so the caller can stop invoking the endpoint

v1/certificate-authorities/{caId}/properties

The following endpoint returns property values on a CA.

i In the current release, only Security Manager CAs support this endpoint.

```
https://<HOST>:<CAGW_HOST_PORT>/<server.servlet.context-path>/v1/certificate-  
authorities/{caId}/properties?fields={properties}
```

Where `{caId}` is the Security Manager CA identifier and `{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 Security Manager CA 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"  
      ]  
    }  
  }  
}
```

v1/certificate-authorities/{caId}/status

The following endpoint returns the up or down status of a Certificate Authority.

```
https://<HOST>:<CAGW_HOST_PORT>/<server.servlet.context-path>/v1/certificate-  
authorities/{caId}/status
```

Where `{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",
}
```

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

CA	Returned value
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

CA	Returned value
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 ADCS	True

ExtensionInCSR

Process the extension request in the CSR.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft ADCS	True

ExtensionInRequest

Process the extension request in the enrollment request.

CA	Returned value
Entrust Certificate Authority	True
ECS	False
Microsoft ADCS	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 AD CS	True

SANInCSR

Process the Subject Alternative Names in the CSR.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft AD CS	True

SANInRequest

Process Subject Alternative Names in the enrollment request.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft AD CS	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

CA	Returned value
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 ADCS	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 ADCS
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	✓	✓	✓

Reason	SM	ECS	MS ADCS
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 ADCS	Recover all certificates, recover the latest certificates.

SubjectDNAction

List the certificate actions by the subject's DN.

Actions	SM	ECS	MS ADCS
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 ADCS	True

SearchBySubjectDN

Lookup certificates by the subject's DN.

CA	Returned value
Entrust Certificate Authority	True
ECS	True
Microsoft ADCS	True

8 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.

 Do not forget to also click **Deploy** after each update of the configuration or the license file.

To configure and deploy Certificate Authority with the Management Console

1. Open the following URL in a Web browser.

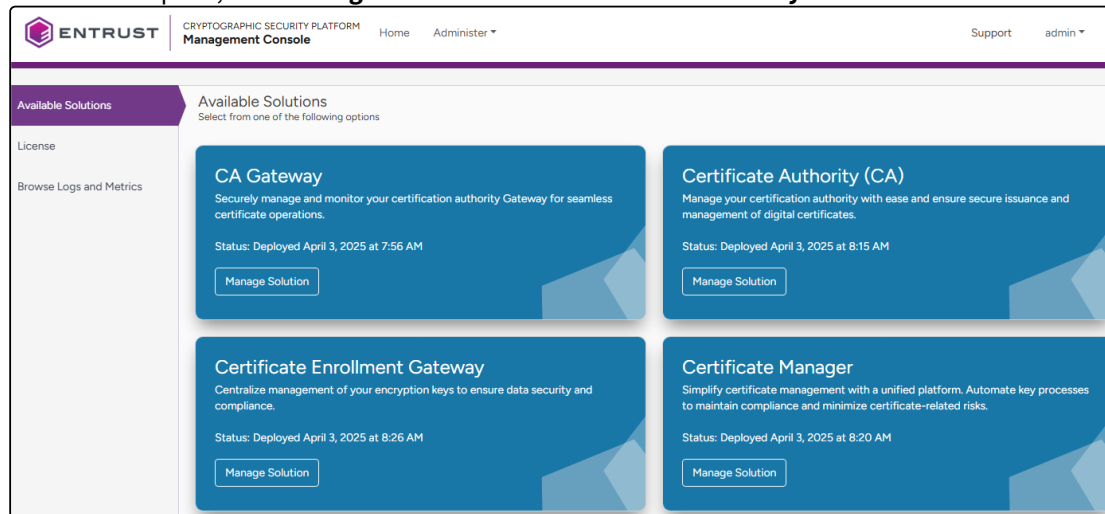
```
https://<machine>/management-console
```

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

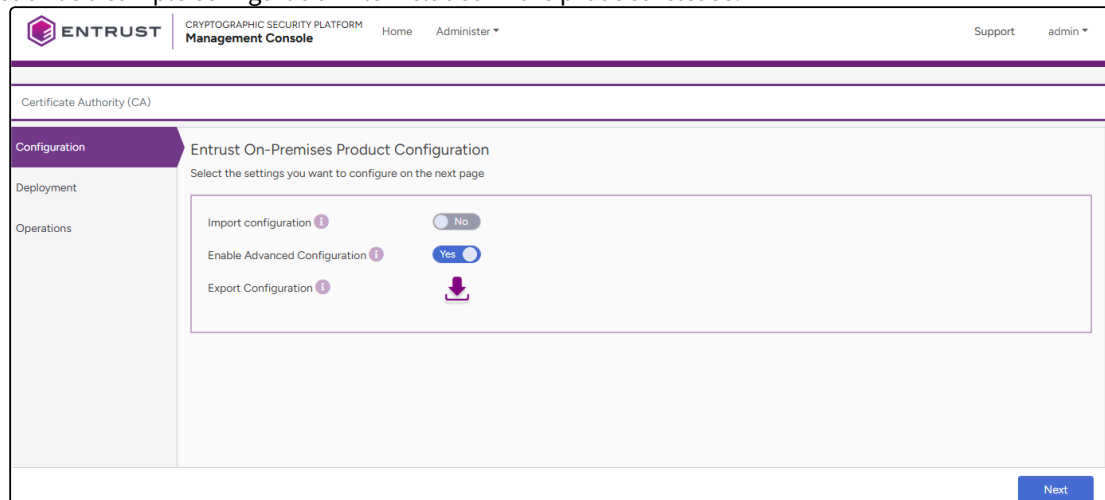
2. Log into the Management Console a user belonging to a role with permissions to manage Certificate Authorities – for example, the initial `admin` administrator user.

 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\(s\)](#)

✖ Certificate Authority and Certificate Manager cannot share the same database.

Database URL

The IP address or Fully Qualified Domain Name (FQDN) of the database host.

⚠ As explained in [Database requirements](#), 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 requirements](#), 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

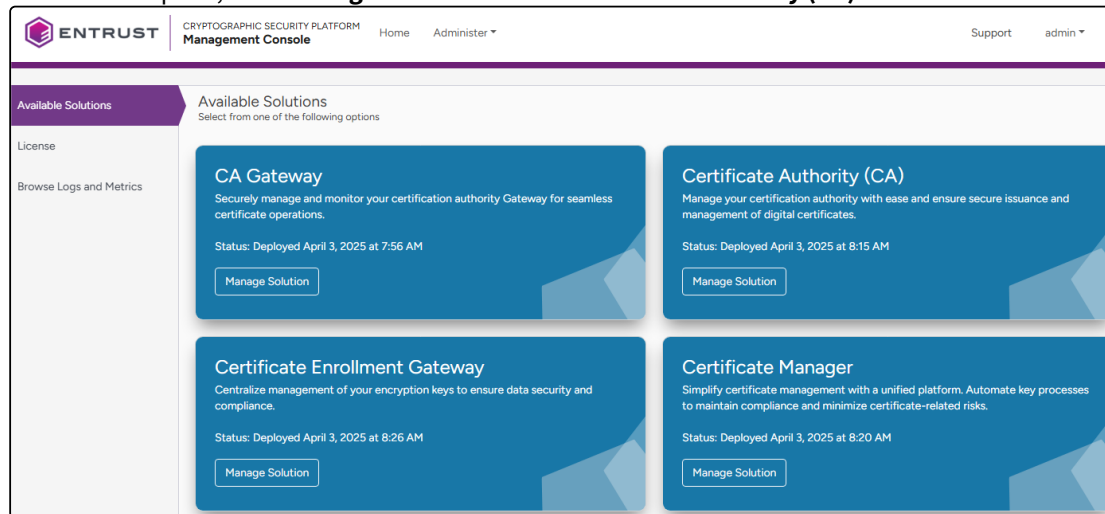
1. Open the following URL in a Web browser.

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

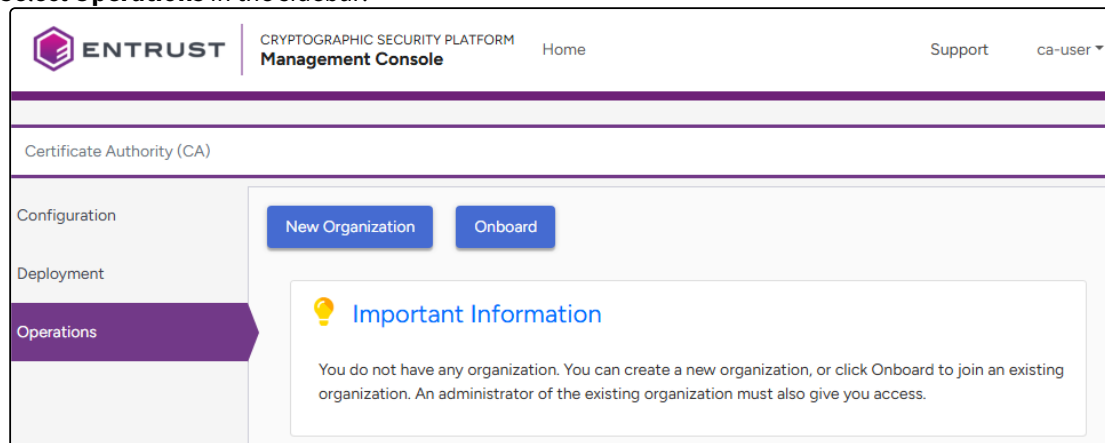
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

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.

3. In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



4. Select **Operations** in the sidebar.



5. Click **New Organization**.
6. 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 start with "test".
 - Cannot match any of the reserved words:
 - acs
 - ca
 - cas
 - crt
 - 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.

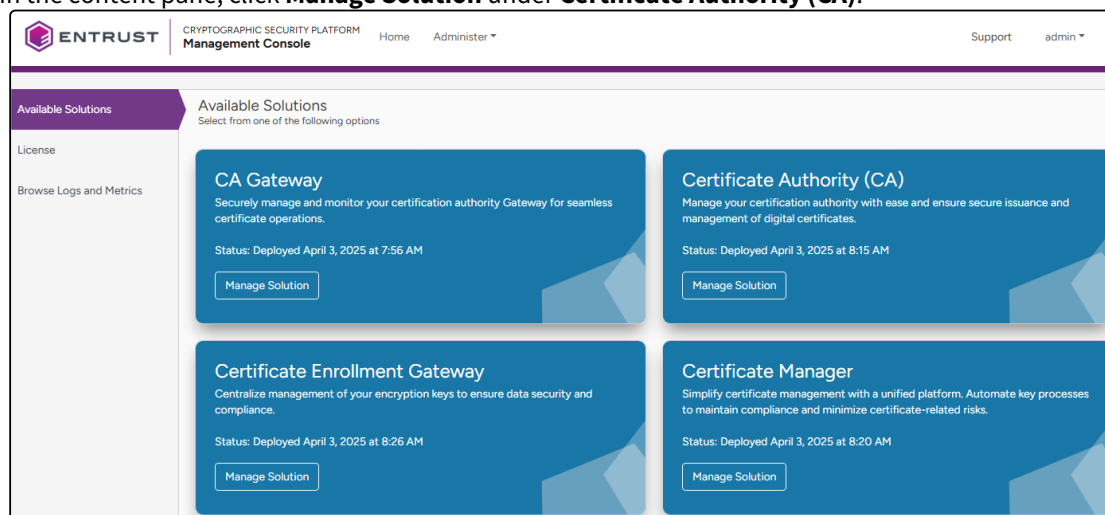
To join an organization

- Open the following URL in a Web browser.

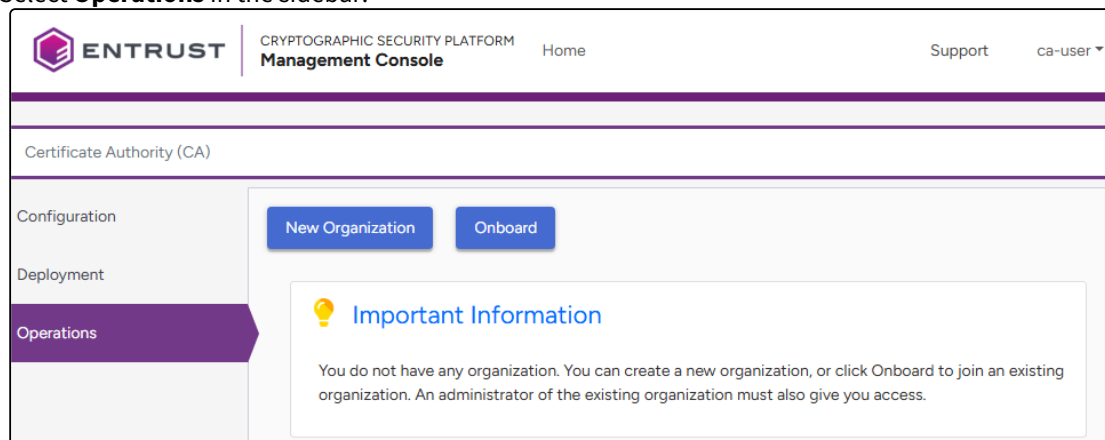
`https://<machine>/management-console`

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.



5. 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.

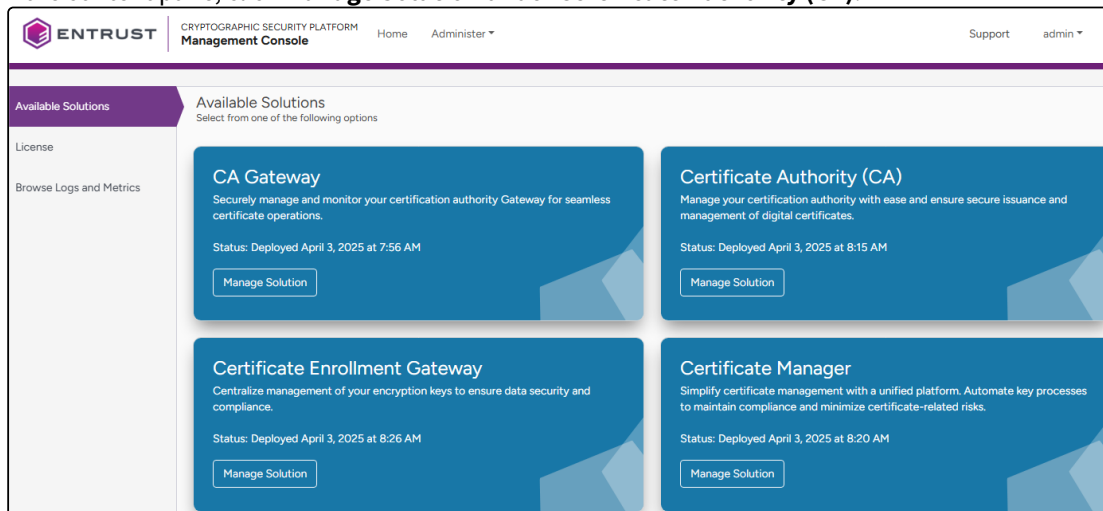
To leave organization

1. Open the following URL in a Web browser.

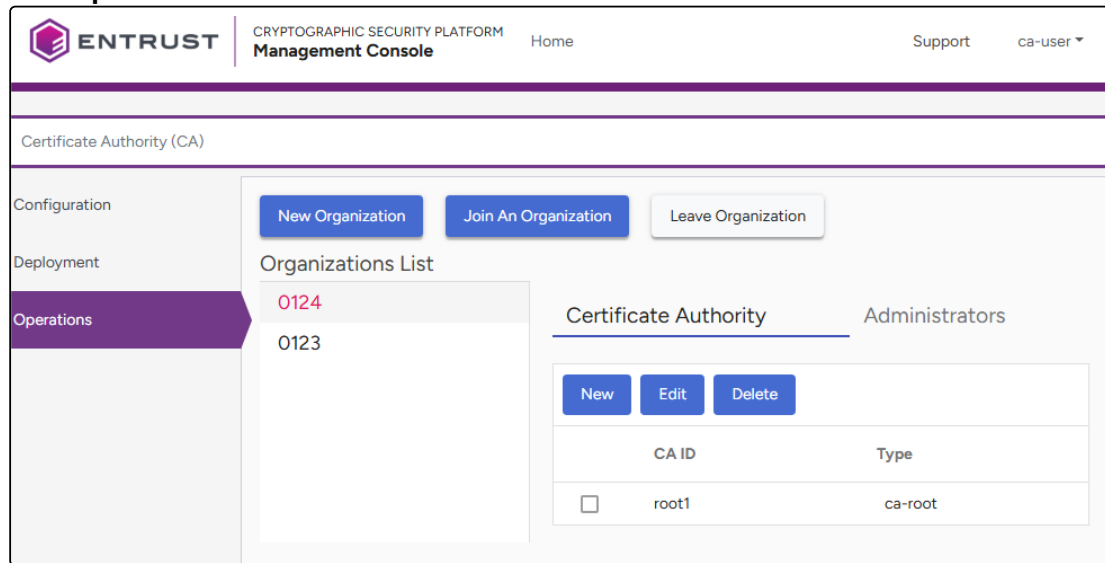
```
https://<machine>/management-console
```

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

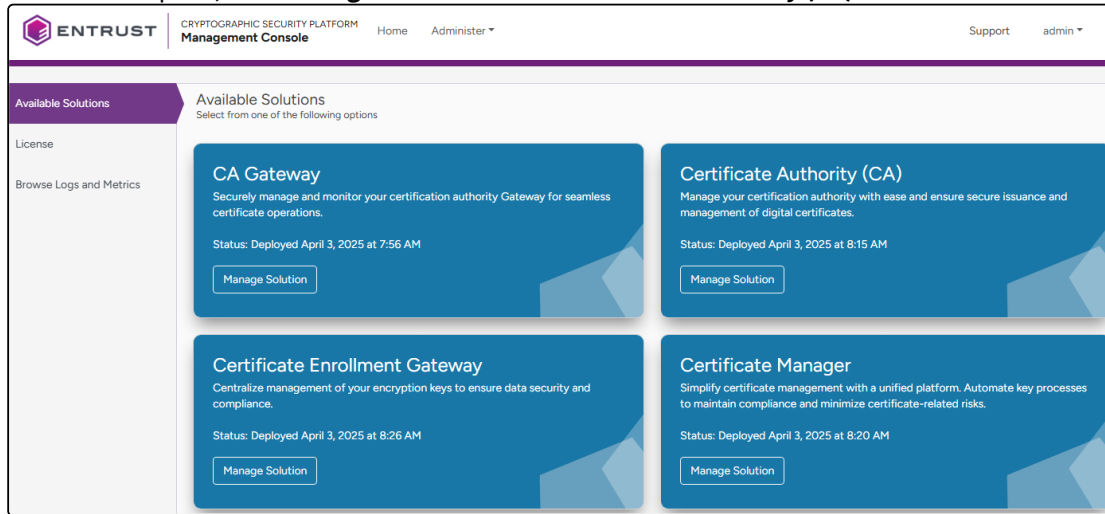
1. Open the following URL in a Web browser.

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

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

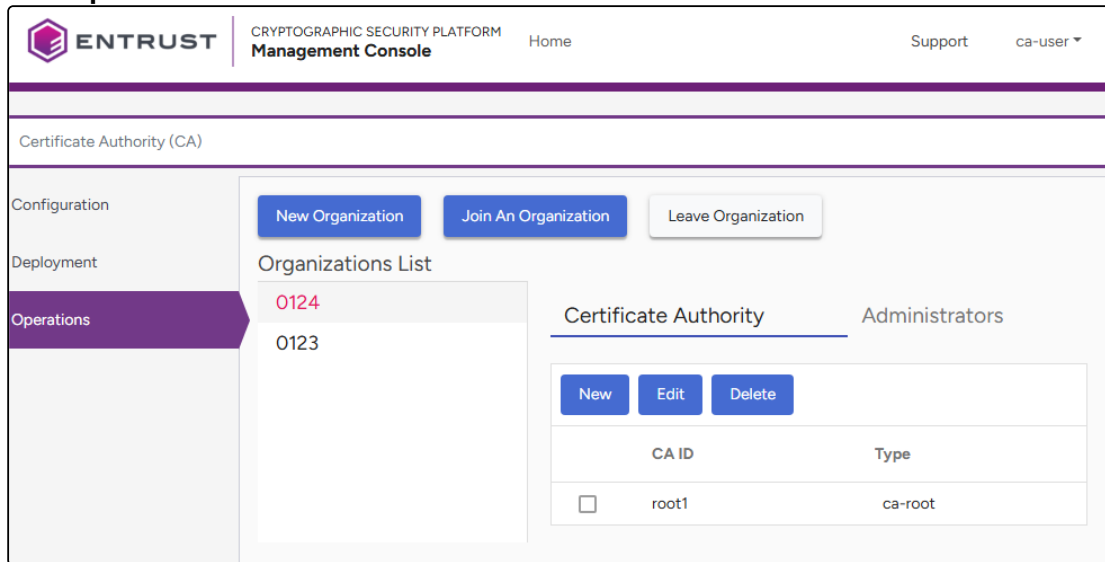
2. Log in to the Management Console as one of the users created in [Creating Certificate Authority tenants](#).

- In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



The screenshot shows the 'Available Solutions' page in the Entrust Management Console. 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 highlighted.

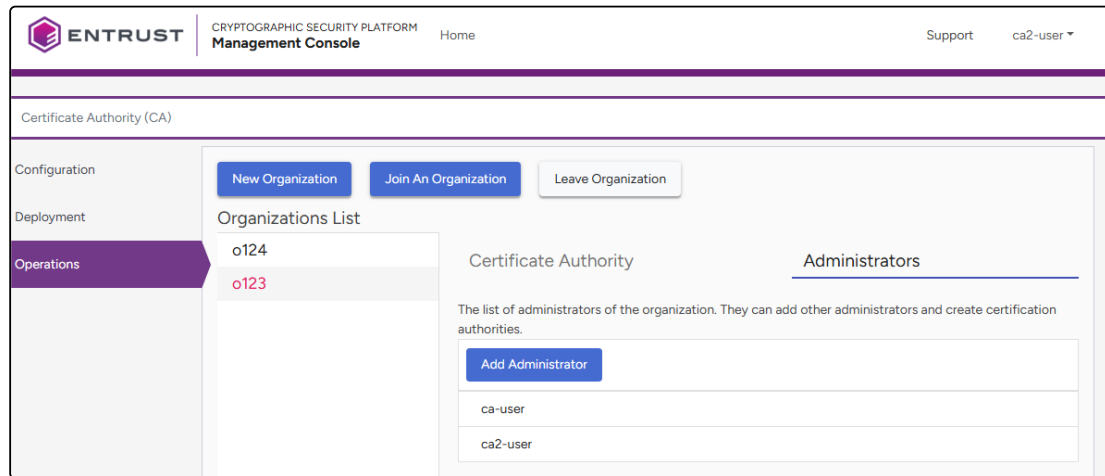
- Select **Operations** in the sidebar.



The screenshot shows the 'Operations' page in the Entrust Management Console. The left sidebar has 'Operations' selected. The main content area displays the 'Organizations List' with buttons for 'New Organization', 'Join An Organization', and 'Leave Organization'. Below the buttons is a list of organizations with IDs '0124' and '0123'. To the right, there are tabs for 'Certificate Authority' and 'Administrators'. The 'Certificate Authority' tab is active, showing a table with columns 'CA ID' and 'Type'. The table contains one entry: 'root1' with type '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 intermediate 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

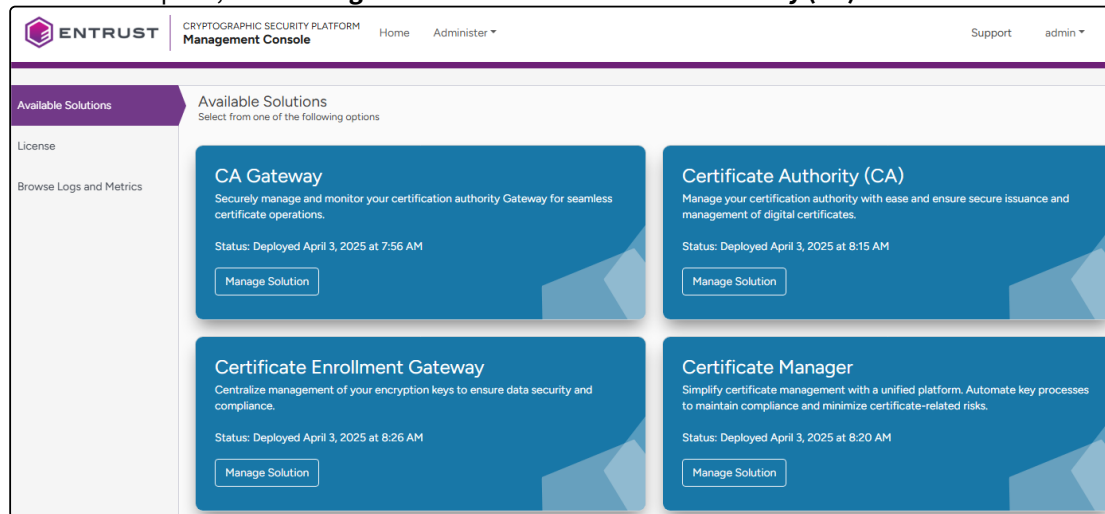
1. Open the following URL in a Web browser.

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

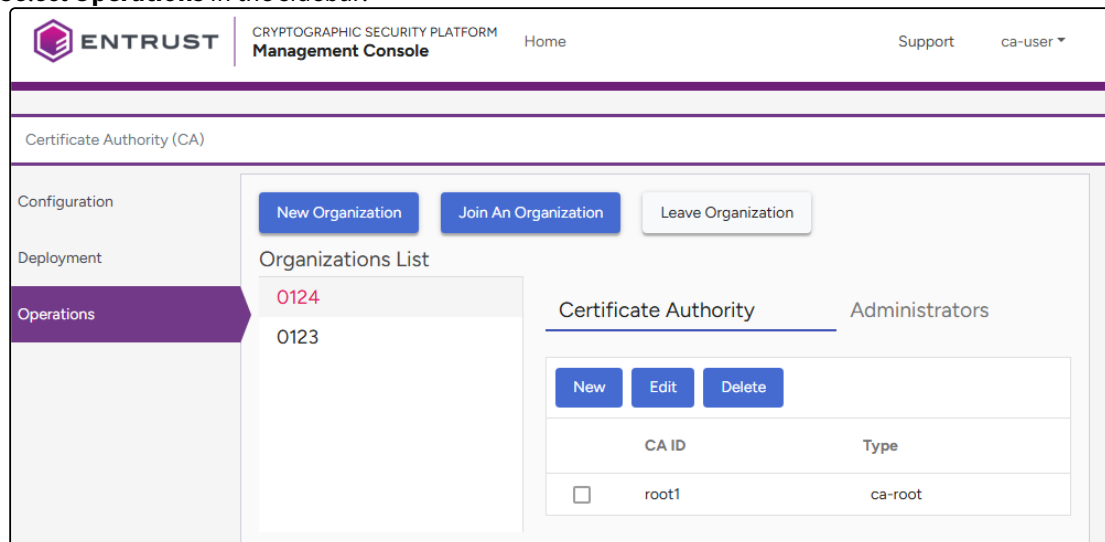
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

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.

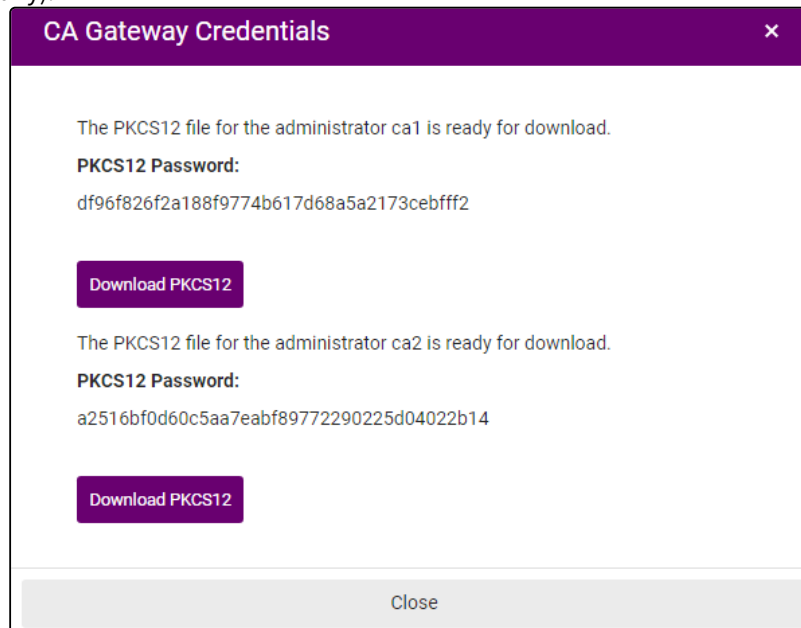


- Select an organization under **Organization List**.

 See [Managing organizations](#) for how to create or join an organization.

- Click **New** under **Certificate Authority**.
- Configure the following settings.
 - CA Type
 - CA Identifier
 - Friendly Name
 - Signing 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).



- Click **Download PKCS12** to download the PKCS #12 files. Each PKCS #12 includes:
 - The certificate of the CA that issues the client certificates.
 - A client certificate.
 - The private key of the client certificate.
- 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 Identifier

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.

Friendly Name

A friendly name for the new Certificate Authority in the user interface.

Mandatory: No. This optional value defaults to the one assigned to the **CA Identifier** field.

Signing Key Type

The type of key the new Certificate Authority will use to sign certificates. For a production environment with hardware cryptography, this drop-down list includes the following key types.

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

For a testing environment with software cryptography, the list also includes the algorithms described in [Post-quantum key types](#).

 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
Intermediate Certificate Authority	10 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.

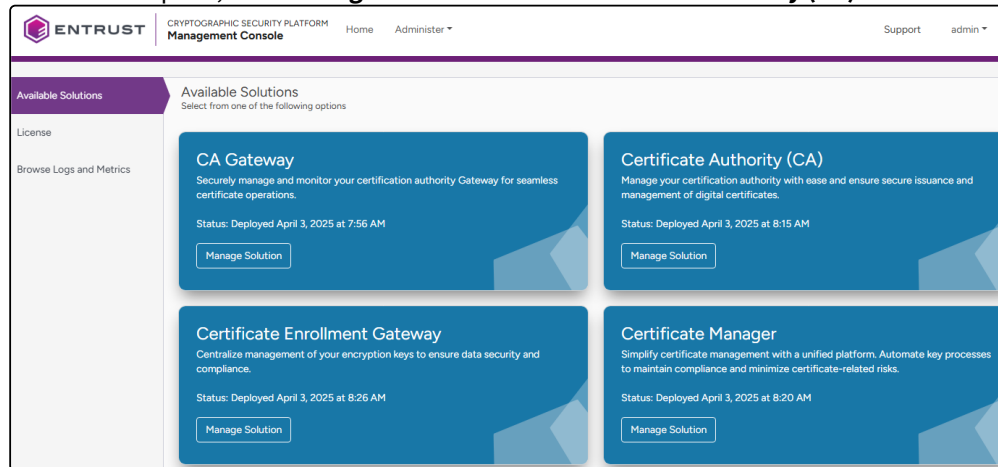
To add an external root Certificate Authority

1. Open the following URL in a Web browser.

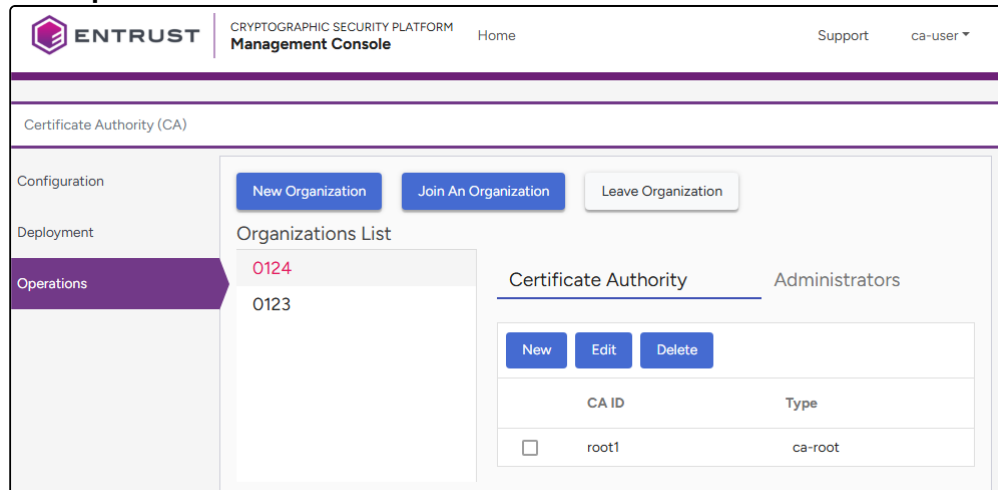
```
https://<machine>/management-console
```

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

- 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.
- 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 Identifier](#)
 - [Friendly Name](#)
 - [Self-Signed Root Certificate](#)
- Click **Submit** to create the new Certificate Authority.

CA Type

Click **External Root Certificate Authority**.

Mandatory: Yes.

CA Identifier

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.

Friendly Name

A friendly name for the new Certificate Authority in the user interface.

Mandatory: No. This optional value defaults to the one assigned to the **CA Identifier** field.

Self-Signed Root Certificate

Paste the PEM-encoded certificate signing certificate of the external CA – for example:

```
-----BEGIN CERTIFICATE-----
MIIEKjCCAxKgAwIBAgIEOGPe+DANBgkqhkiG9w0BAQUFADCBTDEUMBIGA1UEChMLRW50cnVzdC5u
ZXQxQDA+BgNVBAsUN3d3dy5lbnRydXN0Lm5ldC9DUFNFmJA0OCBpbmNvcnAuIGJ5IHJlZi4gKGxp
bWl0cyBsaWFiLikxJTAjBgNVBAsTHChjKSAXOTk5IEVudHJ1c3QubmV0IExpbWl0ZWQxMzAxBgNV
...
zX1XEC+bBA1ahLVu2B064dae0Wx5XnkcFMXj0EyT02U87d89vqb1LRrDtRnDvV5bu/8j72gZyxKT
J1wDLW8w0B62GqzeWvFRqqgnpv55gcR5mTNXuhKwqeBCbJPKVt7+bYQLCIt+jerXmCHG8+c8eS9e
nNFMFY3h7CI3zJpDC5fcgJCns2ebb0gIFVbPv/Er fF6adu1ZkMV8gzURZVE=
-----END CERTIFICATE-----
```

Mandatory: Yes.

Creating an intermediate Certificate Authority

An intermediate Certificate Authority (CA):

- Operates under the authority of a root or intermediate CA.
- Issues digital certificates for subordinate CAs or for other intermediate CAs.

See below for how to create an intermediate CA.

To create an intermediate Certificate Authority

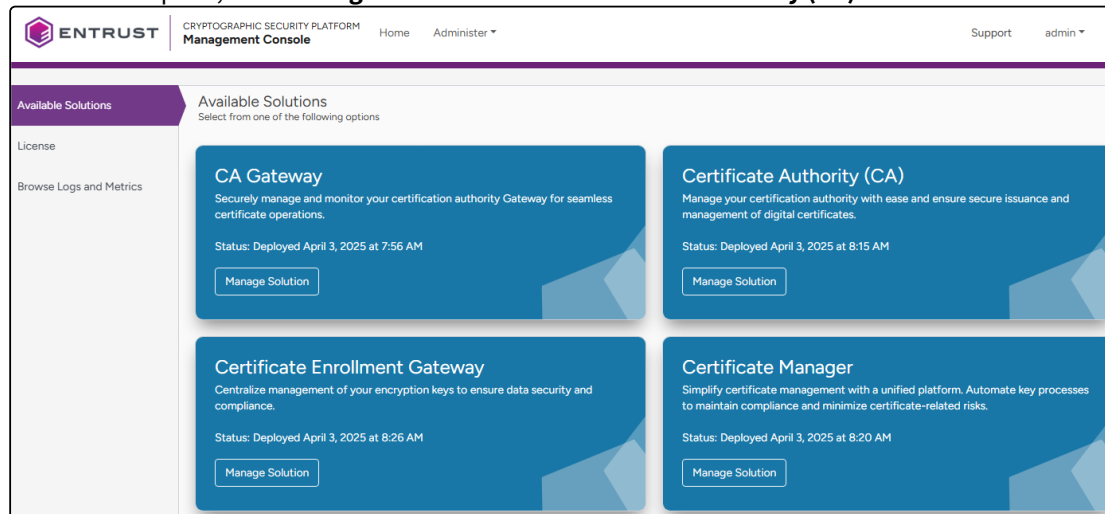
1. Open the following URL in a Web browser.

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

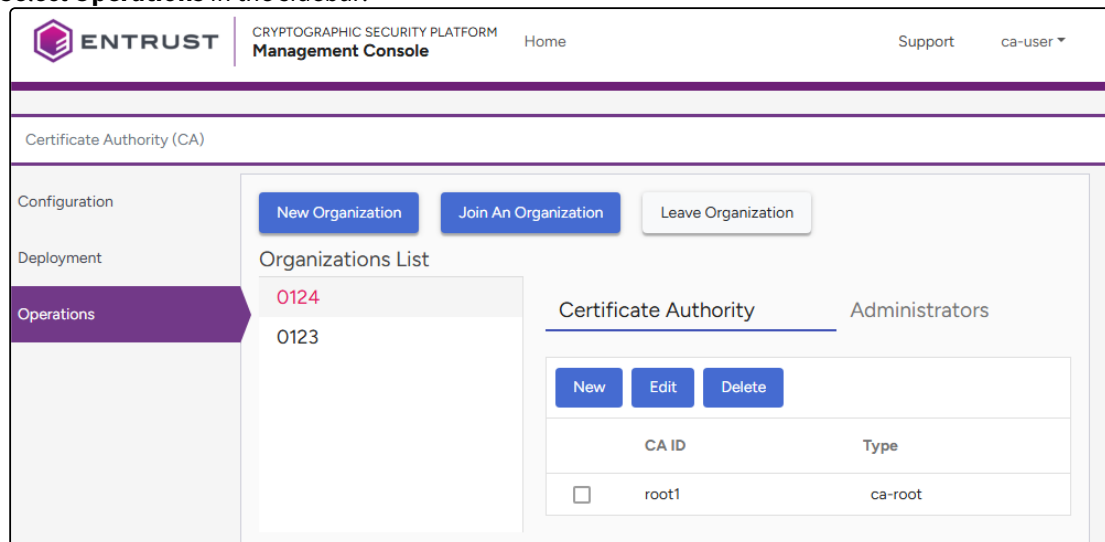
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

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 intermediate Certificate Authority.

- In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



- Select **Operations** in the sidebar.

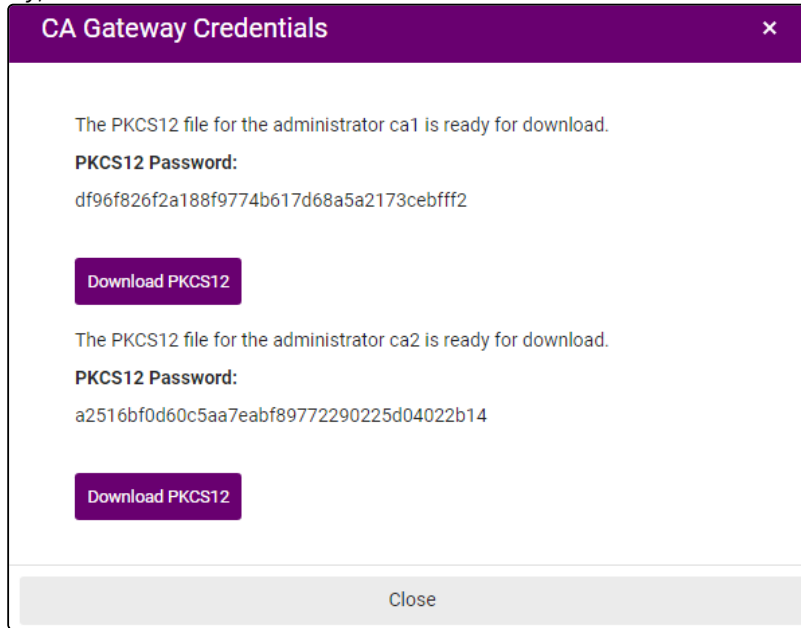


- Select an organization under **Organizations list**.

 See [Managing organizations](#) for how to create or join an organization.

- Click **New** under **Certificate Authority**.
- Configure the following settings.
 - CA Type
 - CA Identifier
 - Signing Key Type
 - Certificate Profiles
 - Parent CA Identifier
 - Expiration Date
 - Attributes
 - Auditors
 - Administrators
- 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).



CA Gateway Credentials [X]

The PKCS12 file for the administrator ca1 is ready for download.

PKCS12 Password:
df96f826f2a188f9774b617d68a5a2173cebfff2

Download PKCS12

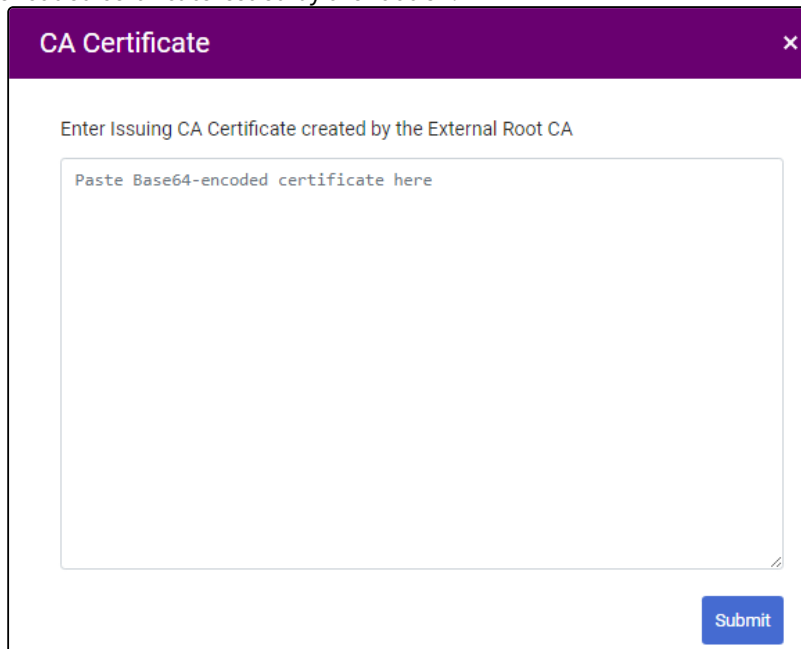
The PKCS12 file for the administrator ca2 is ready for download.

PKCS12 Password:
a2516bf0d60c5aa7eabf89772290225d04022b14

Download PKCS12

Close

10. Click **Download** to download the PKCS #12 files. Each PKCS #12 includes:
 - The certificate of the CA that issues the client certificates.
 - 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 intermediate CA is an external root CA, click **Upload certificate** and paste a PEM-encoded certificate issued by the root CA.



CA Certificate [X]

Enter Issuing CA Certificate created by the External Root CA

Paste Base64-encoded certificate here

Submit

CA Type

Click **Intermediate Subordinate Authority**.

Mandatory: Yes.

CA Identifier

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.

Signing Key Type

The type of key the new Certificate Authority will use to sign certificates. For a production environment with hardware cryptography, this drop-down list includes the following key types.

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

For a testing environment with software cryptography, the list also includes the algorithms described in [Post-quantum key types](#).

 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.

Parent CA Identifier

The identifier of the parent Certificate Authority.

 The [Intermediate authority certificate profile](#) must be enabled in the selected parent 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
Intermediate Certificate Authority	10 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.

Creating an issuing Certificate Authority

See below for creating a certificate issuing or *subordinate* Certificate Authority (CA).

i 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.

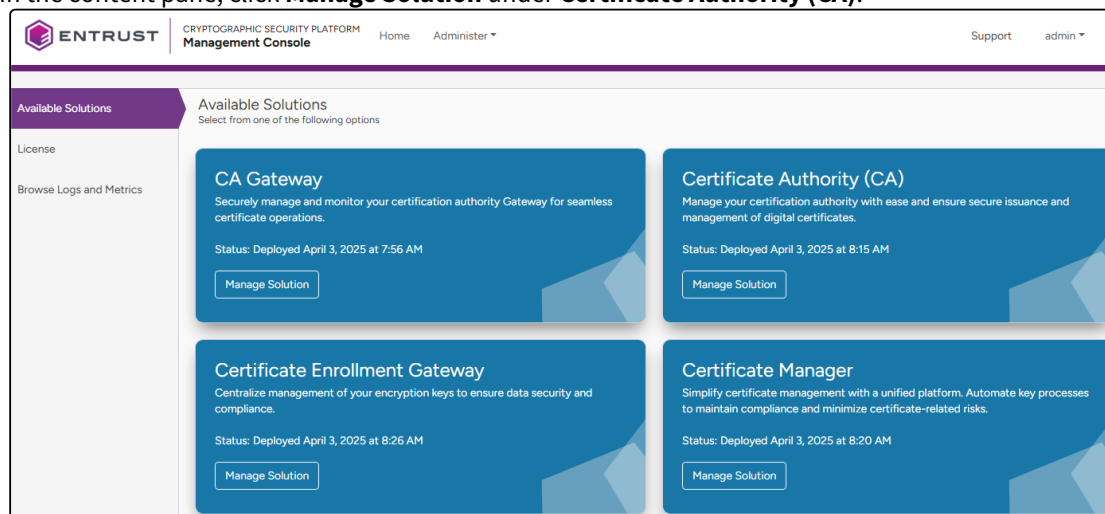
To create an issuing Certificate Authority

1. Open the following URL in a Web browser.

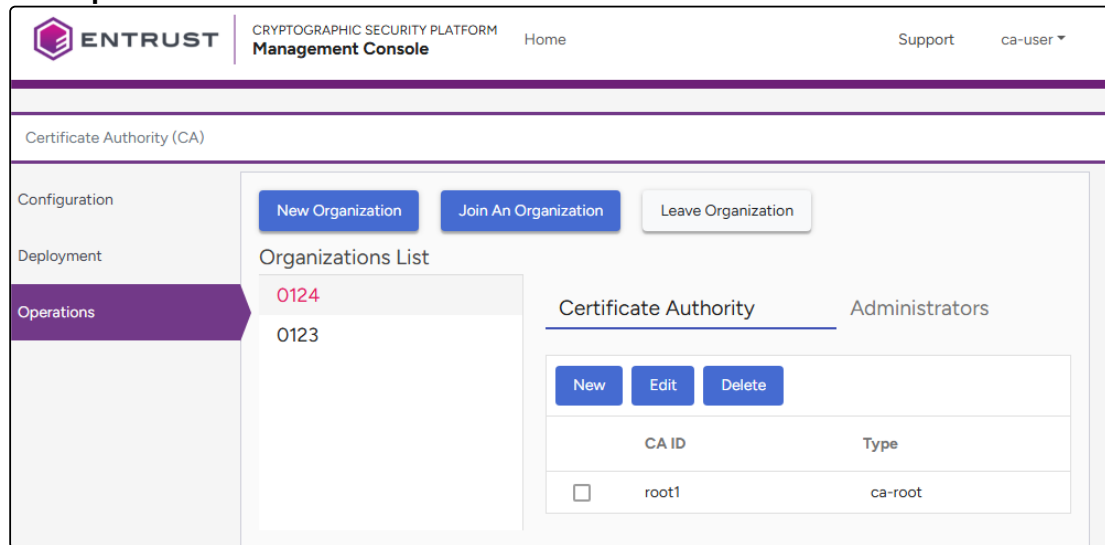
`https://<machine>/management-console`

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.
3. In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



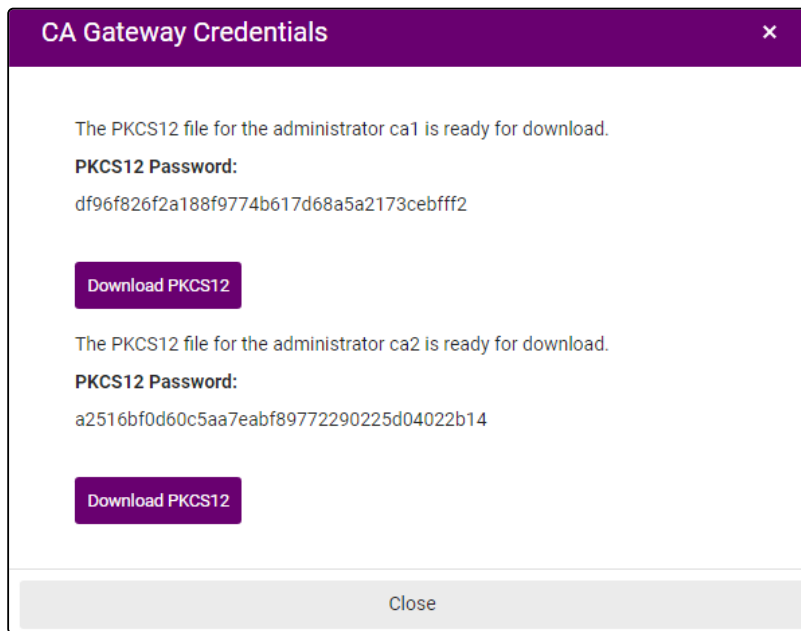
4. Select **Operations** in the sidebar.



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 Identifier](#)
 - [Friendly Name](#)
 - [Signing Key Type](#)
 - [Certificate Profiles](#)
 - [Issuer CA ID](#)
 - [Expiration Date](#)
 - [Attributes](#)
 - [Auditors](#)
 - [Administrators](#)
 - [OCSP Key Type](#)
8. 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).



CA Gateway Credentials [X]

The PKCS12 file for the administrator ca1 is ready for download.

PKCS12 Password:
df96f826f2a188f9774b617d68a5a2173cebfff2

Download PKCS12

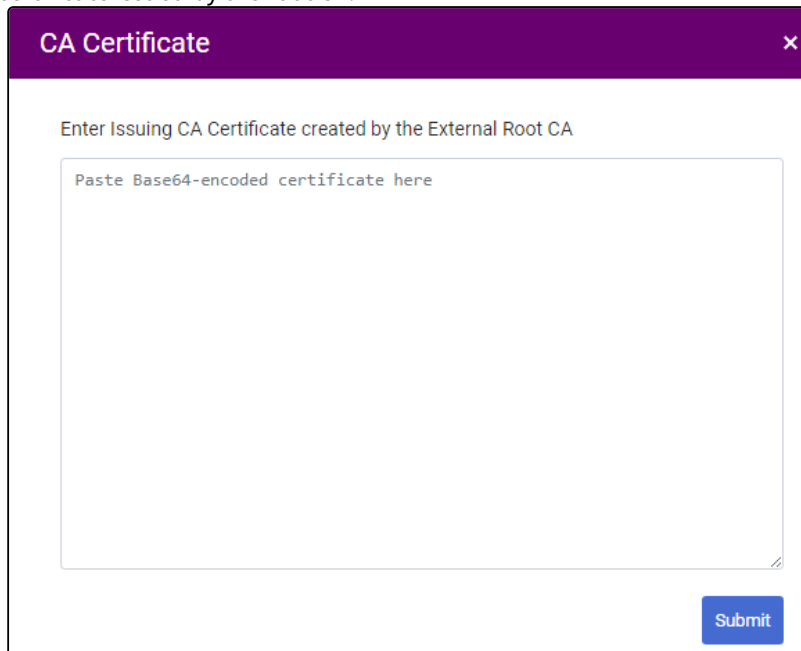
The PKCS12 file for the administrator ca2 is ready for download.

PKCS12 Password:
a2516bf0d60c5aa7eabf89772290225d04022b14

Download PKCS12

Close

10. Click **Download** to download the PKCS #12 files. Each PKCS #12 includes:
 - The certificate of the CA that issues the client certificates.
 - 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 issued by the root CA.



CA Certificate [X]

Enter Issuing CA Certificate created by the External Root CA

Paste Base64-encoded certificate here

Submit

CA Type

Click **Issuing Certificate Authority**.

Mandatory: Yes.

CA Identifier

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.

Friendly Name

A friendly name for the new Certificate Authority in the user interface.

Mandatory: No. This optional value defaults to the one assigned to the **CA Identifier** field.

Signing Key Type

The type of key the new Certificate Authority will use to sign certificates. For a production environment with hardware cryptography, this drop-down list includes the following key types.

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

For a testing environment with software cryptography, the list also includes the algorithms described in [Post-quantum key types](#).

 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
Intermediate Certificate Authority	10 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.

OCSP Key Type

The type of key to sign OCSP 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.

For a production environment with hardware cryptography, this drop-down list includes the following key types.

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

For a testing environment with software cryptography, the list also includes the algorithms described in [Post-quantum key types](#).

i NIST will deprecate some algorithms after Dec 31, 2030. See <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>

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.

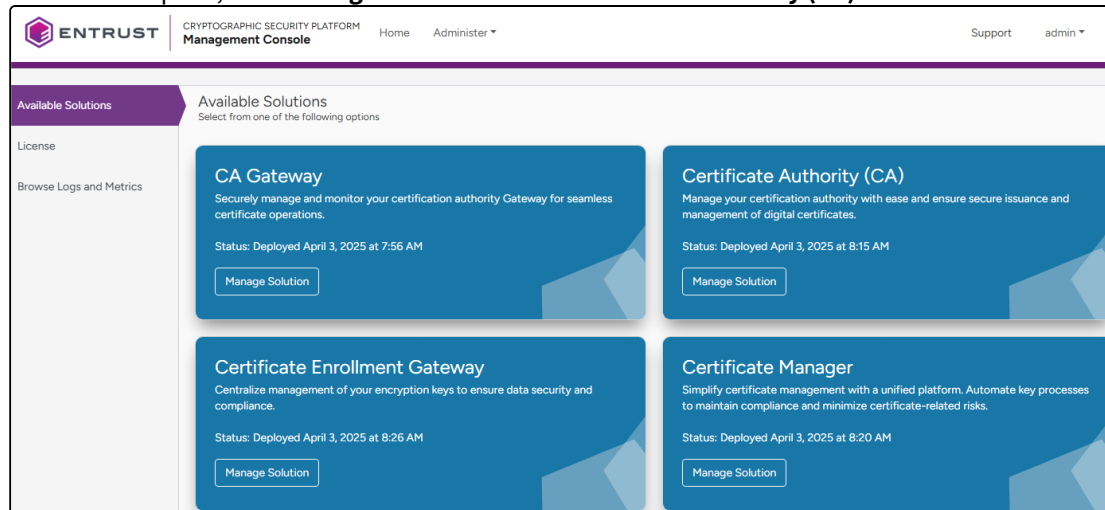
To delete a Certificate Authority

1. Open the following URL in a Web browser.

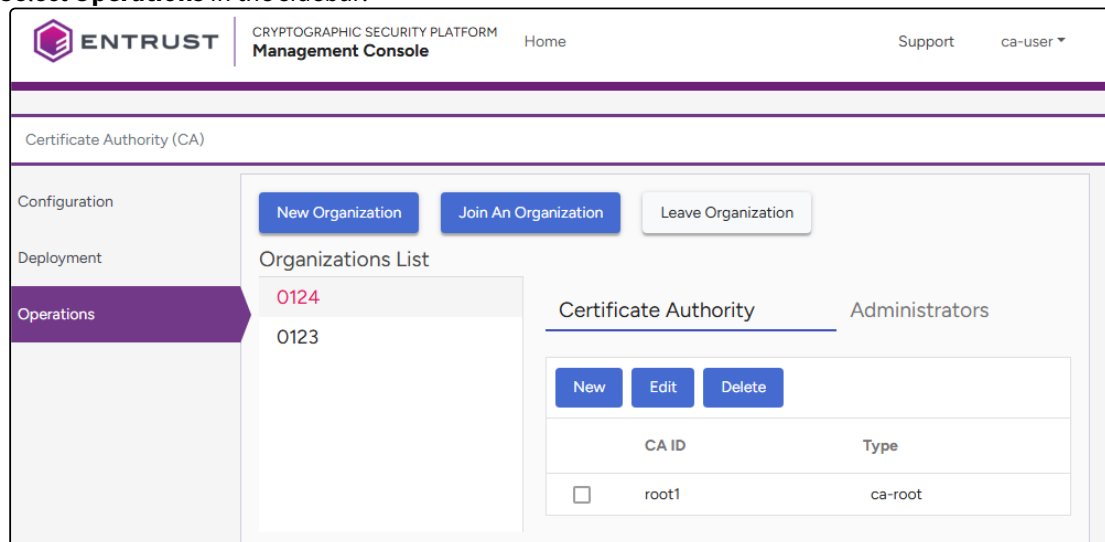
`https://<machine>/management-console`

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).

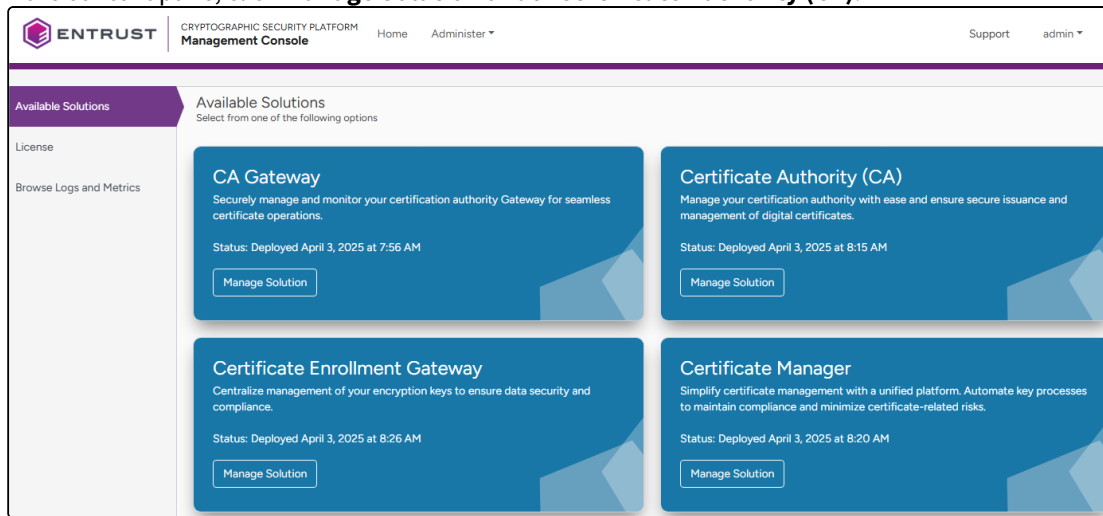
To edit a Certificate Authority

1. Open the following URL in a Web browser.

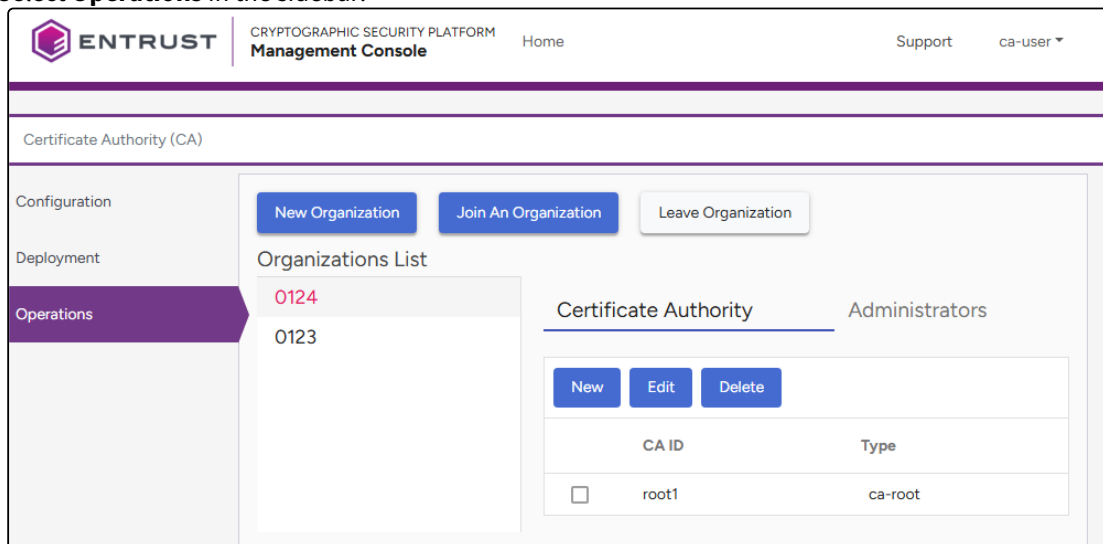
`https://<machine>/management-console`

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 [Creating an issuing Certificate Authority](#).

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 existing 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**.

i 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.

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 1.1.0. 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.

- [Configuring an on-premises Entrust Certificate Authority for Certificate Enrollment Gateway](#)
- [Deploying Entrust CA Gateway for an on-premises CA](#)
- [Deploying an external database for Certificate Enrollment 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 CMPv2 enrollment](#)

- [Configuring an on-premises Entrust Certificate Authority for EST 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 CMPv2 enrollment

If you will use Certificate Enrollment Gateway with an on-premises CA for CMPv2 enrollment, you must configure the CA as described in the following sections. For detailed information about configuring the CA, see the documentation for your CA.

- [Adding certificate types to Entrust Certificate Authority for CMPv2 enrollment](#)
- [Mapping certificate definition policies to the CMPv2 certificate types](#)

Adding certificate types to Entrust Certificate Authority for CMPv2 enrollment

For CMPv2 enrollment, you must add the following certificate types to the on-premises CA for CMPv2 enrollment:

- signing
- encryption
- dual usage (signing and encryption)
- non-repudiation.

To add CMPv2 certificate types to the on-premises CA

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 CMPv2  
; -----  
ent_cmpv2_sig=enterprise,CMPv2 Signing,CMPv2 Signing Certificate  
ent_cmpv2_enc=enterprise,CMPv2 Encryption,CMPv2 Encryption Certificate  
ent_cmpv2_sig_enc=enterprise,CMPv2 Signing and Encryption,CMPv2 Signing and  
Encryption Certificate  
ent_cmpv2_sig_nonrep=enterprise,CMPv2 Signing and Nonrepudiation,CMPv2 Signing  
and Nonrepudiation Certificate  
; -----
```

5. Add the following lines to the [\[Extension Definitions\]](#) section.

```
; -----  
; Certificate definitions to be used with CMPv2  
; -----  
[ent_cmpv2_sig Certificate Definitions]  
1=Verification_p10  
  
[ent_cmpv2_sig Verification_p10 Extensions]  
keyusage=2.5.29.15,n,m,BitString,1  
  
[ent_cmpv2_sig Advanced]  
noUserInDirectory=1  
  
[ent_cmpv2_enc Certificate Definitions]  
1=Encryption_p10  
  
[ent_cmpv2_enc Encryption_p10 Extensions]  
keyusage=2.5.29.15,n,m,BitString,001  
  
[ent_cmpv2_enc Advanced]  
noUserInDirectory=1  
  
[ent_cmpv2_sig_enc Certificate Definitions]  
1=Dual Usage  
  
[ent_cmpv2_sig_enc Dual Usage Extensions]  
keyusage=2.5.29.15,n,m,BitString,101  
  
[ent_cmpv2_sig_enc Advanced]  
noUserInDirectory=1  
  
[ent_cmpv2_sig_nonrep Certificate Definitions]  
1=Nonrepudiation  
  
[ent_cmpv2_sig_nonrep Nonrepudiation Extensions]  
keyusage=2.5.29.15,n,m,BitString,11  
  
[ent_cmpv2_sig_nonrep Advanced]
```

```
noUserInDirectory=1
; -----
```

6. Save and close the file.
7. Import the certificate specifications back into the CA. In Entrust Certificate Authority Administration, select **File > Certificate Specifications > Import**.

Mapping certificate definition policies to the CMPv2 certificate types

In Entrust Certificate Authority, map certificate definition policies to the certificate types created in [Adding certificate types to Entrust Certificate Authority for CMPv2 enrollment](#).

- [Mapping to the CMPv2 Encryption certificate type](#)
- [Mapping to the CMPv2 Signing certificate type](#)
- [Mapping to the CMPv2 Signing and Encryption certificate type](#)
- [Mapping to the CMPv2 Signing and Nonrepudiation certificate type](#)

Mapping to the CMPv2 Encryption certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the CMPv2 Encryption certificate type.

To map a certificate definition policy to the CMPv2 Encryption certificate type

1. Log in to Entrust Certificate Authority Administration or Security Manager Administration for the CA.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > CMPv2 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 CMPv2 Signing certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the CMPv2 Signing certificate type.

To map a certificate definition policy to the CMPv2 Signing certificate type

1. Log in to Entrust Certificate Authority Administration or Security Manager Administration for the CA.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > CMPv2 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 CMPv2 Signing and Encryption certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the CMPv2 Signing and Encryption certificate type.

To map a certificate definition policy to the CMPv2 Signing and Encryption certificate type

1. Log in to Entrust Certificate Authority Administration or Security Manager Administration for the CA.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > CMPv2 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 CMPv2 Signing and Nonrepudiation certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the CMPv2 Signing and Nonrepudiation certificate type.

To map a certificate definition policy to the CMPv2 Signing and Nonrepudiation certificate type

1. Log in to Entrust Certificate Authority Administration or Security Manager Administration for the CA.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > CMPv2 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 EST enrollment

See below for configuring an on-premises Entrust Certificate Authority to use with Certificate Enrollment Gateway and EST enrollment.

- [Configuring Entrust Certificate Authority to allow server-generated keys for EST enrollment](#)
- [Creating a client policy and role for EST enrollments](#)
- [Adding certificate types to Entrust Certificate Authority for EST enrollment](#)
- [Creating certificate definition policies for EST certificate types](#)
- [Mapping certificate definition policies to the EST certificate types](#)

Configuring Entrust Certificate Authority to allow server-generated keys for EST enrollment

For EST 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.

Creating a client policy and role for EST enrollments

In Certificate Enrollment Gateway, EST enrollment enrolls a user with a PKCS #12 digital ID. To allow PKCS #12 enrollment through the EST protocol, the client policy assigned to user's role must allow PKCS #12 enrollment. To allow PKCS #12 enrollment, the user's client policy must have the **Allow PKCS#12 Export** and **All Exportable** policy attributes.

The following procedures describe how to create a new client policy and role that allows PKCS #12 export.

- [Creating a client policy for EST enrollment](#)
- [Creating a role for EST enrollment](#)



Both MDMWS and EST enrollments require PKCS #12 export. You can use the same client policy and role for MDMWS and EST enrollments.

Creating a client policy for EST enrollment

See below to create an Entrust Certificate Authority client policy that allows PKCS #12 export for EST enrollment.

To create a client policy for EST 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 EST enrollment

See below to create an Entrust Certificate Authority role that is assigned the client policy you created earlier for EST enrollment.



In CA Gateway, the CA profile that will be used by Certificate Enrollment Gateway for EST enrollment must assign this role to end users. The XAP administrator profile used to manage the CA profile must also have permissions to administer this role.

To create a role in for EST 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.

Adding certificate types to Entrust Certificate Authority for EST enrollment

For EST enrollment, you must add the following certificate types to Entrust Certificate Authority:

- signing
- encryption
- dual usage (signing and encryption)
- non-repudiation.

To add EST 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 EST
; -----
ent_est_sig=enterprise,EST Signing,EST Signing Certificate
ent_est_enc=enterprise,EST Encryption,EST Encryption Certificate
ent_est_sig_enc=enterprise,EST Signing and Encryption,EST Signing and
Encryption Certificate
ent_est_nonrep=enterprise,EST Signing and Nonrepudiation,EST Signing and
Nonrepudiation Certificate
; -----
```

5. Add the following lines to the `[Extension Definitions]` section.

```
; -----
; Certificate definitions to be used with EST
; -----
[ent_est_sig Certificate Definitions]
1=Verification

[ent_est_sig Verification Extensions]
keyusage=2.5.29.15,n,m,BitString,1

[ent_est_sig Advanced]
noUserInDirectory=1

[ent_est_enc Certificate Definitions]
1=Encryption

[ent_est_enc Encryption Extensions]
keyusage=2.5.29.15,n,m,BitString,001

[ent_est_enc Advanced]
noUserInDirectory=1

[ent_est_sig_enc Certificate Definitions]
1=Dual Usage

[ent_est_sig_enc Dual Usage Extensions]
keyusage=2.5.29.15,n,m,BitString,101

[ent_est_sig_enc Advanced]
noUserInDirectory=1

[ent_est_nonrep Certificate Definitions]
1=Nonrepudiation

[ent_est_nonrep Nonrepudiation Extensions]
keyusage=2.5.29.15,n,m,BitString,11

[ent_est_nonrep Advanced]
noUserInDirectory=1
; -----
```


6. Save and close the file.
7. Import the certificate specifications back into the CA. In Entrust Certificate Authority Administration, select **File > Certificate Specifications > Import**.

Creating certificate definition policies for EST 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 EST 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 EST certificate types](#).

- [Creating a Dual Usage P12 certificate definition policy for EST enrollment](#)
- [Creating an Encryption P12 certificate definition policy for EST enrollment](#)
- [Creating a Verification P12 certificate definition policy for EST enrollment](#)
- [Creating a Nonrepudiation P12 certificate definition policy for EST enrollment](#)

Creating a Dual Usage P12 certificate definition policy for EST enrollment

See below to create a Dual Usage P12 certificate definition policy in Entrust Certificate Authority.

To create a Dual Usage P12 certificate definition policy for EST enrollment

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 EST Policy`.
5. In the **Common name** field, enter `Dual Usage EST 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 for EST enrollment

See below to create an Encryption P12 certificate definition policy in Entrust Certificate Authority.

To create an Encryption P12 certificate definition policy for EST enrollment

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 EST Policy`.
5. In the **Common name** field, enter `Encryption EST 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 for EST enrollment

See below to create a Verification P12 certificate definition policy in Entrust Certificate Authority.

To create a Verification P12 certificate definition policy for EST enrollment

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 EST Policy`.
5. In the **Common name** field, enter `Verification EST 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 for EST enrollment

See below to create a Nonrepudiation P12 certificate definition policy in Entrust Certificate Authority.

To create a Nonrepudiation P12 certificate definition policy for EST enrollment

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 EST Policy`.
5. In the Common name field, enter `Nonrepudiation EST Policy`.
6. Under **Policy Attributes**:
 - Select **Back up private key**.
 - Deselect **Generate key at client**.
7. Click **Apply**.
8. If prompted, authorize the operation.

Mapping certificate definition policies to the EST certificate types

Map the certificate definition policies created in [Creating certificate definition policies for EST certificate types](#).

- [Mapping a certificate definition policy to the EST Encryption certificate type](#)
- [Mapping a certificate definition policy to the EST Signing certificate type](#)
- [Mapping a certificate definition policy to the EST Signing and Encryption certificate type](#)
- [Mapping a certificate definition policy to the EST Signing and Nonrepudiation certificate type](#)

Mapping a certificate definition policy to the EST 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 EST Encryption certificate type

1. Log in to Entrust Certificate Authority Administration or Security Manager Administration for the CA.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > EST Encryption > Encryption**.
3. In the **Certificate definition Policy** drop-down list, select **Encryption EST Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping a certificate definition policy to the EST 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 EST Signing certificate type

1. Log in to [Entrust Certificate Authority Administration](#) or [Security Manager Administration](#) for the CA.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > EST Signing > Verification**.
3. In the **Certificate definition Policy** drop-down list, select **Verification EST Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping a certificate definition policy to the EST 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 EST Signing and Encryption certificate type

1. Log in to [Entrust Certificate Authority Administration](#) or [Security Manager Administration](#) for the CA.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > EST Signing and Encryption > Dual Usage**.
3. In the **Certificate definition Policy** drop-down list, select **Dual Usage EST Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping a certificate definition policy to the EST 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 EST Signing and Nonrepudiation certificate type

1. Log in to [Entrust Certificate Authority Administration](#) or [Security Manager Administration](#) for the CA.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > EST Signing and Nonrepudiation > Nonrepudiation**.
3. In the **Certificate definition Policy** drop-down list, select **Nonrepudiation EST 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.

- [Configuring Entrust Certificate Authority to allow server-generated keys for MDM-SCEP enrollment](#)
- [Adding certificate types to Entrust Certificate Authority for MDM-SCEP enrollment](#)
- [Mapping certificate definition policies to the MDM-SCEP certificate types](#)

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.

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**.

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.

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.

- [Configuring Entrust Certificate Authority to allow server-generated keys for MDMWS enrollment](#)
- [Creating a client policy and role for MDMWS P12 enrollments](#)
- [Adding certificate types to Entrust Certificate Authority for MDMWS P12 enrollment](#)
- [Creating certificate definition policies for MDMWS P12 certificate types](#)
- [Mapping certificate definition policies to the MDMWS P12 certificate types](#)

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.

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](#)



Both MDMWS and EST enrollments require PKCS #12 export. You can use the same client policy and role for MDMWS and EST enrollments.

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 that 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.

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 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 Nonrepudation 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.

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 Nonrepudation 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 Nonrepudation certificate type

See below to map Entrust Certificate Authority certificate definition policies to the MDMWS P12 Signing and Nonrepudation certificate type.

To map a certificate definition policy to the MDMWS P12 Signing and Nonrepudation 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.

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 Nonrepudiation 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.

- [Configuring certificates issued by Entrust Certificate Authority for WSTEP enrollment](#)
- [Adding certificate types to Entrust Certificate Authority for WSTEP enrollment](#)
- [Mapping certificate definition policies to the WSTEP certificate types](#)

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). For information about specifying CRL distribution points, see the [Entrust Certificate Authority documentation](#).

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**.

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.

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.

- [Issuing a client credential for Certificate Enrollment Gateway](#)
- [Generating a file containing the CA certificate chain for the CSP CA Gateway server certificate](#)
- [Defining profiles in CSP CA Gateway for issuing RA certificates](#)
- [Configuring CSP CA Gateway for ACMEv2 enrollment](#)

- [Configuring CSP CA Gateway for CMPv2 enrollment](#)
- [Configuring CSP CA Gateway for EST enrollment](#)
- [Configuring CSP CA Gateway for MDM-SCEP enrollment](#)
- [Configuring CSP CA Gateway for MDMWS P12 enrollment](#)
- [Configuring CSP CA Gateway for SCEP and Intune-SCEP enrollment](#)
- [Configuring CSP CA Gateway for WSTEP enrollment](#)

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](#).

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 Keystore	You can re-use the CA Gateway Keystore if it contains the CA certificate chain. The file must contain at least one Trusted CA Certificate entry (TrustedCertEntry).
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.

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**.

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**.

Configuring CSP CA Gateway for CMPv2 enrollment

For CMPv2 enrollment, you must configure CA Gateway as described in the following topics.

- [Defining profiles in CSP CA Gateway for CMPv2 enrollment](#)
- [Configuring a truststore for validating CMP messages from CMPv2 clients](#)
- [Defining potential transmitters for CMPv2 enrollment](#)
- [Defining specifications for CMPv2 enrollment](#)

Defining profiles in CSP CA Gateway for CMPv2 enrollment

In CA Gateway, you must create profiles for each Managed CA that will issue certificates for CMPv2 enrollment. Each profile must issue one of the CMPv2 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 a truststore for validating CMP messages from CMPv2 clients

For CMPv2 enrollment, CA Gateway requires a truststore containing all the CA certificates required to verify CMP messages. The truststore must contain the CA certificate chain for all certificates used by CMPv2 devices, including certificates that will be issued by Entrust Managed CAs and any pre-installed vendor certificates issued by third-party CAs.

You must configure CA Gateway to use this truststore to validate CMP messages sent from CMPv2 devices. Under **Cmpv2**, the **Truststore** section specifies the truststore settings for CMPv2 enrollment.

- If CMPv2 devices will be authenticating with an expired vendor certificate for the initial enrollment, set **Allow Expired Vendor Certificate** to **True** to allow the CMPv2 device to enroll with the expired vendor certificate.
- The **Alias** section must specify the list of aliases for all CA certificates in the truststore. For each CA certificate:
 - The **Alias** setting must specify the alias of the CA certificate in the truststore.
 - The **DN** setting must specify the distinguished name (DN) of the CA certificate.
 - For third-party certificates, you may want to disable CRL checking if the CA or CRL is no longer available. To disable CRL checking for a certificate, set **Enable revocation checks on issued certificates** to **False**.

Defining potential transmitters for CMPv2 enrollment

For CMPv2 enrollment, you must define potential CMP request transmitters. Transmitters are the distinguished names (DNs) used by CMPv2 devices to sign CMP requests. Under **Cmpv2**, the **Shared Secret** section defines one or more shared secrets for potential transmitters.

Defining specifications for CMPv2 enrollment

In CA Gateway, you may need to define specifications for CMPv2 enrollment. These specifications define how to process CMPv2 requests from CMPv2 clients if they do not adhere to the CMPv2 standard TS-133-310.

 You do not have to define a specification for the CMPv2 "standard" as defined in TS-133-310. If the implementation field is not specified, TS-133-310 will be used.

Under **Cmpv2**, the **Customizations** section allows you to define one or more custom specifications for CMPv2 enrollment.

The following table lists the test methods that you can exclude from validation (**Excluded test** settings).

To exclude a test from a specific operation only, precede a test with an operation name, such as `ir` for Initialization Request or `certConf` for Certificate Confirmation). For example, `ir.Protection.rejectPBM` will exclude the Protection.rejectPBM test from only Initialization Request operations.

Test	Purpose
Message Validation	
Common.cmpVersion	Ensure supported CMP version is provided, i.e. CMP version 2.
Common.headerRecipient	Ensure a recipient was provided in the request header and its value represents a DN.
Common.headerSender	Ensure a sender was provided in the request header and its value represents a DN.
Common.headerSenderKid	Ensure a senderKID was provided in the request header.
Common.recipientNonce	Ensure all but initial requests in a transaction have a recipient NONCE, it is at least 16-bytes long and that it is the same value as the sender NONCE included in header of the previous response.
Common.requestType	Ensure the type is a known CMP type for the supported version, and, if not the initial request in a transaction, that the request type is valid at this point in the transaction.
Common.senderNonce	Ensure the sender NONCE is provided and that it is at least 16-bytes long.
Common.transactionId	Ensure all but initial requests in a transaction have a transaction ID provided.
RFC_4210.protectionAlgorithm	Ensure protection algorithm defined in the response header is valid signature algorithm for the supported specification. Only PBM (Shared Secret) and Signature are currently supported.
RFC_4210.transactionId	Ensure the transaction ID is at least 16 bytes long and does not exceed a system-imposed limit of 1024 bytes.
TS_33_310.certControls	Ensure OldCertId exists
TS_33_310.certRequestId	Ensure there is a certificate request ID provided and its value is zero (0).

Test		Purpose
	TS_33_310.proofOfPossession	Ensure proof of possession is provided, is signature based, and is valid.
	TS_33_310.requestCount	Ensure IR message contains one, and only one, certificate request.
	TS_33_310.requestType	Ensure the request type is a known CMP type for the supported specification, such as IP, KUP, CERTCONF, or ERROR.
	TS_33_310.statusCount	Ensure CERTCONF message contains no more than one certificate status.
	TS_33_310.templateExtensions	Ensure subject alternative name extension contains a subject if one was not provided in the certificate template.
	TS_33_310.templateHostName	Ensure the certificate template contains a subject (either in the subject field or as a subjectAltName extension), the subject is in the form of a DN, and the common name portion of the DN is a correctly-formatted DNS name.
	TS_33_310.templatePublicKeyAlg	Ensure the algorithm used to generate the public key in the request is accepted by the server.
	TS_33_310.templatePublicKeyLength	Ensure the length of the public key in the request meets the server defined minimum.
	TS_33_310.templateSubject	Ensure a subject name is provided in the certificate template. If no true value exists, this field must contain the NULL-DN.
	TS_33_310.templateVersion	Ensure the template version is correct, i.e. if provided it must be two (2).
	TS_33_310.transactionId	Ensure the transaction ID is at least 8-bytes long and doesn't exceed a system-imposed limit of 1024-bytes.
Protection Validation		
	Protection.rejectPBM	Ensure Password Based MAC (PBM) protection of messages are not allowed.

Test	Purpose
Protection.reject Unprotected	Ensure unprotected messages are not allowed.
PasswordBased Mac.applyProtection	Ensure that the protection defined in the response header is applied to the message response.
PasswordBased Mac.checkApply Algorithm	Ensure PBM protection algorithms defined in the response header are supported by the system.
PasswordBased Mac.checkVerify Algorithm	Ensure PBM protection algorithms defined in the request header are supported by the system.
PasswordBased Mac.verifyProtection	Ensure that the protection defined in the request header was applied to the message and that it has been found to be applied correctly.
SignatureBased. applyProtection	Ensure that the protection defined in the response header is applied to the message response.
SignatureBased. checkApplyAlgorithm	Ensure signature protection algorithm defined in the response header is supported by the system.
SignatureBased. checkVerifyAlgorithm	Ensure signature protection algorithm defined in the request header is supported by the system.
SignatureBased. extraCertsPresent	Ensure that extraCerts field does NOT contains any certificates for follow up messages in a transaction.
SignatureBased. verifyProtection	Ensure that the protection defined in the request header was applied to the message and that it has been found to be applied correctly.

Configuring CSP CA Gateway for EST enrollment

In CA Gateway, you must create profiles for each Managed CA that will issue certificate for EST enrollment. Each profile must issue one of the EST 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

i 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 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 SCEP and Intune-SCEP enrollment

i 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 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 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>`.

Deploying an external database for Certificate Enrollment Gateway

Certificate Enrollment Gateway requires a database for storing data. By default, Certificate Enrollment Gateway will use the internal database contained in Cryptographic Security Platform (HSQLDB) for storing data. Instead of using the internal database, you can deploy your own external database for storing Certificate Enrollment Gateway data. You can select which database to use for storing data when you configure Certificate Enrollment Gateway.

An external database is required for the following features:

- High Availability mode
- ACMEv2 External Account Binding.

i You can switch databases after Certificate Enrollment Gateway is deployed. However, data already stored in one database will not be transferred to the other database when you switch databases.

See below for deploying an external database for Certificate Enrollment Gateway.

- [Deploying a Microsoft SQL Server database for Certificate Enrollment Gateway](#)
- [Deploying a PostgreSQL database for Certificate Enrollment Gateway](#)
- [Configuring the external database for secure communications](#)

Deploying a Microsoft SQL Server database for Certificate Enrollment Gateway

You can store Certificate Enrollment Gateway data in an external Microsoft SQL Server database. This topic describes how to deploy a Microsoft SQL Server database for Certificate Enrollment Gateway.

To deploy a Microsoft SQL Server database for Certificate Enrollment Gateway using the Microsoft SQL Server Management Studio

1. Download the Microsoft SQL Server software from <https://www.microsoft.com>.
2. Install Microsoft SQL Server according to the instructions in the Microsoft documentation.
3. Open the Microsoft SQL Server Management Studio. Select **Start > Microsoft SQL Server Tools > Microsoft SQL Server Management Studio**.
The **Microsoft SQL Server Management Studio** dialog box appears.
4. Log in to the Microsoft SQL Server Management Studio.
 - a. Select **File > Connect Object Explorer**.
The **Connect to Server** dialog box appears.
 - b. Log in to the Database Engine as a Windows user account (Windows Authentication) or database administrator (SQL Server Authentication) with permission to administer SQL Server.
5. Create a new database instance for Certificate Enrollment Gateway:
 - a. In the **Object Explorer** pane, expand the server, then right-click **Databases > New Database**.
The **New Database** dialog box appears.
 - b. Under the **General** page:
 - In the **Database** name field, enter a name for the database. For example, `ceg`.
 - Keep **Owner** set to `<default>`.
 - c. Click **OK**.
6. Create a database user for Certificate Enrollment Gateway:
 - a. The login account can use Windows authentication or SQL Server authentication.
 - If the login account will use Windows authentication, use your Windows tools to create the Windows user account.
 - If the login account will use SQL Server authentication, the user will exist only in the database. SQL Server authentication is only available if you selected mixed mode authentication for your SQL Server instance.
 - b. In the **Object Explorer** pane, expand the server > **Security > Logins**, then right-click **Logins > New Login**.
The **Login - New** dialog box appears.
 - c. Under the **General** page:
 - In the **Login name** field, enter a name for the database user.
If the login account will use Windows authentication, enter the Windows user account name in the format `<DOMAIN>\<user>`. For example, `DOMAIN\ceguser`.
 - Select the authentication method for the new login account.
To use Windows authentication, select **Windows authentication**. The login account will be created as a Windows user account.
To use SQL Server authentication, select **SQL Server authentication**. The login account will

- be created in the database only. SQL Server authentication is only available if you selected mixed mode authentication for your SQL Server instance.
- In the **Default database** drop-down list, select the database you created earlier.
- d. If you selected **SQL Server authentication**, configure the following additional options under the **General** page:
- Enter a password for the login account into the **Password** and **Confirm password** fields.
 - (Optional.) To enforce the SQL Server password policy, select **Enforce password policy**. By default, this option is already selected.
Deselecting **Enforce password policy** will also deselect the **Enforce password expiration** and **User must change password at next login** options.
 - (Optional.) To never have the password expire, deselect **Enforce password expiration**. By default, this option is selected (the password expires).
 - Deselect **User must change password at next login**.
- e. Under the **User Mapping** page:
- For **Users mapped to this login**, select the database instance you created earlier.
When you select the database, the **User** field is filled with the login name you provided earlier.
 - For **Database role membership**, select the following roles:
 - db_accessadmin
 - db_backupoperator
 - db_datareader
 - db_datawriter
 - db_ddladmin
 - db_owner
 - db_securityadmin
 - public
- f. Click **OK**.

To deploy a Microsoft SQL Server database for Certificate Enrollment Gateway using the sqlcmd utility

1. Download the Microsoft SQL Server software from <https://www.microsoft.com>.
2. Install Microsoft SQL Server according to the instructions in the Microsoft documentation.
3. Start the sqlcmd utility:
 - a. Open a Command Prompt. Select **Start > Windows System > Command Prompt**.
 - b. Enter the following command:

```
sqlcmd -E -S <server>
```

Where **<server>** is the server name. For example:

```
sqlcmd -E -S MSSQLSERVER
```

4. Create a new database instance for Certificate Enrollment Gateway:
 - a. Enter the following commands to switch to the master database context:

```
USE MASTER;  
GO
```

- b. Enter the following commands to create a new database for Certificate Enrollment Gateway:

```
CREATE DATABASE <database>
GO
```

Where `<database>` is a name for the new database. For example:

```
CREATE DATABASE ceg
GO
```

5. Create a database user for Certificate Enrollment Gateway:

- a. Enter the following commands to create a new login for Certificate Enrollment Gateway:

```
CREATE LOGIN <user> WITH PASSWORD = '<password>', DEFAULT_DATABASE =
<database>;
GO
```

Where:

- `<user>` is a name for the login account.
- `<password>` is a password for the login account.
- `<database>` is the database instance you created for Certificate Enrollment Gateway.

- b. For example:

```
CREATE LOGIN ceguser WITH PASSWORD = 'EXAMPLE_password1234',
DEFAULT_DATABASE = ceg;
GO
```

- c. Enter the following commands to create a user in the Certificate Enrollment Gateway database for the login account:

```
CREATE USER <user> FOR LOGIN <user>;
GO
```

Where `<user>` is the name of the login account you created in the previous step. The user name must be the same as the login name. For example:

```
CREATE USER ceguser FOR LOGIN ceguser;
GO
```

6. Enter the following commands to switch to the database you created for Certificate Enrollment Gateway:

```
USE <database>;
GO
```

Where `<database>` is the database instance you created for Certificate Enrollment Gateway. For example:

```
USE ceg;  
GO
```

7. Enter the following commands to assign the correct database roles to the account:

```
ALTER ROLE db_accessadmin ADD MEMBER <user>;  
ALTER ROLE db_backupoperator ADD MEMBER <user>;  
ALTER ROLE db_datareader ADD MEMBER <user>;  
ALTER ROLE db_datawriter ADD MEMBER <user>;  
ALTER ROLE db_ddladmin ADD MEMBER <user>;  
ALTER ROLE db_owner ADD MEMBER <user>;  
ALTER ROLE db_securityadmin ADD MEMBER <user>;  
GO
```

Where `<user>` is the name of the login account you just created. For example:

```
ALTER ROLE db_accessadmin ADD MEMBER ceguser;  
ALTER ROLE db_backupoperator ADD MEMBER ceguser;  
ALTER ROLE db_datareader ADD MEMBER ceguser;  
ALTER ROLE db_datawriter ADD MEMBER ceguser;  
ALTER ROLE db_ddladmin ADD MEMBER ceguser;  
ALTER ROLE db_owner ADD MEMBER ceguser;  
ALTER ROLE db_securityadmin ADD MEMBER ceguser;  
GO
```

Deploying a PostgreSQL database for Certificate Enrollment Gateway

You can store Certificate Enrollment Gateway data in an external PostgreSQL database. This topic describes how to deploy a PostgreSQL database for Certificate Enrollment Gateway.

To deploy a PostgreSQL database for Certificate Enrollment Gateway

1. Download the PostgreSQL database from <https://www.postgresql.org>.
2. Install PostgreSQL according to the instructions in the PostgreSQL documentation. As you install PostgreSQL:
 - a. Enter and record the password for the database superuser. You need this password later. By default, the database superuser is named **postgres**.
 - b. Enter and record the port used to connect to the database. You need this port later. By default, the port is 5432.
3. Create a database user for Certificate Enrollment Gateway:
 - a. On the PostgreSQL server, navigate to the directory containing the PostgreSQL `createuser` command.
 - b. Enter the following command to create a new database user for Certificate Enrollment Gateway:

```
createuser -U <superuser> -P <user>
```

Where:

- `<superuser>` is the name of the database superuser.

- `<user>` is the name of the new database user.
- c. For example:
- ```
createuser -U postgres -P ceguser
```
- d. When prompted, enter a password for the new database user.  
e. When prompted, confirm the password by entering it again.  
f. When prompted, enter the password of the database superuser.
4. Create a new database instance for Certificate Enrollment Gateway:
- a. On the PostgreSQL server, navigate to the directory containing the PostgreSQL `createdb` command.
  - b. Enter the following command to create a new database instance for Certificate Enrollment Gateway:

```
createdb -U <superuser> -O <user> <database>
```

Where:

- `<superuser>` is the name of the database superuser.
  - `<user>` is the name of the database user you created in the previous step. This database user will own the new database instance.
  - `<database>` is the name of the new database instance.
- c. For example:

```
createdb -U postgres -O ceguser ceg
```

- d. When prompted, enter the password of the database user.
5. Configure PostgreSQL to allow connections from Certificate Enrollment Gateway:
- a. In the `postgresql.conf` file, modify the `listen_addresses` setting to include the address of the appliance hosting Certificate Enrollment Gateway.
  - b. In the `pg_hba.conf` file, enable host-based authentication for the appliance hosting Certificate Enrollment Gateway. For example:

```
host ceg ceguser server.example.com scram-sha-256
```

For details about this file, see the PostgreSQL documentation.

- c. Restart PostgreSQL for the changes to take effect.

## Configuring the external database for secure communications

By default, communications between Certificate Enrollment Gateway and the external database are unencrypted. It is recommended that you configure secure communications between Certificate Enrollment Gateway and the database. Configuring the database for secure communications requires configuring the database to use SSL/TLS communications. For instructions about configuring the database for SSL/TLS, see the database documentation.

When configuring Certificate Enrollment Gateway, you must configure the database connection settings. When connecting to the database over SSL/TLS, Certificate Enrollment Gateway requires one of the following files:

- When using the default database connection settings for PostgreSQL or Microsoft SQL Server, Certificate Enrollment Gateway requires a CA certificates file in PEM format to validate the database server certificate.

- When using a custom JDBC connection string to connect to the database, Certificate Enrollment Gateway requires the PEM or P12 certificate file referenced in the JDBC connection string.

## 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 1.1.0 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.

- [Creating a CSR for the Certificate Enrollment Gateway certificate](#)
- [Issuing TLS certificates with Entrust PKI as a Service](#)
- [Issuing TLS certificates with an on-premises CA](#)
- [Building a TLS certificate chain for the Certificate Enrollment Gateway certificate](#)
- [Installing the Certificate Enrollment Gateway certificate chain into Cryptographic Security Platform](#)

### 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 1.1.0 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 1.1.0. |
| <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"
```

### 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 1.1.0 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 1.1.0 – 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 1.1.0 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.

## 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.

- [Creating or recovering a user account in an on-premises CA](#)
- [Processing the CSR with an on-premises CA](#)
- [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 1.1.0. 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 1.1.0 cluster.

For information about creating or recovering user accounts, see the documentation for the client application.

## 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]:

**i** 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](#).

## Obtaining the CA certificate chain

CSP 1.1.0 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](#).

## Building a TLS certificate chain for the Certificate Enrollment Gateway certificate

CSP 1.1.0 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-----
MIIDejCCAmKgAwIBAgIQ8e7ock59Y21Mtcy7rGJUDANBgkqhkiG9w0BAQs...
-----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 1.1.0](#).

## Installing the Certificate Enrollment Gateway certificate chain into Cryptographic Security Platform

After building the TLS certificate chain for the Certificate Enrollment Gateway certificate, you can install the certificate into Cryptographic Security Platform. To install the certificate, Cryptographic Security Platform 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 Cryptographic Security Platform 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
```

## Configuring and deploying Certificate Enrollment Gateway

See below for configuring and deploying Certificate Enrollment Gateway with the Management Console.

 Do not forget to also click **Deploy** after each update of the configuration or the license file.

### To configure and deploy Certificate Enrollment Gateway with the Management Console

1. Open the following URL in a Web browser.

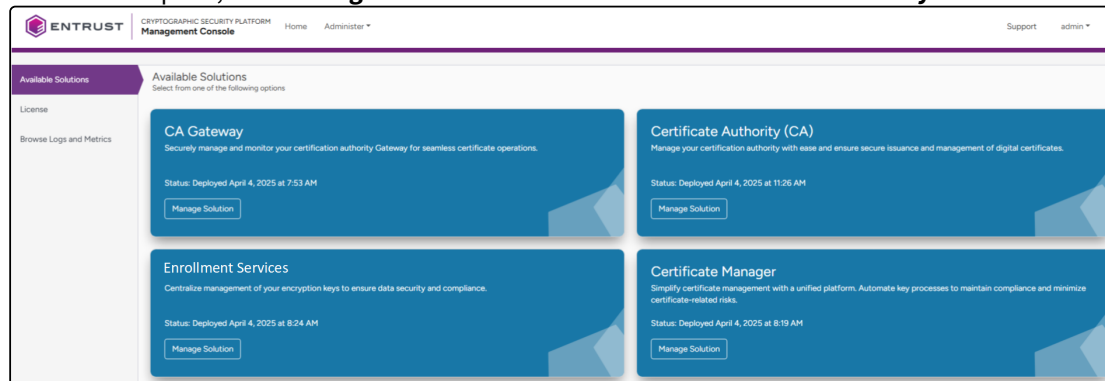
```
https://<machine>/management-console
```

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

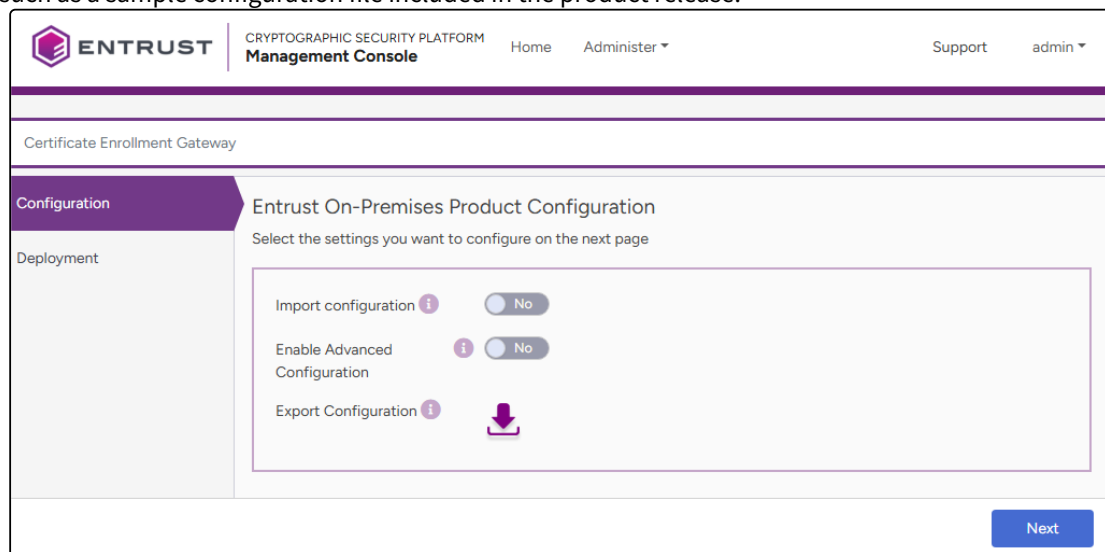
2. Log into the Management Console a user belonging to a role with Certificate Enrollment Gateway management permissions – for example, the initial `admin` administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

3. In the content pane, click **Manage Solution** under **Certificate Enrollment Gateway**.



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. Click **Next**.
6. Configure the solution settings described in the following sections.
  - [General](#)
  - [ACMEv2](#)
  - [CMPv2](#)
  - [EST](#)
  - [MDMWS](#)
  - [Intune](#)
  - [SCEP](#)
  - [WSTEP](#)
7. Click **Validate** to validate the configured settings.
8. Correct any detected configuration error until the **Validate** option displays no warnings.
9. Optionally, click the **Download** button to export the current configuration. You can later import this configuration using the already mentioned **Import configuration** toggle switch.
10. Click **Submit** and wait while Cryptographic Security Platform uploads the configuration and any attached file, such as a P12 file with authentication credentials.
11. Click **Deploy**.



## General

Select the **General** tab of the **Configuration** page to configure the following general settings.

- [CEG Tenant Unique ID](#)
- [CEG Logging Level](#)
- [Database Settings](#)
- [CEG Deployment Type](#)

### 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.
- Will be present in incoming enrollment request URLs.
- Is case-sensitive.
- Can include only the following characters:
  - Dashes (-)
  - Underscores (\_)

 Do not use underscores in the tenant ID if Certificate Enrollment Gateway supports the EST protocol. The EST protocol includes a concatenated enrollment URL with underscores to separate some values.

- Tildes (~)
- Uppercase letters (A to Z)
- Lowercase letters (a to z)
- Numbers (0 to 9)

 Certificate Enrollment Gateway supports only one tenant.

**Mandatory:** Yes.

### CEG Logging Level

The logging level for Certificate Enrollment Gateway.

| Level   | Description                                                                                                                     |
|---------|---------------------------------------------------------------------------------------------------------------------------------|
| default | Non-verbose level.                                                                                                              |
| trace   | Verbose level. Use this level for troubleshooting only, as it logs sensitive information and can negatively impact performance. |

**Mandatory:** No. This optional value defaults to **default**.

### Database Settings

Select a type of external database in the **Database Type** list and configure the corresponding settings.

- [Internal Database](#)
- [Postgres](#)
- [Microsoft SQL](#)

- [Custom JDBC String](#)

 See [Database requirements](#) for the supported DBMS.

#### Internal Database

Select this option to use the internal database provided with Certificate Enrollment Gateway.

 The **Database SSL Mode** field only supports the **disable** option for this type of database.

#### Postgres

Select this option to use an external PostgreSQL database. See below for the required parameters.

| Setting                  | Value                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name of the Database     | The name of the database instance in Certificate Enrollment Gateway.                                                                                      |
| Database User Name       | The user name for authenticating in the database.                                                                                                         |
| Database User Password   | The user password for authenticating in the database.                                                                                                     |
| Database Host            | The hostname or IP address of the database server.                                                                                                        |
| Database Port            | The port for accessing the database.                                                                                                                      |
| Database SSL Mode        | The SSL mode for connecting to the database: <b>*verify-full</b> , <b>**verify-ca*</b> or <b>*disable*</b> (not recommended for production environments). |
| Database SSL Certificate | A file containing the PEM-encoded CA certificates to verify the database server certificate.                                                              |

#### Microsoft SQL

Select this option to use an external Microsoft SQL database. See below for the required parameters.

| Setting                | Value                                                                |
|------------------------|----------------------------------------------------------------------|
| Name of the Database   | The name of the database instance in Certificate Enrollment Gateway. |
| Database User Name     | The user name for authenticating in the database.                    |
| Database User Password | The user password for authenticating in the database.                |

| Setting                  | Value                                                                                                                        |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Database Host            | The hostname or IP address of the database server.                                                                           |
| Database Port            | The port for accessing the database.                                                                                         |
| Database SSL Mode        | <b>enable</b> to enable SSL security for connecting, <b>disable</b> otherwise (not recommended for production environments). |
| Database SSL Certificate | A file containing the PEM-encoded CA certificates to verify the database server certificate.                                 |

### Custom JDBC String

Select this option to connect to an external database using a custom JDBC string.

 This database type is an advanced option and should be used only if you need to specify advanced connection parameters not supported by other database settings.

| Setting                  | Value                                                                                                                                                                       |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Database User Name       | The user name for authenticating in the database.                                                                                                                           |
| Database User Password   | The user password for authenticating in the database.                                                                                                                       |
| JDBC Connection String   | A complete JDBC string for connecting to the database. This string must begin with <code>jdbc:</code> and must not contain the username or password.                        |
| Database SSL Certificate | The PEM or P12 certificate file referenced in the JDBC connection string. Once uploaded, this file is copied to the <code>/opt/entrust/ceg/pvc_rwx_config/db</code> folder. |

### CEG Deployment Type

The type of backend that will accept connections from Certificate Enrollment Gateway.

- [CAGW](#)
- [PKIaaS](#)

#### CAGW

Select the **CAGW** tab of the **Configuration** page to configure the connection with an Entrust CA Gateway instance.

- [RA Certificate Profile IDs](#)
- [CEG Deployment Type: CA Gateway](#)

## RA Certificate Profile IDs

Click + **RA Certificate Profile IDs** and enter one or more mappings to issue an RA certificate.

- [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 identifier in CA Gateway instance for CA that will generate the RA certificate.

 See [Choose a key name](#) for details on this CA identifier in the CA Gateway configuration.

### Value

The name in CA Gateway of a profile with Dual Usage (both Digital Signature and Key Encipherment).

 See [Choose a key name](#) for details on this profile identifier in the CA Gateway configuration.

## CEG Deployment Type: CA Gateway

Configure the following settings.

- [CA Gateway URL](#)
- [CAGW Keystore File \(P12\)](#)
- [CAGW Keystore Password](#)
- [CAGW Keystore Alias](#)
- [Trusted CA Certificates File Format](#)

### 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.

### 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.

CAGW Keystore Password

The password of the **CAGW Keystore File**.

**Mandatory:** Yes.

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.

Trusted CA Certificates File Format

The format of the file containing the CA certificate chain for the CA Gateway client credential.

- Select **Re-use the CAGW Keystore File** to re-use the CAGW Keystore File.

✖ The deployment will fail if the CAGW Keystore File does not contain at least a Trusted CA Certificate entry.

- Select **P12** to import a P12 truststore file and enter the corresponding password.
- Select **PEM** to import a PEM-formatted certificate file.

**Mandatory:** Yes.

PKIaaS

Select this deployment type for Entrust PKI as a Service (PKIaaS) to accept connections from Certificate Enrollment Gateway.

- [Bypass Global Proxy for CAGW/PKIaaS Traffic](#)
- [PKIaaS license URL](#)
- [PKIaaS license OTP](#)

Bypass Global Proxy for CAGW/PKIaaS Traffic

The routing mode for all outgoing traffic to CA Gateway or Entrust PKI as a Service.

| Value | Routing                                                                                                                                           |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Yes   | Bypass the Global Proxy and route all outgoing CA Gateway or Entrust PKI as a Service traffic directly to CA Gateway or Entrust PKI as a Service. |

| Value | Routing                                                                                        |
|-------|------------------------------------------------------------------------------------------------|
| No    | Route all outgoing traffic to CA Gateway or Entrust PKI as a Service through the Global Proxy. |

#### PKIaaS license URL

The base64-encoded license URL for Entrust PKI as a Service. This setting is only required in the following cases:

- Deploying Certificate Enrollment Gateway on an appliance for the first time.
- When replacing the existing license with a new license.

This setting is not required when

- Re-deploying Certificate Enrollment Gateway
- Migrating from a deployment on Entrust Deployment Manager to Cryptographic Security Platform.

#### PKIaaS license OTP

The One-Time Password (OTP) license string for Entrust PKI as a Service. This setting is only required in the following cases:

- Deploying Certificate Enrollment Gateway on an appliance for the first time.
- When replacing the existing license with a new license.

This setting is not required when

- Re-deploying Certificate Enrollment Gateway
- Migrating from a deployment on Entrust Deployment Manager to Cryptographic Security Platform.

## ACMEv2

Select the **ACMEv2** tab of the **Configuration** page to configure ACMEv2 enrollment.

- [ACMEv2 Service](#)
- [ACMEv2 Scheduled Jobs](#)
- [DNS-01 Challenge](#)
- [ACMEv2 DNS-01 Nameservers](#)
- [HTTP-01 Challenge](#)

### ACMEv2 Service

Configure the following settings of the ACMEv2 service.

- [Enable ACMEv2](#)
- [Bypass Global Proxy for HTTP ACME Traffic](#)
- [ACMEv2 Order Expiry Interval](#)

#### Enable ACMEv2

**Yes** to enable the ACMEv2 protocol, **No** otherwise.

**Mandatory:** No. This option defaults to **No**.

#### Bypass Global Proxy for HTTP ACME Traffic

The routing mode for all outgoing HTTP ACMEv2 traffic.

| value | Routing                                                                                          |
|-------|--------------------------------------------------------------------------------------------------|
| Yes   | Bypass the Global Proxy and route all outgoing HTTP ACMEv2 traffic directly to ACMEv2 endpoints. |
| No    | Route all outgoing HTTP ACMEv2 traffic through the Global Proxy.                                 |

**Mandatory:** No. This option defaults to **No**.

#### ACMEv2 Order Expiry Interval

The period an ACMEv2 order can remain unprocessed by a client before the ACMEv2 server marks the order as "invalid". Enter a period in the ISO-8601 duration format:

PnDTnHnMn.nS

For example, to run the cron job every 1 hour:

'0 0 \* ? \* \*'

**Mandatory:** No. This option defaults to **Yes**.

#### ACMEv2 Scheduled Jobs

Configure the following job scheduling settings.

- [Delete Expired Authorizations Cron Job](#)
- [Delete Expired Order Cron Job](#)

##### 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.

## DNS-01 Challenge

Configure the following setting.

### 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

Click + **ACMEv2 DNS-01 Nameservers** to enter the list of DNS nameservers for DNS-01 validation for ACMEv2. Use the following syntax for each entry.

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

Where:

- `<ip>` is the IPv4 address of the DNS nameserver.
- `<port>` is the port (typically port 53) of the DNS nameserver.

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.

## HTTP-01 Challenge

Configure the following HTTP-01 settings.

- [ACMEv2 HTTP-01 Retry Count](#)
- [ACMEv2 HTTP-01 Retry Interval](#)
- [ACMEv2 HTTP-01 Redirect on POST](#)

### ACMEv2 HTTP-01 Retry Count

The maximum number of times the CEG ACMEv2 Enrollment Service will retry HTTP-01 Validation before timing out.

 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 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 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**.

## CMPv2

Select the **CMPv2** tab of the **Configuration** page to configure **CMPv2** enrollment.

- [Enable CMPv2](#)
- [Allow HTTP in addition to HTTPS for CMPv2](#)
- [Permitted sender file](#)

### Enable CMPv2

**Yes** to enable the CMPv2 protocol, **No** otherwise.

**Mandatory:** No. This option defaults to **No**.

### Allow HTTP in addition to HTTPS for CMPv2

Yes to allow HTTP connections to CMPv2; No otherwise.

 HTTPS connections to CMPv2 are always allowed.

**Mandatory:** No. This settings defaults to **No**.

### Permitted sender file

A file containing a list of fully qualified domain names (FQDNs) or IP addresses permitted to send CMPv2 requests.

**Mandatory:** No. If no file is specified, requests from all senders are allowed.

## EST

To enable EST enrollment, select **Yes** in the **Enable EST** switch and configure the following settings.

- [EST SSL settings](#)
- [EST CA Configurations](#)

## EST SSL settings

Configure the following settings.

### SSL certificate for EST

A P12 file containing a single SSL certificate and key pair for the EST web front end.

**Mandatory:** Yes.

### Password for SSL certificate for EST P12

The P12 file password.

**Mandatory:** Yes.

### CA Certificates File Format (P12 or PEM)

The file format for importing the certification chain for the SSL certificate.

- **P12** to import a password-protected P12 file.
- **\*PEM\*** to import a PEM-encoded file.

**Mandatory:** Yes.

## EST CA Configurations

Click + **EST CA Configurations** to configure the following settings.

- [CAGW CA ID](#)
- [Choose authentication method to validate the EST request](#)

### CAGW CA ID

The identifier in CA Gateway of the CA that will issue the enrolled certificates.

 See [Choose a key name](#) for details on this CA identifier in the CA Gateway configuration.

**Mandatory:** Yes.

### Choose authentication method to validate the EST request

Select the method to validate EST certificate enrollment requests.

- [Username/Password](#)
- [Vendor certificate](#)
- [UserName/Password and Vendor Certificate](#)

### Username/Password

Select this method to authenticate with username and password.

| Field                   | Value                                                            |
|-------------------------|------------------------------------------------------------------|
| EST pre-shared Username | The pre-shared username for HTTP Basic or Digest authentication. |

| Field                                | Value                                                            |
|--------------------------------------|------------------------------------------------------------------|
| Password for the pre-shared Username | The pre-shared password for HTTP Basic or Digest authentication. |

#### Vendor certificate

Select this method to authenticate with a vendor certificate.

| Field                                               | Value                                                                                                                               |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Enable CRL checking                                 | <b>Yes</b> to validate the vendor certificate against a CRL; <b>No</b> otherwise.                                                   |
| CA Certificates File Format for vendor certificates | The file format for importing the certification chain of the vendor certificate: a P12 password-encoded file or a PEM-encoded file. |

#### UserName/Password and Vendor Certificate

Select this method to authenticate with both the **Username/Password** and **Vendor certificate** methods.

## MDMWS

Select the **MDMWS** tab of the **Configuration** page to configure MDMWS enrollment.

- [MDM Web Service \(MDMWS\)](#)
- [MDMWS Scheduled Jobs](#)
- [MDMWS Users](#)
- [MDMWS Enrollment Service Configuration](#)

### MDM Web Service (MDMWS)

Configure the following settings of the MDMWS enrollment.

- [Enable MDMWS](#)
- [MDM-SCEP Token Expire Lifetime](#)

#### 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**.

#### MDM-SCEP Token Expire Lifetime

The lifetime of MDM challenges, in seconds. The minimum permitted value is 1 second.

**Mandatory:** Yes.

### MDMWS Scheduled Jobs

Configure the following setting.

### 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.

### MDMWS Users

Configure at least **Username** and **Password** for each user of the MDMWS protocol.

- i** 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 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](#)

- i** 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 in CA Gateway of the CA for certificate enrollments.

- i** See [Choose a key name](#) for details on this CA identifier in the CA Gateway configuration.

**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.

## Intune

Select the **Intune** tab of the **Configuration** page to configure Intune-SCEP enrollment.

- [Intune-SCEP](#)
- [Scheduled Jobs](#)
- [Intune-SCEP Enrollment Service Configurations](#)

## Intune-SCEP

Configure the following Intune-SCEP enrollment settings.

- [Enable Intune-SCEP](#)
- [Bypass Global Proxy for Intune Traffic](#)

### 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**.

### Bypass Global Proxy for Intune Traffic

The touring mode for all outgoing HTTP traffic to Microsoft Intune servers.

| Value | Routing                                                                                                  |
|-------|----------------------------------------------------------------------------------------------------------|
| Yes   | Bypass the Global Proxy and route all outgoing HTTP Intune traffic directly to Microsoft Intune servers. |
| No    | Route all outgoing HTTP Intune traffic through the Global Proxy.                                         |

## Scheduled Jobs

Configure the following setting.

### 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.

## InTune-SCEP Enrollment Service Configurations

Click + **InTune-SCEP Enrollment Service Configuration** and set the following parameters for each service configuration.

- [CAGW CA ID](#)
- [Azure Application ID](#)
- [Azure Tenant](#)
- [Azure Authentication Method](#)
- [Override Default InTune Endpoints](#)
- [Registered Azure Application Key](#)

### CAGW CA ID

The CA identifier for certificate enrollments defined in Entrust PKI as a Service or an on-premises CA Gateway.

 See [Choose a key name](#) for details on this CA identifier in the CA Gateway configuration.

**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.

#### Azure Tenant

The tenant for connecting to the Intune instance. For example:

test.example.com

**Mandatory:** Yes.

#### 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.

#### 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.            |
| 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**.

### Registered Azure Application Key

This application key (client secret) for connecting to the Intune instance.

**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](#)

### 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.

### SCEP Challenge Password

A challenge password for SCEP clients.

 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.

### 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.

### 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.



**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:** No. By default, this box is not checked.

## WSTEP

Select the **WSTEP** tab of the **Configuration** page to configure WSTEP enrollment.

- [Enable WSTEP](#)
- [WSTEP CAGW Settings](#)
- [Active Directory Domains](#)

### Enable WSTEP

Select **Yes** to enable the WSTEP protocol; **No** to disable the WSTEP protocol.

**Mandatory:** No. This setting defaults to **No**.

### 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](#)

#### CAGW CA ID

The identifier in CA Gateway of the CA for WSTEP enrollment.

**i** See [Choose a key name](#) for details on this CA identifier in the CA Gateway configuration.

**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 Profile ID for Digital Signature

The unique ID defined in CA Gateway for the WSTEP signing certificate profile.

**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 and Key Encipherment

This unique ID defined in CA Gateway for the WSTEP signing and encryption certificate profiles.

**Mandatory:** Yes.

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.

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**.

**Mandatory:** No.

## Active Directory Domains

Configure the following settings for each connection with Active Directory domains.

- [Domain Name](#)
- [Computer Name](#)
- [Enable WSTEP Kerberos Authentication for WSTEP Enrollment](#)
- [Authentication Type for LDAP and Global Catalog Connections](#)

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.

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.

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.

#### 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**.

## Enrollment URLs for Certificate Enrollment Gateway

When deploying or redeploying Certificate Enrollment Gateway, CSP 1.1.0 will display a list of local test commands and enrollment URLs for Certificate Enrollment Gateway.

- [ACMEv2 enrollment URLs](#)
- [CMPv2 enrollment URLs](#)
- [EST enrollment URLs](#)
- [Intune-SCEP enrollment URL](#)
- [MDM-SCEP enrollment URL](#)
- [MDMWS enrollment URL](#)
- [SCEP enrollment URL](#)
- [WSTEP enrollment URL](#)

## ACMEv2 enrollment URLs

ACMEv2 clients must use one of the following URLs to communicate with Certificate Enrollment Gateway.

### Default ACMEv2 enrollment URL

When External Account Binding is disabled, all ACMEv2 clients must use the following URL:

```
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 Certification 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
```

#### ACMEv2 Request URL for an External Account Binding credential

When External Account Binding is enabled, each External Account Binding credential will have its own URL. For example:

```
https://<hostname>/acme/ceg/Agu-fwShl2jDXsMYe4Ti3w/0mj615kbbkbb/directory
```

Where `<hostname>` is the hostname or IP address of the Certificate Enrollment Gateway server. For example:

```
https://cegserver.example.com/acme/ceg/Agu-fwShl2jDXsMYe4Ti3w/0mj615kbbkbb/directory
```

## CMPv2 enrollment URLs

CMPv2 clients must use one of the following URLs to communicate with Certificate Enrollment Gateway:

 The `http` URL only works if you configured the CMPv2 Service to allow HTTP connections.

```
https://<CEG-server>/cmpv2/<tenant-ID>/<CA-ID>/<profile-ID>/<spec-id>
http://<CEG-server>/cmpv2/<tenant-ID>/<CA-ID>/<profile-ID>/<spec-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 Certification Authority (CA) defined in CA Gateway that will issue certificates to the CMPv2 client.
- `<profile-ID>` is the profile ID defined in CA Gateway that defines the certificate type issued to the CMPv2 client.

- `<spec-id>` is a specification ID for CMPv2 that is defined in CA Gateway.

For example:

```
https://cegserver.example.com/cmpv2/tenant1/example_ca1/example-profile1/standard
http://cegserver.example.com/cmpv2/tenant1/example_ca1/example-profile1/standard
```

## EST enrollment URLs

EST clients must use one of the following URLs to communicate with Certificate Enrollment Gateway.

- ✗ When using the concatenated URL, the tenant ID, CA ID, and certificate profile ID cannot use underscores.

### Default EST enrollment URL:

```
https://<CEG-server>:1443/.well-known/est/<tenant-ID>/<CA-ID>/<profile-ID>/
```

### Concatenated EST enrollment URL:

```
https://<CEG-server>:1443/.well-known/est/<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 Certification Authority (CA) defined in CA Gateway that will issue certificates to the EST client.
- `<profile-ID>` is the profile ID defined in CA Gateway that defines the certificate type issued to the EST client. For Entrust PKI as a Service, the profile ID is one of the following:
  - est-digital-signature-key-encipherment
  - est-digital-signature
  - est-key-encipherment
  - est-non-repudiation

For example:

```
https://cegserver.example.com/.well-known/est/tenant1/example-ca1/est-digital-
signature/
https://cegserver.example.com/.well-known/est/tenant1_example-ca1_est-digital-
signature/
```

## Intune-SCEP enrollment URL

Microsoft Intune must be configured to use one of the following URLs to communicate with Certificate Enrollment Gateway:



**i** 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:

**i** 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:

-  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 ACMEv2 clients with Certificate Enrollment Gateway](#)
- [Integrating CMPv2 clients with Certificate Enrollment Gateway](#)
- [Integrating EST clients with Certificate Enrollment Gateway](#)
- [Integrating MDM and MDM-SCEP clients with Certificate Enrollment Gateway](#)
- [Integrating Microsoft Intune with Certificate Enrollment Gateway](#)
- [Integrating SCEP clients with Certificate Enrollment Gateway](#)
- [Integrating WSTEP clients with Certificate Enrollment Gateway](#)

## Integrating ACMEv2 clients with Certificate Enrollment Gateway

The following topics explain how to integrate ACMEv2 clients with the Certificate Enrollment Gateway service.

- [Configuring Certificate Enrollment Gateway for ACMEv2 enrollment](#)
- [Managing External Account Binding credentials](#)
- [Configuring ACMEv2 clients for enrollment with Certificate Enrollment Gateway](#)
- [ACMEv2 client examples](#)

### 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 as 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 Service](#)
  - [ACMEv2 Scheduled Jobs](#)
  - [DNS-01 Challenge](#)
  - [ACMEv2 DNS-01 Nameservers](#)
  - [HTTP-01 Challenge](#)
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.

## Managing External Account Binding credentials

External Account Binding is an ACMEv2 feature that allows you to associate an ACMEv2 account with an external account such as a database account. In Certificate Enrollment Gateway, External Account Binding credentials are used to restrict ACMEv2 access to permitted ACMEv2 clients.

To create and manage External Account Binding credentials for ACMEv2 enrollment with Certificate Enrollment Gateway, you must use the EAB Utility. The EAB Utility is available as a separate download package on Entrust TrustedCare.

**i** To use External Account Binding, Certificate Enrollment Gateway must be using an external database to store data, and External Account Binding must be enabled for ACMEv2.

- [Installing the EAB Utility](#)
- [Creating External Account Binding credentials](#)
- [Viewing External Account Binding credentials](#)
- [Modifying External Account Binding credentials](#)
- [Disabling HMAC keys for External Account Binding credentials](#)
- [Enabling HMAC keys for External Account Binding credentials](#)
- [Disabling ACMEv2 operations for External Account Binding credentials](#)
- [Enabling ACMEv2 operations for External Account Binding credentials](#)
- [Deleting HMAC keys for External Account Binding credentials](#)

### Installing the EAB Utility

To create and manage External Account Binding credentials for ACMEv2 enrollment with Certificate Enrollment Gateway, you must use the EAB Utility. The EAB Utility is available as a separate download package on Entrust TrustedCare.

The following procedure describes how to download and install the EAB Utility. You must install the EAB Utility on an Entrust Deployment Manager or Cryptographic Security Platform node.

#### To install the EAB Utility on a Entrust Deployment Manager or Cryptographic Security Platform node

1. Download the EAB Utility from Entrust TrustedCare:
  - a. In a Web browser, log in to Entrust TrustedCare (<https://trustedcare.entrust.com>).
  - b. Browse to the Certificate Enrollment Gateway product page.
  - c. Download the EAB Utility binary file ( `eab-util` ),
2. Copy the EAB Utility binary to one of the Entrust Deployment Manager or Cryptographic Security Platform nodes (for example, using `scp` command).
3. Log in to the node as `sysadmin`.
4. Navigate to the directory where you copied the binary file.
5. Enter the following command to make the binary executable:

```
sudo chmod +x eab-util
```

6. Enter the following command to move the file into the `/usr/bin/` directory:

```
sudo mv eab-util /usr/bin/
```

## Creating External Account Binding credentials

For ACMEv2 clients to use External Account Binding, you must create one or more External Account Binding credentials.

An External Account Binding credential contains the following information:

- A friendly name that uniquely identifies the External Account Binding credential.
- The CA ID in Entrust CA Gateway of the Certificate Authority (CA) that will issue certificates to the ACMEv2 clients.
- The Profile ID in Entrust CA Gateway of the certificate profile that defines the certificate type issued to the ACMEv2 clients.
- A list of permitted algorithms that ACMEv2 clients can use for enrollment with External Account Binding.
- An HMAC (Hash-Based Message Authentication Code) key that new ACMEv2 clients will use to create an account. The key will be created when you create the External Account Binding credential.
- The Key ID of the HMAC key for the External Account Binding credential. New ACMEv2 clients will use this Key ID to create an account. The Key ID will be created when you create the External Account Binding credential.
- An ACMEv2 Request URL that ACMEv2 clients must use to access the External Account Binding credential and perform ACMEv2 operations. The URL will be created when you create the External Account Binding credential.

Multiple ACMEv2 clients can use the same External Account Binding credential to create an account and perform ACMEv2 operations.

### To create a new External Account Binding credential

1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

```
Certificate Enrollment Gateway
ACMEv2 External Account Binding (EAB) Utility

1 Create new EAB credential
2 Manage EAB credentials

Page 1/1

UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC/Q/CTRL+C: Quit
```

4. Select **Create new EAB credential**, then press Enter.  
The **Create New EAB Credential** page appears.

Create New EAB Credential

Enter the details for the new EAB credential

**Friendly Name:**

Certificate Authority:      intaa250328003~root92432

Certificate Profile:        basic-ca-subord

Permitted Algorithms:      HS256,HS384,HS512

[ Submit ]      [ Cancel ]

UP/DOWN/TAB: Navigate   ENTER/SPACE: Edit/Select   B/ESC: Back   Q/CTRL+C: Quit  
Enter: Edit field

5. Each External Account Binding credential in the EAB Utility is identified by a unique string called a friendly name. Provide a friendly name for the credential:
  - a. Select **Friendly Name**, then press Enter.
  - b. Type a friendly name for the credential. The name must start and end with an alphanumeric character. The name must be a maximum 25 characters long. The name can contain uppercase and lowercase letters, numbers, spaces, and the following non-alphanumeric characters:

, ! @ # & \* : ( )

- c. Press Enter.
6. Select the Certification Authority that will enroll the ACMEv2 client for a certificate:
  - a. Select **Certificate Authority**, then press Enter.  
The **Select Certificate Authority** page appears.

Select Certificate Authority

Choose an option

|   |                                 |
|---|---------------------------------|
| 1 | intaa250328003~root92432        |
| 2 | intaa250328003~subordinate56559 |

Page 1/1

'/' : Search  
UP/DOWN/TAB: Navigate   ENTER/SPACE: Select   B/ESC: Back   Q/CTRL+C: Quit

- b. Select a Certification Authority from the list, then press Enter.
7. Select the certificate profile defined in CA Gateway that will be used to issue the certificate to the ACMEv2 clients:

- a. Select **Certificate Profile**, and then press Enter.  
The **Select Certificate Profile** page appears.

Select Certificate Profile  
Choose an option

|    |                                        |
|----|----------------------------------------|
| 1  | cmp-digital-signature                  |
| 2  | cmp-digital-signature-key-encipherment |
| 3  | cmp-key-encipherment                   |
| 4  | cmp-non-repudiation                    |
| 5  | codesigning-digital-signature          |
| 6  | est-digital-signature                  |
| 7  | est-digital-signature-key-encipherment |
| 8  | est-key-encipherment                   |
| 9  | est-non-repudiation                    |
| 10 | idaas-card-authentication              |
| 11 | idaas-digital-signature                |
| 12 | idaas-domain-controller                |
| 13 | idaas-key-management                   |
| 14 | idaas-piv-authentication               |

Page 1/4

'/' : Search LEFT/RIGHT : Navigate pages  
UP/DOWN/TAB : Navigate ENTER/SPACE : Select B/ESC : Back Q/CTRL+C : Quit

- b. Select the certificate profile that will issue the certificate to the ACMEv2 clients, and then press Enter.  
For Entrust PKI as a Service, the profile ID is one of the following:
    - privatesl-tls-client-server
    - privatesl-tls-server
    - privatesl-tls-client
8. Select the algorithms that ACMEv2 clients can use for enrollment with External Account Binding:
  - a. Select **Permitted Algorithms**, and then press Enter.  
The **Select HMAC Algorithms** page appears.

Select HMAC Algorithms  
At least one algorithm must be selected

|   |                                     |          |
|---|-------------------------------------|----------|
| 1 | <input checked="" type="checkbox"/> | HS256    |
| 2 | <input checked="" type="checkbox"/> | HS384    |
| 3 | <input checked="" type="checkbox"/> | HS512    |
| 4 |                                     | [ Done ] |

Page 1/1

UP/DOWN/TAB : Navigate ENTER/SPACE : Toggle A : Select All B/ESC : Back Q/CTRL+C : Quit

- b. You can enable or disable an algorithm by selecting the algorithm, and then pressing Enter or spacebar. A checkmark next to the algorithm indicates that algorithm is permitted to be used for External Account Binding.
    - c. Select **Done**, and then press Enter.
9. Select **Submit** and then press Enter.  
The External Account Binding credential is created. The **EAB Credential Details** page appears. For example:

✘ The HMAC key will be displayed only on this page, and cannot be retrieved later. You must copy this HMAC key before closing the page.



EAB Credential Details

WARNING: The HMAC Key will only be displayed once and cannot be retrieved later!

|                       |                                                                           |
|-----------------------|---------------------------------------------------------------------------|
| EAB Friendly Name:    | Example                                                                   |
| CAID:                 | intaa250328003~subordinate56559                                           |
| Profile ID:           | privatessl-tls-client-server                                              |
| EAB Key ID:           | jt58-zpca5r13PV8bMxJNQ                                                    |
| EAB HMAC Key:         | d012Uk4tcck1czBSM0pjVlA3bFduS21zd08xUnVQRzhRVkFtWXliSEtDWQ                |
| Permitted Algorithms: | HS256, HS384, HS512                                                       |
| EAB Key Status:       | Fully Functional                                                          |
| ACMEv2 Status:        | Fully Functional                                                          |
| ACMEv2 Request URL:   | https://<hostname>/acme/ceg/jt58-zpca5r13PV8bMxJNQ/ytdntaqcok8u/directory |

[ I have saved the information ]

10. Copy the information. The ACMEv2 Request URL and HMAC key are required to enroll the ACMEv2 client for a certificate.
11. Press Enter to return to the main menu.

#### Viewing External Account Binding credentials

You can view details about any existing External Account Binding credential that you have created. You can view the following information about an External Account Binding credential:

- The friendly name that uniquely identifies the External Account Binding credential.
- The CA ID in Entrust CA Gateway of the Certificate Authority (CA) that will issue certificates to the ACMEv2 clients.
- The Profile ID in Entrust CA Gateway of the certificate profile that defines the certificate type issued to the ACMEv2 clients.
- The list of permitted algorithms that ACMEv2 clients can use for enrollment with External Account Binding.
- The Key ID of the HMAC key for the External Account Binding credential.
- The status of the HMAC key.
- The ACMEv2 client status (the status of the External Account Binding credential).
- The ACMEv2 Request URL that ACMEv2 clients must use to perform ACMEv2 operations with the External Account Binding credential.

**i** The EAB Utility will display the HMAC key for an External Account Binding credential only when you create the credential. The EAB Utility will not display the key when viewing details about an External Account Binding credential.

#### To view details about an External Account Binding credential

1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

```

Certificate Enrollment Gateway
ACMEv2 External Account Binding (EAB) Utility

1 Create new EAB credential
2 Manage EAB credentials
Page 1/1

UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC/Q/CTRL+C: Quit

```

4. Select **Manage EAB credentials**, and then press Enter.  
A list of External Account Binding credentials appears. For example:

```

Certificate Enrollment Gateway
ACMEv2 External Account Binding (EAB) Utility

EAB Friendly Name | Key ID | Key Status | ACMEv2 Status
1 Certbot | 2B7x4pX2WrJI63RC4YNmcg | Enabled | Enabled
2 Example | jt58-zpca5rl13PV8bMxJNQ | Enabled | Enabled

'/': Search
UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC: Back Q/CTRL+C: Quit

```

For each External Account Binding credential:

- The **EAB Friendly Name** column displays the name that uniquely identifies the External Account Binding credential.
- The **Key ID** displays the ID of the HMAC key for the External Account Binding credential. This value is not the HMAC Key.
- The **Key Status** displays the status of the HMAC key for the External Account Binding credential. The value is Enabled or Disabled.
- The **ACMEv2 Status** displays the status of ACMEv2 operations for the External Account Binding credential. The value is Enabled or Disabled.

5. Select the credential you want to edit, and then press Enter.

A **Manage EAB Credentials** page appears. For example:

```

Manage EAB Credentials
Modify the details for the existing EAB credentials

Friendly Name: Example
Certificate Authority: intaa250328003~subordinate56559
Certificate Profile: privatessl-tls-client-server
Permitted Algorithms: HS256,HS384,HS512

[View Details] [Cancel] [Disable EAB Key] [Disable ACMEv2] [Delete EAB Key]

UP/DOWN/TAB: Navigate ENTER/SPACE: Edit/Select B/ESC: Back Q/CTRL+C: Quit
Enter: Edit field

```

- **Friendly Name** displays the name that uniquely identifies the External Account Binding credential.

- **Certificate Authority** displays the CA ID defined in Entrust CA Gateway of the Certificate Authority (CA) that will issue certificates to the ACMEv2 clients.
  - **Certificate Profile** displays the Profile ID defined in Entrust CA Gateway of the certificate profile that defines the certificate type issued to the ACMEv2 clients.
  - **Permitted Algorithms** displays the list of permitted algorithms that ACMEv2 clients can use for enrollment with External Account Binding.
6. Select **View Details**, and then press Enter.  
An **EAB Credential Details** page appears. For example:

EAB Credential Details

---

EAB Friendly Name:

Example

CAID:

intaa250328003~subordinate56559

Profile ID:

privatessl-tls-client-server

EAB Key ID:

jt58-zpca5rl3PV8bMxJNQ

EAB HMAC Key:

\*\*\*\*\*

Permitted Algorithms:

HS256,HS384,HS512

EAB Key Status:

Fully Functional

ACMEv2 Status:

Fully Functional

ACMEv2 Request URL:

https://<hostname>/acme/ceg/jt58-zpca5rl3PV8bMxJNQ/ytdntaqcok8u/directory

OK

- **Friendly Name** displays the name that uniquely identifies the External Account Binding credential.
  - **CAID** displays the CA ID defined in Entrust CA Gateway of the Certificate Authority (CA) that will issue certificates to the ACMEv2 clients.
  - **Profile ID** displays the Profile ID defined in Entrust CA Gateway of the certificate profile that defines the certificate type issued to the ACMEv2 clients.
  - **EAB Key ID** displays the Key ID of the HMAC key for the External Account Binding credential. This value is not the HMAC Key.
  - **Permitted Algorithms** displays the list of permitted algorithms that ACMEv2 clients can use for enrollment with External Account Binding.
  - **EAB Key Status** displays the status of the HMAC key for the External Account Binding credential. The value is Enabled or Disabled.
  - **ACMEv2 Status** displays the status of ACMEv2 operations for the External Account Binding credential. The value is Enabled or Disabled.
  - **ACMEv2 Request URL** displays the URL that ACMEv2 clients must use to access the External Account Binding credential and perform ACMEv2 operations.
7. Press Enter to return to the list of External Account Binding credentials.

#### Modifying External Account Binding credentials

You can modify an External Account Binding credential if you need to update or correct some information provided by the External Account Binding credential. When modifying an External Account Binding credential, you can change the following information:

- A friendly name that uniquely identifies the External Account Binding credential.
- The CA ID in Entrust CA Gateway of the Certificate Authority (CA) that will issue certificates to the ACMEv2 clients.
- The Profile ID in Entrust CA Gateway of the certificate profile that defines the certificate type issued to the ACMEv2 clients.
- A list of permitted algorithms that ACMEv2 clients can use for enrollment with External Account Binding.

**i** You cannot change the HMAC (Hash-Based Message Authentication Code) key or ACMEv2 Request URL used by ACMEv2 clients. The key and URL were automatically generated when the credential was created and cannot be changed.

### To modify an External Account Binding credential

1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

```
Certificate Enrollment Gateway
ACMEv2 External Account Binding (EAB) Utility

1 Create new EAB credential
2 Manage EAB credentials

Page 1/1

UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC/Q/CTRL+C: Quit
```

4. Select **Manage EAB credentials**, and then press Enter.  
A list of External Account Binding credentials appears. For example:

```
Certificate Enrollment Gateway
ACMEv2 External Account Binding (EAB) Utility

EAB Friendly Name | Key ID | Key Status | ACMEv2 Status
1 Certbot | 2B7x4pXZWrfJI63RC4YNmcg | Enabled | Enabled
2 Example | jt58-zpca5rl13PV8bMxJNQ | Enabled | Enabled

': Search
UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC: Back Q/CTRL+C: Quit
```

5. Select the credential you want to edit, and then press Enter.  
A **Manage EAB Credentials** page appears. For example:

**Manage EAB Credentials**

Modify the details for the existing EAB credentials

|                        |                                 |
|------------------------|---------------------------------|
| <b>Friendly Name:</b>  | <b>Example</b>                  |
| Certificate Authority: | intaa250328003~subordinate56559 |
| Certificate Profile:   | privatessl-tls-client-server    |
| Permitted Algorithms:  | HS256,HS384,HS512               |

[ View Details ] [ Cancel ] [ Disable EAB Key ] [ Disable ACMEv2 ] [ Delete EAB Key ]

UP/DOWN/TAB: Navigate ENTER/SPACE: Edit/Select B/ESC: Back Q/CTRL+C: Quit  
Enter: Edit field

If you change any details, the **View Details** option will change to a **Submit** option.

6. To change the friendly name of the credential:
  - a. Select **Friendly Name**, then press Enter.
  - b. Edit the friendly name for the credential. The name must start and end with an alphanumeric character. The name must be a maximum 25 characters long. The name can contain uppercase and lowercase letters, numbers, spaces, and the following non-alphanumeric characters:

, ! @ # & \* : ( )

- c. Press Enter.
7. To change the Certification Authority that will enroll the ACMEv2 client for a certificate:
  - a. Select **Certificate Authority**, then press Enter.

The **Select Certificate Authority** page appears.

**Select Certificate Authority**

Choose an option

|   |                                 |
|---|---------------------------------|
| 1 | intaa250328003~root92432        |
| 2 | intaa250328003~subordinate56559 |

Page 1/1

'/': Search  
UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC: Back Q/CTRL+C: Quit

- b. Select a Certification Authority from the list, then press Enter.
8. To change the certificate profile defined in CA Gateway that will be used to issue the certificate to the ACMEv2 client:

- a. Select **Certificate Profile**, and then press Enter.  
The **Select Certificate Profile** page appears.

Select Certificate Profile

Choose an option

|    |                                        |
|----|----------------------------------------|
| 1  | cmp-digital-signature                  |
| 2  | cmp-digital-signature-key-encipherment |
| 3  | cmp-key-encipherment                   |
| 4  | cmp-non-repudiation                    |
| 5  | codesigning-digital-signature          |
| 6  | est-digital-signature                  |
| 7  | est-digital-signature-key-encipherment |
| 8  | est-key-encipherment                   |
| 9  | est-non-repudiation                    |
| 10 | idaas-card-authentication              |
| 11 | idaas-digital-signature                |
| 12 | idaas-domain-controller                |
| 13 | idaas-key-management                   |
| 14 | idaas-piv-authentication               |

Page 1/4

'/' : Search LEFT/RIGHT : Navigate pages  
UP/DOWN/TAB : Navigate ENTER/SPACE : Select B/ESC : Back Q/CTRL+C : Quit

- b. Select the certificate profile that will issue the certificate to the ACMEv2 client, and then press Enter.
9. To change the algorithms that ACMEv2 clients can use for enrollment with External Account Binding:
  - a. Select **Permitted Algorithms**, and then press Enter.  
The **Select HMAC Algorithms** page appears.

Select HMAC Algorithms

At least one algorithm must be selected

|   |                                     |       |
|---|-------------------------------------|-------|
| 1 | <input checked="" type="checkbox"/> | HS256 |
| 2 | <input checked="" type="checkbox"/> | HS384 |
| 3 | <input checked="" type="checkbox"/> | HS512 |
| 4 | <input type="checkbox"/>            | Done  |

Page 1/1

UP/DOWN/TAB : Navigate ENTER/SPACE : Toggle A : Select All B/ESC : Back Q/CTRL+C : Quit

- b. You can enable or disable an algorithm by selecting the algorithm, and then pressing Enter or spacebar. A checkmark next to the algorithm indicates the algorithm is permitted to be used for External Account Binding.
- c. Select **Done**, and then press Enter.
10. Select **Submit** and then press Enter.  
The External Account Binding credential is updated with the changes you made. The **EAB Credential Details**

page appears.

EAB Credential Details

|                       |                                                                             |
|-----------------------|-----------------------------------------------------------------------------|
| EAB Friendly Name:    | Example                                                                     |
| CAID:                 | intaa250328003~subordinate56559                                             |
| Profile ID:           | privatessl-tls-client-server                                                |
| EAB Key ID:           | jt58-zpca5rl3PV8bMxJNQ                                                      |
| EAB HMAC Key:         | *****                                                                       |
| Permitted Algorithms: | HS256,HS384,HS512                                                           |
| EAB Key Status:       | Fully Functional                                                            |
| ACMEv2 Status:        | Fully Functional                                                            |
| ACMEv2 Request URL:   | https://<hostname>/acme/ceg/jt58-zpca5rl3PV8bMxJNQ/yt dn tagcok8u/directory |

[ OK ]

11. Click **OK**.  
The list of External Account Binding credentials reappears.

#### Disabling HMAC keys for External Account Binding credentials

When you create a credential for External Account Binding, an HMAC (Hash-Based Message Authentication Code) key is created for that credential. Each External Account Binding credential has its own HMAC key. Each ACMEv2 client that enrolls with an External Account Binding credential will use the HMAC key only once. An ACMEv2 client will use the HMAC key only when it initially connects to the ACMEv2 server and creates an ACMEv2 account. After the account is created, the ACMEv2 client no longer needs the key.

You can disable the HMAC key for an External Account Binding credential. Disabling a key will block new ACMEv2 clients from using the key to create an account with External Account Binding credential. ACMEv2 clients that have already used the key to create an account can still perform ACMEv2 operations if the ACMEv2 operations are enabled for the External Account Binding credential.

#### To disable the HMAC key for an External Account Binding credential

1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

Certificate Enrollment Gateway  
ACMEv2 External Account Binding (EAB) Utility

1 Create new EAB credential

2 Manage EAB credentials

Page 1/1

UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC/Q/CTRL+C: Quit

4. Select **Manage EAB credentials**, and then press Enter.  
A list of External Account Binding credentials appears. For example:

| Certificate Enrollment Gateway<br>ACMEv2 External Account Binding (EAB) Utility |                   |                         |                            |
|---------------------------------------------------------------------------------|-------------------|-------------------------|----------------------------|
|                                                                                 | EAB Friendly Name | Key ID                  | Key Status   ACMEv2 Status |
| 1                                                                               | Certbot           | 2B7x4pXZWzJI63RC4YNmcg  | Enabled   Enabled          |
| 2                                                                               | Example           | jtc58-zpca5rl3PV8bMxJNQ | Enabled   Enabled          |

'/': Search

UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC: Back Q/CTRL+C: Quit

The **Key Status** column displays the status of the HMAC key for each External Account Binding credential, either Enabled or Disabled.

5. Select the credential whose HMAC key you want to disable, and then press Enter.

A **Manage EAB Credentials** page appears. For example:

Manage EAB Credentials

Modify the details for the existing EAB credentials

Friendly Name: Example

Certificate Authority: intaa250328003~subordinate56559

Certificate Profile: privatessl-tls-client-server

Permitted Algorithms: HS256,HS384,HS512

[ View Details ] [ Cancel ] [ Disable EAB Key ] [ Disable ACMEv2 ] [ Delete EAB Key ]

UP/DOWN/TAB: Navigate ENTER/SPACE: Edit/Select B/ESC: Back Q/CTRL+C: Quit

Enter: Edit field

6. Select **Disable EAB Key**, and then press Enter.

The **Disable ACMEv2 EAB Key** page appears.

Disable ACMEv2 EAB Key?

ACMEv2 EAB Keys are used only once when an ACMEv2 client initially connects to the ACMEv2 server. This first interaction is used to create an ACMEv2 account. Once an ACMEv2 account is created, the ACMEv2 client no longer needs the EAB key. Disabling this ACMEv2 EAB key will only block new ACMEv2 clients from using this key.

Note - This does not block certificate enrollment for ACMEv2 clients that have already used this EAB Key to create an ACMEv2 account.

Are you sure you want to disable this ACMEv2 EAB key?

[ Cancel ] [ Disable EAB Key ]

7. Select **Disable EAB Key** and press Enter.

The HMAC key for the External Account Binding credential is disabled. The **Manage EAB Credentials** page reappears



## Enabling HMAC keys for External Account Binding credentials

When you create a credential for External Account Binding, an HMAC (Hash-Based Message Authentication Code) key is created for that credential. Each External Account Binding credential has its own HMAC key. Each ACMEv2 client that enrolls with an External Account Binding credential will use the HMAC key only once. An ACMEv2 client will use the HMAC key only when it initially connects to the ACMEv2 server and creates an ACMEv2 account. After the account is created, the ACMEv2 client no longer needs the key.

When an HMAC key is disabled for an External Account Binding credential, new ACMEv2 clients are blocked from using the key to create new accounts. ACMEv2 clients that have already used the key to create an account can still perform ACMEv2 operations if the ACMEv2 operations are enabled for the External Account Binding credential.

You can enable a key that has been disabled for an External Account Binding credential. When you enable a key, new ACMEv2 clients can use the key to create a new ACMEv2 account.

### To enable the HMAC key for an External Account Binding credential

1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

```

Certificate Enrollment Gateway
ACMEv2 External Account Binding (EAB) Utility

1 Create new EAB credential
2 Manage EAB credentials
Page 1/1

UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC/Q/CTRL+C: Quit

```

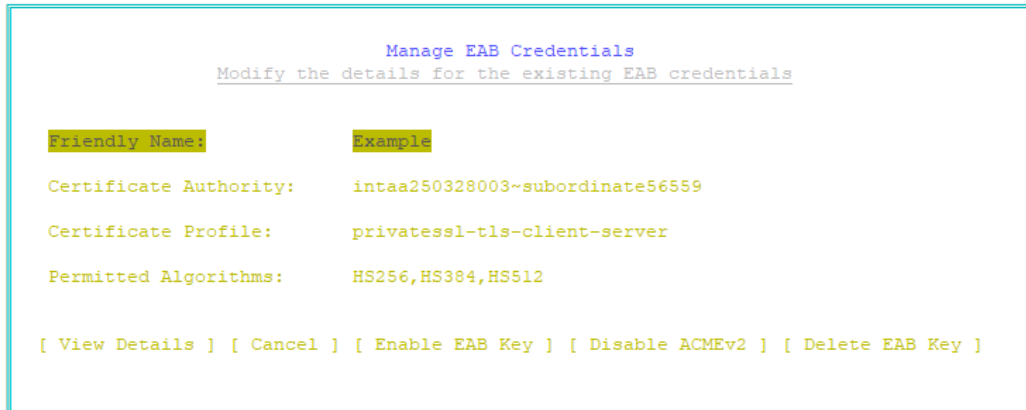
4. Select **Manage EAB credentials**, and then press Enter.  
A list of External Account Binding credentials appears. For example:

| Certificate Enrollment Gateway<br>ACMEv2 External Account Binding (EAB) Utility |                   |                         |                            |
|---------------------------------------------------------------------------------|-------------------|-------------------------|----------------------------|
|                                                                                 | EAB Friendly Name | Key ID                  | Key Status   ACMEv2 Status |
| 1                                                                               | Certbot           | 2B7x4pXZWrJI63RC4YNmcg  | Enabled   Enabled          |
| 2                                                                               | Example           | jt58-zpca5rl13PV8bMxJNQ | Disabled   Enabled         |

'/' : Search  
 UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC: Back Q/CTRL+C: Quit

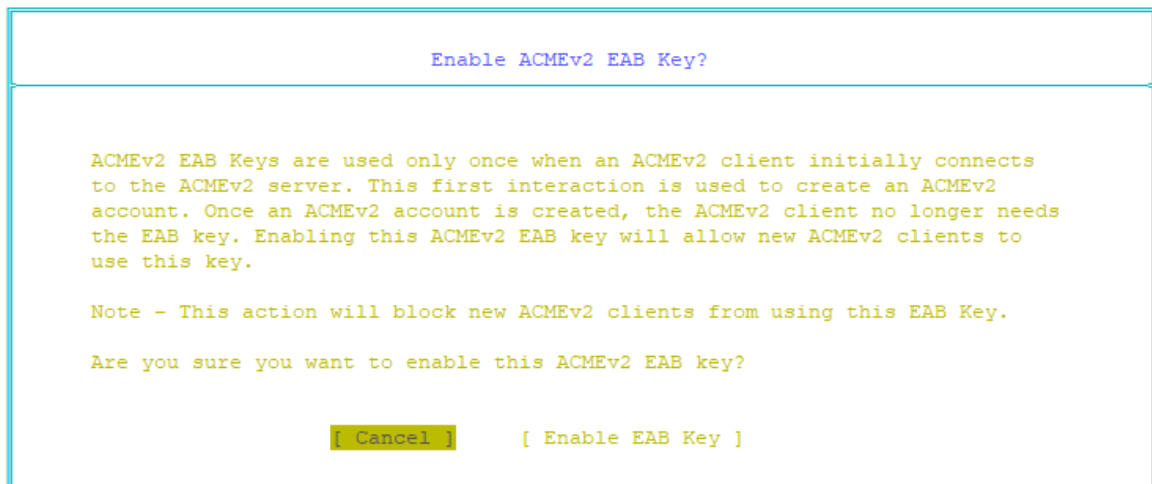
The **Key Status** column displays the status of the HMAC key for each External Account Binding credential, either Enabled or Disabled.

5. Select the credential whose HMAC key you want to enable, and then press Enter. A **Manage EAB Credentials** page appears. For example:



UP/DOWN/TAB: Navigate ENTER/SPACE: Edit/Select B/ESC: Back Q/CTRL+C: Quit  
Enter: Edit field

6. Select **Enable EAB Key**, and then press Enter. The **Enable ACMEv2 EAB Key** page appears.



7. Select **Enable EAB Key** and press Enter. The HMAC key for the External Account Binding credential is enabled. The **Manage EAB Credentials** page reappears

#### Disabling ACMEv2 operations for External Account Binding credentials

You can disable ACMEv2 operations for an External Account Binding credential. Disabling ACMEv2 operations for an External Account Binding credential will disable the credential. When you disable ACMEv2 operations for an External Account Binding credential, new ACMEv2 clients cannot use the credential to create an account, and ACMEv2 clients with an existing account cannot perform any ACMEv2 operations with the credential.

You should disable ACMEv2 operations for an External Account Binding credential if you want to temporarily prevent any ACMEv2 clients from using the External Account Binding credential. If you want to permanently prevent ACMEv2 clients from using an External Account Binding credential, delete the HMAC key for the credential (see [Deleting HMAC keys for External Account Binding credentials](#)).

#### To disable ACMEv2 operations for an External Account Binding credential

1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

```

Certificate Enrollment Gateway
ACMEv2 External Account Binding (EAB) Utility

1 Create new EAB credential
2 Manage EAB credentials
Page 1/1

UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC/Q/CTRL+C: Quit

```

4. Select **Manage EAB credentials**, and then press Enter.  
A list of External Account Binding credentials appears. For example:

```

Certificate Enrollment Gateway
ACMEv2 External Account Binding (EAB) Utility

EAB Friendly Name | Key ID | Key Status | ACMEv2 Status
1 Certbot | 2B7x4pXZWrfJI63RC4YNmcg | Enabled | Enabled
2 Example | jt58-zpca5rl13PV8bMxJNQ | Enabled | Enabled

'/': Search
UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC: Back Q/CTRL+C: Quit

```

The **ACMEv2 Status** column displays the status of ACMEv2 operations for each External Account Binding credential, either Enabled or Disabled.

5. Select the credential you want to disable, and then press Enter.  
A **Manage EAB Credentials** page appears. For example:

```

Manage EAB Credentials
Modify the details for the existing EAB credentials

Friendly Name: Example

Certificate Authority: intaa250328003~subordinate56559
Certificate Profile: privatesl-tls-client-server
Permitted Algorithms: HS256,HS384,HS512

[View Details] [Cancel] [Disable EAB Key] [Disable ACMEv2] [Delete EAB Key]

UP/DOWN/TAB: Navigate ENTER/SPACE: Edit/Select B/ESC: Back Q/CTRL+C: Quit
Enter: Edit field

```

6. Select **Disable ACMEv2** and press Enter.  
The **Disable ACMEv2 operations for this EAB Credential** page appears.

Disable ACMEv2 operations for this EAB Credential?

Disabling ACMEv2 for this EAB Credential will block all ACMEv2 operations. New ACMEv2 clients will not be able to use this EAB Key to create ACMEv2 accounts. Existing ACMEv2 clients will no longer be able to use this EAB Key to perform Certificate Enrollments, Certificate Renewals, and Certificate Revocations. This action has the same effect as deleting an EAB Credential, but this action is reversible.

Note - This action will block all ACMEv2 operations for this EAB Key.

Are you sure you want to disable ACMEv2 for the EAB Key?

[ Cancel ]      [ Disable ACMEv2 ]

7. Select **Disable ACMEv2** and press Enter.  
The External Account Binding credential is disabled. The **Manage EAB Credentials** page reappears

#### Enabling ACMEv2 operations for External Account Binding credentials

You may have previously disabled ACMEv2 operations for an External Account Binding credential. When ACMEv2 operations are disabled for an External Account Binding credential, new ACMEv2 clients cannot use the credential to create an account, and ACMEv2 clients with an existing account cannot perform any ACMEv2 operations with the credential.

You can enable ACMEv2 operations that have been disabled for an External Account Binding credential. When you enable ACMEv2 operations for an External Account Binding credential, ACMEv2 clients with an existing account can perform ACMEv2 operations with the credential, and new ACMEv2 clients can use the credential to create an account if the HMAC key is enabled.

#### To enable ACMEv2 operations for an External Account Binding credential

1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

Certificate Enrollment Gateway  
ACMEv2 External Account Binding (EAB) Utility

1 Create new EAB credential  
2 Manage EAB credentials

Page 1/1

UP/DOWN/TAB: Navigate   ENTER/SPACE: Select   B/ESC/Q/CTRL+C: Quit

4. Select **Manage EAB credentials**, and then press Enter.  
A list of External Account Binding credentials appears. For example:

Certificate Enrollment Gateway

ACMEv2 External Account Binding (EAB) Utility

|   | EAB Friendly Name | Key ID                  | Key Status | ACMEv2 Status |
|---|-------------------|-------------------------|------------|---------------|
| 1 | Certbot           | 2B7x4pXZWrJI63RC4YNmcg  | Enabled    | Enabled       |
| 2 | Example           | jt58-zpca5rl13PV8bMxJNQ | Enabled    | Disabled      |

'/': Search

UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC: Back Q/CTRL+C: Quit

The **ACMEv2 Status** column displays the status of ACMEv2 operations for each External Account Binding credential, either Enabled or Disabled.

5. Select the credential you want to enable, and then press Enter.

A **Manage EAB Credentials** page appears. For example:

Manage EAB Credentials

Modify the details for the existing EAB credentials

Friendly Name: Example

Certificate Authority: intaa250328003~subordinate56559

Certificate Profile: privatessl-tls-client-server

Permitted Algorithms: HS256,HS384,HS512

[ View Details ] [ Cancel ] [ Disable EAB Key ] [ Enable ACMEv2 ] [ Delete EAB Key ]

UP/DOWN/TAB: Navigate ENTER/SPACE: Edit/Select B/ESC: Back Q/CTRL+C: Quit

Enter: Edit field

6. Select **Enable ACMEv2** and press Enter.

The **Enable ACMEv2 operations for this EAB Credential** page appears.

Enable ACMEv2 operations for this EAB Credential?

Enabling ACMEv2 for this EAB Credential will allow ACMEv2 clients to perform all ACMEv2 operations. New ACMEv2 clients will be able to use this EAB Key to create ACMEv2 accounts if the key is enabled. Existing ACMEv2 clients will be able to use this EAB Key to perform Certificate Enrollments, Certificate Renewals, and Certificate Revocations.

Note - This action will restore the ability to perform ACMEv2 operations for all ACMEv2 clients associated with this EAB Key.

Are you sure you want to enable ACMEv2 operations for this EAB Credential?

[ Cancel ] [ Enable ACMEv2 ]

7. Select **Enable ACMEv2** and press Enter.

The External Account Binding credential is enabled. The **Manage EAB Credentials** page reappears

## Deleting HMAC keys for External Account Binding credentials

Deleting the HMAC key for an External Account Binding credential will permanently remove the HMAC key and its associated External Account Binding credential from Certificate Enrollment Gateway. After the key and the External Account Binding credential are deleted, new ACMEv2 clients will no longer be able to use the key to create new ACMEv2 accounts, and existing ACMEv2 accounts associated with the credential will no longer be able to perform any ACMEv2 operations.

If you want to temporarily prevent an External Account Binding credential from being used by ACMEv2 clients, disable ACMEv2 operations for the credential instead (see [Disabling ACMEv2 operations for External Account Binding credentials](#)).

### To delete an External Account Binding credential

1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

```
Certificate Enrollment Gateway
ACMEv2 External Account Binding (EAB) Utility

1 Create new EAB credential
2 Manage EAB credentials

Page 1/1

UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC/Q/CTRL+C: Quit
```

4. Select **Manage EAB credentials**, and then press Enter.  
A list of External Account Binding credentials appears. For example:

```
Certificate Enrollment Gateway
ACMEv2 External Account Binding (EAB) Utility

EAB Friendly Name | Key ID | Key Status | ACMEv2 Status
1 Certbot | 2B7x4pXZWrfJI63RC4YNmcg | Enabled | Enabled
2 Example | jt58-zpca5rl13PV8bMxJNQ | Enabled | Enabled

'/': Search
UP/DOWN/TAB: Navigate ENTER/SPACE: Select B/ESC: Back Q/CTRL+C: Quit
```

5. Select the credential you want to delete, and then press Enter.  
A **Manage EAB Credentials** page appears. For example:

```

 Manage EAB Credentials
 Modify the details for the existing EAB credentials

Friendly Name: Example
Certificate Authority: intaa250328003~subordinate56559
Certificate Profile: privatessl-tls-client-server
Permitted Algorithms: HS256,HS384,HS512

[View Details] [Cancel] [Disable EAB Key] [Disable ACMEv2] [Delete EAB Key]

```

UP/DOWN/TAB: Navigate ENTER/SPACE: Edit/Select B/ESC: Back Q/CTRL+C: Quit  
Enter: Edit field

6. Select **Delete EAB Key** and press Enter.  
The **Delete this ACMEv2 EAB Key** page appears.

```

 Delete this ACMEv2 EAB Key?

Deleting the EAB key will permanently remove the EAB key and its associated
credential from the server. Once deleted, new ACMEv2 clients will no longer
be able to use this EAB key to create new ACMEv2 accounts, and existing ACMEv2
accounts associated with this EAB key will no longer be able to perform any
ACMEv2 operations.

Note - This action is permanent and cannot be undone. The ACMEv2 EAB Key along
with all associated ACMEv2 accounts will no longer be functional.

Are you sure you want to delete this ACMEv2 EAB Key?

 [Cancel] [Delete EAB Key]

```

7. Select **Delete EAB Key** and press Enter.  
The External Account Binding credential is deleted. The list of External Account Binding credentials reappears.

## 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 one of the following URLs to communicate with Certificate Enrollment Gateway.

#### Default ACMEv2 enrollment URL

When External Account Binding is disabled, all ACMEv2 clients must use the following URL:

```
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 Certification 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
```

#### ACMEv2 Request URL for an External Account Binding credential

When External Account Binding is enabled, each External Account Binding credential will have its own URL. For example:

```
https://<hostname>/acme/ceg/AgU-fwShl2jDXsMYe4Ti3w/0mj615kbbkbb/directory
```

Where `<hostname>` is the hostname or IP address of the Certificate Enrollment Gateway server. For example:

```
https://cegserver.example.com/acme/ceg/AgU-fwShl2jDXsMYe4Ti3w/0mj615kbbkbb/directory
```

For details about managing External Account Binding credentials, see [Managing External Account Binding credentials](#).

#### 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:

| Meth<br>od | 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.

## 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.

- [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](#)

**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

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/
 privatessl_tls_client/directory
 # Email address used for ACME registration
 email: certmanager@example.com
 # Name of a secret used to store the ACME account private key
 privateKeySecretRef:
 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 -sfL 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 contain 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 Gateway. 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
```

## Integrating CMPv2 clients with Certificate Enrollment Gateway

This section explains how to integrate CMPv2 clients with the Certificate Enrollment Gateway service.

- [Configuring a permitted senders file to restrict access to the CMPv2 Service](#)
- [Configuring Certificate Enrollment Gateway for CMPv2 enrollment](#)
- [Configuring CMPv2 clients for enrollment with Certificate Enrollment Gateway](#)

### Configuring a permitted senders file to restrict access to the CMPv2 Service

You can restrict access to the CMPv2 Service so that it can accept requests only from permitted CMPv2 clients. You can restrict access using a permitted senders file.

The permitted senders file must contain a list of fully qualified domain names (FQDNs) or IP addresses of clients that are permitted to send CMPv2 requests. Host names in an FQDN must contain only ASCII letters (A to Z, a to z), numbers (0 to 9), and hyphens.

You can specify the permitted senders file when configuring Certificate Enrollment Gateway for CMPv2 enrollment.

#### To configure a permitted senders file

1. Create a new file or open an existing permitted senders file in a text editor.
2. In the file, enter a list of fully qualified domain names (FQDNs) or IP addresses of hosts permitted to send CMPv2 requests. Each line must contain either an IP address or FQDN. For example:

```
domain1.example.com
domain2.example.com
domain3.example.com
192.0.2.0
192.0.2.1
192.0.2.2
```

3. Save and close the file.
4. Configure the CMPv2 protocol to use the permitted senders file (see [Configuring Certificate Enrollment Gateway for CMPv2 enrollment](#)).

### Configuring Certificate Enrollment Gateway for CMPv2 enrollment

To configure Certificate Enrollment Gateway for CMPv2 enrollment, you must configure the CMPv2 enrollment settings in Certificate Enrollment Gateway. You can edit the CMPv2 enrollment settings using the Management Console interface.

#### To configure Certificate Enrollment Gateway for CMPv2 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. Configure the settings under the **CMPv2 (CEG)** tab.
8. Configure any other settings if required.
9. After configuring the settings, click **Validate** to validate the settings.
10. If any configuration errors are detected, correct the errors then click **Validate** again.
11. After validating the configuration settings, click **Next**.
12. Cryptographic Security Platform uploads the configuration and any attached files, such as P12 credentials.
13. 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 CMPv2 clients for enrollment with Certificate Enrollment Gateway

CMPv2 clients must use one of the following URLs to communicate with Certificate Enrollment Gateway:

 The `http` URL only works if you configured the CMPv2 Service to allow HTTP connections.

```
https://<CEG-server>/cmpv2/<tenant-ID>/<CA-ID>/<profile-ID>/<spec-id>
http://<CEG-server>/cmpv2/<tenant-ID>/<CA-ID>/<profile-ID>/<spec-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 Certification Authority (CA) defined in CA Gateway that will issue certificates to the CMPv2 client.
- `<profile-ID>` is the profile ID defined in CA Gateway that defines the certificate type issued to the CMPv2 client.
- `<spec-id>` is a specification ID for CMPv2 that is defined in CA Gateway.

For example:

```
https://cegserver.example.com/cmpv2/tenant1/example_ca1/example-profile1/standard
http://cegserver.example.com/cmpv2/tenant1/example_ca1/example-profile1/standard
```

## Integrating EST clients with Certificate Enrollment Gateway

This section explains how to integrate EST clients with the Certificate Enrollment Gateway service.

- [Preparing to configure Certificate Enrollment Gateway for EST enrollment](#)
- [Configuring Certificate Enrollment Gateway for EST enrollment](#)
- [Configuring EST clients for enrollment with Certificate Enrollment Gateway](#)

### Preparing to configure Certificate Enrollment Gateway for EST enrollment

Certificate Enrollment Gateway requires some additional files to communicate with EST clients. You must specify these files when configuring Certificate Enrollment Gateway for EST enrollment.

- [Creating a P12 file for the EST front end](#)
- [Creating a truststore for the EST front-end SSL certificate](#)
- [Creating a truststore for EST vendor certificates](#)

#### Creating a P12 file for the EST front end

For EST enrollment, Certificate Enrollment Gateway uses a web front end. The web front end requires an SSL certificate to terminate SSL connections coming from EST clients. The SSL certificate must be stored in a PKCS #12 (P12) file. This P12 file must contain a single server public key and private key pair.

The private key and certificate contained in the P12 file must be the same private key and certificate (not certificate chain) used for the cluster. For information about this private key and certificate, see [Issuing TLS certificates for Certificate Enrollment Gateway](#).

You can use OpenSSL to create the P12 using the private key and certificate. You can use the following OpenSSL command to create the P12 file:

```
openssl pkcs12 -export -out <p12-file> -inkey <private-key> -in <certificate>
```

Where:

- `<p12-file>` is a path and file name for the P12 file.
- `<private-key>` is the path and file name of the private key file.
- `<certificate>` is the path and file name of the TLS certificate.

For example:

```
openssl pkcs12 -export -out cluster.p12 -inkey servernokey.key -in server.crt
```

#### Creating a truststore for the EST front-end SSL certificate

For EST enrollment, Certificate Enrollment Gateway requires an SSL certificate to terminate SSL connections coming from EST clients. To validate the EST SSL certificate, Certificate Enrollment Gateway requires a truststore containing the CA certificate chain for the SSL certificate, from the Issuing CA to the root CA.

The truststore for the EST SSL certificate must be stored in one of the following files:

| File           | Description                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| P12 truststore | This file must be a PKCS #12 (P12) file. The file must contain at least one Trusted CA Certificate entry (TrustedCertEntry).                                                                         |
| PEM truststore | 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. |

#### To generate a P12 truststore for the EST SSL certificate using the Java keytool utility

1. Obtain the CA certificate chain for the EST SSL certificate, from the issuing CA 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 P12 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 P12 truststore file. For example, `est-truststore.p12`. The utility will create the file if it does not exist.

4. For example:

```
keytool -import -alias cagw-root -trustcacerts -file /tmp/root.cer -keystore /home/user/est-truststore.p12
```

5. When prompted, enter a password for the truststore.

#### To generate a PEM truststore for the EST SSL certificate

1. Obtain the CA certificate chain for the EST SSL certificate, from the issuing CA 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 issuing CA 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-----
MIIDqQYJKoZIhvcNAQcCoIIDmJCCA5YCAQExADALBgkqhkiG9w0BBwGggN...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDejCCAmKgAwIBAgIQQ8e7ock59Y21Mtcy7rGJUDANBgkqhkiG9w0BAQs...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIQ0EgRW50cnkwHhcNMjMwMjA4MTUxNzEwWWhcNMzMwMjA4MTU0NzEwWjAyM...
-----END CERTIFICATE-----
```

6. Save and close the file.

#### Creating a truststore for EST vendor certificates

EST devices may be issued a certificate from a third-party CA. These vendor certificates were issued during manufacture. Certificate Enrollment Gateway can authenticate the initial enrollment request from these EST devices by validating their vendor certificate. To validate a vendor certificate, Certificate Enrollment Gateway requires a truststore containing the CA certificate chain for the vendor certificate.

The truststore must be stored in one of the following files:

| File           | Description                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| P12 truststore | This file must be a PKCS #12 (P12) file. The file must contain at least one Trusted CA Certificate entry (TrustedCertEntry).                                                                         |
| PEM truststore | 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. |

#### To generate a P12 truststore for a vendor certificate using the Java keytool utility

1. Obtain the certificate chain for the vendor certificate, from the issuing CA 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 P12 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 P12 truststore file. For example, `vendor-truststore.p12`. The utility will create the file if it does not exist.

4. For example:

```
keytool -import -alias cagw-root -trustcacerts -file /tmp/root.cer -keystore /home/user/vendor-truststore.p12
```

5. When prompted, enter a password for the truststore.

### To generate a PEM truststore for a vendor certificate

1. Obtain the certificate chain for the vendor certificate, from the issuing CA 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 issuing CA 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-----
MIIDqQYJKoZIhvcNAQcCoIIDmJCCA5YCAQExADALBgkqhkiG9w0BBwGggN...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDejCCAmKgAwIBAgIQQ8e7ock59Y21Mtcy7rGJUDANBgkqhkiG9w0BAQs...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIQ0EgRW50cnkWHhcNMjMwMjA4MTUxNzEwWWhcNMzMwMjA4MTU0NzEwWjAyM...
-----END CERTIFICATE-----
```

6. Save and close the file.

## Configuring Certificate Enrollment Gateway for EST enrollment

To configure Certificate Enrollment Gateway for EST enrollment, you must configure the EST enrollment settings in Certificate Enrollment Gateway. You can edit the EST enrollment settings using the Management Console interface.

### To configure Certificate Enrollment Gateway for EST 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. Configure the settings under the **EST** tab.
8. Configure any other settings if required.
9. After configuring the settings, click **Validate** to validate the settings.
10. If any configuration errors are detected, correct the errors then click **Validate** again.
11. After validating the configuration settings, click **Next**.
12. Cryptographic Security Platform uploads the configuration and any attached files, such as P12 credentials.
13. 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 EST clients for enrollment with Certificate Enrollment Gateway

EST clients must use one of the following URLs to communicate with Certificate Enrollment Gateway.

 When using the concatenated URL, the tenant ID, CA ID, and certificate profile ID cannot use underscores.

### Default EST enrollment URL:

```
https://<CEG-server>:1443/.well-known/est/<tenant-ID>/<CA-ID>/<profile-ID>/
```

### Concatenated EST enrollment URL:

```
https://<CEG-server>:1443/.well-known/est/<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 Certification Authority (CA) defined in CA Gateway that will issue certificates to the EST client.
- `<profile-ID>` is the profile ID defined in CA Gateway that defines the certificate type issued to the EST client. For Entrust PKI as a Service, the profile ID is one of the following:

- est-digital-signature-key-encipherment
- est-digital-signature
- est-key-encipherment
- est-non-repudiation

For example:

```
https://cegserver.example.com/.well-known/est/tenant1/example-ca1/est-digital-
signature/
https://cegserver.example.com/.well-known/est/tenant1_example-ca1_est-digital-
signature/
```

## 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 a Mobile Device Management product for enrollment with CSP Certificate Enrollment Gateway](#)
- [Configuring MDM-SCEP clients 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.
  - [MDM Web Service \(MDMWS\)](#)
  - [MDMWS Scheduled Jobs](#)
  - [MDMWS Users](#)
  - [MDMWS Enrollment Service Configuration](#)
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 a Mobile Device Management product for enrollment with CSP 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.

- [Supported MDM authentication methods](#)
- [Adding the CA certificate chain to the MDM product](#)
- [Issuing a signing certificate to the MDM product](#)
- [Enrollment URL for MDMWS clients](#)

### Supported MDM authentication methods

Certificate Enrollment Gateway supports user name and password authentication to authenticate with MDM products. You must configure at least one user name and password credential in the MDM product.

All user name and password credentials that Certificate Enrollment Gateway will use to authenticate to the MDM product must be specified in the Certificate Enrollment Gateway configuration. For details, see [Configuring and deploying Certificate Enrollment Gateway](#).

### 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.

### 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.

### 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
```

## 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
```

## 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.

- [How Certificate Enrollment Gateway works with Microsoft Intune](#)
- [Configuring Microsoft Intune for Certificate Enrollment Gateway](#)
- [Configuring Certificate Enrollment Gateway for Microsoft Intune](#)
- [Updating the client secret \(application key\) used by the integration](#)

## 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.

## 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.

- [Registering an application for Certificate Enrollment Gateway](#)
- [Generating a client secret for password-based authentication with Certificate Enrollment Gateway](#)
- [Generating and importing a TLS certificate for certificate-based authentication with Certificate Enrollment Gateway](#)
- [Adding API permissions to the CEG Service application](#)
- [Adding CAs to Microsoft Intune as trusted third-party CAs](#)
- [Configuring identity protection profiles for Windows Hello for Business](#)
- [Configuring SCEP certificate profiles](#)
- [Obtaining information required 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`.

#### 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.

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. Certificate Enrollment Gateway requires a P12 file for certificate-based authentication to Microsoft Intune. The P12 file for Certificate Enrollment Gateway must contain both the TLS certificate and associated private key,

### 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.

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) |
| 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.

#### 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**.

#### 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.

### 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:

**i** 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`

## 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 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](#)
  - [Scheduled Jobs](#)
  - [Intune-SCEP Enrollment Service Configurations](#)
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.

## 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.

## Integrating SCEP clients with Certificate Enrollment Gateway

This section explains how to integrate SCEP clients with the Certificate Enrollment Gateway service.

- [Configuring Certificate Enrollment Gateway for SCEP enrollment](#)
- [Configuring SCEP clients for enrollment with Certificate Enrollment Gateway](#)
- [Google ChromeOS integration use case](#)

### 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.

## 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/
```

## 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:

**i** 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.



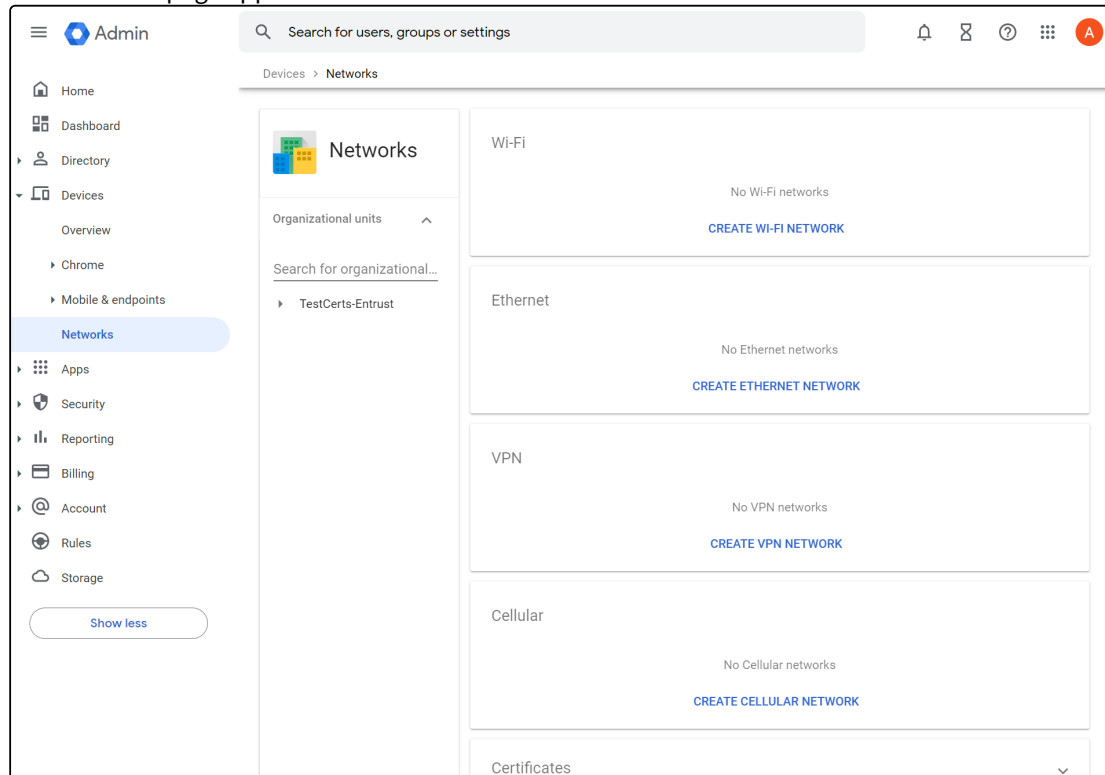
## Configuring Google Admin for SCEP enrollment

SCEP enrollment for ChromeOS is controlled using Google Admin, a Web-based interface for managing users and groups for an organization.

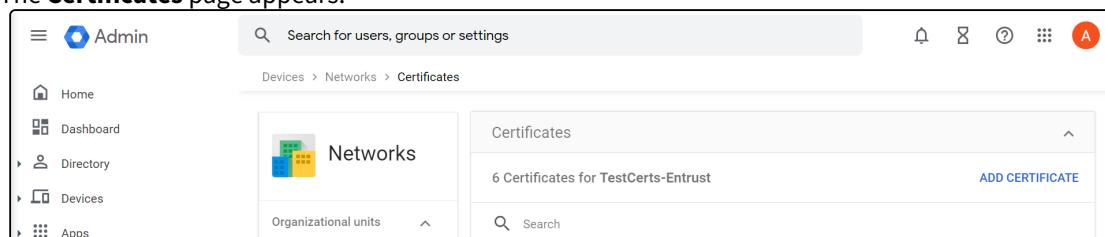
### To configure Google Admin for SCEP enrollment

1. Log in to Google Admin (<https://admin.google.com>).
2. Navigate to **Devices > Networks**.

The **Networks** page appears.

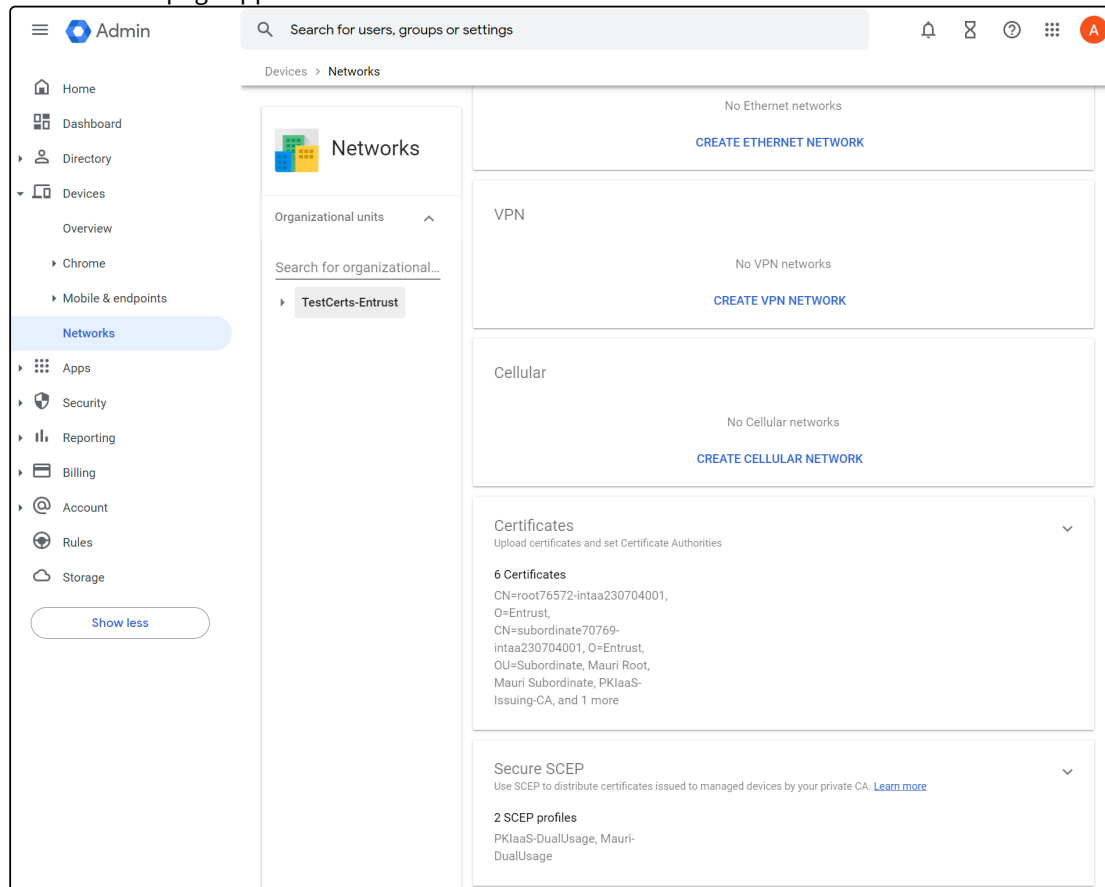


3. Click on the **Certificates** pane.
- The **Certificates** page appears.

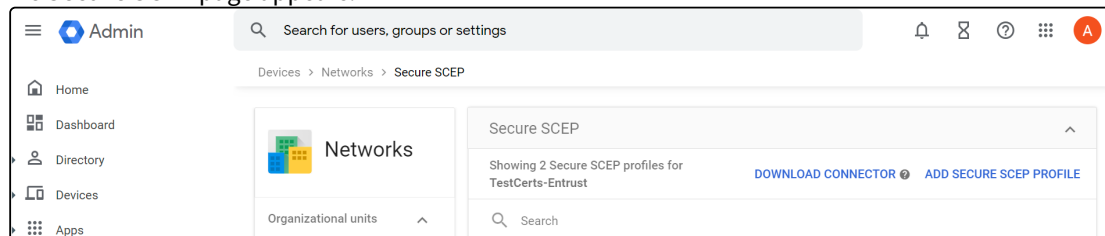


4. Add the entire CA certificate chain (from the root CA to the issuing CA) for the Managed CA. To add a CA certificate:
  - a. Click **Add Certificate**. The **Add Certificate** page appears.
  - b. In the **Name** field, enter a unique friendly name for the CA certificate,
  - c. Click **Upload** and 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`.

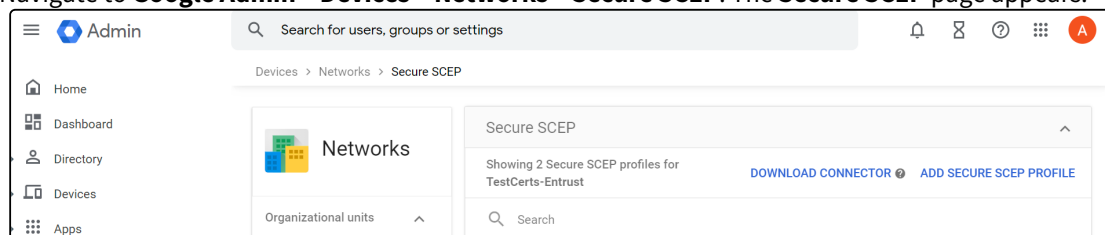
- e. For **Key Usage**, select each key usage that will be included in the issued certificates.
- f. For **Key size (bits)**, select a key size for the issued certificates.
- g. For **Security**, select the security level (attestation requirement) for the issued certificates.
- h. In the **SCEP server 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.

Cryptographic Security Platform 1.1.0 - Installation and administration guide

392

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.

## 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.

### 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.

## 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 write-able domain controller.

- [Active Directory schema requirements](#)
- [Active Directory role requirements for running the Entrust-provided PowerShell scripts](#)
- [Creating a service logon account for read-only access to Active Directory](#)
- [Creating a Kerberos Service Account for Kerberos authentication](#)
- [Configuring the Group Policy for cross-forest deployments](#)
- [Adding referrals for cross-forest deployments](#)

### 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.

### 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".

### 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](#).

#### 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.

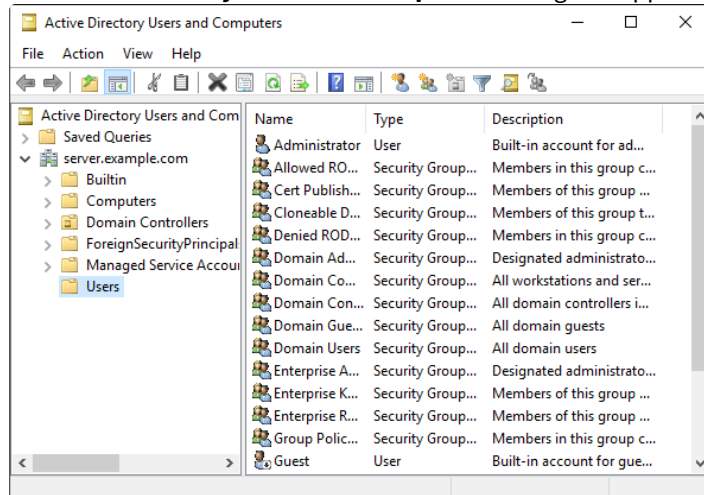
**i** Certificate Enrollment Gateway supports connections to an entire Domain Forest. Certificate Enrollment Gateway must point to the top-level domain of the forest to work across the entire forest.

You must create the same Kerberos account for all forests in cross-forest deployments.

#### To create a Kerberos Service Account

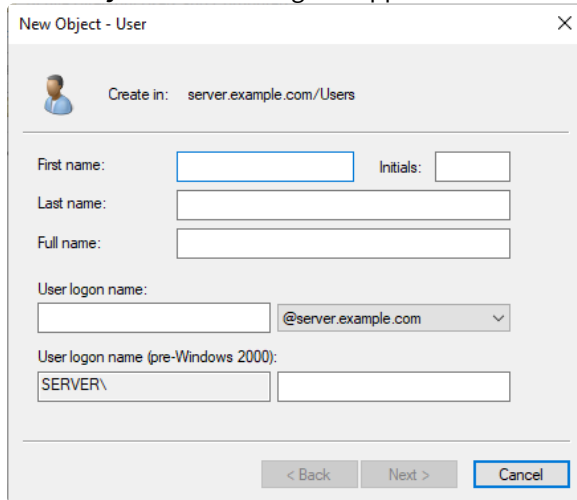
1. Log in to the server hosting the Active Directory domain controller as a domain administrator or a user who is a member of the built-in Account Operators domain group.
2. Open the Active Directory Users and Computers administrative tool (select **Start > Windows Administrative Tools > Active Directory Users and Computers**).

The **Active Directory Users and Computers** dialog box appears.

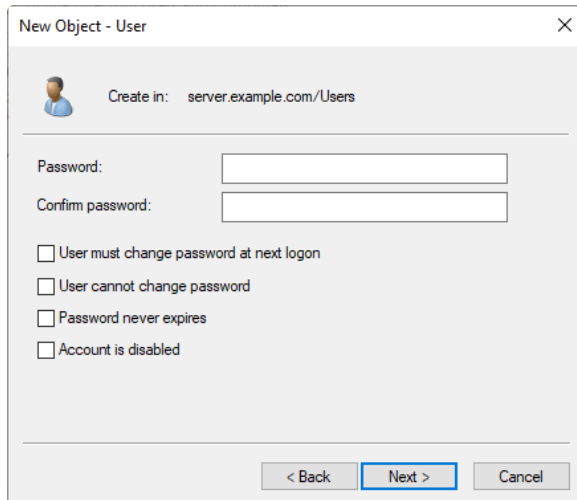




3. Right-click the folder where you want to create the new account and select **New > User**. A **New Object – User** dialog box appears.

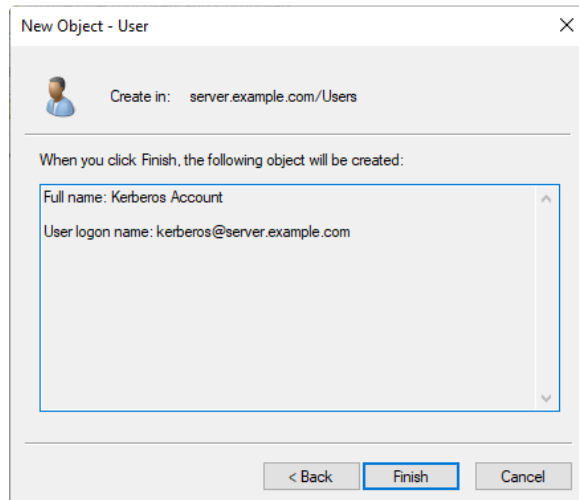
The dialog box is titled "New Object - User" and has a close button (X) in the top right corner. It features a user icon and the text "Create in: server.example.com/Users". The form contains several input fields: "First name:" with a text box and "Initials:" with a text box; "Last name:" with a text box; "Full name:" with a text box; "User logon name:" with a text box and a dropdown menu showing "@server.example.com"; and "User logon name (pre-Windows 2000):" with a text box containing "SERVER\" and an empty text box. At the bottom, there are three buttons: "< Back", "Next >", and "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 dialog box is titled "New Object - User" and has a close button (X) in the top right corner. It features a user icon and the text "Create in: server.example.com/Users". The form contains several input fields: "Password:" with a text box and "Confirm password:" with a text box. Below these are four checkboxes: "User must change password at next logon", "User cannot change password", "Password never expires", and "Account is disabled". At the bottom, there 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**.

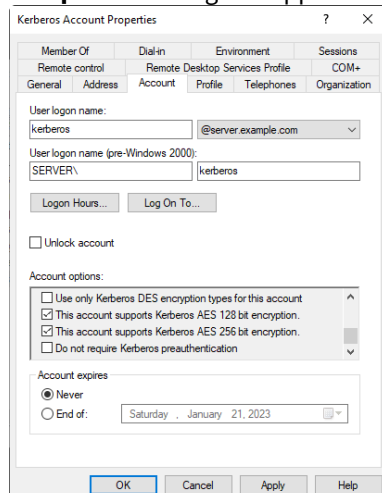


13. Record the user logon name of the account (such as `kerberos@example.com`). You will use this logon name later to create the Kerberos keytab file.

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**.

## 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

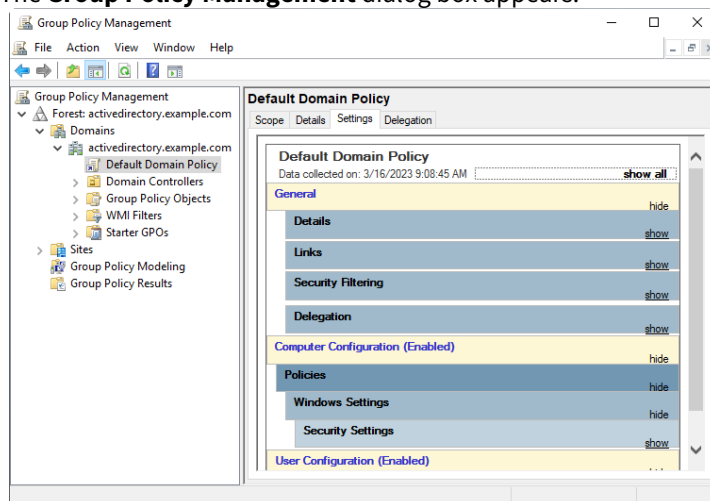
For cross-forest deployments, both the Key Distribution Center (KDC) and the Kerberos client must search a list of trusted forests when attempting to resolve a two-part SPN if the SPN cannot be found in the local forest. The list of trusted forests that the KDC and Kerberos clients can search is controlled 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

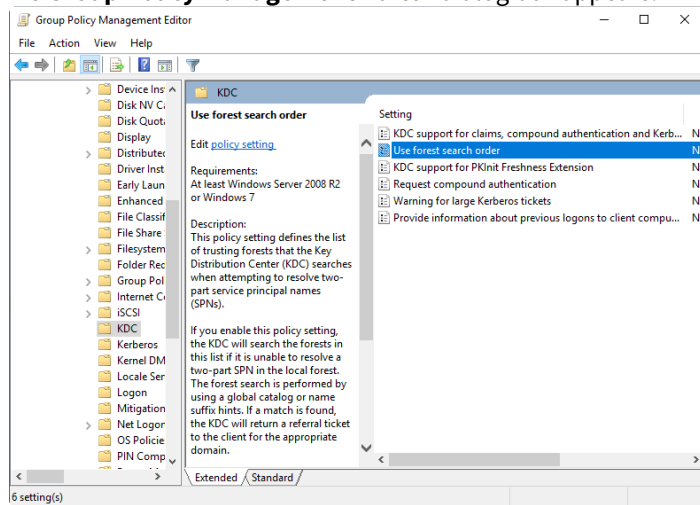
1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
2. Select **Start > Windows Administrative Tools > Group Policy Management**.

The **Group Policy Management** dialog box appears.

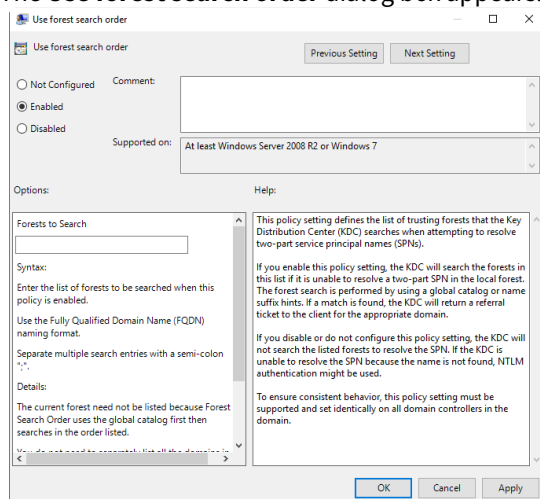


3. In the tree view, select **Group Policy Management > Forest: <forest> > Domains > <domain> > Default Domain Policy**.  
Where **<forest>** is the FQDN (fully qualified domain name) of the forest, and **<domain>** is the FQDN of the domain.

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.

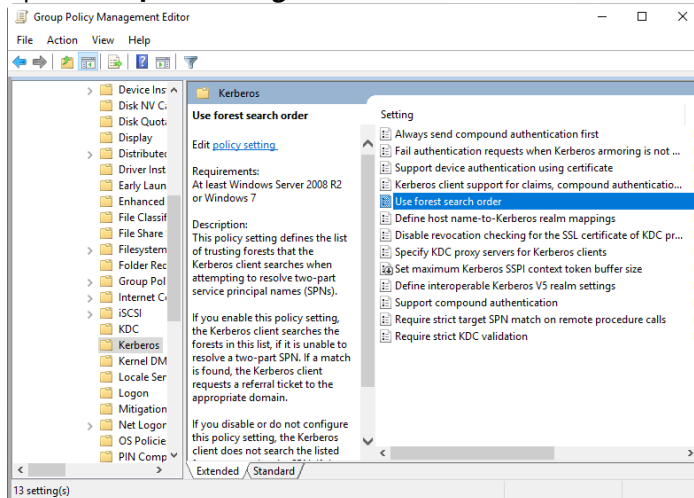


8. Select **Enabled**.
9. In the **Options** pane, in the **Forests to Search** field, enter the list of trusted forests that the Key Distribution Center (KDC) will search when attempting to resolve a two-part SPN that does not exist in the local forest. Separate each forest with a semicolon. For example:

example.com;example.net;example.org

10. Click **OK**.

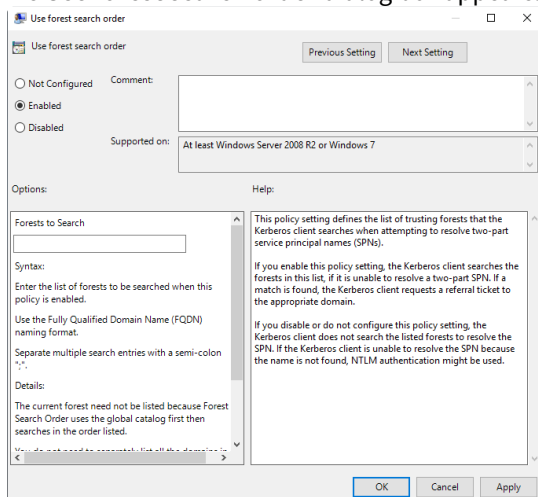
11. Expand **Computer Configuration > Policies > Administrative Templates > System > Kerberos**.



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**.

### Adding referrals for cross-forest deployments

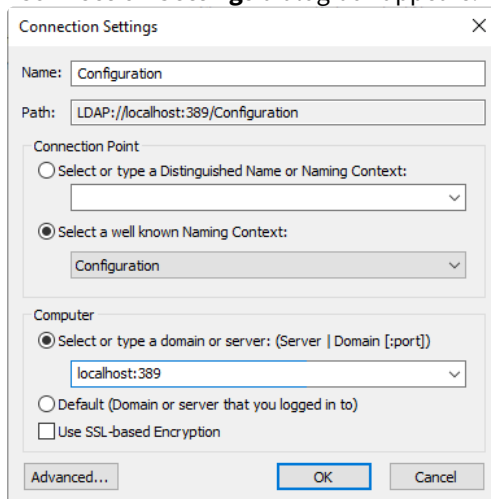
WSTEP enrollment can use Kerberos authentication to authenticate Windows endpoints. For cross-forest deployments, Windows endpoints are located using Kerberos V5 LDAP referrals. The domain controller (Active Directory Domain Services), maintains referral data in its Configuration container, in crossRef 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.

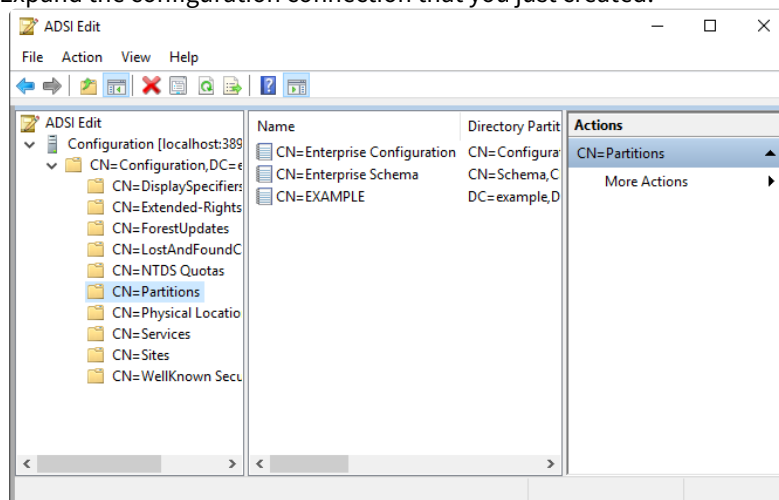
### To add a cross-forest referral in a domain controller for cross-forest deployments

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.

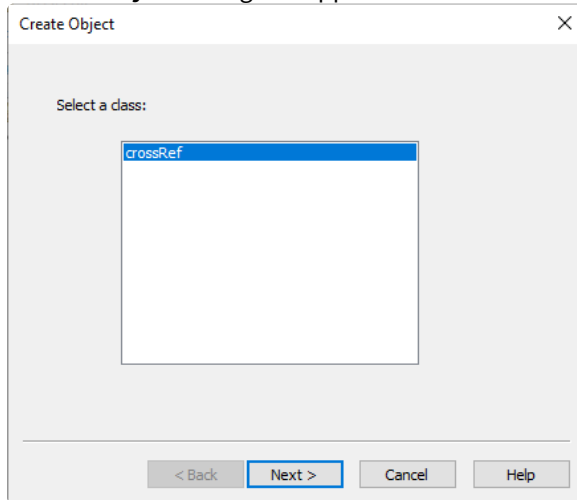


- b. In the **Name** field, enter a unique name for the connection.
  - c. Under **Connection Point**, click **Select a well known Naming Context**, and then select **Configuration**.
  - d. Under **Computer**, click **Select or type a domain or server**, and then enter the server and port of the domain 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.

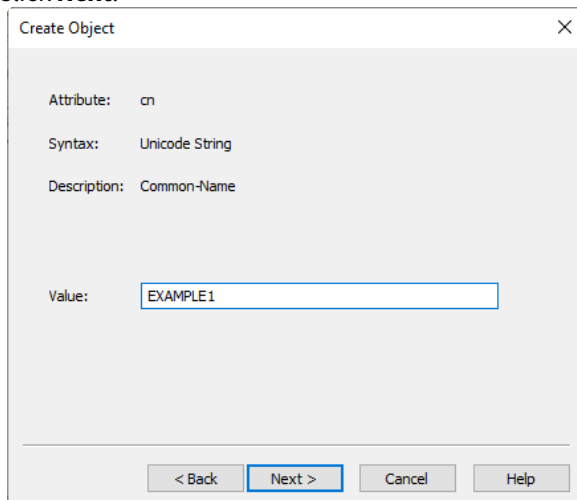


4. Expand **CN=Configuration,<suffix> > CN=Partitions**.  
Where **<suffix>** is the suffix (distinguished name) of the domain controller.

5. Select **CN=Partitions**, and then select **Action > New > Object**.  
A **Create Object** dialog box appears.

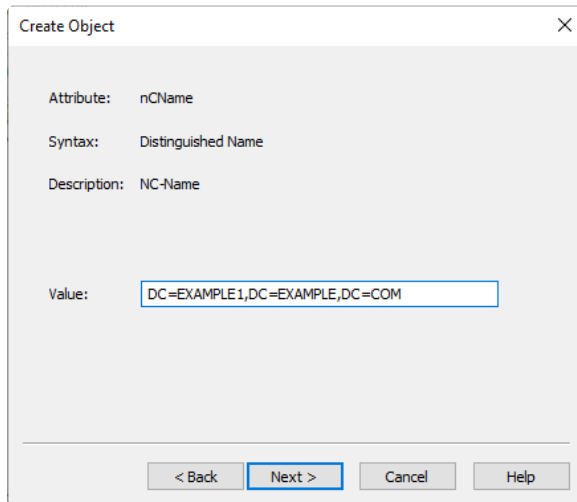
A screenshot of the 'Create Object' dialog box. The title bar says 'Create Object' with a close button. Inside, it says 'Select a class:' above a list box. The list box contains 'crossRef' and is currently empty. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' 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**.



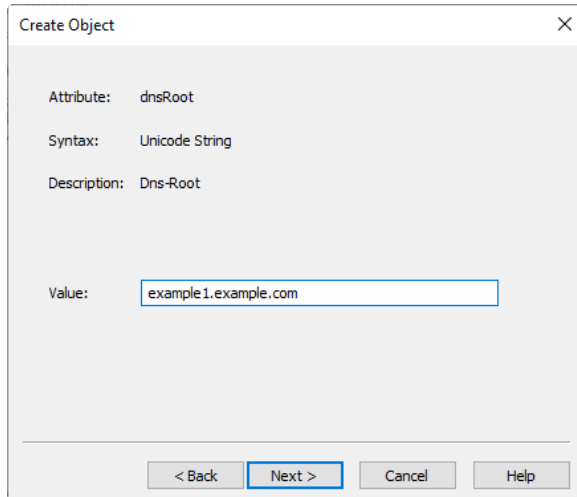
The 'Create Object' dialog box shows the following information:

- 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**.



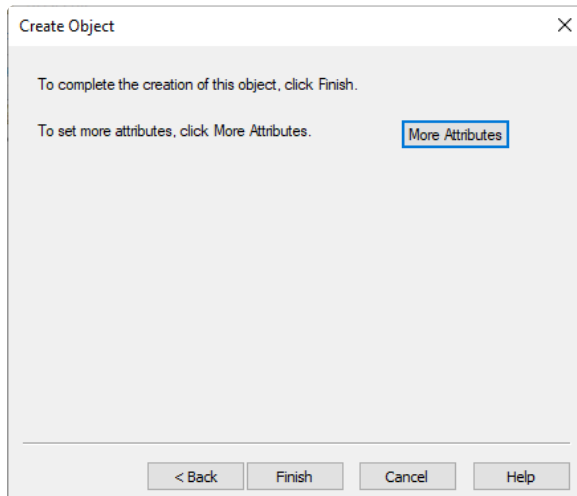
The 'Create Object' dialog box shows the following information:

- 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 information:

- 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.

## 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 keytab file for WSTEP enrollment](#)
- [Creating a Kerberos configuration file for cross-forest WSTEP enrollment](#)

### 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.

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](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html).

## 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.

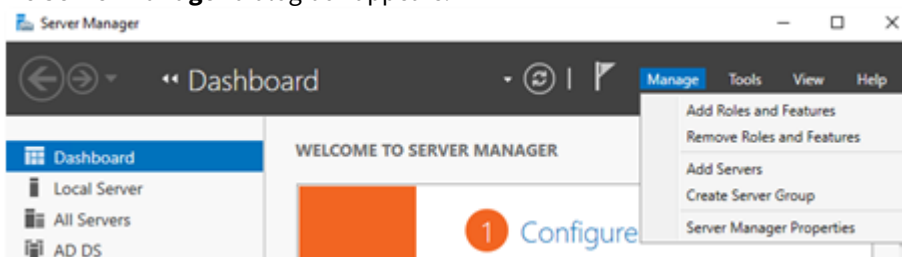
```
C:\Windows\System32\certtmpl.msc
```

5. Answer **Yes** when prompted to install the templates into Active Directory.

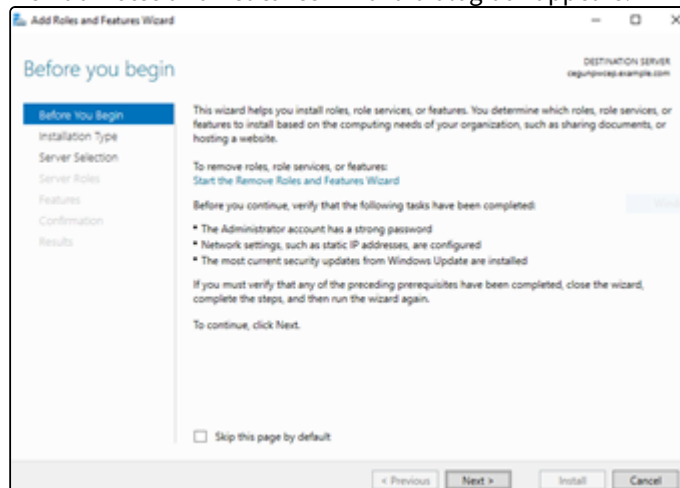
Adding the certificate templates feature using the Windows graphical interface

To add Certificate Templates using the Windows graphical interface, complete the following procedure.

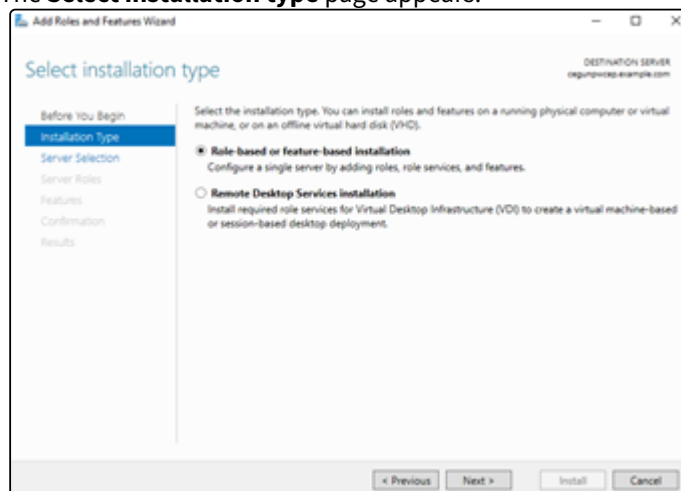
1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
2. Open Server Manager. Select **Start > Server Manager**. The **Server Manager** dialog box appears.



3. Select **Manage > Add Roles and Features**. The **Add Roles and Features Wizard** dialog box appears.

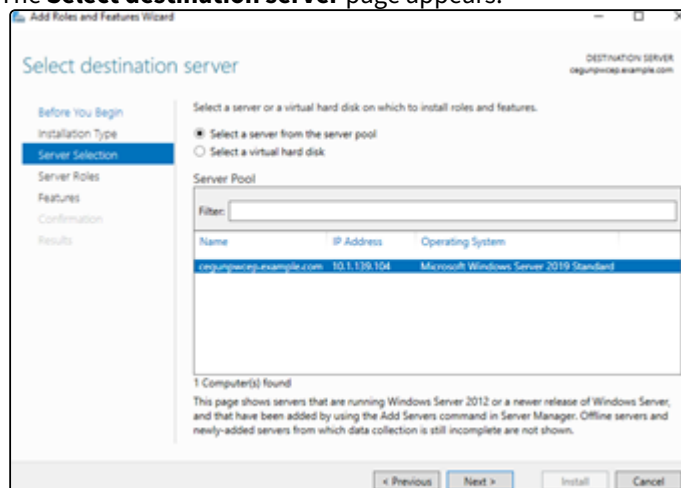


4. If the **Before you Begin** page appears, click **Next**.  
The **Select installation type** page appears.



5. Select **Role-based or feature-based installation**.
6. Click **Next**.

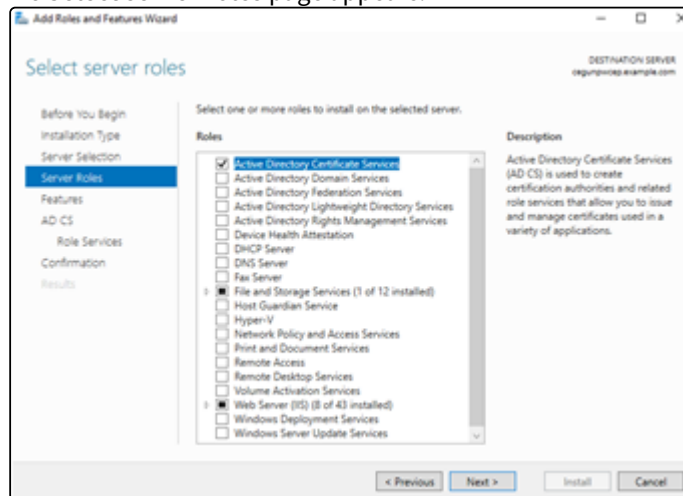
The **Select destination server** page appears.



7. Click **Select a server from the pool**.
8. In the **Server Pool** list, select the server.

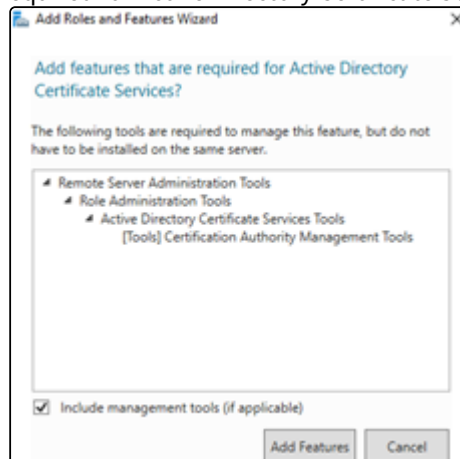
9. Click **Next**.

The **Select server roles** page appears.



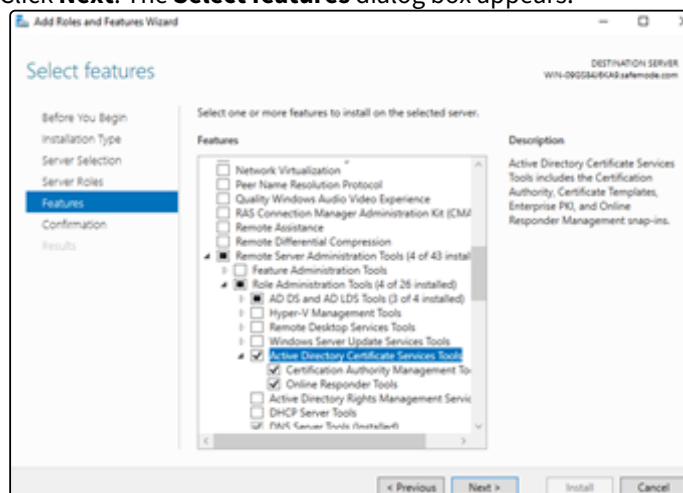
10. Select **Active Directory Certificate Services**.

Another **Add Roles and Features Wizard** dialog box may appear, informing you that some features are required for Active Directory Certificate Services.

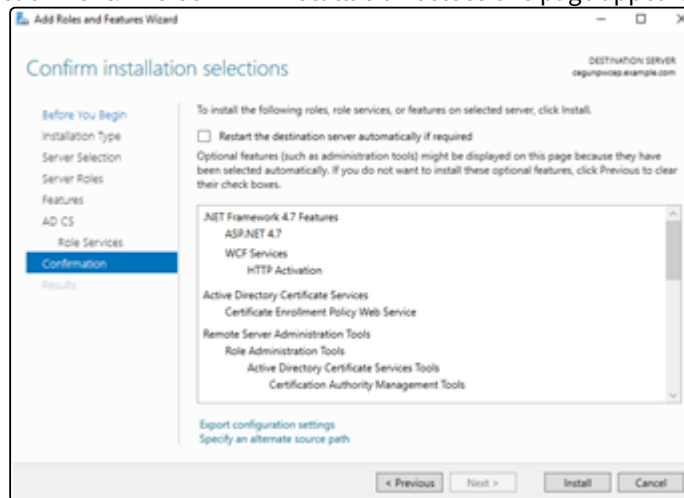


11. Click **Add Features** to add these required features and close the dialog box.

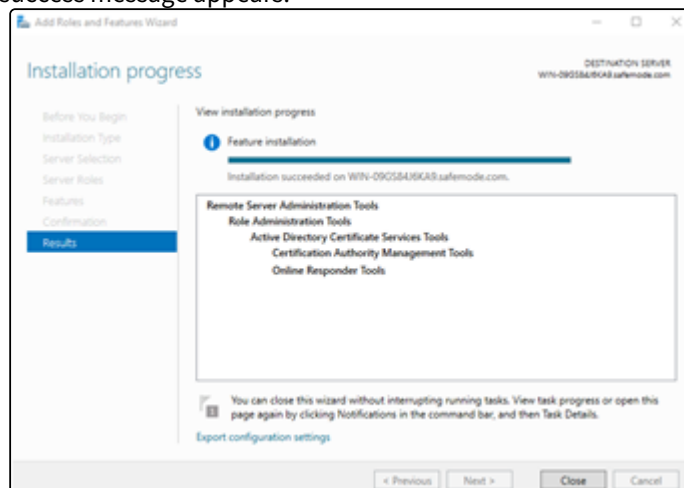
12. Click **Next**. The **Select features** dialog box appears.



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.

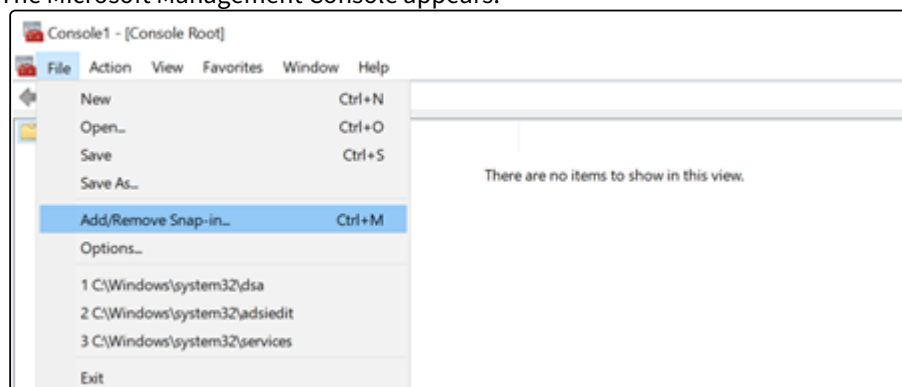


15. Click **Install**. The **Installation Progress** page appears.  
A progress indicator displays the progress of the installation. After the roles and features are installed, a success message appears.

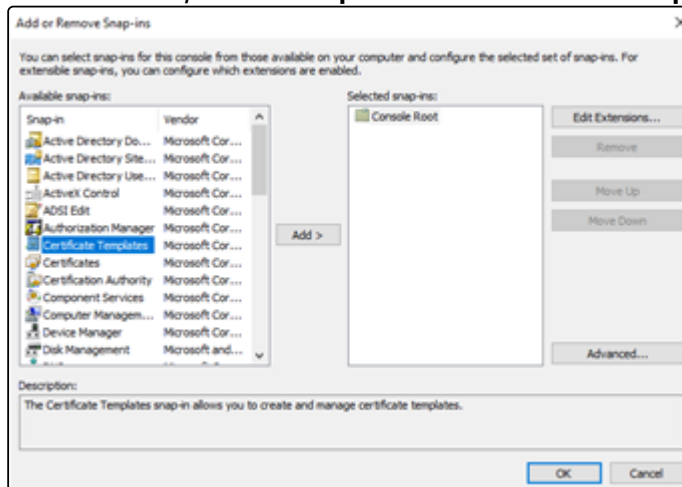


16. Click **Close**.
17. Run `mmc.exe`.

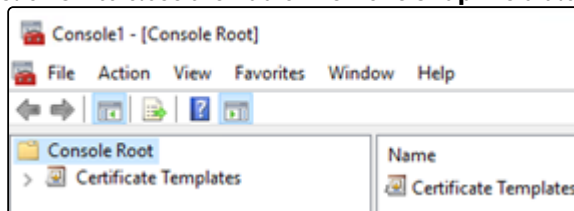
The Microsoft Management Console appears.



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 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).

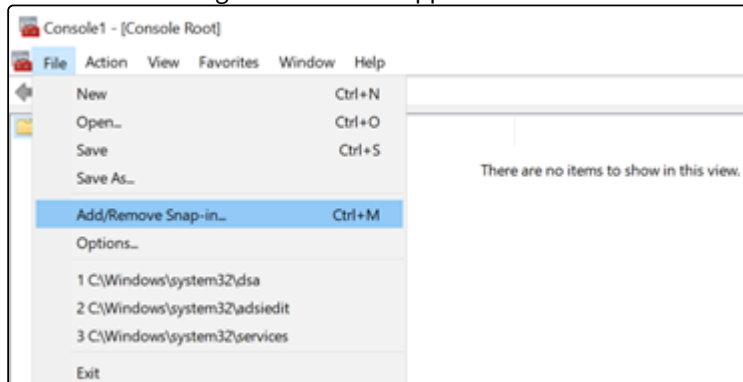
### To create a Windows certificate template for WSTEP

1. Log into Active Directory as a member of the Domain Admins group.



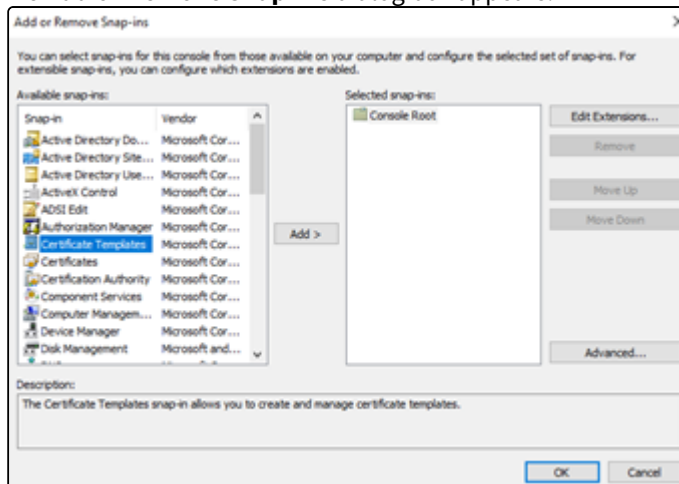
2. Run `mmc.exe` (Select **Start > Windows System > Run**, then enter `mmc.exe`).

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 **Certificate Templates**.
5. Click **Add**.
6. In the tree view, select the **Certificate Templates** snap-in.
7. 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.



9. Under each tab, configure template options as described in the following sections.

- [Compatibility tab](#)
- [General tab](#)
- [Security tab](#)
- [Request Handling tab](#)
- [Cryptography tab](#)
- [Key Attestation tab](#)
- [Subject Name tab](#)
- [Issuance Requirements tab](#)
- [Extensions tab](#)

✗ 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**.

### 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<br><div>  If you install a Windows Server 2016 CA, read the following Microsoft troubleshooting guide: <a href="#">Cannot select Windows Server 2016 CA-compatible certificate templates from Windows Server 2016 or later-based CAs or CEP servers.</a> </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.                                                                                                                                                                                                 |

### 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 <b>Template display name</b> field but without spaces. We recommend using this value.<br><br>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.                                                                                                                                                                                            |
| Renewal Period                          | Yes       | Controlled by the client.                                                                                                                                                                                                                              |
| Publish certificate in Active Directory | 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 <b>Domain Users</b> group to use a copy of the <b>User certificate</b> template. If the group is not listed, click <b>Add</b> to add the group to the list. |
| Permissions for Authenticated Users | Set the following <b>Allow</b> permissions for the selected group: Read, Enroll, Autoenroll.                                                                                                                                                     |

#### 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       |                                                                                    |
| Enroll subject without requiring any user input                                                       | Yes       |                                                                                    |

| Option                                                                                | Supported | Value |
|---------------------------------------------------------------------------------------|-----------|-------|
| Prompt the user during enrollment                                                     | No        |       |
| Prompt the user during enrollment and require user input when the private key is used | No        |       |

#### Cryptography tab

Under the **Cryptography** tab, set the supported options.

| Option                                                            | Supported | Value |
|-------------------------------------------------------------------|-----------|-------|
| Provider Category                                                 | Yes       |       |
| Algorithm name                                                    | Yes       |       |
| 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        |       |

#### Key Attestation tab

Options under the **Key Attestation** tab are not supported.

#### Subject Name tab

Under the **Subject Name** tab, set the supported options.

| Option            | Supported | Value                                                                                                                                                   |
|-------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supply in request | Yes       | The Subject Alternative Name <b>RegisteredID</b> is not supported.<br>The <b>Subject name</b> types <b>Title</b> and <b>Initials</b> are not supported. |

| Option                                                                                 | Supported | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use subject information from existing certificates for autoenrollment renewal requests | Yes       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Build from Active Directory information                                                | Yes       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Subject name format                                                                    | Yes       | <p>For User certificate templates, the following formats are supported:</p> <ul style="list-style-type: none"> <li>• <b>Common name.</b></li> <li>• <b>Fully distinguished name.</b> This value is not supported when Certificate Enrollment Gateway has mapped the Windows certificate template to a Profile ID in CA Gateway.</li> </ul> <p>For Computer or Domain Controller certificate templates, the following formats are supported:</p> <ul style="list-style-type: none"> <li>• <b>Common name.</b></li> <li>• <b>DNS.</b></li> <li>• <b>Fully distinguished name.</b> This value is not supported when Certificate Enrollment Gateway has mapped the Windows certificate template to a Profile ID in CA Gateway.</li> </ul> |
| 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       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

#### 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                                                                             |

#### 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<br>Digital Signature+Non-repudiation |
| Signature and Encryption       | Digital Signature+Key Encipherment                     |
| Signature and smartcard logon. | Digital Signature                                      |

#### 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.

 The server certificate for Active Directory LDAPS communications must include a valid HTTP CRL Distribution Point.

- [Creating a CSR for an Active Directory server certificate](#)
- [Installing the CA certificate chain for the Active Directory certificate](#)
- [Issuing the Active Directory server certificate with Entrust PKI as a Service](#)
- [Issuing the Active Directory server certificate with an on-premises CA](#)
- [Installing the Active Directory server certificate](#)
- [Verifying LDAPS in Active Directory](#)
- [Generating a file containing the CA certificate chain for the Active Directory server certificate](#)
- [Configuring channel binding enforcement to Active Directory](#)

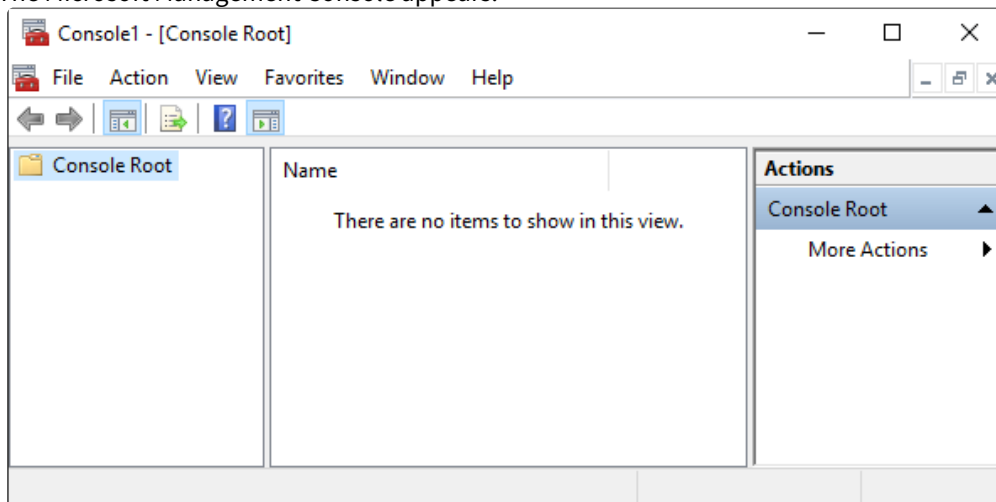
## Creating a CSR for an Active Directory server certificate

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

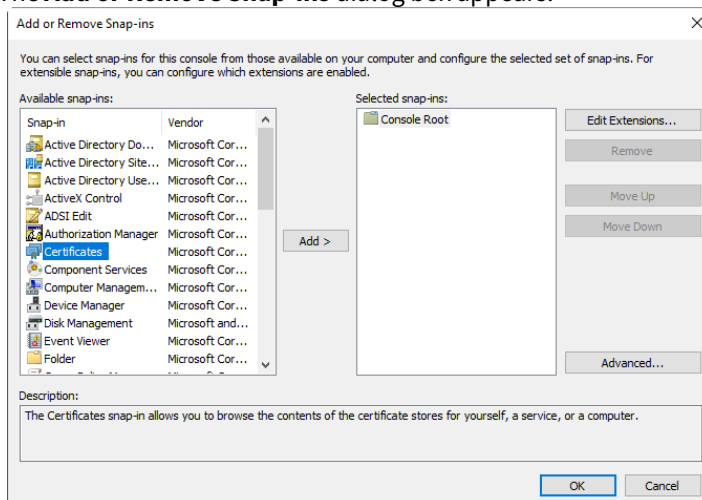
1. Log into Active Directory as a member of the Domain Admins group.
2. Run `mmc.exe` (Select **Start > Windows System > Run**, then enter `mmc.exe`).

The Microsoft Management Console appears.



3. Select **File > Add/Remove Snap-in**.

The **Add or Remove Snap-ins** dialog box appears.

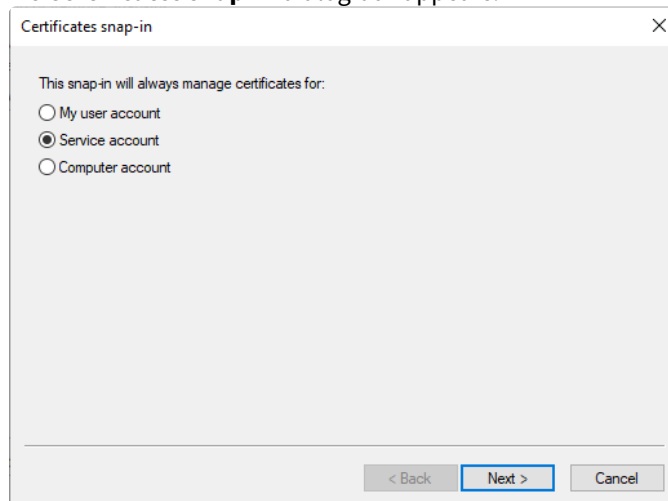


4. In the **Available snap-ins** list, select **Certificates**.



5. Click **Add**.

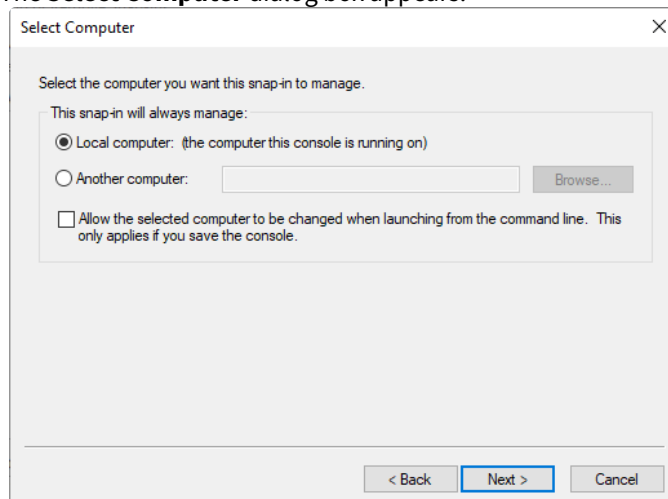
The **Certificates snap-in** dialog box appears.



6. Select **Service account**.

7. Click **Next**.

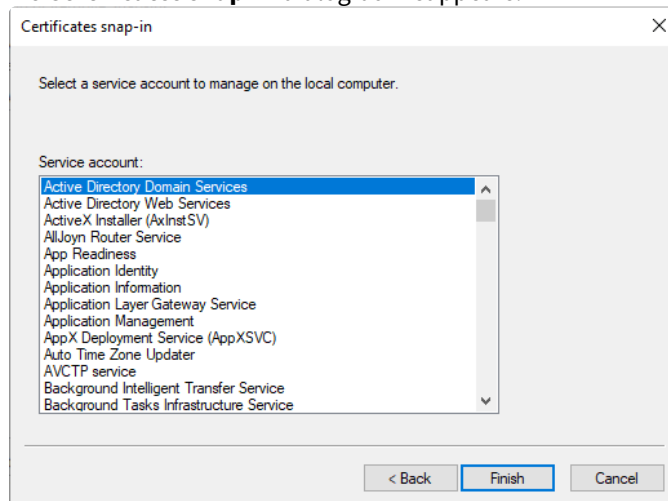
The **Select Computer** dialog box appears.



8. Select **Local computer**.

9. Click **Next**.

The **Certificates snap-in** dialog box reappears.



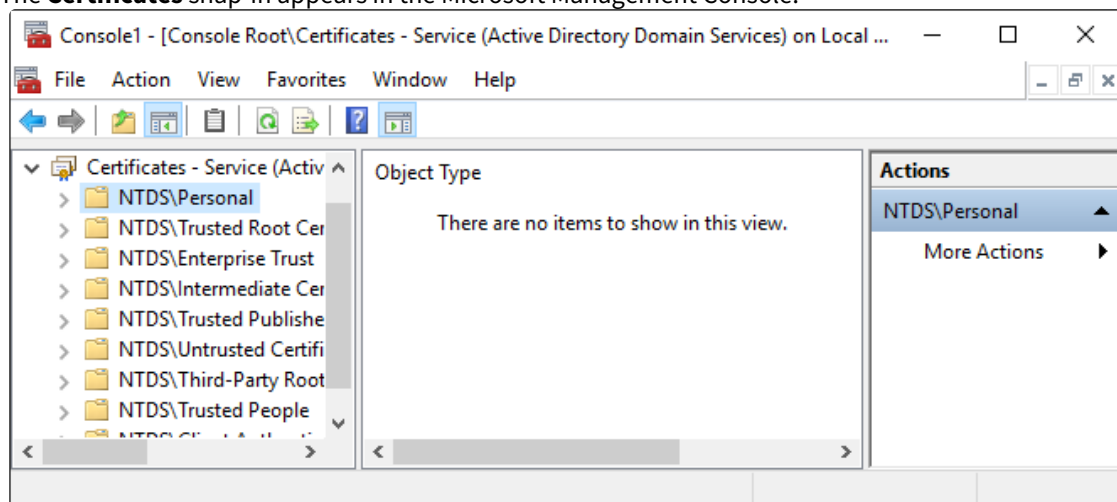
10. Select **Active Directory Domain Services**.

11. Click **Finish**.

The **Certificates** snap-in is added to the list of Selected snap-ins.

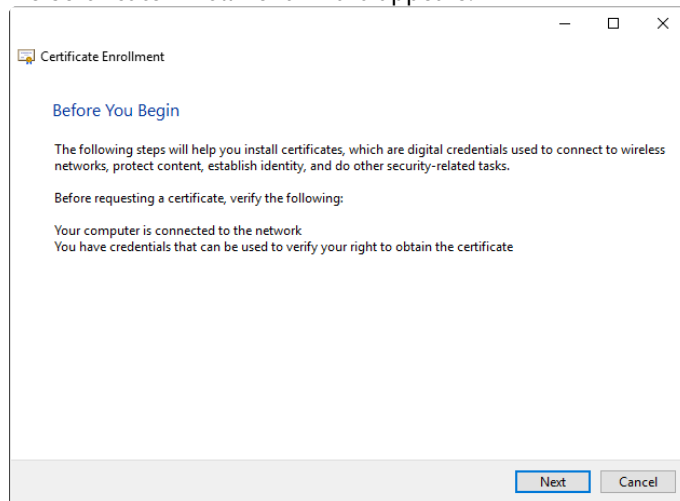
12. Click **OK**.

The **Certificates** snap-in appears in the Microsoft Management Console.

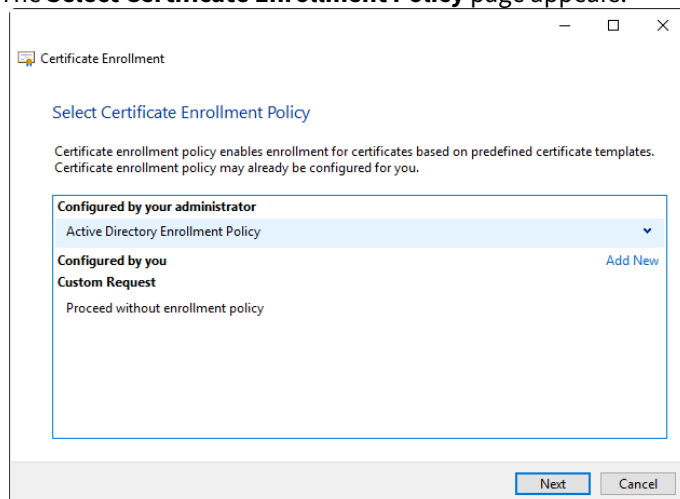


13. In the tree view, select **Certificates > NTDS\Personal**.

14. Select **Action > All Tasks > Advanced Operations > Create Custom Request**.  
The Certificate Enrollment wizard appears.



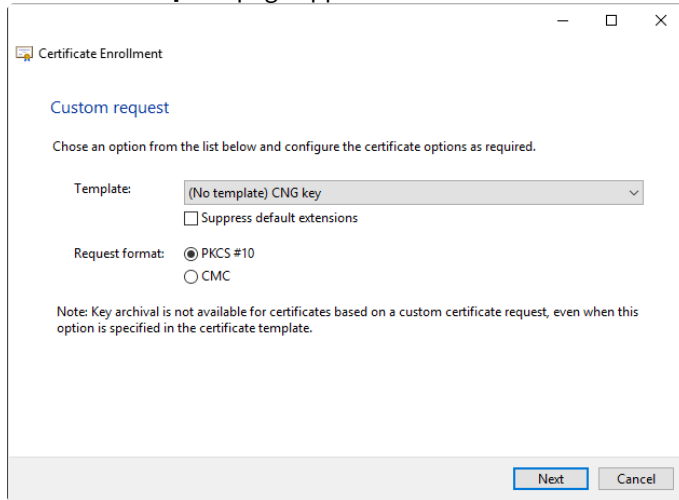
15. Click **Next**.  
The **Select Certificate Enrollment Policy** page appears.



16. Under **Configured by your administrator**, select **Active Directory Enrollment Policy**.

17. Click **Next**.

The **Custom request** page appears.



Certificate Enrollment

Custom request

Chose an option from the list below and configure the certificate options as required.

Template: (No template) CNG key

☐ Suppress default extensions

Request format: ☒ PKCS #10  
☐ CMC

Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template.

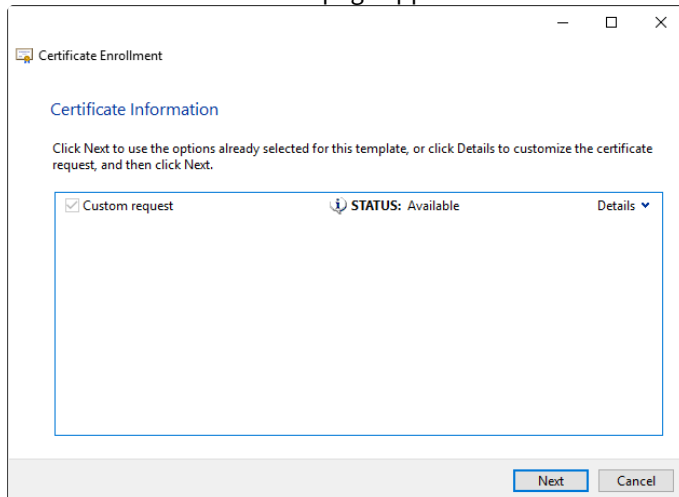
Next Cancel

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.



Certificate Enrollment

Certificate Information

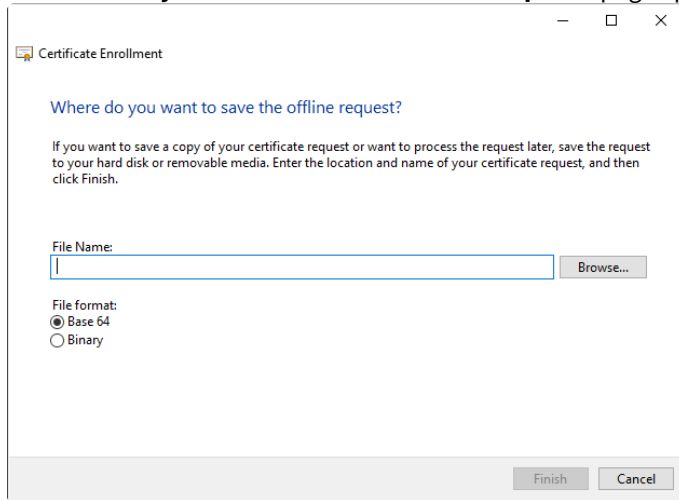
Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

|                                                    |                   |           |
|----------------------------------------------------|-------------------|-----------|
| <input checked="" type="checkbox"/> Custom request | STATUS: Available | Details ▾ |
|----------------------------------------------------|-------------------|-----------|

Next Cancel

21. Click **Next**.

The **Where do you want to save the offline request?** page appears.



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**.

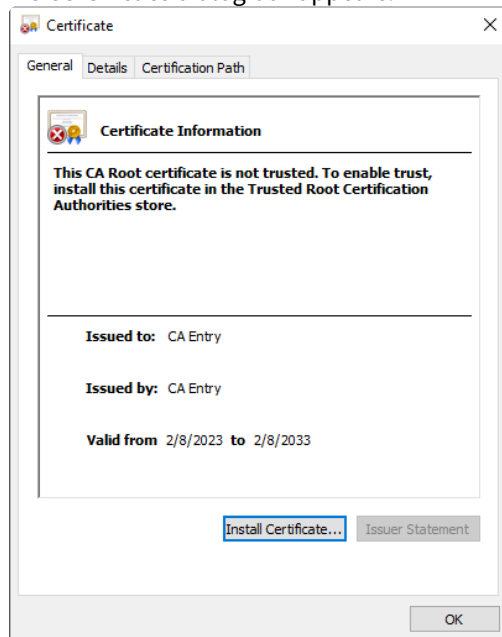
#### Installing the CA certificate chain for the Active Directory certificate

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.

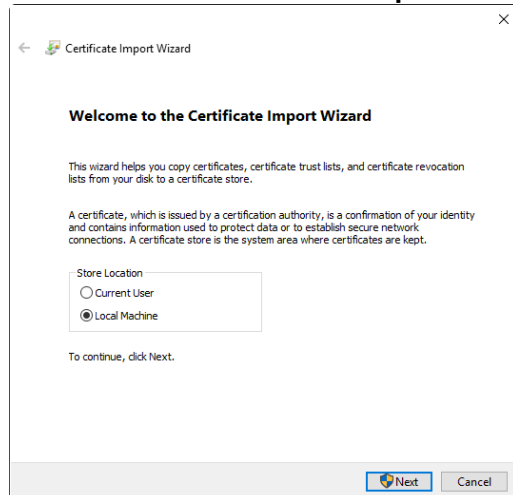
#### To install a CA certificate into Active Directory

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.

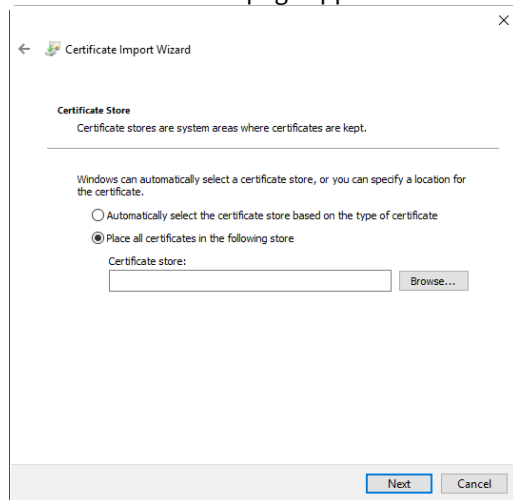


4. Click **Install Certificate**.  
The Certificate Import Wizard appears.
5. The **Welcome to the Certificate Import Wizard** page appears.



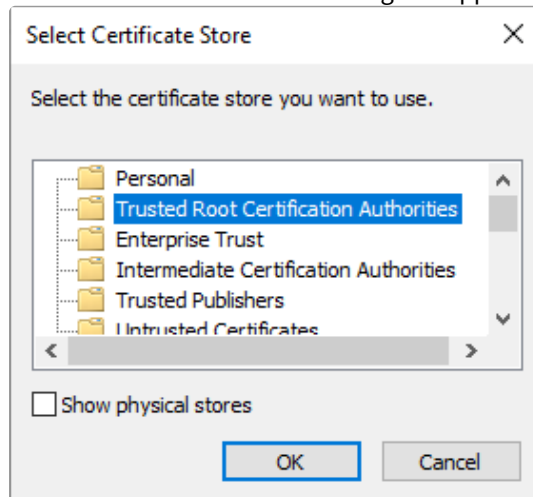
- a. For **Store Location**, select **Local Machine**.
- b. Click **Next**.

6. The **Certificate Store** page appears.



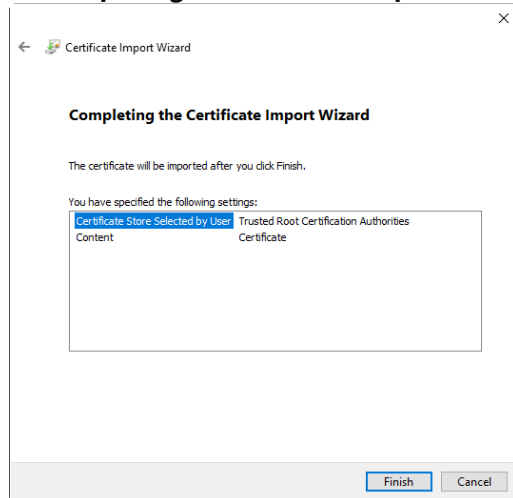
- a. Select **Place all certificates in the following store.**
- b. Click **Browse.**

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**.

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

- Log in the Entrust Certificate Services interface.
- Select **Create > PKIaaS**.  
The Select **Certificate Authority** pane appears.
- From the **Certificate Authority** drop-down list, select the CA you want to issue the TLS certificate.
- 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.
- Click **Next**.  
The **Certificate Details** pane appears.
- 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`.
- For **Certificate Expiry**, provide an expiry date for TLS certificate. It is recommended that the TLS certificate be valid for 1 year or less.
- 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:
  - For **SAN type**, select **DNS Name**.
  - In the **Value** field, enter a DNS name that may be used by the domain controller.
  - 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
  - To remove a component from the Subject Alternative Name extension, click **Remove** next to the extension that you want to remove.
- Copy the contents of the CSR you generated earlier, and paste the contents into the **Certificate Signing Request (CSR)** text box.
- Click **Submit**.  
If the certificate is generated successfully, a success message appears.
- Click **Download the newly created certificate** to download the TLS certificate.



After processing the CSR, proceed to [Installing the Active Directory server certificate](#).

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.

✖ The server certificate for Active Directory LDAPS communications must include a valid HTTP CRL Distribution Point.

- [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](#).

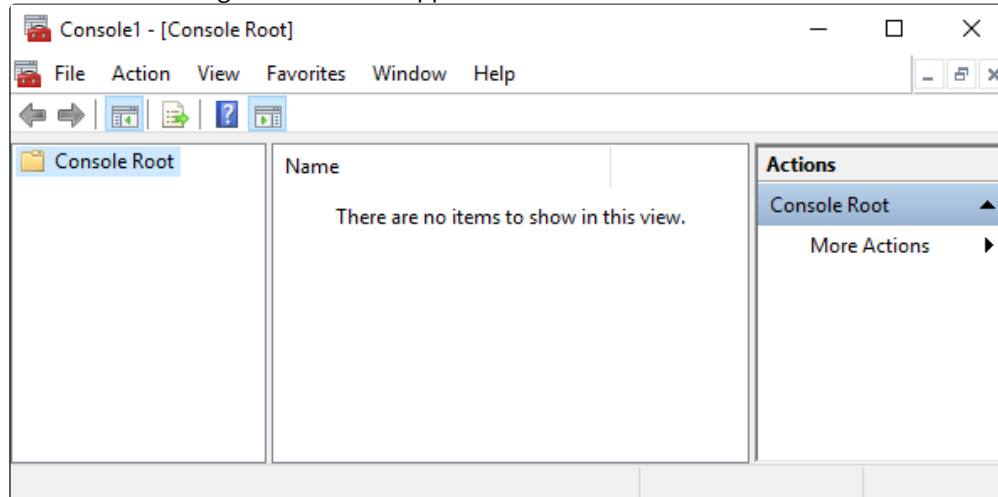
#### Installing the Active Directory server certificate

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

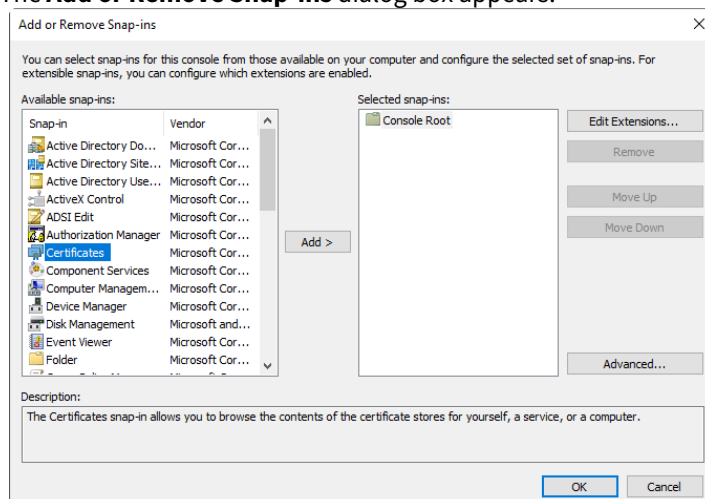
1. Log into Active Directory as a member of the Domain Admins group.
2. Run `mmc.exe` (Select **Start > Windows System > Run**, then enter `mmc.exe`).

The Microsoft Management Console appears.



3. Select **File > Add/Remove Snap-in**.

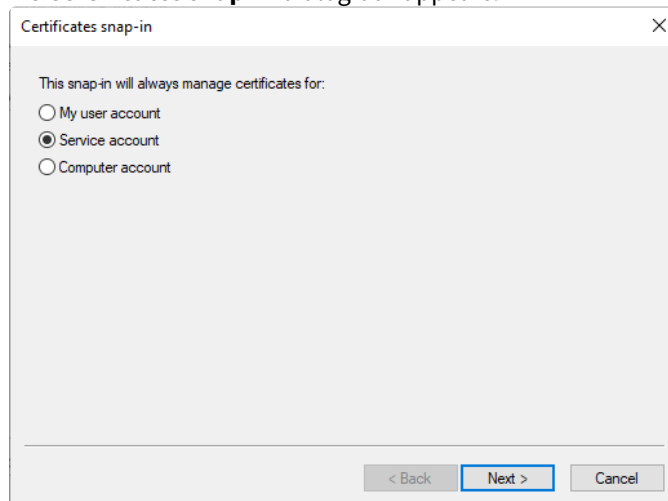
The **Add or Remove Snap-ins** dialog box appears.



4. In the **Available snap-ins** list, select **Certificates**.

5. Click **Add**.

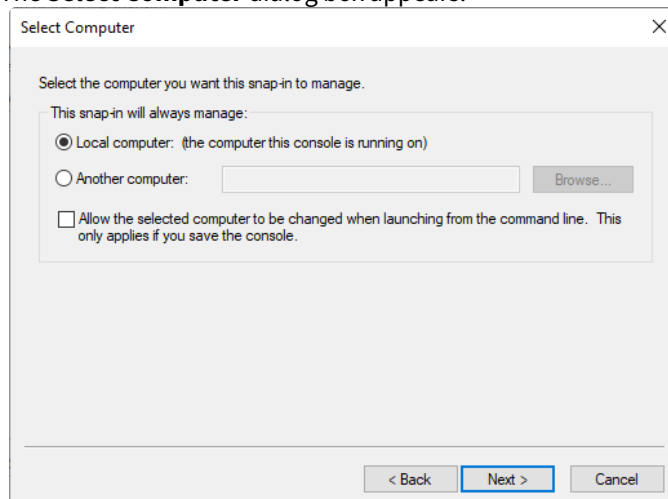
The **Certificates snap-in** dialog box appears.



6. Select **Service account**.

7. Click **Next**.

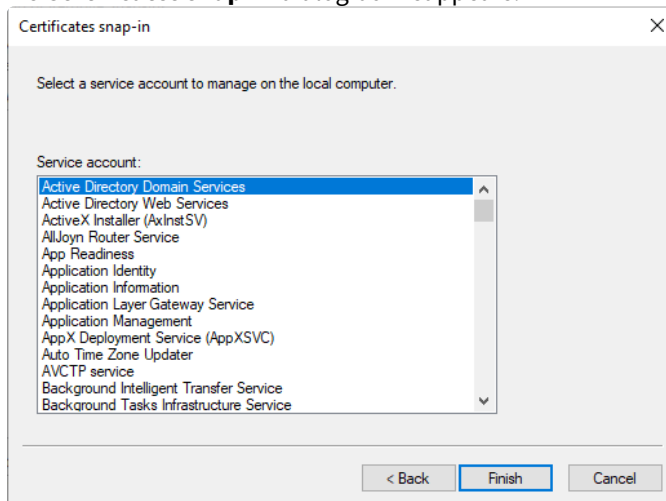
The **Select Computer** dialog box appears.



8. Select **Local computer**.

9. Click **Next**.

The **Certificates snap-in** dialog box reappears.



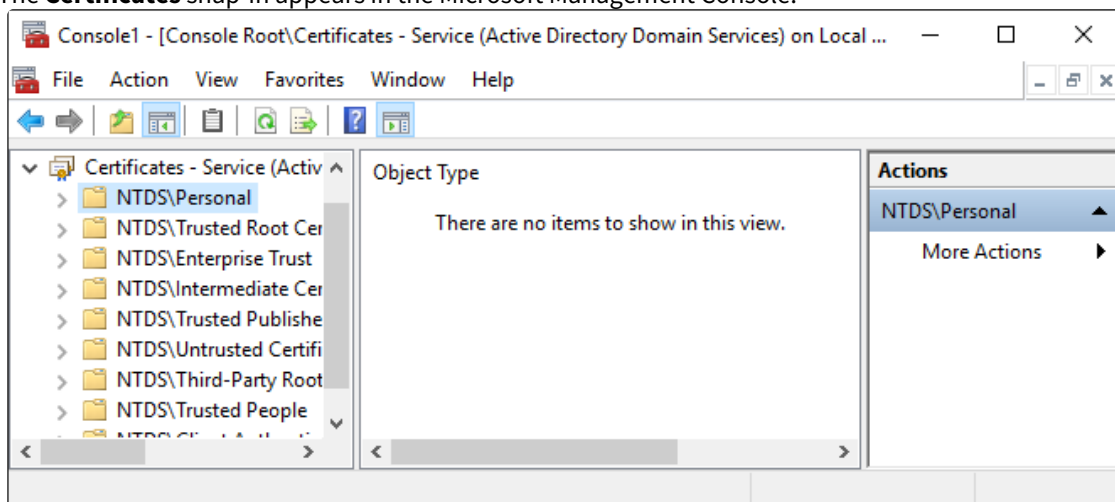
10. Select **Active Directory Domain Services**.

11. Click **Finish**.

The **Certificates** snap-in is added to the list of Selected snap-ins.

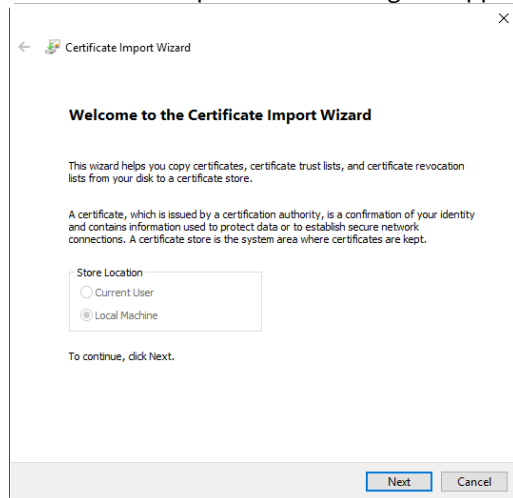
12. Click **OK**.

The **Certificates** snap-in appears in the Microsoft Management Console.

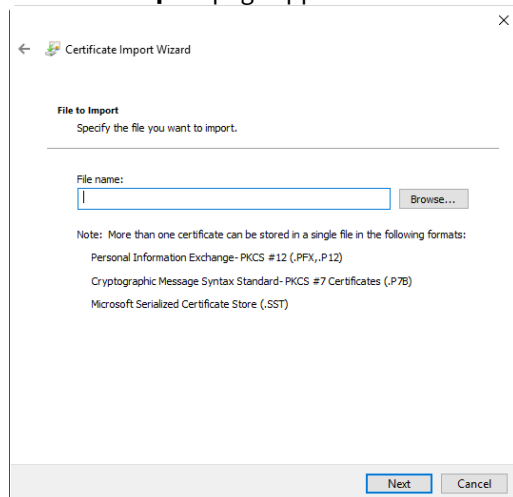


13. In the tree view, select **Certificates > NTDS\Personal**.

14. Select **Action > All Tasks > Import**.  
The Certificate Import Wizard dialog box appears.



15. Click **Next**.  
The **File to Import** page appears.

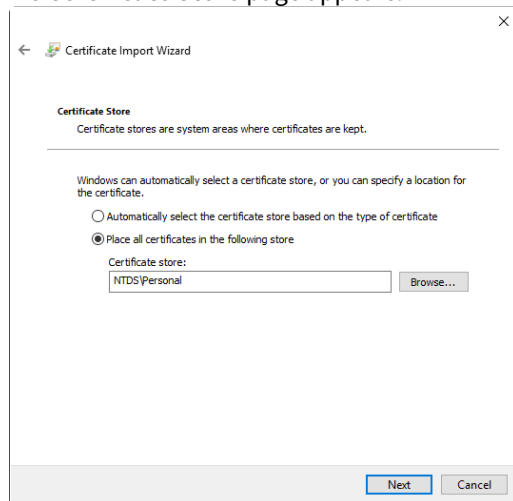


16. Click **Browse** and then select the Active Directory server certificate.



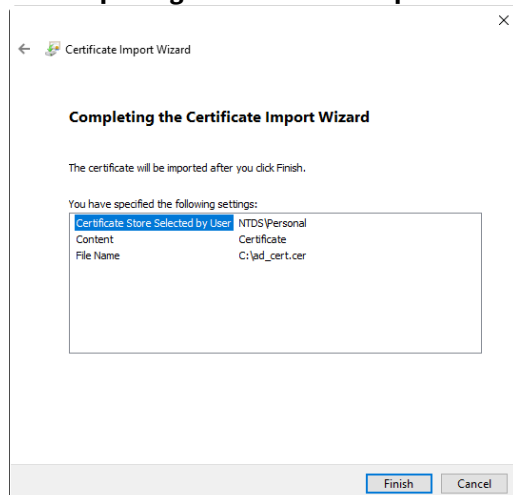
17. Click **Next**.

The **Certificate Store** page appears.



18. The NTDS\Personal certificate store is already selected. Click **Next**.

The **Completing the Certificate Import Wizard** page appears.



19. Click **Finish**.

## 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**.

Generating a file containing the CA certificate chain for the Active Directory server certificate

Certificate Enrollment Gateway requires the CA certificate chain of Active Directory's server certificate. When connecting to Active Directory, Certificate Enrollment Gateway will use the CA certificate chain to validate Active Directory's server certificate.

The CA certificate chain must be stored in one of the following files:

| File                               | Description                                                                                                                                                                                                         |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LDAPS Truststore                   | This file must be a PKCS #12 (P12) file. The file must contain at least one Trusted CA Certificate entry (TrustedCertEntry).<br><br>You can re-use the CA Gateway Keystore if it contains the CA certificate chain. |
| LDAPS Trusted 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.                |

#### To generate an LDAPS Truststore (P12 file) using the Java keytool utility

1. Obtain the CA certificate chain for Active Directory's server certificates, from the issuing CA 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 LDAPS Trust Store file and import CA certificates into the trust store:

```
keytool -import -alias <alias> -trustcacerts -file <cert-file> -keystore
<truststore>
```

Where:

- `<alias>` is an alias for the CA certificate. Use a different alias for each CA certificate you will import.
- `<cert-file>` is the path and file name of the CA certificate.
- `<truststore>` is the path and file name of the LDAPS Truststore. For example, `ldapstruststore.p12`. The utility will create the file if it does not exist.

4. For example:

```
keytool -import -alias cagw-root -trustcacerts -file /tmp/root.cer -keystore /
home/user/ldapstruststore.p12
```

5. When prompted, enter a password for the truststore.

#### To generate an LDAPS Trusted CA Certificates File (PEM file)

1. Log in to the server hosting Entrust Deployment Manager as the user account that owns Entrust Deployment Manager.
2. Obtain the certificate chain for Active Directory's server certificates, from the issuing CA certificate to the root CA certificate.
3. Open a text editor.

4. Create a new file.
5. Paste the contents of each CA certificate file into the new file, from the issuing CA certificate to the root CA certificate. Each CA certificate must include any BEGIN CERTIFICATE and END CERTIFICATE lines if present. For example:

```
-----BEGIN CERTIFICATE-----
<Issuing CA certificate in Base64 encoding>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA certificate in Base64 encoding>
-----END CERTIFICATE-----
```

6. The text file should look similar to the following:

```
-----BEGIN CERTIFICATE-----
MIIDejCCAmKgAwIBAgIQ8e7ock59Y21Mtcy7rGJUDANBgkqhkiG9w0BAQs...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIQ0EgRW50cnkwHhcNMjMwMjA4MTUxNzEwWhcNMzMwMjA4MTU0NzEwWjAyM...
-----END CERTIFICATE-----
```

7. Save and close the file.

#### Configuring channel binding enforcement to Active Directory

When connecting with Active Directory over LDAPS, clients can provide channel binding information to the server. Active Directory can enforce channel binding for LDAPS connections. However, if Active Directory always requires channel binding information from clients, WSTEP enrollments with Certificate Enrollment Gateway can fail. Active Directory provides the registry setting **LdapEnforceChannelBinding** that controls whether channel binding information is required from clients. For more information about this registry setting, see the Microsoft documentation.

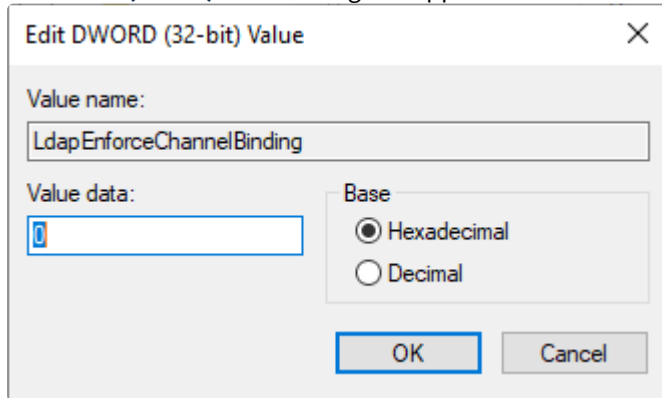
#### To configure channel binding enforcement to Active Directory

1. Log into Active Directory as a member of the Domain Admins group.
2. Open the Windows registry:
  - a. Select **Start > Windows System > Run**,  
The **Run** dialog box appears.
  - b. Enter `regedit`.
  - c. Click **OK**.
3. In the tree view, navigate to the following location:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters
```

4. Add the registry setting **LdapEnforceChannelBinding** if it does not exist:
  - a. Select **Edit > New > DWORD (32-bit) Value**.
  - b. Enter `LdapEnforceChannelBinding`.

5. Select **LdapEnforceChannelBinding**, and then select **Edit > Modify**. An **DWORD (32-bit) Value** dialog box appears.



6. In the **Value data** field, enter one of the following values:
  - 0 to disable channel binding validation, if supported. Clients that support channel binding tokens must provide channel binding information to the server.
  - (Recommended.) 1 to enable channel binding when supported.
  - 2 to always enable channel binding validation. All clients must provide channel binding information. Active Directory will reject requests from clients that do not provide channel binding information.
7. Click **OK**.

## Configuring Certificate Enrollment Gateway for WSTEP enrollment

To configure Certificate Enrollment Gateway for WSTEP enrollment, you must configure the WSTEP enrollment settings in Certificate Enrollment Gateway. You can edit the WSTEP enrollment settings using the Management Console interface.

### To configure Certificate Enrollment Gateway for EST 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. Configure the settings under the **WSTEP** tab.
8. Configure any other settings if required.
9. After configuring the settings, click **Validate** to validate the settings.
10. If any configuration errors are detected, correct the errors then click **Validate** again.
11. After validating the configuration settings, click **Next**.

12. Cryptographic Security Platform uploads the configuration and any attached files, such as P12 credentials.
13. 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.

## 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 a server for the Certificate Enrollment Policy Web Service](#)
- [Installing Microsoft Internet Information Services](#)

### 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:

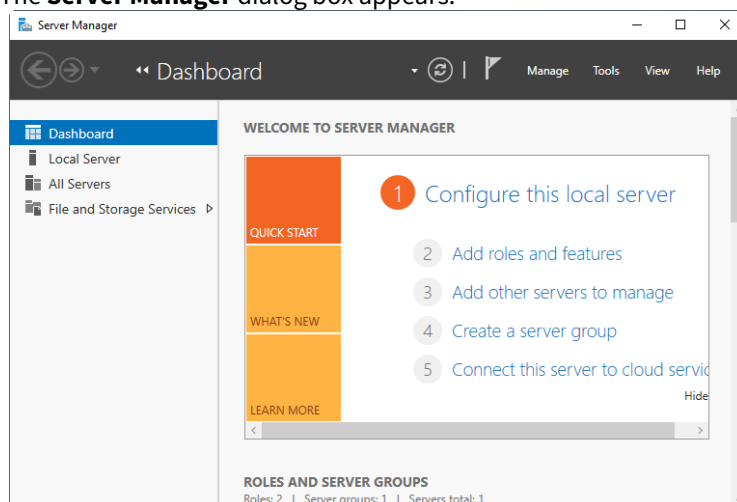
- Windows Server 2016 or later
- Minimum 4 GB of RAM
- Minimum 2 CPU
- Minimum 40 GB free hard disk space

### Installing Microsoft Internet Information Services

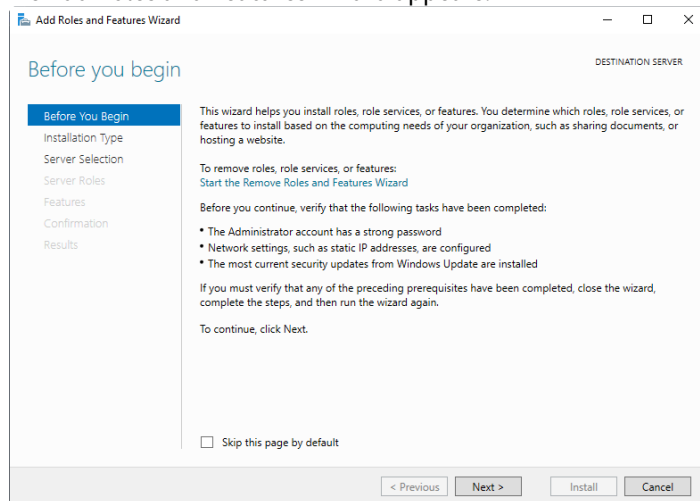
Microsoft Internet Information Services (IIS) is a Web server. The Certificate Enrollment Policy Web Service will be installed as an application in Microsoft IIS. The following procedure describes how to install Microsoft IIS.

#### To install Microsoft Internet Information Services

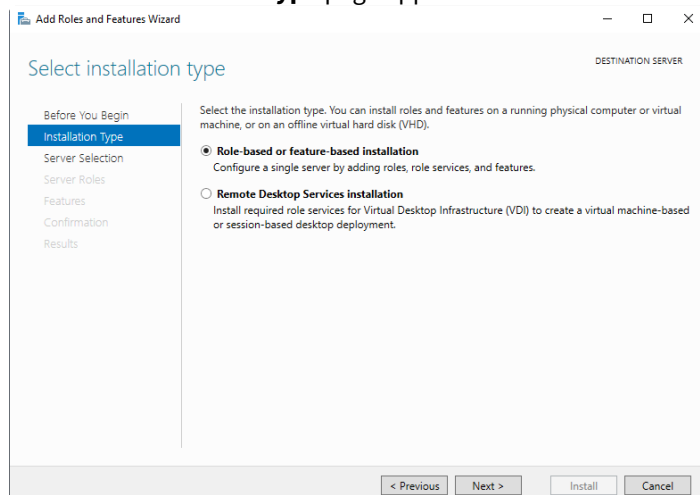
1. Log in to the server that will host the Certificate Enrollment Policy Web Service.
2. Open Server Manager. Select **Start > Server Manager**.  
The **Server Manager** dialog box appears.



3. In the top navigation bar, select **Manage > Add Roles and Features**. The Add Roles and Features Wizard appears.



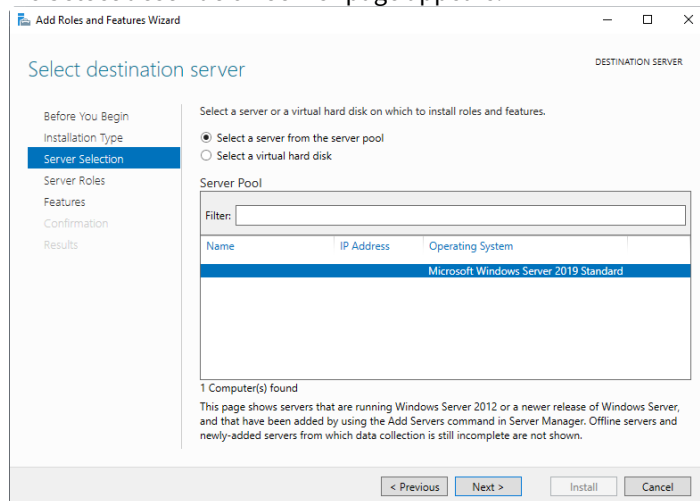
4. Click **Next**. The **Select installation type** page appears.



5. Click **Role-based or feature-based installation**. By default, this option is already selected.

6. Click **Next**.

The **Select destination server** page appears.

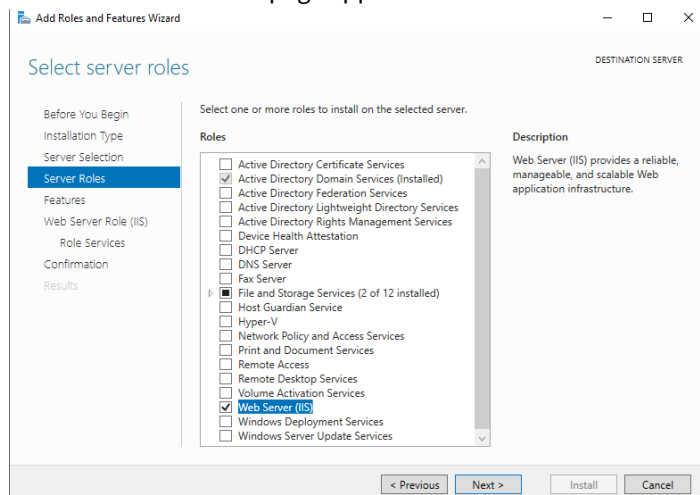


7. Click **Select a server from the server pool**. By default, this option should already be selected.

8. In the **Server Pool** list, select your server. By default, the server should already be selected.

9. Click **Next**.

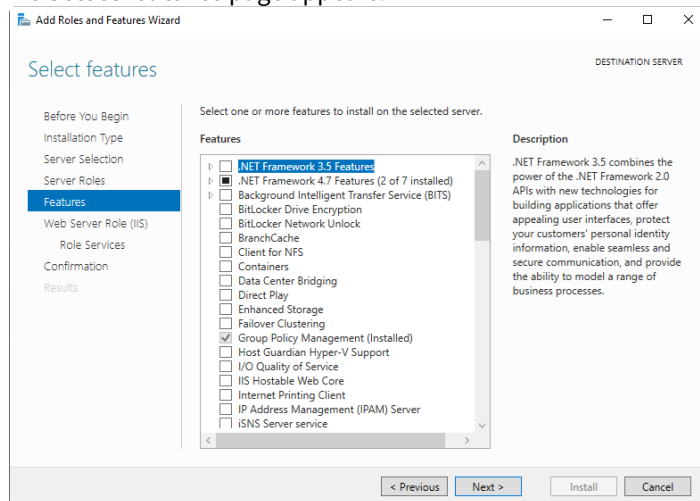
The **Select server roles** page appears.



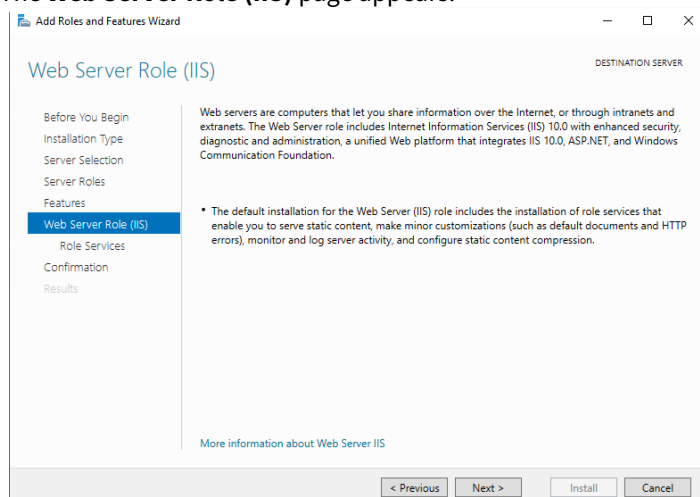
10. Select **Web Server (IIS)**.

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.



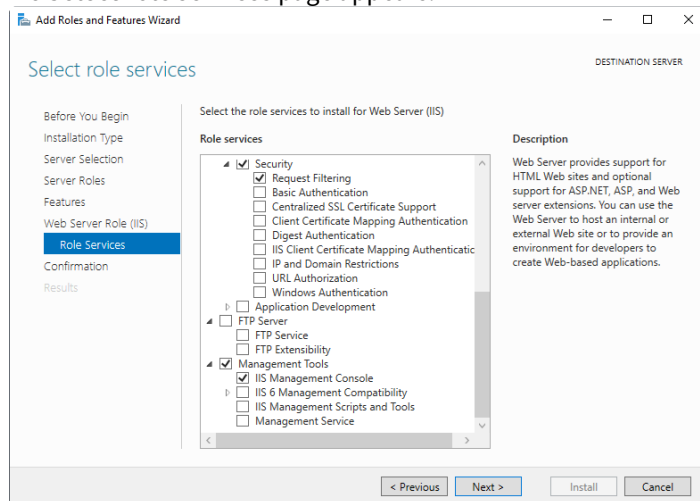
13. You do not need to add any features on this page. Click **Next**.  
The **Web Server Role (IIS)** page appears.





14. Click **Next**.

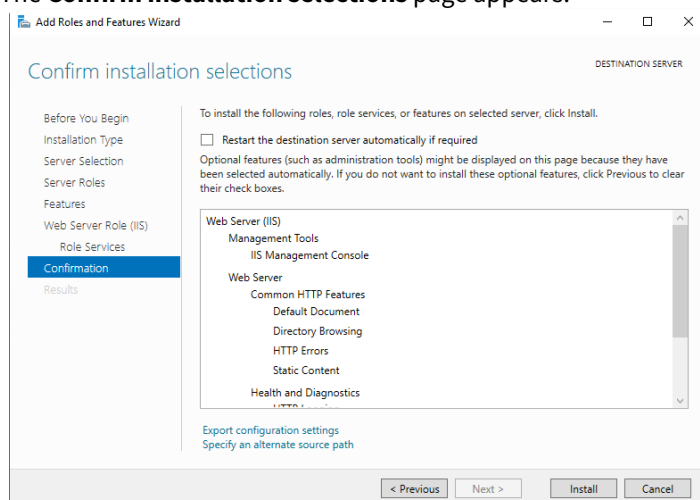
The **Select role services** page appears.



15. Under **Management Tools**, verify that **IIS Management Console** is selected.

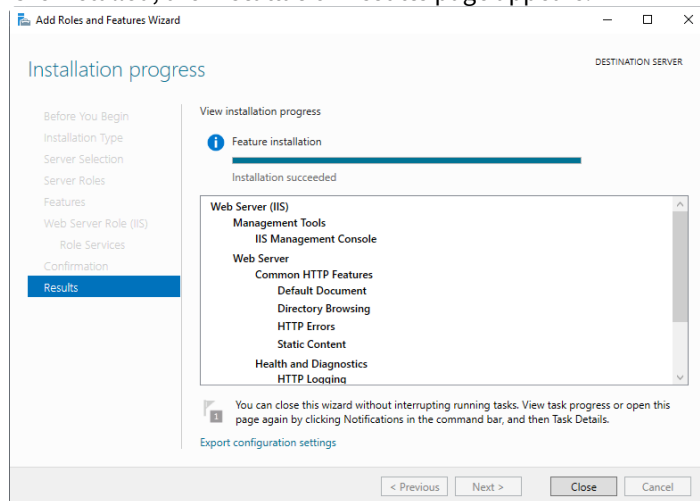
16. Click **Next**.

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**.

## 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.

- [Creating a CSR for the Web server certificate](#)
- [Issuing the Web server certificate with an on-premises CA](#)
- [Issuing the Web server certificate with Entrust PKI as a Service](#)
- [Installing the Web server certificate into Microsoft IIS](#)
- [Updating Microsoft IIS to use the Web server certificate](#)
- [Installing the CA certificate chain for the Web server certificate](#)

### Creating a CSR for the Web server certificate

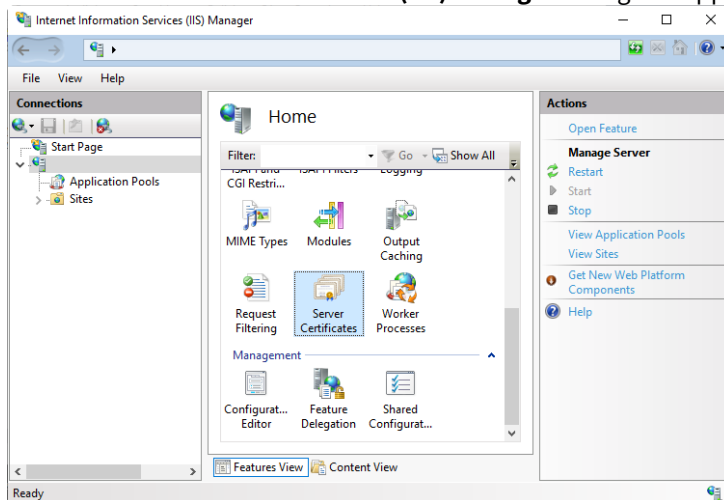
The Certificate Enrollment Policy Web Service is installed as an application in Microsoft Internet Information Services (IIS). Microsoft IIS requires a TLS certificate so that the Certificate Enrollment Policy Web Service can accept WSTEP enrollment requests over HTTPS.

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.

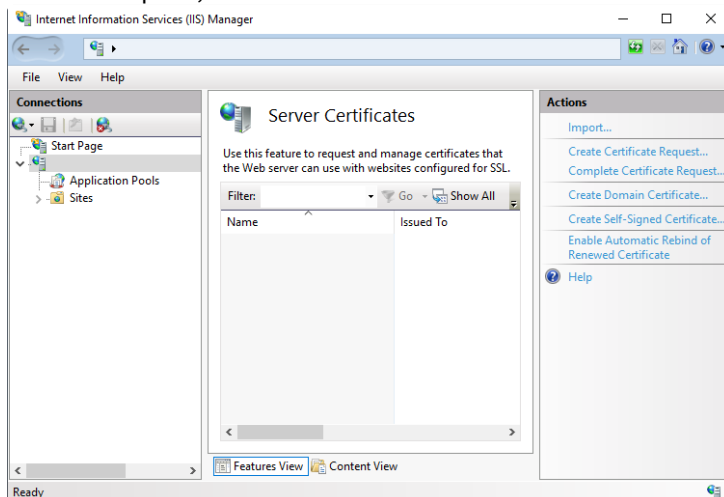
### To create a CSR for Microsoft IIS

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.

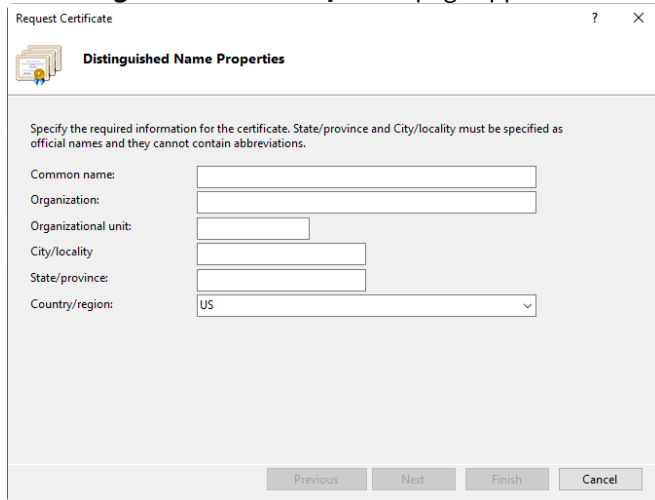


2. Under **Connections**, select the host name of the server.
3. In the **Home** pane, double-click **Server Certificates**.



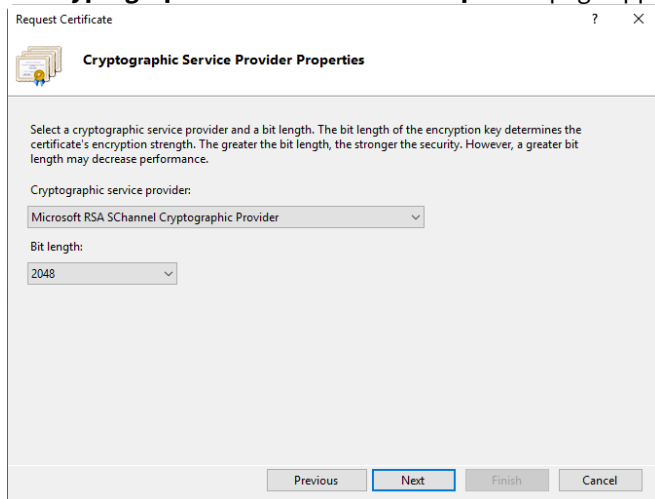
4. In the **Actions** pane, click **Create Certificate Request**.  
The **Request Certificate** wizard appears.

5. The **Distinguished Name Properties** page appears.



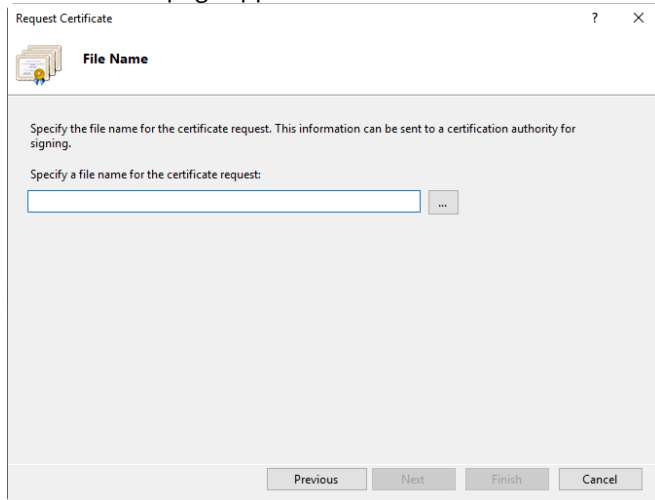
- In the provided fields, enter information that will be included in the CSR. Note that the issuing CA (either a CA in Entrust PKI as a Service, or an on-premises Entrust CA) will ignore this information.
- Click **Next**.

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.

#### 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](#)



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 from Entrust 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](#).

#### 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](#).

#### Installing the Web server certificate into Microsoft IIS

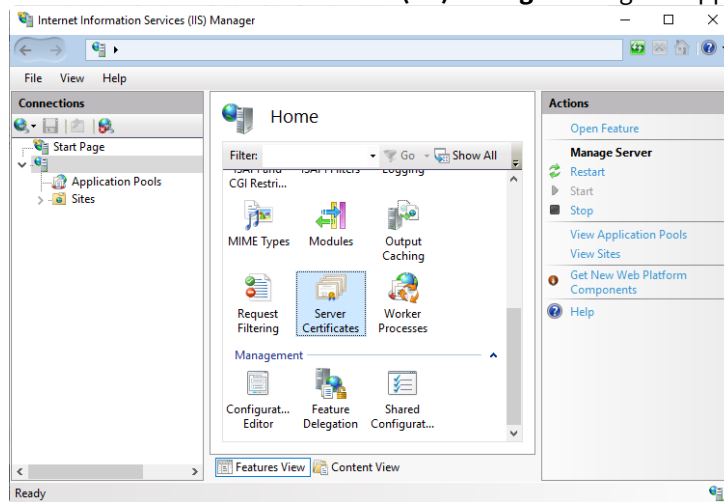
After obtaining the Web server certificate, you must install the certificate into Microsoft IIS. After processing the CSR with Entrust PKI as a Service or an on-premises CA, complete the certificate request in Microsoft IIS to install the certificate.

- 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.

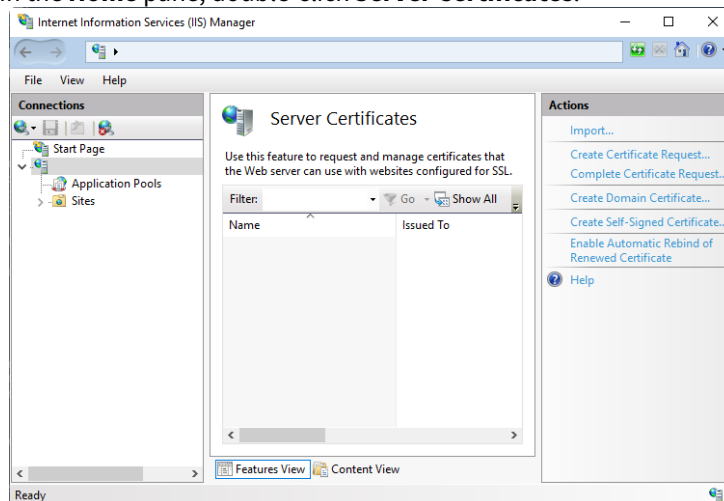
### To complete a certificate request in Microsoft IIS

1. Open the Internet Information Services (IIS) Manager. Select **Start > Windows Administrative Applications > Internet Information Services (IIS) Manager**.

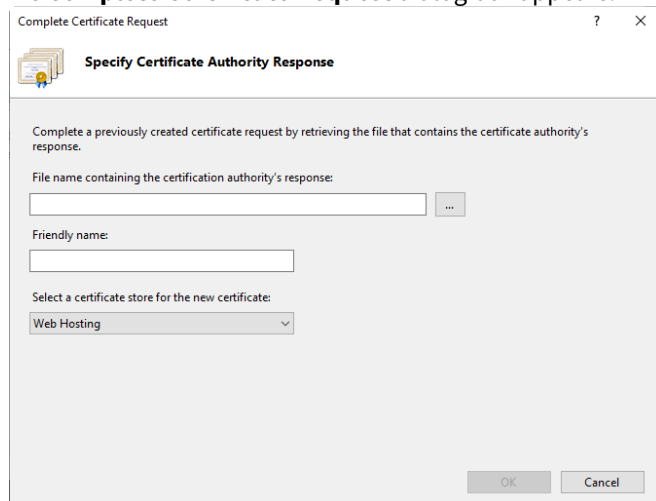
The **Internet Information Services (IIS) Manager** dialog box appears.



2. Under **Connections**, select the host name of the server.
3. In the **Home** pane, double-click **Server Certificates**.



- In the **Actions** pane, click **Complete Certificate Request**. The **Complete Certificate Request** dialog box appears.



- 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.
- 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.
- From the **Select a certificate store for the new certificate** drop-down list, select **Web Hosting**.
- Click **OK**.  
In the **Server Certificates** pane, the certificate appears in the list of server certificates. The certificate is listed by its friendly name.

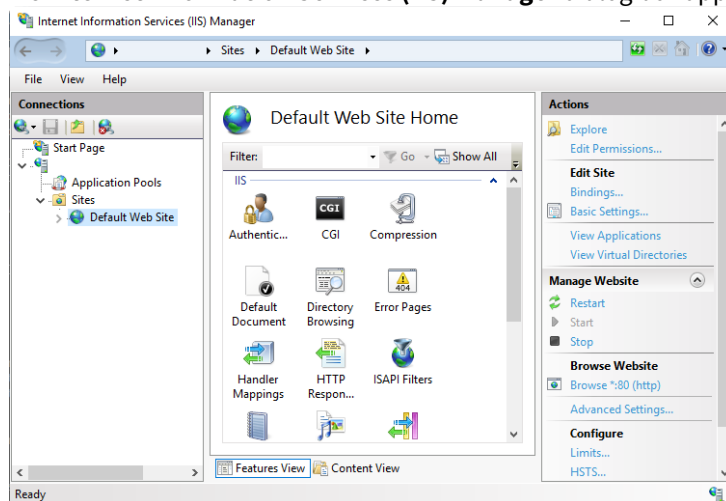
Updating Microsoft IIS to use the Web server certificate

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.

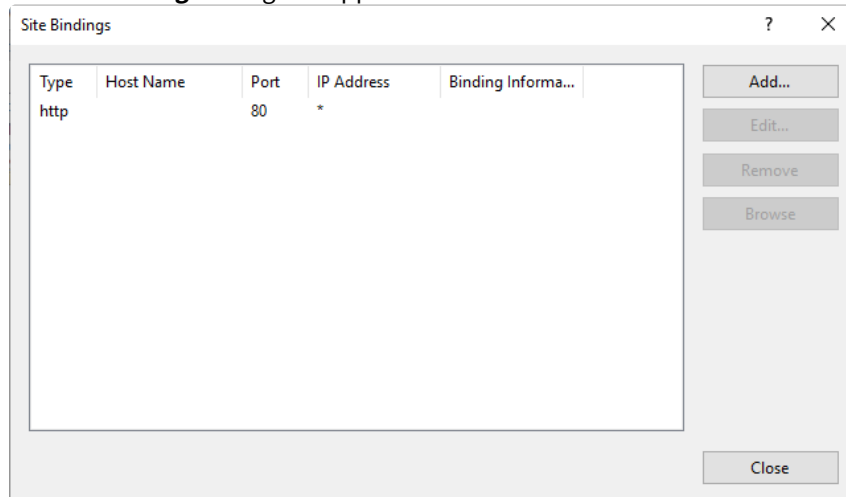
#### To add an initial HTTPS site binding in Microsoft IIS to use the Web server certificate

- Open IIS Manager. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.

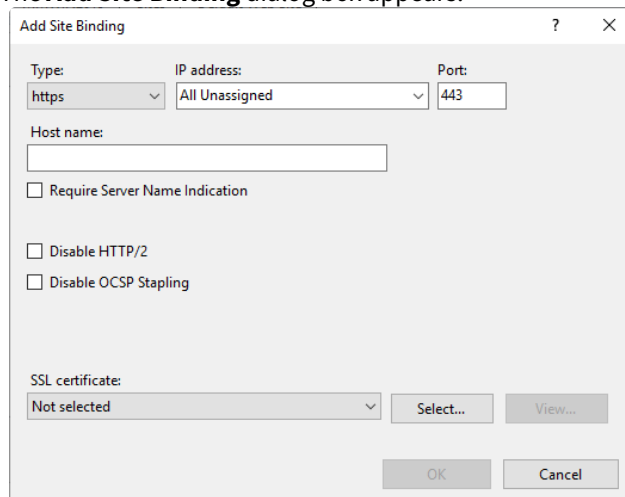
The **Internet Information Services (IIS) Manager** dialog box appears.



2. 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.
3. In the **Actions** pane, click **Bindings**.  
The **Site Bindings** dialog box appears.



4. Click **Add**.  
The **Add Site Binding** dialog box appears.

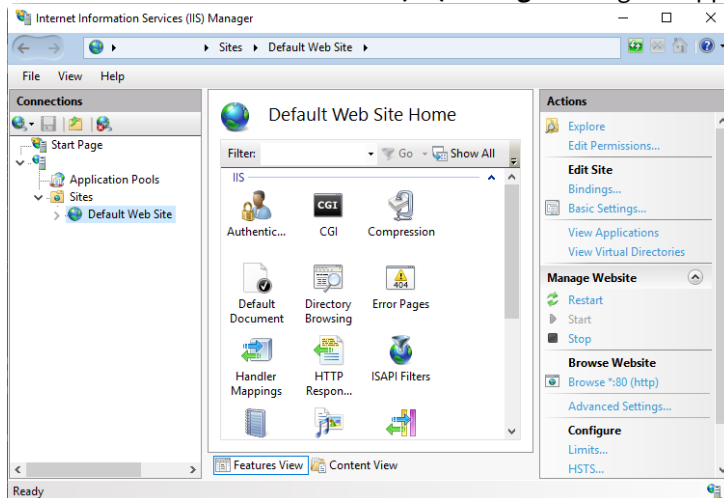


5. In the **Type** drop-down list, select **https**.
6. Keep **IP address** as **All Unassigned**.
7. For **Port**, keep the default 443.
8. From the **SSL certificate** drop-down list, select the Web server certificate you installed into Microsoft IIS earlier.
9. Click **OK**.  
The HTTPS binding is added to the list of site bindings.

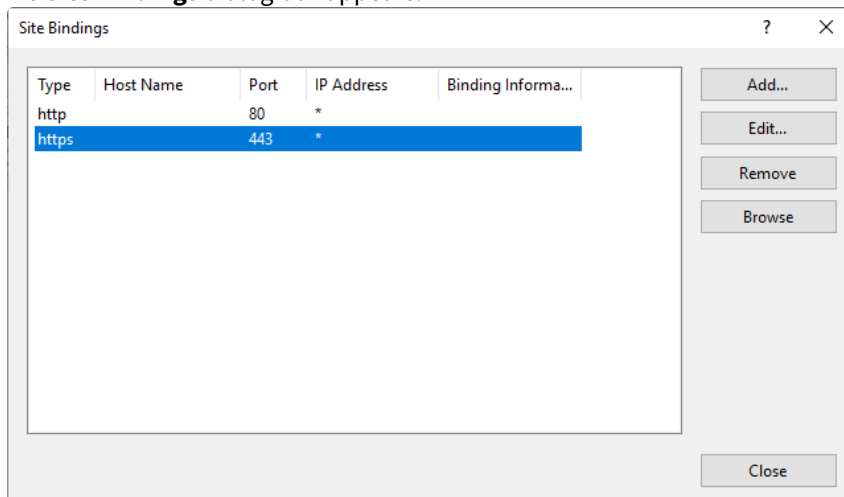
#### To update an existing HTTPS site binding in Microsoft IIS to use the Web server certificate

1. Open IIS Manager. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** dialog box appears.



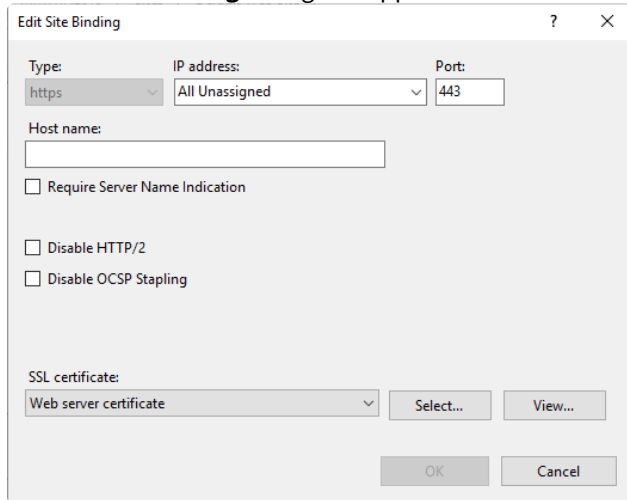
- In the **Connections** pane, select **Sites > Default Web Site**.  
If the Certificate Enrollment Policy Web Service is installed, it appears as an application under the default Web site.
- In the **Actions** pane, click **Bindings**.  
The **Site Bindings** dialog box appears.



- 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**.

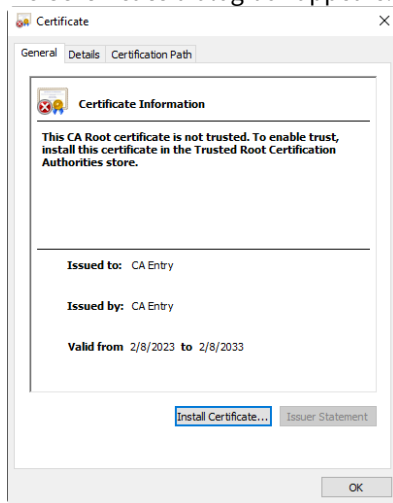
Installing the CA certificate chain for the Web server certificate

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.

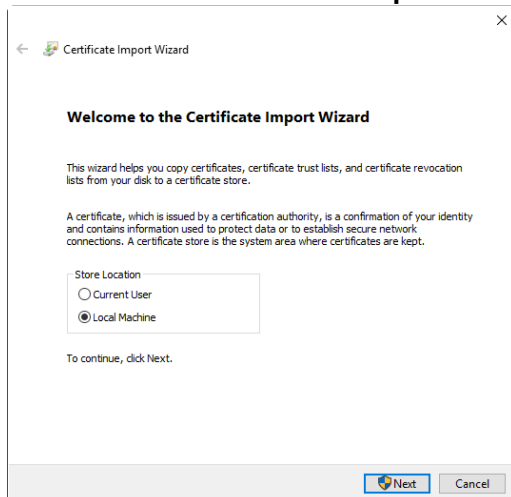
#### To install a CA certificate into the Web server

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.

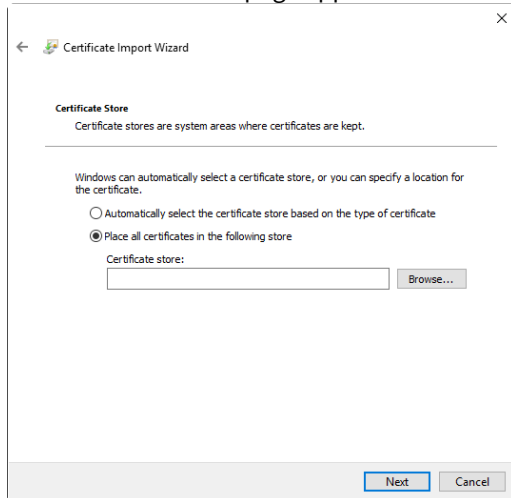


4. Click **Install Certificate**.  
The Certificate Import Wizard appears.
5. The **Welcome to the Certificate Import Wizard** page appears.



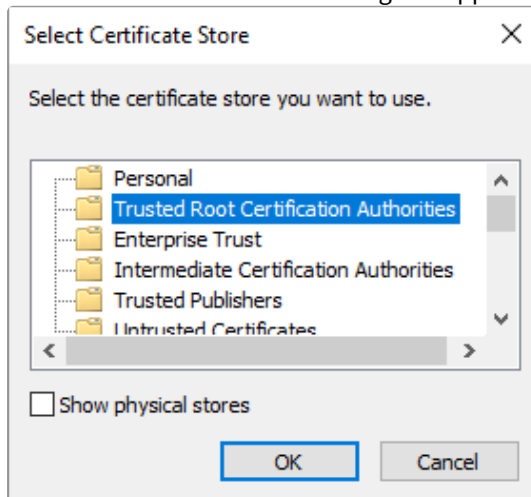
- a. For **Store Location**, select **Local Machine**.
- b. Click **Next**.

6. The **Certificate Store** page appears.



- a. Select **Place all certificates in the following store.**
- b. Click **Browse.**

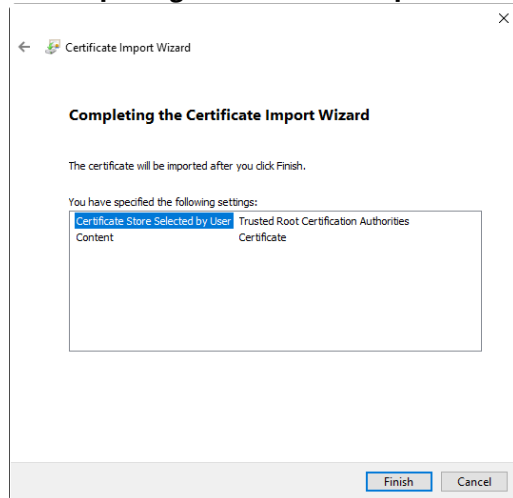
The **Select Certificate Store** dialog box appears.



- 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.**



7. The **Completing the Certificate Import Wizard** page appears.



8. Click **OK**.

## 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:

- a. 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
- b. 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=cepxusername.example.com
Issuer : CN=cepxusername.example.com
KeyUsage : DataEncipherment, KeyEncipherment
EKU List : Server Authentication (1.3.6.1.5.5.7.3.1)
DNS SAN : cepusername.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**.
- c. 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 cepusername.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 : cepusername.example.com
Serial Number : 6AFEE3C47A569F95A9C5622D679B42C1
Thumbprint : 2E6601A98E2ADBD4EBE5DF6D8C3A514CD7660BAD
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=cepusername.example.com
Issuer : CN=cepusername.example.com
KeyUsage : DataEncipherment, KeyEncipherment
EKU List : Server Authentication (1.3.6.1.5.5.7.3.1)
DNS SAN : cepusername.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"):

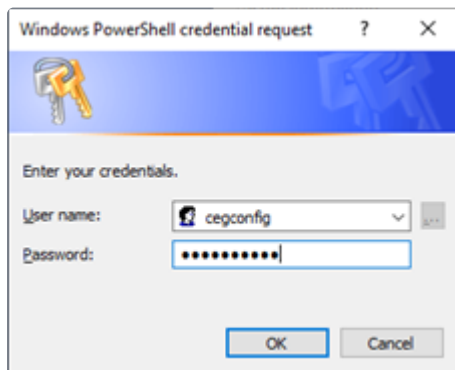
- To go back and select a different existing certificate, enter **S**.
- To go back and supply and different certificate, enter **N**.
- To continue with the selected certificate, enter **C**.

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.

- [Installing the CEP Web Service using the Windows graphical interface](#)
- [Selecting the authentication mode of the CEP Web Service using the Windows graphical interface](#)
- [Assigning a friendly name to the CEP Web Service using the Windows graphical interface](#)
- [Assigning a unique Enrollment Policy Identifier](#)

## Installing the CEP Web Service using the Windows graphical interface

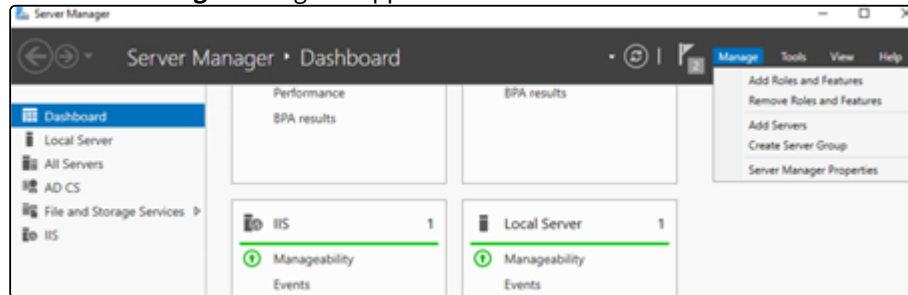
On a Windows server, install the Certificate Enrollment Policy Web Service.

- 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.

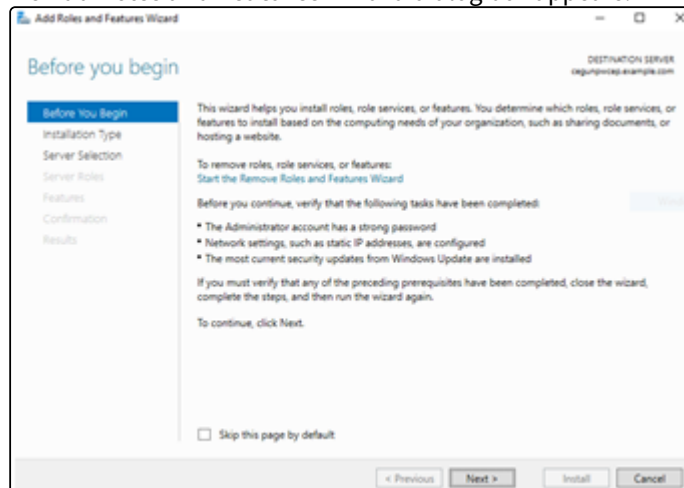
### To install the CEP Web Service using the Windows graphical interface

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.

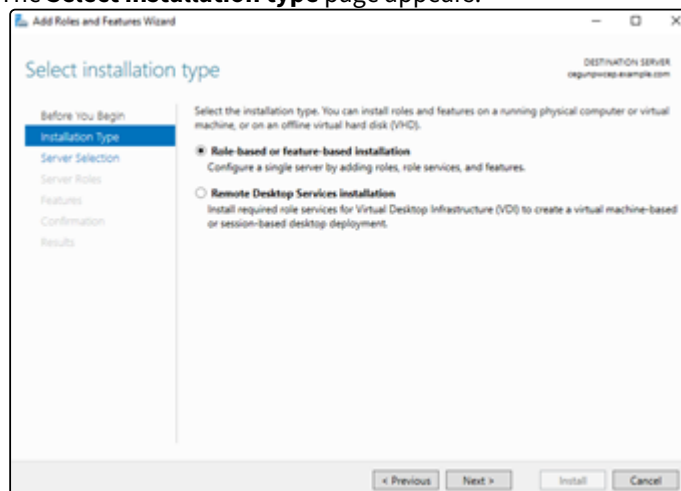


3. Select **Manage > Add Roles and Features**.
- The **Add Roles and Features Wizard** dialog box appears.



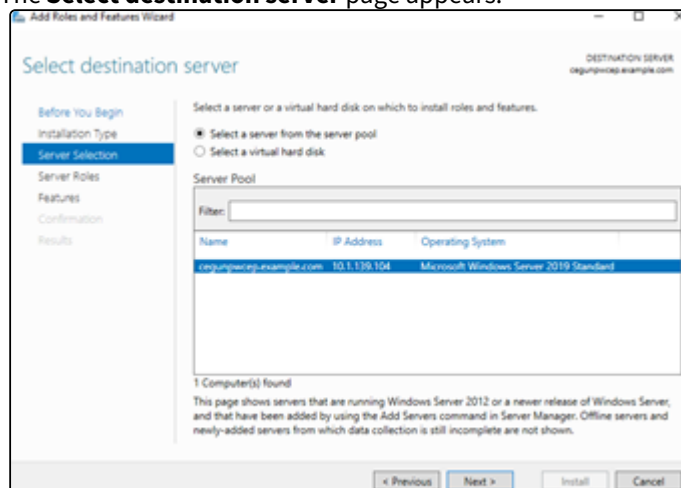


4. If the **Before you Begin** page appears, click **Next**.  
The **Select installation type** page appears.



5. Select **Role-based or feature-based installation**.
6. Click **Next**.

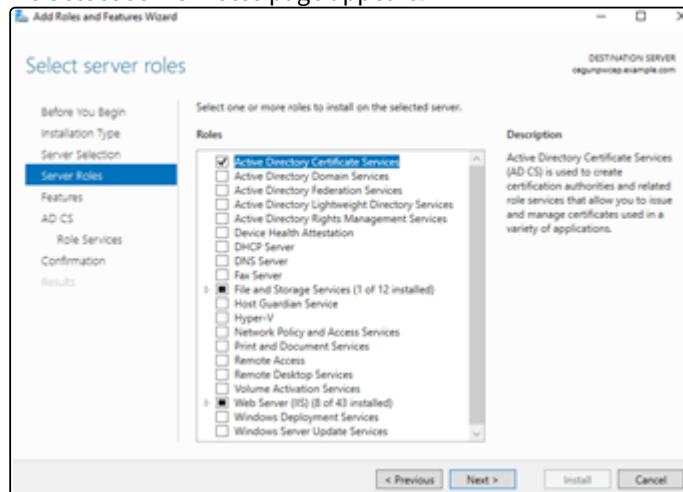
The **Select destination server** page appears.



7. Click **Select a server from the pool**.
8. In the **Server Pool** list, select the server.

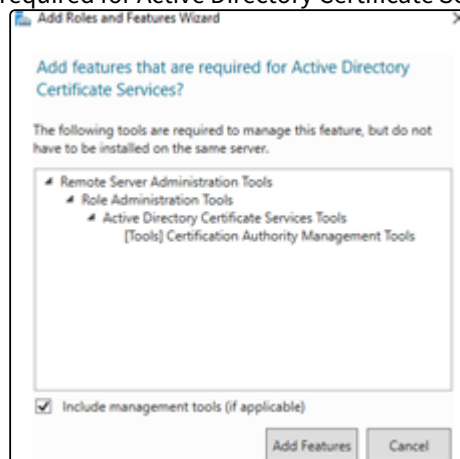
9. Click **Next**.

The **Select server roles** page appears.



10. Select **Active Directory Certificate Services**.

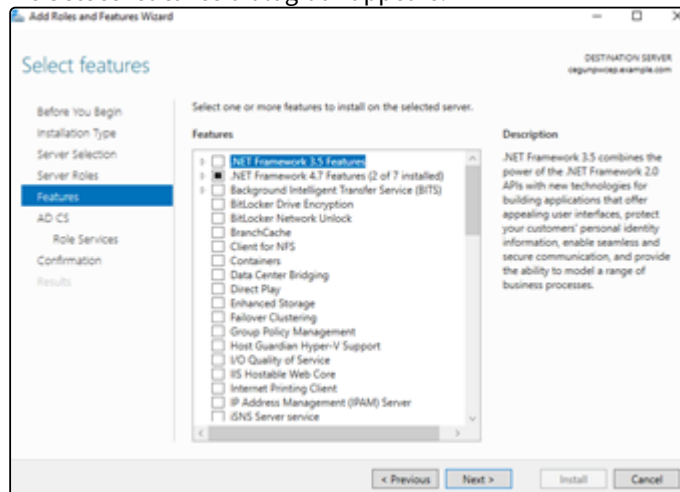
Another **Add Roles and Features Wizard** dialog box may appear, informing you that some features are required for Active Directory Certificate Services.



11. Click **Add Features** to add these required features and close the dialog box.

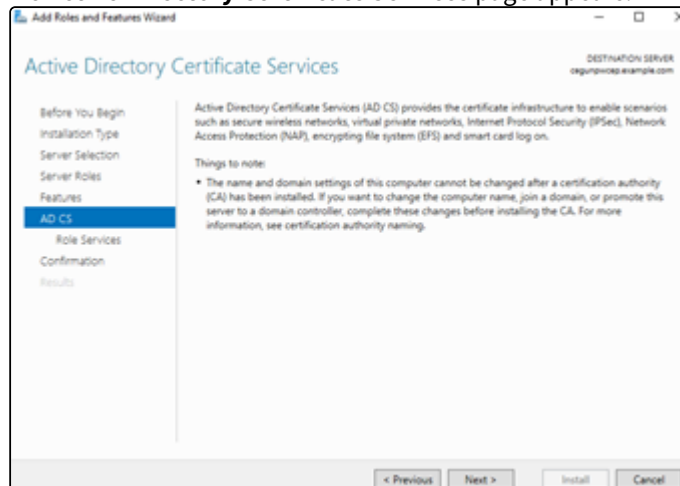
12. Click **Next**.

The **Select features** dialog box appears.



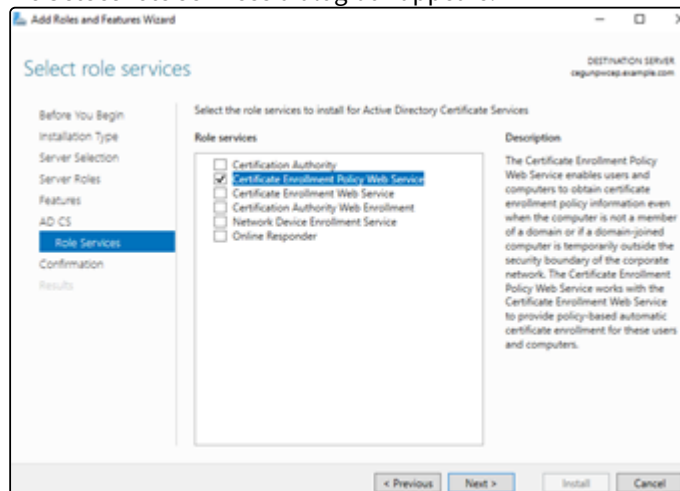
13. Click **Next**.

The **Active Directory Certificate Services** page appears.

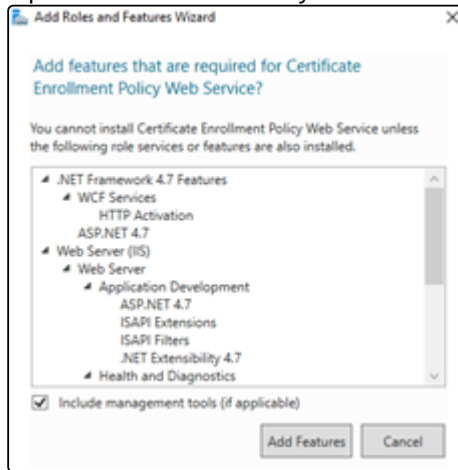


14. Click **Next**.

The **Select role services** dialog box appears.

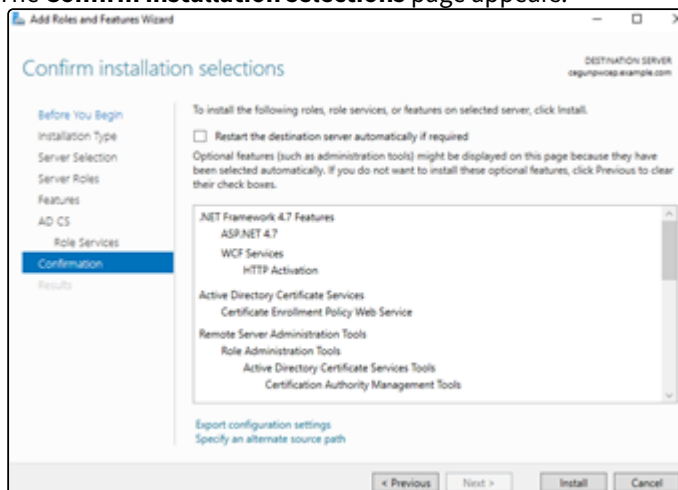


15. If you are on a different server than Active Directory, deselect **Certificate Authority**.
16. Select Certificate Enrollment Policy Web Service.  
Another **Add Roles and Features Wizard** dialog box may appear, informing you that some features are required for Active Directory Certificate Services.



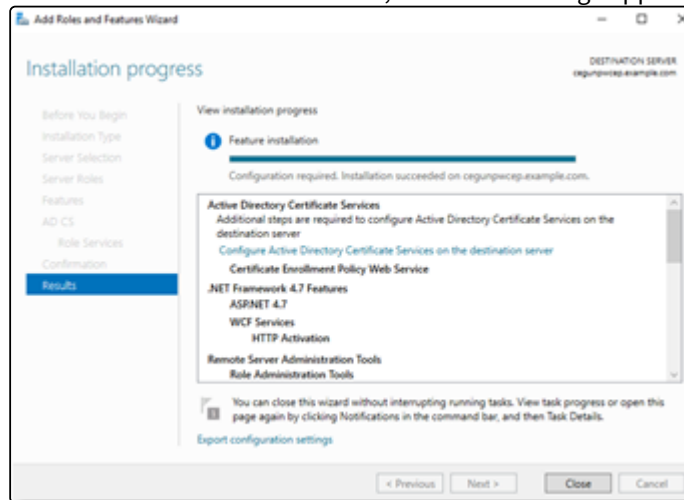
17. Click **Add Features** to add these required features and close the dialog box.
18. Click **Next**.

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**.

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.

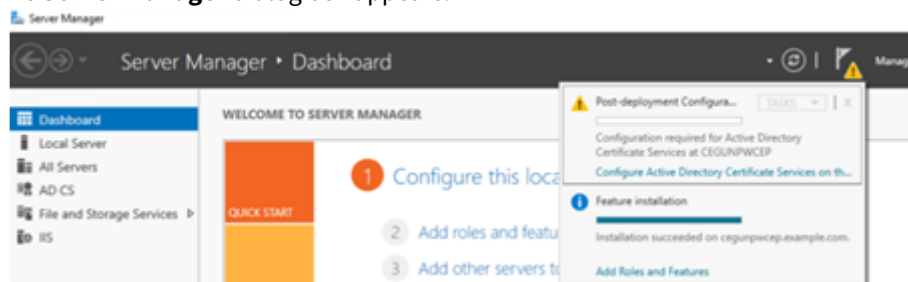
- username
- domain\username
- username@domain
- domainfqdn\username
- username@domainfqdn

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.

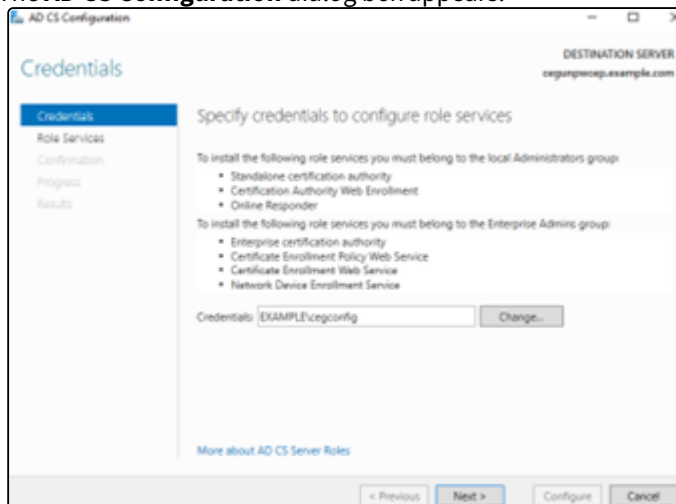
### **To select the authentication mode for the CEP Web Service using the Windows graphical interface**

1. Log in to the server where you installed the Certificate Enrollment Policy Web Service.

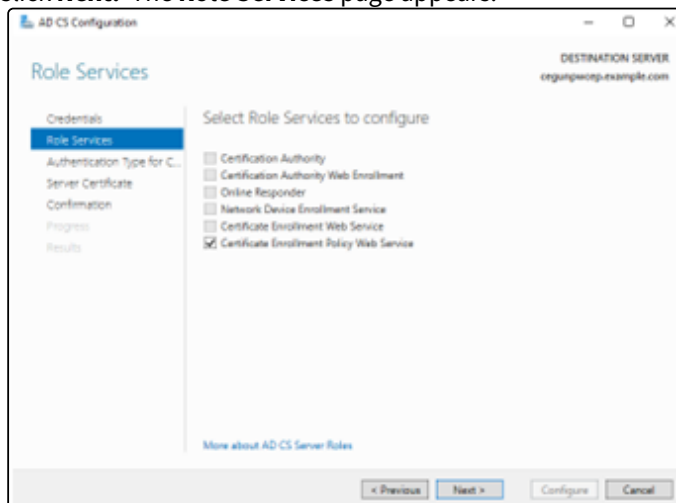
- Open Server Manager. Select **Start > Server Manager**.  
The **Server Manager** dialog box appears.



- Select **Notifications > Configure Active Directory Certificate Services** on the destination server.  
The **AD CS Configuration** dialog box appears.



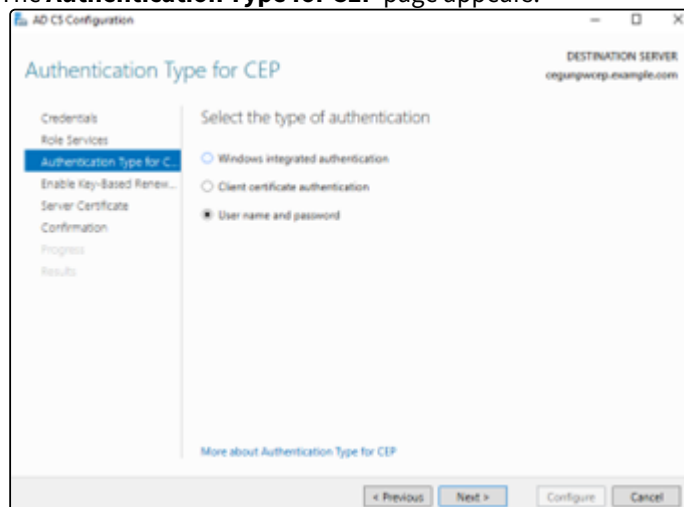
- Enter or select the administrator credentials you will use to configure role services.
- Click **Next**. The **Role Services** page appears.



- Select **Certificate Enrollment Policy Web Service**.

7. Click **Next**.

The **Authentication Type for CEP** page appears.



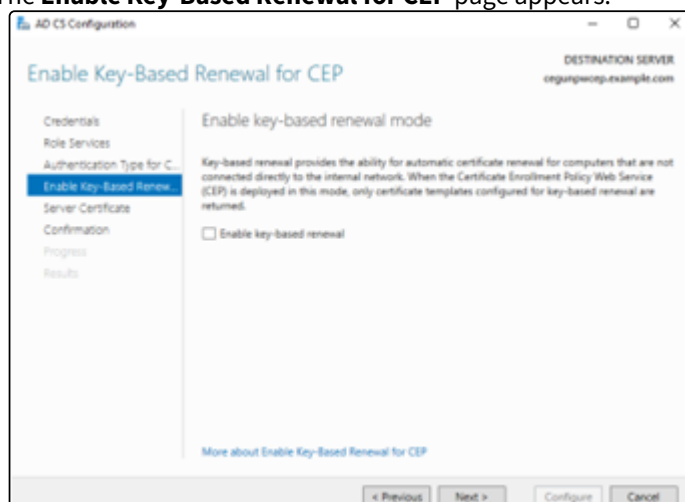
8. Select an authentication method supported by Certificate Enrollment Gateway.

 Client certificate authentication is currently not supported by Certificate Enrollment Gateway.

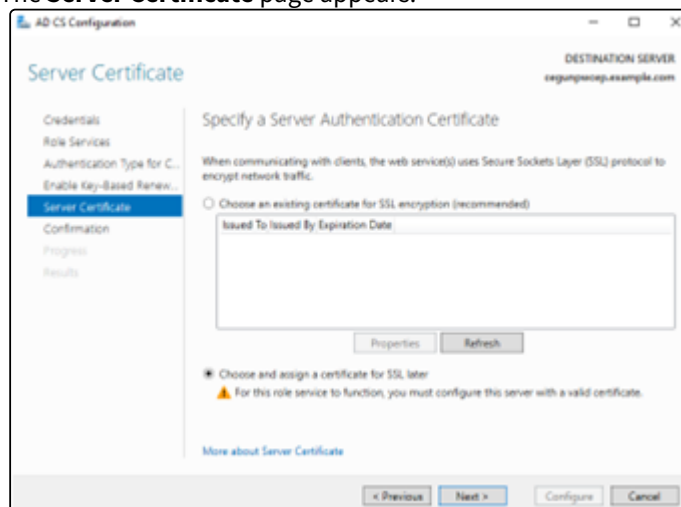
If you support non-domain enrollment endpoints, you must select **User name and password** as the authentication method.

9. Click **Next**.

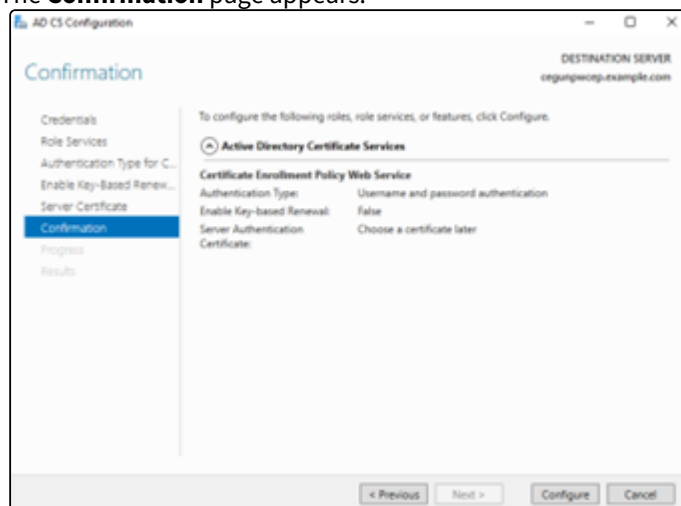
The **Enable Key-Based Renewal for CEP** page appears.



10. Do not select any options. Click **Next**.  
The **Server Certificate** page appears.

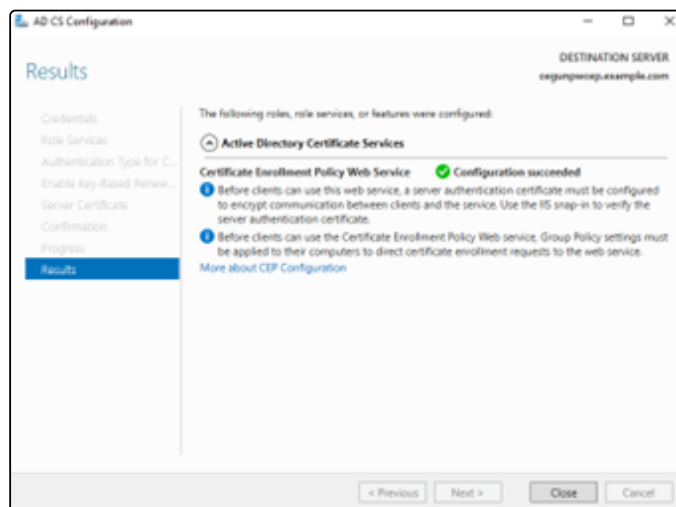


11. Select **Choose and assign a certificate for SSL later**.
12. Click **Next**.  
The **Confirmation** page appears.



13. Click **Configure**.  
After the authentication mode is configured, the **Results** page appears.





14. Click **Close**.

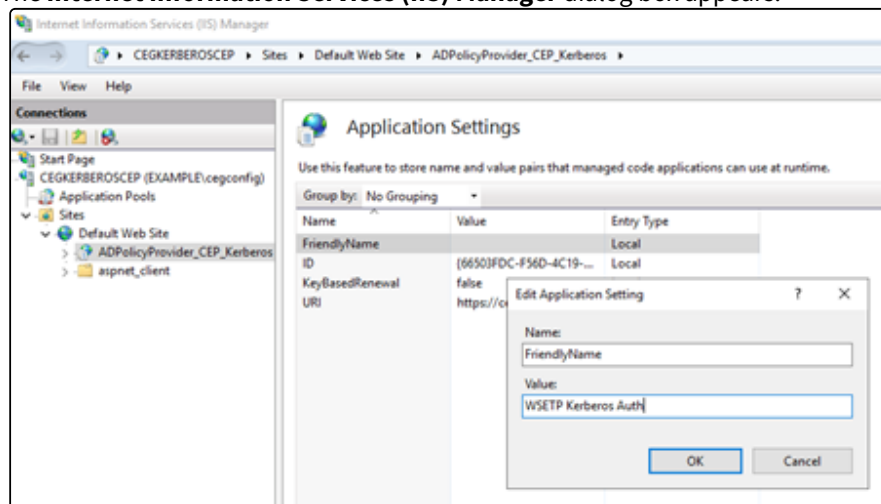
Assigning a friendly name to the CEP Web Service using the Windows graphical interface

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

1. Log in to the server where you installed 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 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**.

#### 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"
```

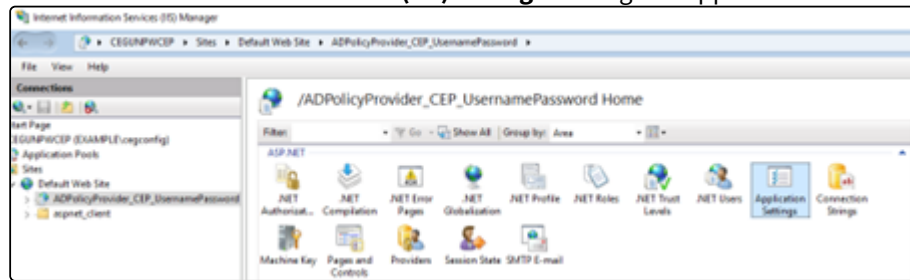
#### Assigning a unique Enrollment Policy Identifier with the Windows graphical interface

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**.

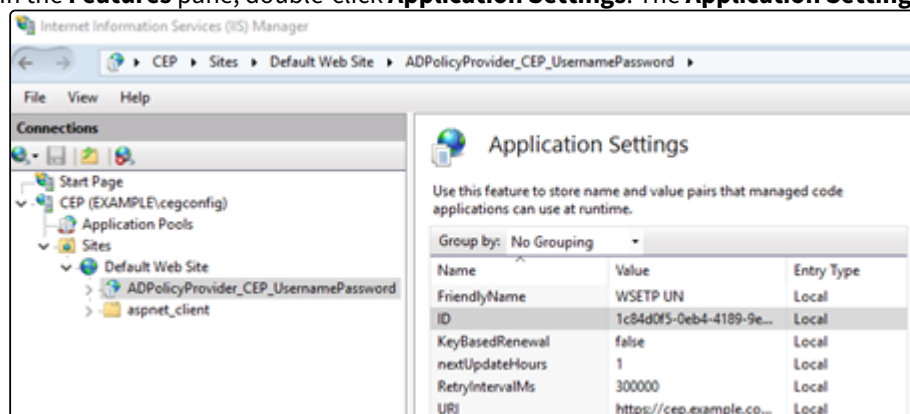
The **Internet Information Services (IIS) Manager** dialog box appears.



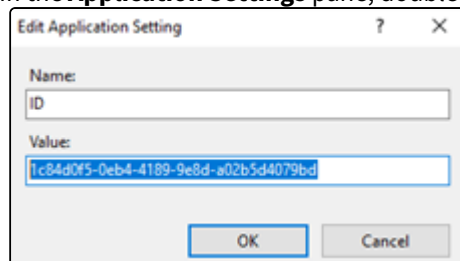
3. In the **Connections** pane, expand **Sites > Default Web Site**.
4. Select the name of the Certificate Enrollment Policy Web Service application.
  - If you configured user name and password authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider\_CEP\_UsernamePassword**.
  - If you configured Kerberos (Windows integrated) authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider\_CEP\_Kerberos**.
5. 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
```

6. In the **Features** pane, double-click **Application Settings**. The **Application Settings** pane appears.



7. In the **Application Settings** pane, double-click on ID. The **Edit Application Setting** dialog box appears.



8. In the **Value** field of the **Edit Application Setting** dialog box, enter a unique identifier.
9. Click **OK**.
10. Restart IIS.
11. 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.

## 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
```

## 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 create 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**.

## 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.

- 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.

- 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.

- 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**.

- 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.

## 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](#)
- [Adding the enrollment URL to the enrollment service using the certutil utility](#)
- [Changing the enrollment URL of the enrollment service using ADSI Edit](#)

### 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
```

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: "cegm sca.example.com\CEGMSCA"
 Exchange Certificate: ""
 Signature Certificate: ""
 Description: ""
 Server: "cegm sca.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.
```

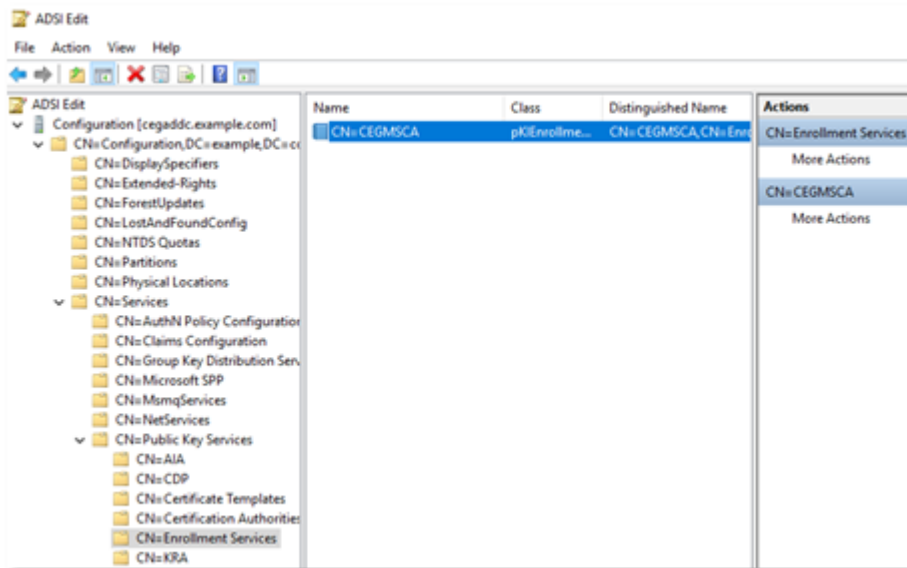
Changing the enrollment URL of the enrollment service using ADSI Edit

To add the enrollment service URL to Active Directory using ADSI Edit, complete the following procedure.

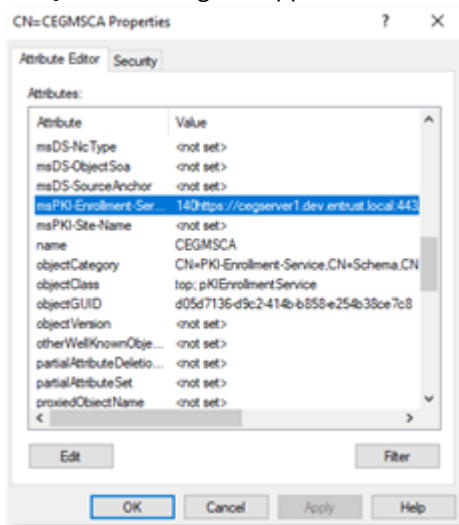
**To add the enrollment service URL to Active Directory using ADSI Edit**

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**.

## 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"):

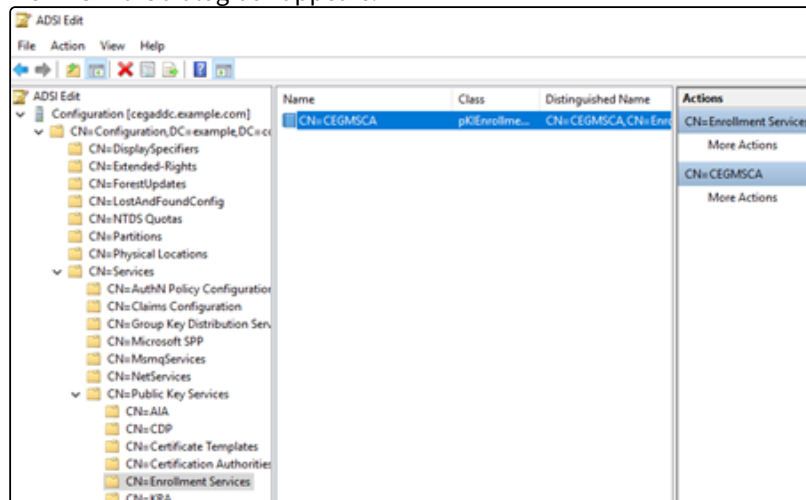
- b. Enter **Q** to exit the script.

## 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.

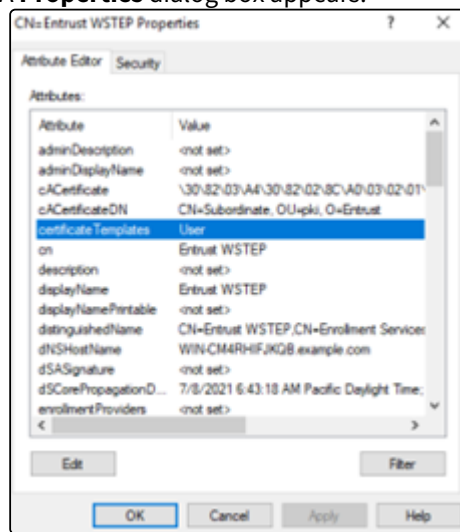
### To add certificate templates to the enrollment service

1. Log in to the server hosting Active Directory.
2. Open ADSI Edit. Select **Start > Windows Administrative Tools > ADSI Edit**. The **ADSI Edit** dialog box appears.

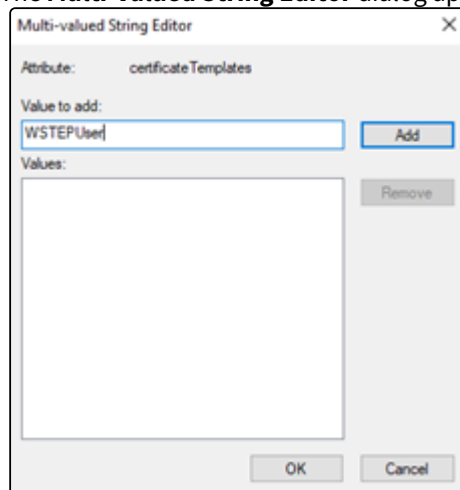


3. In the tree view, expand **ADSI Edit > Configuration > CN=Configuration,<suffix> > CN=Services > CN=Public Key Services > CN=Certificate Enrollment Gateway**.

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**.

## Configuring enrollment endpoints

You must configure all Windows 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.

- [Obtaining the URL of the Certificate Enrollment Policy Web Service](#)
- [Importing the CA certificate into Windows domain endpoints](#)
- [Configuring the Certificate Enrollment Policy Web Service for Windows users](#)
- [Configuring the Certificate Enrollment Policy Web Service for Windows domain endpoints](#)
- [Enabling certificate auto-enrollment for users](#)
- [Enabling certificate auto-enrollment for computers and domain controllers](#)

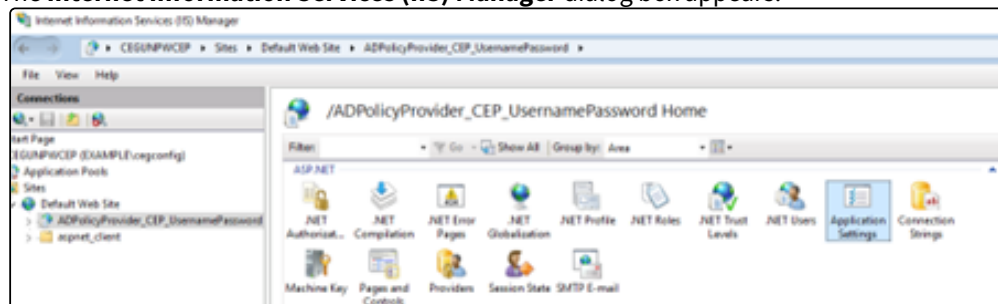
### Obtaining the URL of the Certificate Enrollment Policy Web Service

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

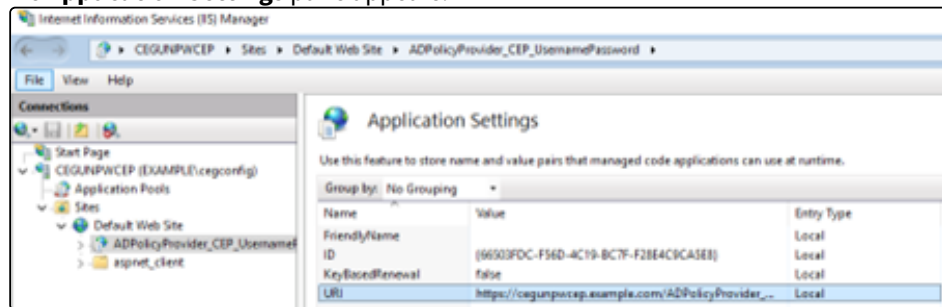
1. Log in to the server hosting the Certificate Enrollment Policy Web Service.
2. Open IIS Manager. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** dialog box appears.

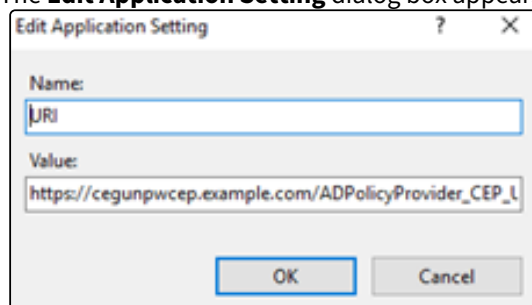


3. In the **Connections** pane, expand **Sites > Default Web site**.
4. Select the name of the Certificate Enrollment Policy Web Service application.
  - If you configured user name and password authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider\_CEP\_UsernamePassword**.
  - If you configured Kerberos (Windows integrated) authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider\_CEP\_Kerberos**.

- In the Features pane, double-click **Application Settings**.  
The **Application Settings** pane appears.



- In the **Application Settings** pane, right-click **URI** > **Edit**.  
The **Edit Application Setting** dialog box appears.



- Copy the URL from the **Value** field.

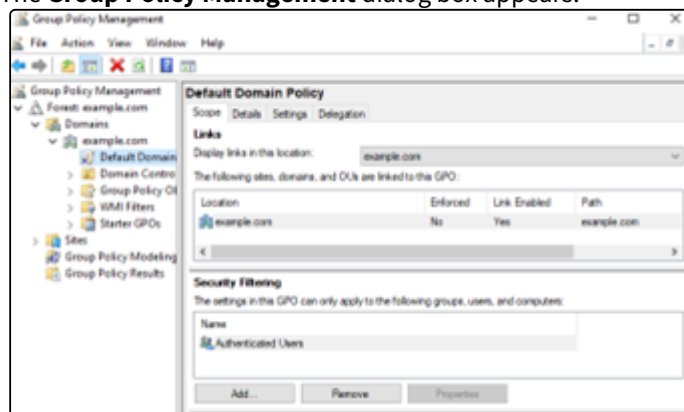
Importing the CA certificate into Windows domain endpoints

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

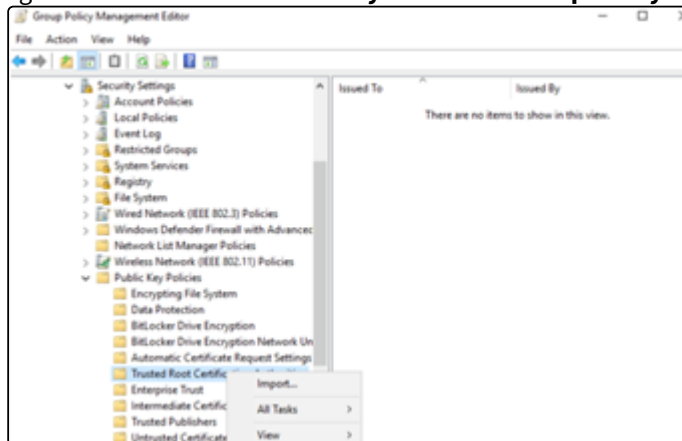
- Log in to the server hosting Active Directory.
- Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.

The **Group Policy Management** dialog box appears.

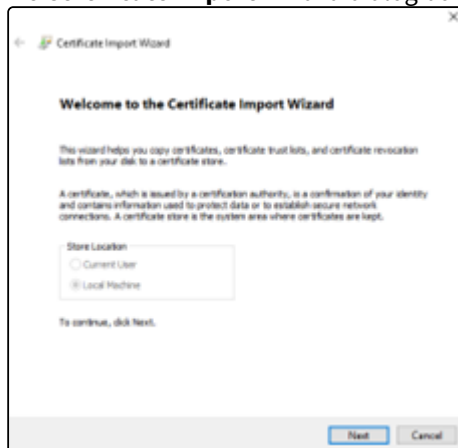


- In the tree view, expand the Domain Controller you will modify.

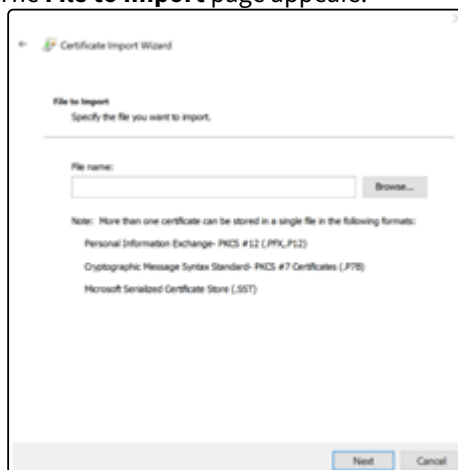
- Right-click **Default Domain Policy > Edit**. The **Group Policy Management Editor** dialog box appears.



- 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**.

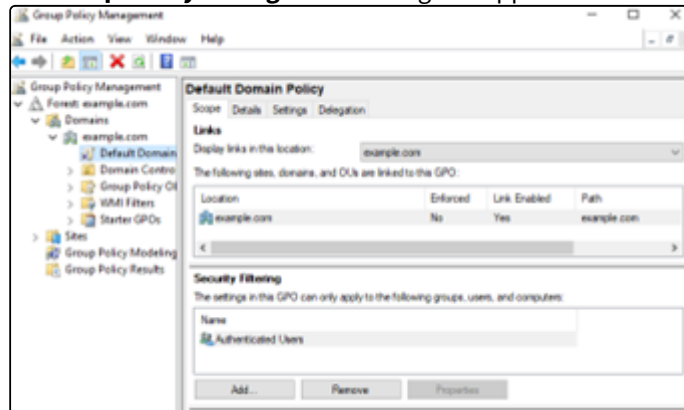
Configuring the Certificate Enrollment Policy Web Service for Windows users

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

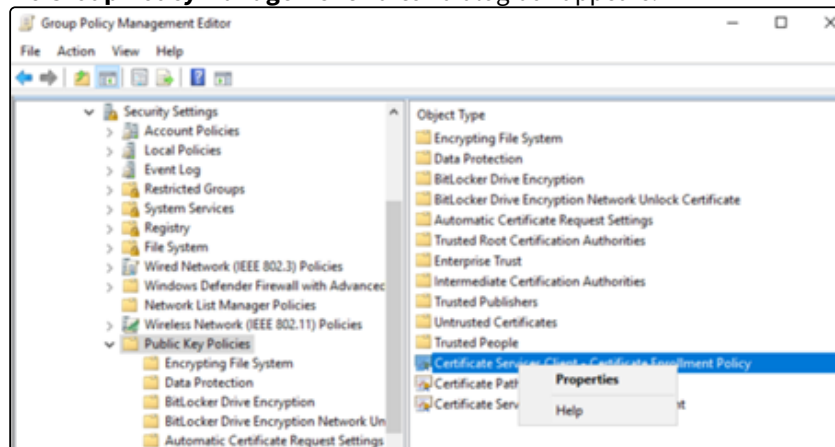
1. Log in to the server hosting Active Directory.
2. Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.

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**.

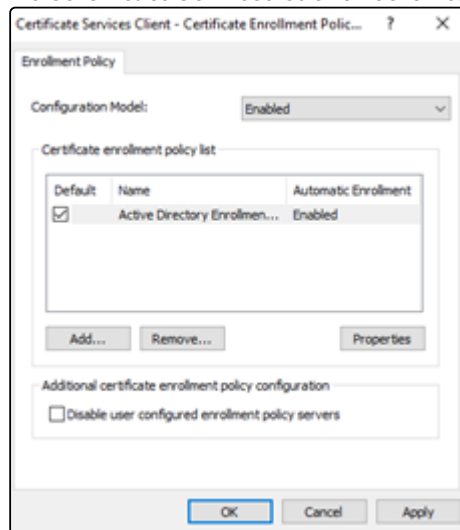
The **Group Policy Management Editor** dialog box appears.



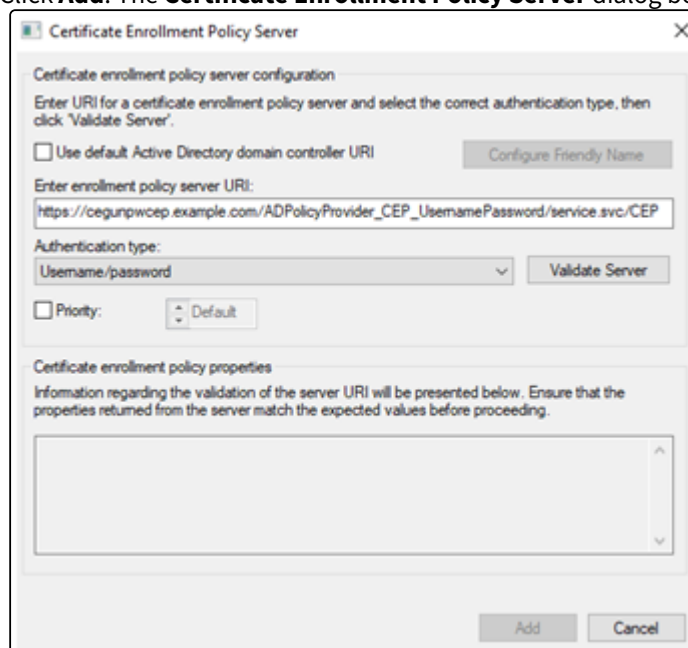
5. In the tree view, expand **User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.



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.

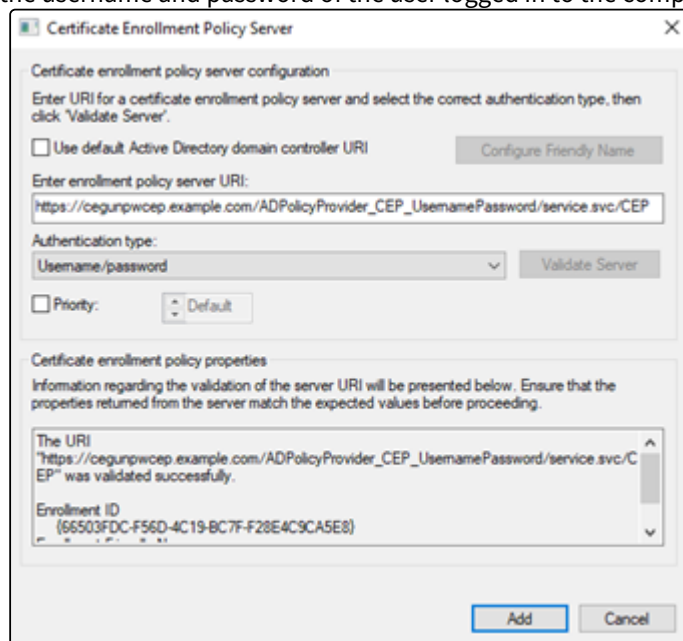


7. In the **Configuration Model** drop-down list, select **Enabled**.
8. If you are not installing WSTEP along with an existing Microsoft CA, select **Active Directory Enrollment** in the **Certificate enrollment policy list** pane, and then click **Remove**.
9. Click **Add**. The **Certificate Enrollment Policy Server** dialog box appears.

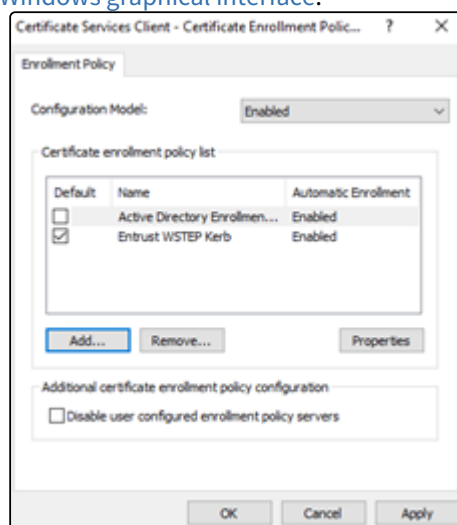


10. In the **Enter enrollment policy server URI** field, enter the Certificate Enrollment Policy Web Service URL that you obtained earlier.
11. In the **Authentication type** drop-down list, select the same authentication mode that you configured earlier in [Selecting the authentication mode of the CEP 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.



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](#).



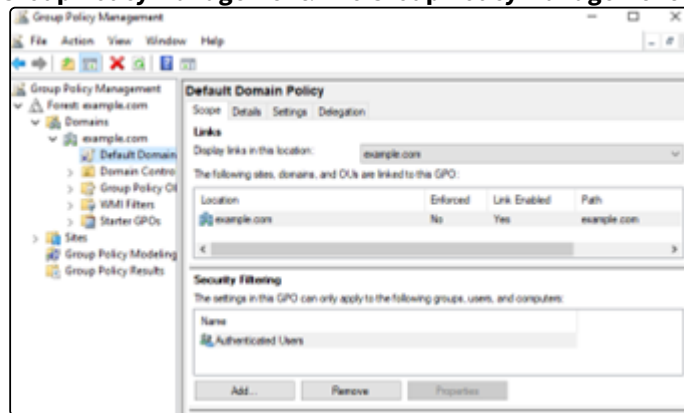
14. In the **Certificate enrollment policy list** pane, select the checkbox for the Certificate Enrollment Policy Web Service you just added to make it the default Certificate Enrollment Policy.
15. Click **OK**.

### Configuring the Certificate Enrollment Policy Web Service for Windows domain endpoints

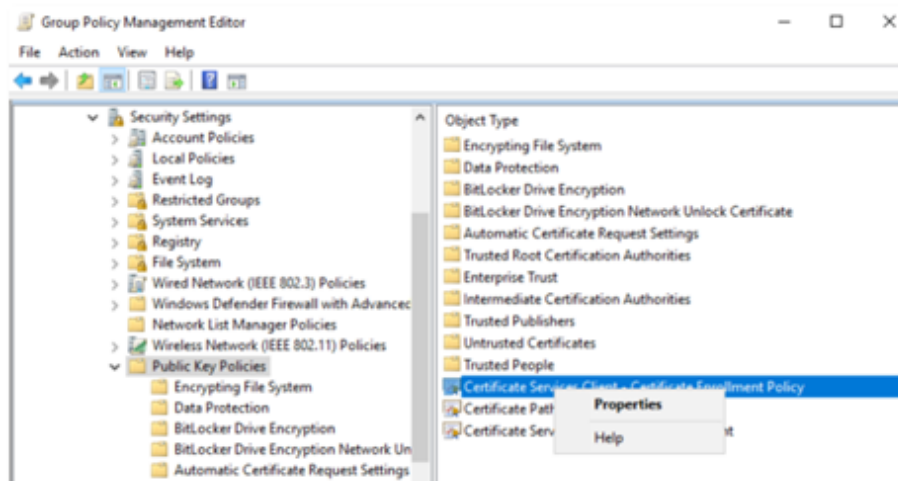
To work with Certificate Enrollment Gateway, Windows domain endpoints need the Certificate Enrollment Policy Web Service URL. Complete the following procedure to add the Certificate Enrollment Policy Web Service URL for Windows domain endpoints.

#### 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.

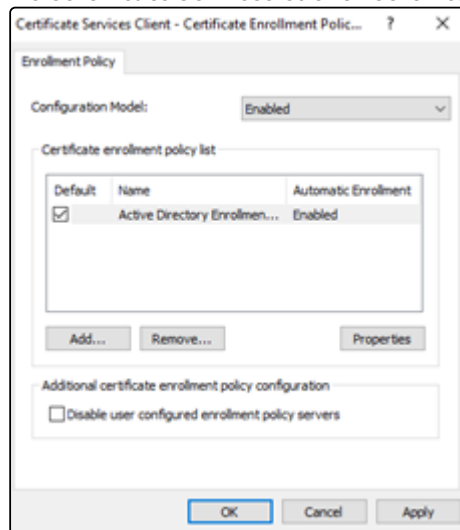


3. In the tree view, expand the Domain Controller you will modify.
4. Right-click **Default Domain Policy > Edit**. The **Group Policy Management Editor** dialog box appears.

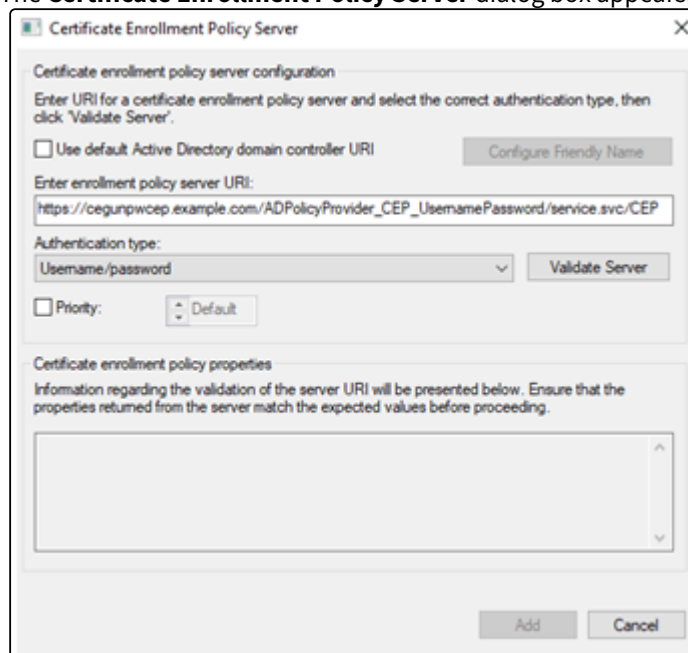


5. In the tree view, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.

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.

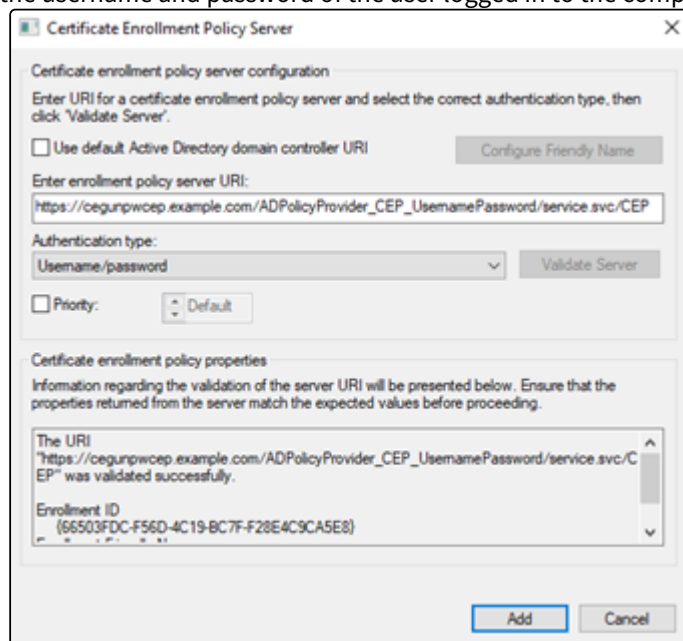


7. In the **Configuration Model** drop-down list, select **Enabled**.
8. If you are not installing WSTEP along with an existing Microsoft CA, select **Active Directory Enrollment** in the **Certificate enrollment policy list** pane, and then click **Remove**.
9. Click **Add**. The **Certificate Enrollment Policy Server** dialog box appears.

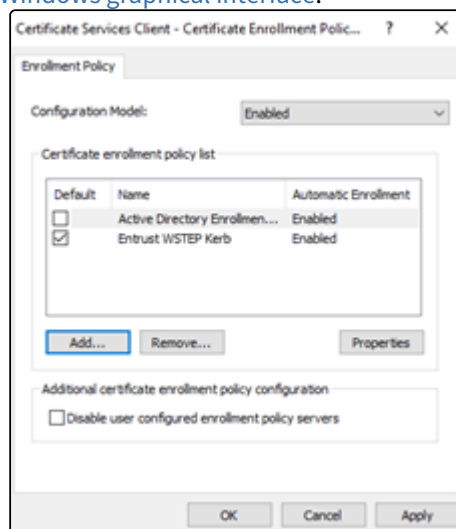


10. In the **Enter enrollment policy server URI** field, enter the Certificate Enrollment Policy Web Service URL that you obtained earlier.
11. In the **Authentication type** drop-down list, select the same authentication mode that you configured earlier in [Selecting the authentication mode of the CEP 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.



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**.

Enabling certificate auto-enrollment for users

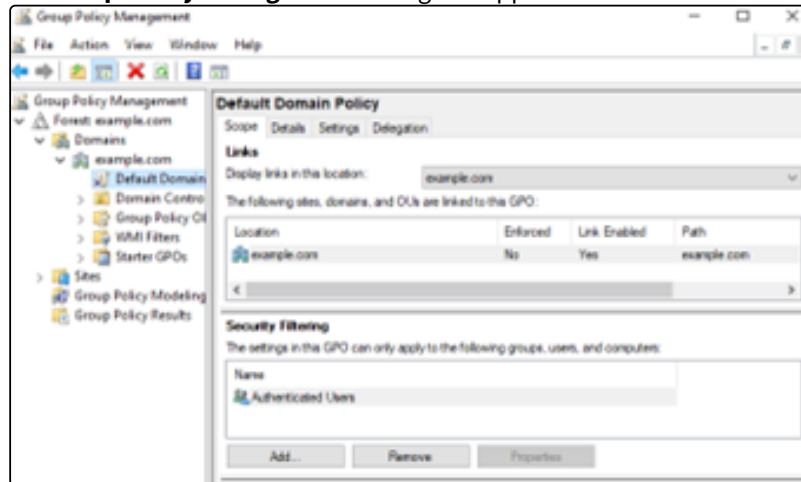
In the Windows Domain, enable the certificate auto-enrollment for users.

#### To enable the certificate auto-enrollment for users

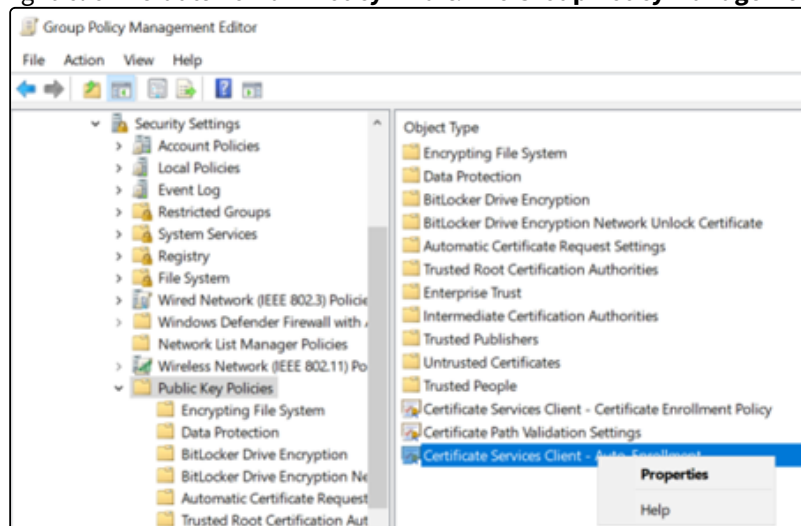
1. Log in to the server hosting Active Directory.

- Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.

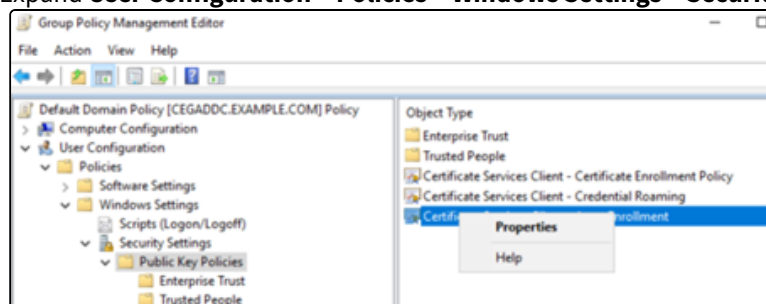
The **Group Policy Management** dialog box appears.



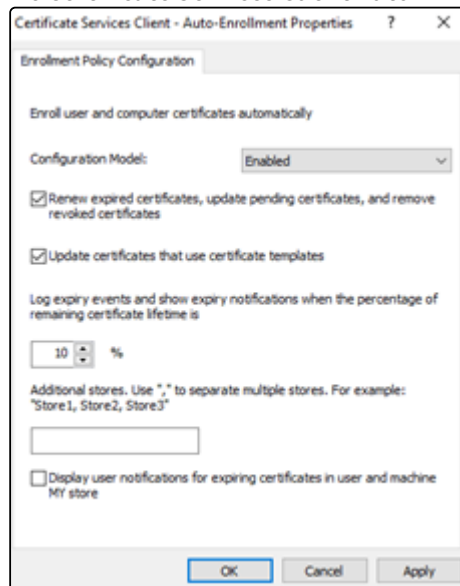
- In the tree view, expand the Domain Controller you will modify.
- Right-click **Default Domain Policy > Edit**. The **Group Policy Management Editor** dialog box appears.



- Expand **User 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**.

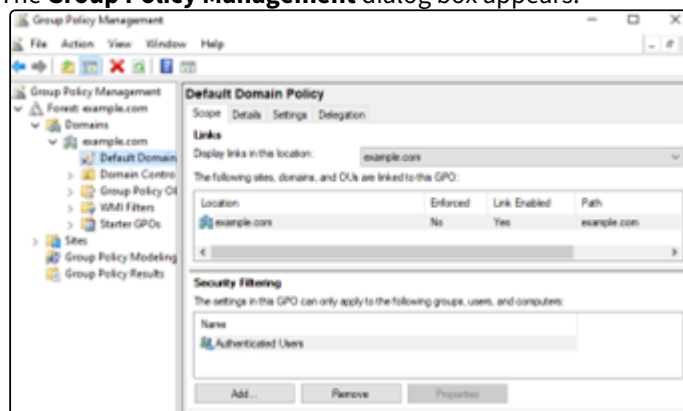
Enabling certificate auto-enrollment for computers and domain controllers

In the Windows domain, enable the certificate auto-enrollment for computers and domain controllers.

#### To enable certificate auto-enrollment for computers and domain controllers

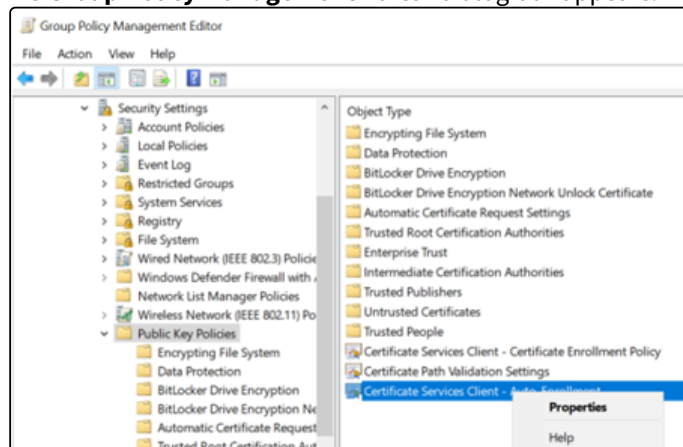
- Log in to the server hosting Active Directory.
- Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.

The **Group Policy Management** dialog box appears.

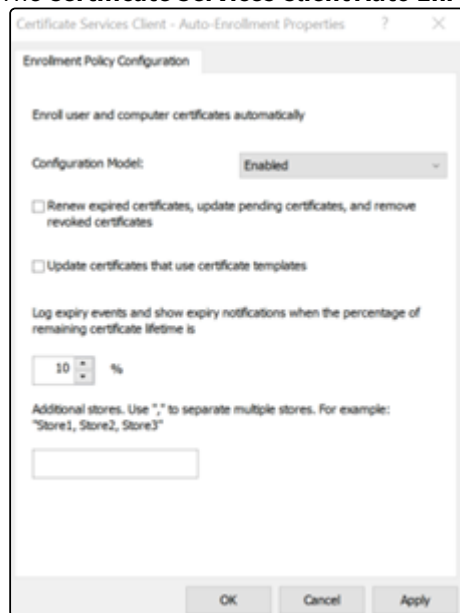


- In the tree view, expand the Domain Controller you will modify.

4. Right-click **Default Domain Policy > Edit**.  
The **Group Policy Management Editor** dialog box appears.



5. Expand to **Computer 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**.

#### 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](#)



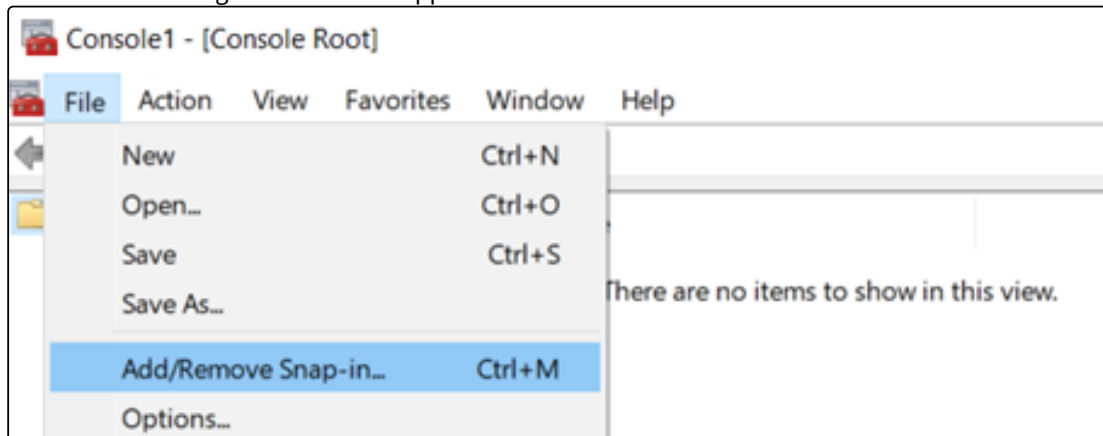
Configuring the enrollment policy in non-domain endpoints

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**

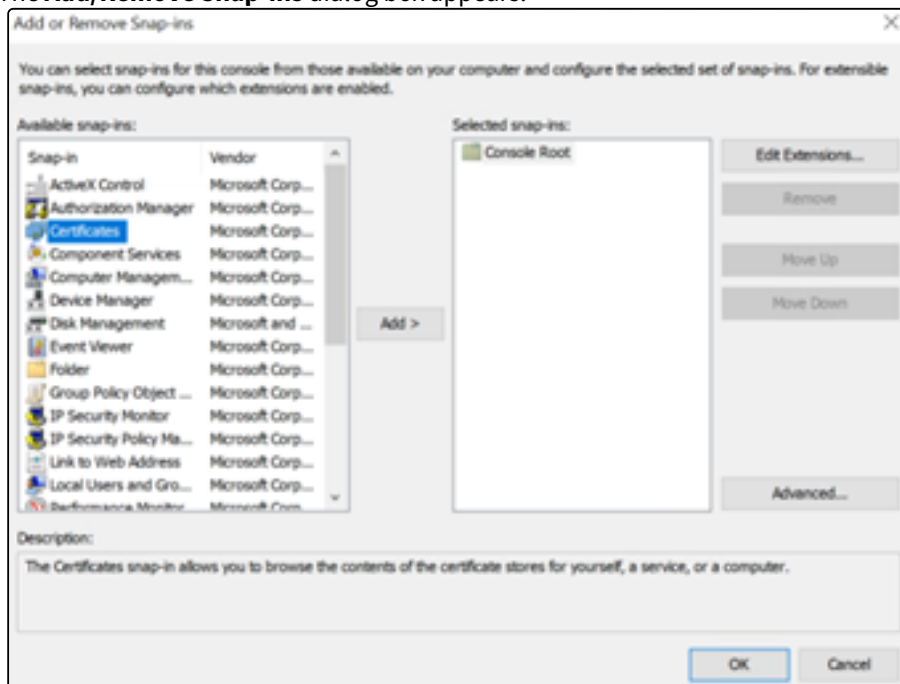
1. Log in to the non-domain endpoint.
2. Run `mmc.exe`.

The Microsoft Management Console appears.



3. Select **File > Add/Remove Snap-in**.

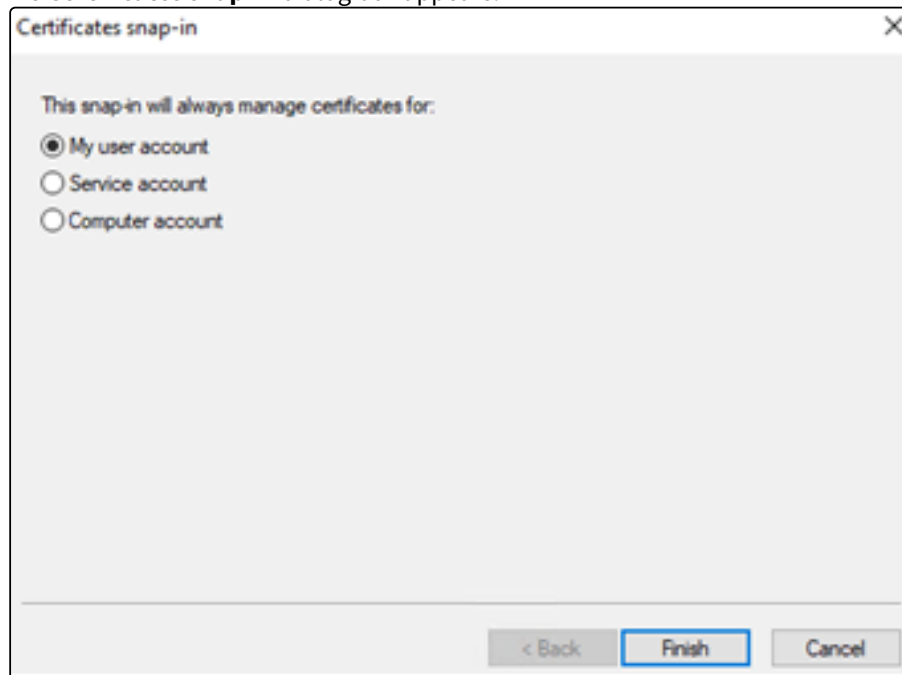
The **Add/Remove Snap-ins** dialog box appears.



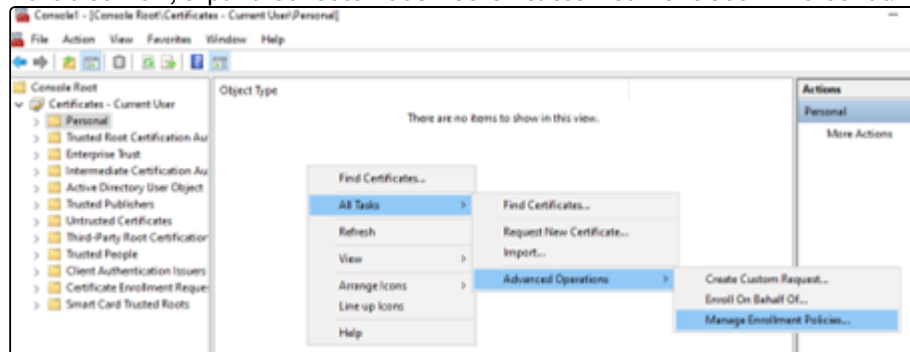
4. In the **Available snap-ins** list, select **Certificates**.

5. Click **Add**.

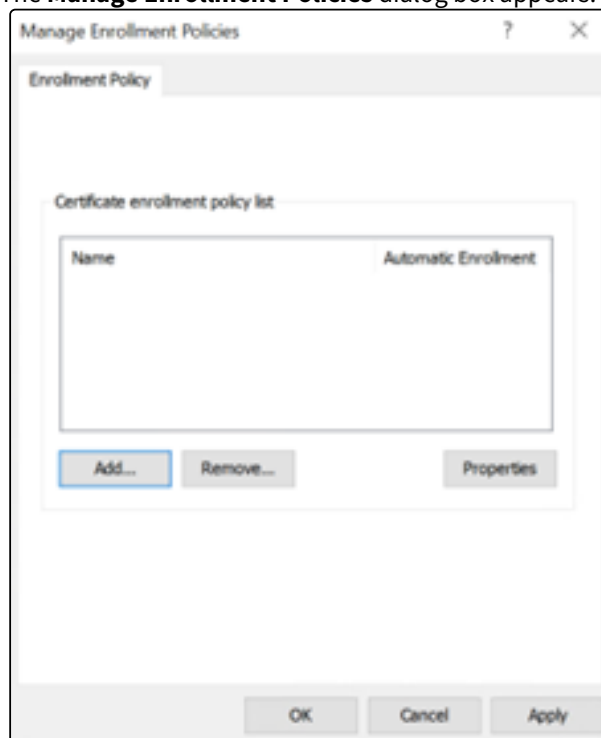
The **Certificates snap-in** dialog box appears.



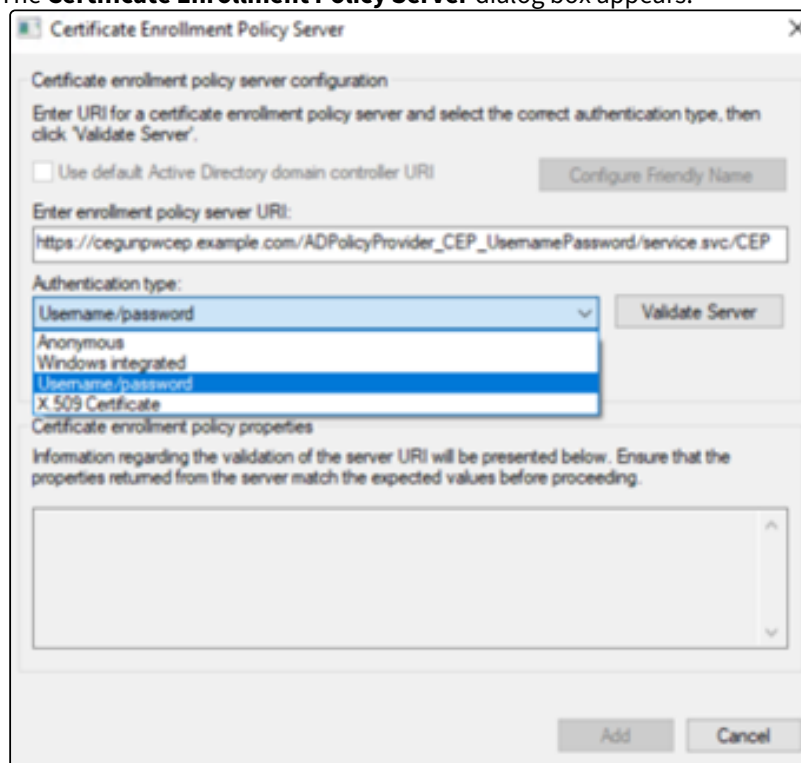
6. Select **My user account**.
7. Click **Finish** to close the **Certificates snap-in** dialog box.
8. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
9. In the tree view, expand **Console Root > Certificates – Current User > Personal**.



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.



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.

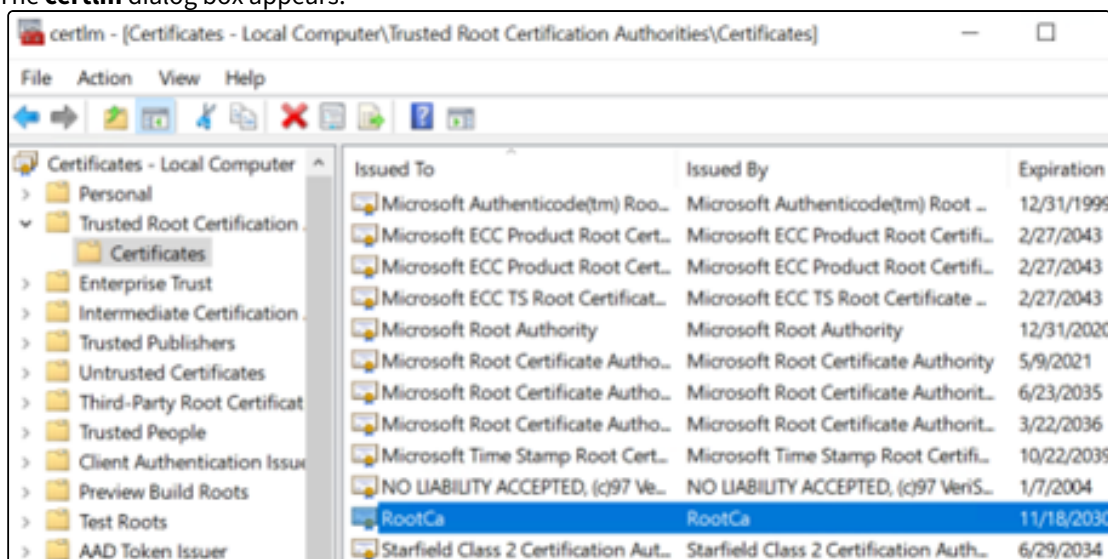
#### To import the root CA certificate in non-domain endpoints

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.

4. Open the Certificate Manager snap-in. Select **Start > Run**, then enter `certlm.msc`.  
The **certlm** dialog box appears.



5. In the tree view, expand **Certificates – Local Computer > Trusted Root Certification Authorities > Certificates**.
6. In the content pane, verify that the root CA certificate you imported appears in the list of trusted root CA certificates.

#### 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.

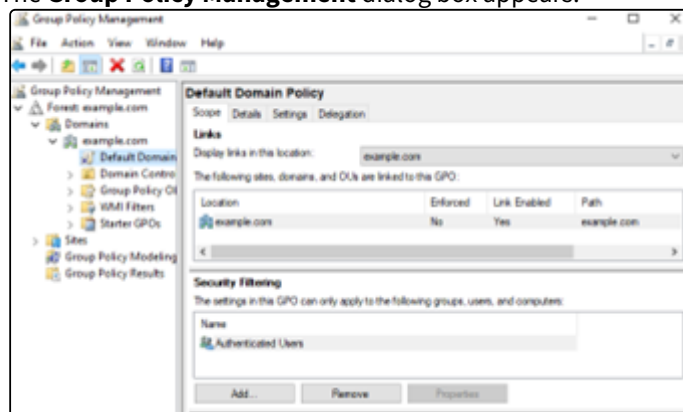
- If you are integrating Certificate Enrollment Gateway with an existing Windows domain, this domain already has trusted TLS certificates, and you can skip this section.
- If you are integrating a new Windows domain, In the Active Directory Domain Controller, install all certificates in the CA certificate chain as trusted root certificates. Follow the steps below to install the TLS certificate chain.

For CAs hosted by Entrust PKI as a Service, you should have obtain the CA certificates from the Entrust Certificate Services portal.

### To install the CA certificates in the Active Directory Domain Controller

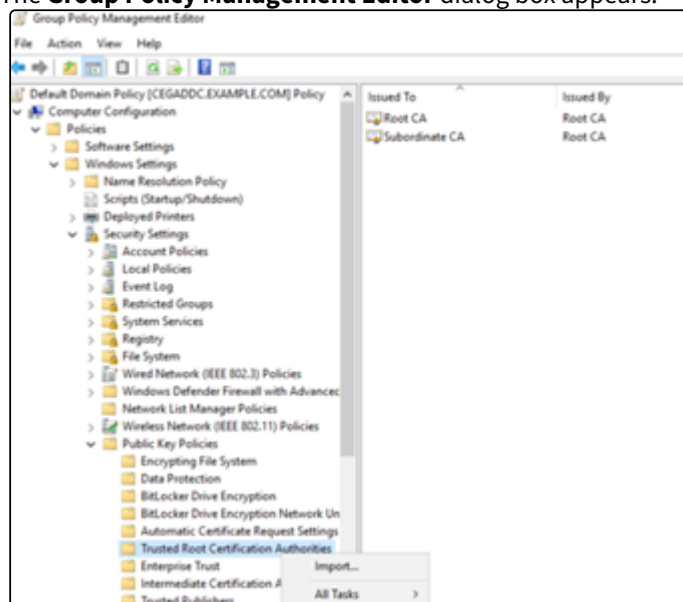
1. Log in to the server hosting Active Directory.
2. Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.

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](#).

## 10 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.

 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 <a href="#">Managing Certificate Authority</a> , 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 <a href="#">Managing CA Gateway</a> .                                  |

## 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.

 Do not forget to also click **Deploy** after each update of the configuration or the license file.

### To configure and deploy Certificate Manager with the Management Console

1. Open the following URL in a Web browser.

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

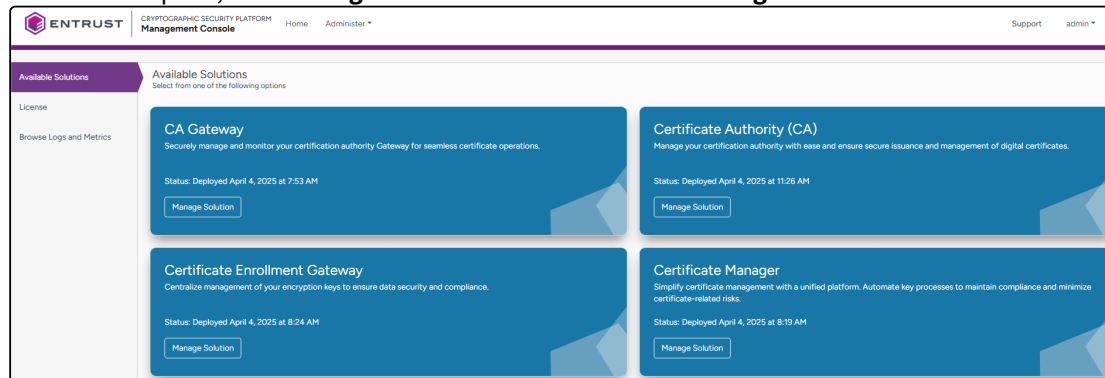
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

2. Log into the Management Console a user belonging to a role with Certificate Manager management permissions – for example, the initial `admin` administrator user.

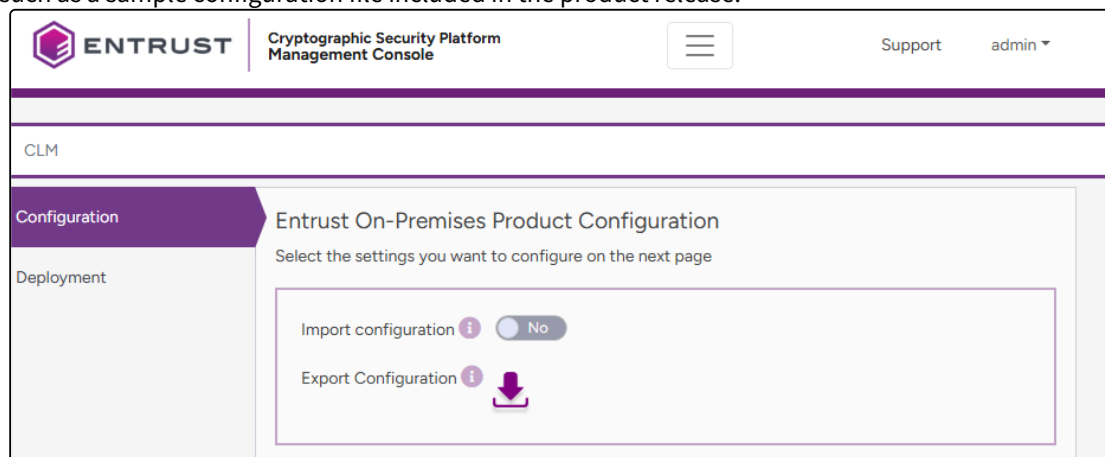
 See [Starting up the Management Console](#) for how to manage users and roles.



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 meeting the [Database requirements](#). The Certificate Management deployment process will automatically create all the required tables.



Certificate Authority and Certificate Manager cannot share the same 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.

In case this password changes in the external database.

1. Update the value also on this field of the Management Console.
2. Click **Submit** and wait while the new configuration is applied.
3. Click **Deploy**.
4. Open a command line session on any installation node.
5. Run the following command.

```
sudo kubectl get deploy -o name -n certhub | xargs -n1 sudo kubectl rollout restart -n certhub
```

**Mandatory:** Yes.

## Host of the PostgreSQL database

The IP address or Fully Qualified Domain Name (FQDN) of the database host.

⚠ As explained in [Database requirements](#), 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 requirements](#), 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.

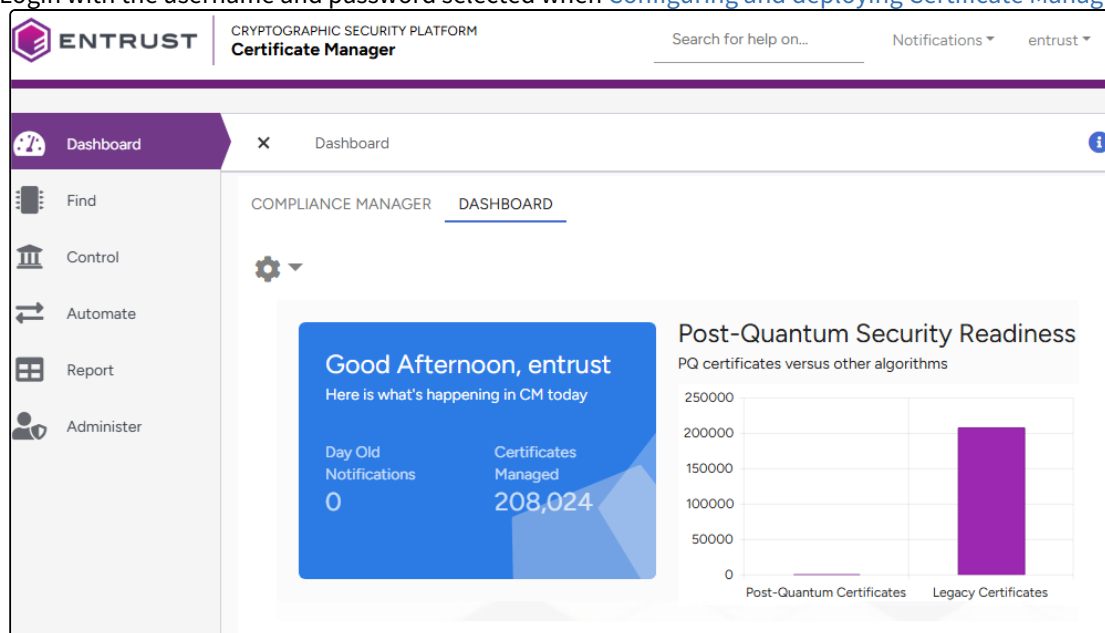
**To manage certificates with Certificate Manager**

1. Open a web browser in the following URL.

`https://<host>/certhub`

Where `<host>` is the value of the **CM Hostname** parameter described in [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 connecting Compliance Manager and Certificate Manager.

- [Creating a data source connection on Compliance Manager](#)
- [Uploading the data source connection to Certificate Manager](#)

Creating a data source connection on Compliance Manager

Create and download a data source connection as explained in the Compliance Manager documentation.

<https://docs.hytrust.com/CryptographicSecurityPlatformComplianceManager/10.4.5/Online/Content/KC-Compliance-Manager/Collections-and-Data-Sources/Creating-Data-Source-Connections.htm>

Specifically, on the **Initialize Connection to a Data Source** page, enter the following URL.

```
https://<csp>/certhub
```

Where `<csp>` is the domain name or IP address of a Cryptographic Security Platform node.

Uploading the data source connection to Certificate Manager

Upload the data source connection to Certificate Manager.

### To upload a Data Source Connection

1. Log in as an administrator with either:
  - The `global_admin` role.
  - A `<user_defined>` role with permission to manage connections with Compliance Manager.
2. Click the **Dashboard** command in the sidebar menu.
3. 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.
4. Under **Data Source Name**, enter a unique identifier for the Certificate Manager instance in Certificate Manager.
5. 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.
6. Click **Verify** to check the connection and fix any reported issues.
7. 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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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                                      | <a href="http://www.example.com">www.example.com</a>               |
| An individual IP address                                    | 192.51.100.20                                                      |
| A comma-separated list of IP addresses or hostnames         | <a href="http://www.example.com">www.example.com</a> ,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.

| Priori<br>ty | 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.                                                                                                              |
| Norm<br>al   | 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                                      | <a href="http://www.example.com">www.example.com</a>               |
| An individual IP address                                    | 192.51.100.20                                                      |
| A comma-separated list of IP addresses or hostnames         | <a href="http://www.example.com">www.example.com</a> ,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](http://www.example.com)

[www.example.com](http://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                  |

| Scan Rate       | Initial scan delay (ms) | Max attempts to reach host port | Max time before sending another probe (ms) | Max scan delay (ms) |
|-----------------|-------------------------|---------------------------------|--------------------------------------------|---------------------|
| 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.

**i** 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.                                                                                                              |
| 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                                      | <a href="http://www.example.com">www.example.com</a>               |
| An individual IP address                                    | 192.51.100.20                                                      |
| A comma-separated list of IP addresses or hostnames         | <a href="http://www.example.com">www.example.com</a> ,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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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](#)

ℹ 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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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 <b>Profile Key Type</b> is <b>Unspecified</b> . |

**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 <b>Profile Key Type</b> is <b>Unspecified</b> or <b>Override key type</b> 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 <b>Profile Key Type</b> is <b>Unspecified</b> . |

**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 <b>Profile Key Type</b> is <b>Unspecified</b> or <b>Override key type</b> 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 <a href="#">Making a certificate request</a> by registered Administrators logged in to Certificate Manager.                      |
| External     | Created by non-registered users from a <a href="#">Public Enrollment Form</a> 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](#)

i 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.

 Column headers display a sorting icon when the column values can be sorted with a click.

### 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 <a href="#">Making a certificate request</a> or <a href="#">Requesting a certificate renewal</a> .   |
| <public_form>    | Request created by non-registered users using the <a href="#">Public Enrollment Form</a> with <code>&lt;public_form&gt;</code> 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 <a href="#">Public Enrollment Form</a> published online, or entered by an administrator as explained in <a href="#">Making a certificate request</a> .                              |
| Description   | The certificate description entered by an end-user on a <a href="#">Public Enrollment Form</a> published online, or entered by an administrator as explained in <a href="#">Making a certificate request</a> .                    |
| 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 <a href="#">Public Enrollment Form</a> published online, or an administrator requested the certificate as explained in <a href="#">Making a certificate request</a> . |
| 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 <a href="#">Public Enrollment Form</a> published online, or selected by an administrator as explained in <a href="#">Making a certificate request</a> .                         |
| Profile       | The certificate authority profile configured for a <a href="#">Public Enrollment Form</a> published online, or selected by an administrator as explained in <a href="#">Making a certificate request</a> .                        |

| Setting           | Description                                                                                                                                                                                                                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <a href="#">Public Enrollment Form</a> published online, or pasted by an administrator as explained in <a href="#">Making a certificate request</a> . |
| SAN               | The subject alternative name (SAN) entered by an end-user on a <a href="#">Public Enrollment Form</a> published online, or entered by an administrator as explained in <a href="#">Making a certificate request</a> .                                                                                   |
| Subject Variables | The certificate subject variables, if required by the selected profile defined by an end-user on a <a href="#">Public Enrollment Form</a> published online, or entered by an administrator as explained in <a href="#">Making a certificate request</a> .                                               |

#### 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.                  |

| Setting             | Description                                                                                                                 |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------|
| 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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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.

 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 <a href="#">Public Enrollment Form</a> published online, or entered by an administrator as explained in <a href="#">Making a certificate request</a> .                              |
| Description   | The certificate description entered by an end-user on a <a href="#">Public Enrollment Form</a> published online, or entered by an administrator as explained in <a href="#">Making a certificate request</a> .                    |
| 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 <a href="#">Public Enrollment Form</a> published online, or an administrator requested the certificate as explained in <a href="#">Making a certificate request</a> . |
| 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 <a href="#">Public Enrollment Form</a> published online, or selected by an administrator as explained in <a href="#">Making a certificate request</a> .                         |
| Profile       | The certificate authority profile configured for a <a href="#">Public Enrollment Form</a> published online, or selected by an administrator as explained in <a href="#">Making a certificate request</a> .                        |



| Setting           | Description                                                                                                                                                                                                                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <a href="#">Public Enrollment Form</a> published online, or pasted by an administrator as explained in <a href="#">Making a certificate request</a> . |
| SAN               | The subject alternative name (SAN) entered by an end-user on a <a href="#">Public Enrollment Form</a> published online, or entered by an administrator as explained in <a href="#">Making a certificate request</a> .                                                                                   |
| Subject Variables | The certificate subject variables, if required by the selected profile defined by an end-user on a <a href="#">Public Enrollment Form</a> published online, or entered by an administrator as explained in <a href="#">Making a certificate request</a> .                                               |

#### 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.                  |

| Setting             | Description                                                                                                                 |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------|
| 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.                                                        |

| Destination | Limitations                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------|
| 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](https://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](https://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.

**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 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.

#### 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**.

 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                                       | <a href="#">Find</a>                    |
| Imported into Certificate Manager                                        | <a href="#">Importing certificates</a>  |
| Imported into Certificate Manager using the Certificate Manager API      | <a href="#">Certificate Manager API</a> |
| Issued using the Certificate Manager Web browser interface               | <a href="#">Creating a certificate</a>  |
| Provided by a source and inserted with source synchronization operations | <a href="#">Sources</a>                 |
| Imported with key manager synchronization operations                     | <a href="#">Key Managers</a>            |

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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) |
| 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)  |
| 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.                                                                                                                                                                                                                                            |
| Source Type           | The type of the certificate <a href="#">Source</a> .                                                                                                                                                                                                                                                            |
| Serial                | The serial number (SN) of the certificate.                                                                                                                                                                                                                                                                      |
| Valid From            | The <b>Not Before</b> date of the certificate.                                                                                                                                                                                                                                                                  |
| Valid To              | The <b>Not After</b> date of the certificate.                                                                                                                                                                                                                                                                   |
| Last Modified         | The time and date of the latest <a href="#">Key State</a> 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 <a href="#">Signing Algorithm Security Level</a>                                                                                                                                                                                                                           |
| Key Algorithm         | The key-pair generation algorithm and the <a href="#">Key Algorithm Security Level</a> .                                                                                                                                                                                                                        |
| Validity              | The certificate status: Empty for certificates from unknown sources (because either imported or discovered); <b>Issued</b> for certificates from known sources and still valid; <b>Revoked</b> for certificates from known sources and already revoked as explained in <a href="#">Revoking a certificate</a> . |
| 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](https://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](https://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.

**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.

#### Automating certificate renewal

See below for automating the successive renewals of a certificate.

**i** 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](https://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](https://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). |
| 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](https://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](https://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.

 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.

 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](https://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](https://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.

**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.

#### 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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

 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.                                                  |
| 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. |

| Method | Description                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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

Crerating 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.

 Column headers display a sorting icon when the column values can be sorted with a click.

4. For each destination in the main grid, browse the following settings.
  - [ID](#)
  - [Label](#)
  - [Description](#)
  - [Plugin](#)
  - [Associated Certificates](#)
  - [Owner](#)
  - [Authorization Tags](#)

#### ID

A destination UUID (Universally Unique Identifier) internally generated 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.

**i** 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.

**i** 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](#)
  - [Backup path](#)
  - [Retain Backup files](#)
  - [Is sudo access required?](#)
  - [Sudo password](#)
  - [Restart the Apache web server](#)
  - [HTTPS Port](#)
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

Backup path

The folder to back up the certificate and the private key until they are successfully deployed.

- The certificate is backed up in the following file.

```
<backup-path>/<uuid>/backup/backup_cert_<YYYYMMDDHHMMSS>.pem
```

- The private key is backed up in the following file.

```
<backup-path>/<uuid>/backup/key_cert_<YYYYMMDDHHMMSS>.pem
```

Where:

- `<backup-path>` is the path entered in the **Backup path** field.
- `<uuid>` is a timestamp-based UUID that changes with each issuance backup.
- `<YYYYMMDDHHMMSS>` is a timestamp in `YYYYMMDDHHMMSS` format.

**Mandatory:** No. This optional parameter defaults to the `/tmp` folder, which the operating system periodically purges.

Retain Backup files

Check this box to retain the backup files of old keys and certificates, even after successfully deploying the new ones and restarting the server.

 Enabling this option requires entering a custom path in the **Backup path** field.

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.

 This password is typically the SSH password of the user selected in the **User** field.

**Mandatory:** When **Is sudo access required?** is checked,

Restart the Apache web server

**Yes** to restart the web server after pushing the certificate and the key, **No** otherwise.

HTTPS Port

The TLS port of the host machine.

 The standard TLS port is 443.

**Mandatory:** When **Restart the Apache server** is **Yes**.

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.

 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.

 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](#)
- [Backup path](#)
- [Retain Backup files](#)
- [Is sudo access required?](#)
- [Sudo password](#)
- [Restart the Nginx web server](#)
- [HTTPS Port](#)

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

#### Backup path

The folder to back up the certificate and the private key until they are successfully deployed.

- The certificate is backed up in the following file.

```
<backup-path>/<uuid>/backup/backup_cert_<YYYYMMDDHHMMSS>.pem
```

- The private key is backed up in the following file.

```
<backup-path>/<uuid>/backup/key_cert_<YYYYMMDDHHMMSS>.pem
```

Where:

- `<backup-path>` is the path entered in the **Backup path** field.
- `<uuid>` is a timestamp-based UUID that changes with each issuance backup.
- `<YYYYMMDDHHMMSS>` is a timestamp in `YYYYMMDDHHMMSS` format.

**Mandatory:** No. This optional parameter defaults to the `/tmp` folder, which the operating system periodically purges.

#### Retain Backup files

Check this box to retain the backup files of old keys and certificates, even after successfully deploying the new ones and restarting the server.

 Enabling this option requires entering a custom path in the **Backup path** field.

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.

 This password is typically the SSH password of the user selected in the **User** field.

**Mandatory:** When **Is sudo access required?** is checked,

Restart the Nginx web server

**Yes** to restart the web server after pushing the certificate and the key, **No** otherwise.

HTTPS Port

The TLS port of the host machine.

 The standard TLS port is 443.

**Mandatory:** When **Restart the Nginx server** is **Yes**.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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 <a href="#">Address Book</a> 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 <b>Owner</b> 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.



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 <a href="#">Address Book</a> 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.                                                            |

| Address Source    | Email addresses                                                            |
|-------------------|----------------------------------------------------------------------------|
| Certificate Owner | The email address configured in the <b>Owner</b> 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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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 <a href="#">global_admin</a> 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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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_111<br>4 | Events retention period set to <code>&lt;retention_period&gt;</code> days                                                              |
| AUDIT_111<br>5 | Reports settings updated. Retention period: <code>&lt;retention_period&gt;</code> , Copyright text <code>&lt;copyright_text&gt;</code> |
| AUDIT_111<br>6 | Plugin <code>&lt;plugin_name&gt;</code> updated. State set to <code>&lt;plugin_active_state&gt;</code>                                 |
| AUDIT_111<br>7 | Public Enrollment Forms <code>&lt;general_setting_enabled/disabled&gt;</code>                                                          |

| Audit Code | Log                                                                                     |
|------------|-----------------------------------------------------------------------------------------|
| AUDIT_1119 | Address <address_name> updated                                                          |
| AUDIT_1120 | Single address created: <address_name>                                                  |
| AUDIT_1121 | Mapped address created: <address_name>                                                  |
| AUDIT_1122 | List of addresses created: <address_name>                                               |
| AUDIT_1124 | Address deleted: <address_name>                                                         |
| AUDIT_1125 | Address <address_name> removed from rules                                               |
| AUDIT_1126 | Address <address_name> removed from schedules                                           |
| AUDIT_1127 | New addresses imported in list of address <address_name>                                |
| AUDIT_1128 | Imported single address <address_name>                                                  |
| AUDIT_1129 | Imported list of addresses <address_name>                                               |
| AUDIT_1168 | License with order number: <order_number> , Revision number: <revision_number> uploaded |
| AUDIT_1169 | License with order number: <order_number> , Revision number: <revision_number> updated. |
| AUDIT_1170 | Entitlement usage updated for <consumption_type> . Usage count: <usage_count>           |

## Authentication and authorization logs

The following logs record authentication and authorization events.

| Audit Code | Log                                                                                                                                                                                |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUDIT_1010 | Auth provider <code>&lt;auth_provider_name&gt;</code> registered                                                                                                                   |
| AUDIT_1011 | Auth provider <code>&lt;auth_provider_name&gt;</code> updated                                                                                                                      |
| AUDIT_1012 | LDAP login failed for user: <code>&lt;username&gt;</code>                                                                                                                          |
| AUDIT_1013 | LDAP login failed as user: <code>&lt;username&gt;</code> is not in the required group: <code>&lt;auth_provider_registration_group_name&gt;</code> , dn: <code>&lt;email&gt;</code> |
| AUDIT_1017 | API token created for user <code>&lt;username&gt;</code>                                                                                                                           |
| AUDIT_1018 | API token deleted for user <code>&lt;username&gt;</code>                                                                                                                           |
| AUDIT_1023 | Roles updated for user <code>&lt;username&gt;</code>                                                                                                                               |
| AUDIT_1030 | API token deleted for user <code>&lt;username&gt;</code>                                                                                                                           |
| AUDIT_1031 | API token updated for user <code>&lt;username&gt;</code>                                                                                                                           |
| AUDIT_1032 | All API tokens deleted for user <code>&lt;username&gt;</code>                                                                                                                      |
| AUDIT_1033 | All API tokens deactivated for user <code>&lt;username&gt;</code>                                                                                                                  |
| AUDIT_1036 | Created initial user with username: <code>&lt;username&gt;</code> .                                                                                                                |

| Audit Code | Log                                                                          |
|------------|------------------------------------------------------------------------------|
| 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_1042 | Updated user: <username> .                                                   |
| AUDIT_1043 | Updated LDAP user: <username> .                                              |
| AUDIT_1044 | Updated external user: <username> .                                          |
| AUDIT_1046 | Updated account password for user: <username> .                              |
| AUDIT_1047 | Updated last login for user: <username> .                                    |
| AUDIT_1048 | Successful login by User: <username> .                                       |
| AUDIT_1057 | Failed login attempt for user: <username>                                    |
| AUDIT_1058 | Failed login attempt for user: <username>                                    |
| AUDIT_1059 | Maximum login attempts exceeded. Rejected login attempt for user: <username> |

| Audit Code | Log                                                                                      |
|------------|------------------------------------------------------------------------------------------|
| AUDIT_1060 | Login denied. Tenant id not found for user <code>&lt;username&gt;</code>                 |
| AUDIT_1061 | Global role created: <code>&lt;role_name&gt;</code>                                      |
| AUDIT_1062 | Custom role created: <code>&lt;role_name&gt;</code>                                      |
| AUDIT_1063 | Custom role updated: <code>&lt;role_name&gt;</code>                                      |
| AUDIT_1064 | Authority role created: <code>&lt;role_name&gt;</code>                                   |
| AUDIT_1065 | Composite role created: <code>&lt;role_name&gt;</code>                                   |
| AUDIT_1066 | Role deleted: <code>&lt;role_name&gt;</code>                                             |
| AUDIT_1067 | Role updated: <code>&lt;role_name&gt;</code>                                             |
| AUDIT_1068 | Role <code>&lt;role_name&gt;</code> assigned to user <code>&lt;username&gt;</code> .     |
| AUDIT_1069 | Role <code>&lt;role_name&gt;</code> unassigned from user <code>&lt;username&gt;</code> . |
| AUDIT_1070 | Certificate role created: <code>&lt;role_name&gt;</code>                                 |
| AUDIT_1071 | Certificate role updated: <code>&lt;role_name&gt;</code>                                 |
| AUDIT_1092 | Failed login attempt for user: <code>&lt;username&gt;</code> . User is not active.       |

| Audit Code | Log                                        |
|------------|--------------------------------------------|
| AUDIT_1093 | Failed login attempt. User does not exist. |

#### Automation logs

The following logs record rule and report events.

| Audit Code | Log                                                                      |
|------------|--------------------------------------------------------------------------|
| AUDIT_1201 | <rule_type> Rule created: <rule_name>                                    |
| AUDIT_1205 | <rule_type> Rule updated: <rule_name>                                    |
| AUDIT_1209 | <rule_type> Rule deleted: <rule_name>                                    |
| AUDIT_1250 | Generated certificate report: <rule_name>                                |
| AUDIT_1251 | Created report: <rule_name>                                              |
| AUDIT_1252 | Updated report: <rule_name>                                              |
| AUDIT_1253 | Deleted report: <rule_name>                                              |
| AUDIT_1254 | Report Schedule <schedule_name> deleted                                  |
| AUDIT_1255 | Report Schedule <schedule_name> created for report <rule_name>           |
| AUDIT_1256 | Report Schedule <schedule_name> updated                                  |
| AUDIT_1257 | Delete report execution at <executed_at> for report <rule_name>          |
| AUDIT_1258 | Successfully renewed certificate <cert_name> (Serial Number: <cert_sn> ) |

#### Certificate logs

The following logs record certificate events.

| Audit Code | Log                                                                                                                                                                      |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUDIT_1434 | Certificate <code>&lt;cert_name&gt;</code> (Serial Number: <code>&lt;cert_sn&gt;</code> ) archived                                                                       |
| AUDIT_1435 | Certificate <code>&lt;cert_name&gt;</code> (Serial Number: <code>&lt;cert_sn&gt;</code> ) unarchived                                                                     |
| AUDIT_1436 | Certificate <code>&lt;cert_name&gt;</code> (Serial Number: <code>&lt;cert_sn&gt;</code> ) revoked                                                                        |
| AUDIT_1437 | Certificate <code>&lt;cert_name&gt;</code> (Serial Number: <code>&lt;cert_sn&gt;</code> ) released from hold                                                             |
| AUDIT_1472 | Custom Field created: <code>&lt;custom_field_name&gt;</code> .                                                                                                           |
| AUDIT_1473 | Custom Field deleted: <code>&lt;custom_field_name&gt;</code> .                                                                                                           |
| AUDIT_1474 | Custom Field updated: <code>&lt;custom_field_name&gt;</code> .                                                                                                           |
| AUDIT_1480 | Certificate exported: Common Name <code>&lt;cert_name&gt;</code> , Serial Number <code>&lt;decimal_cert_sn&gt;</code> , export type: <code>&lt;export_type&gt;</code>    |
| AUDIT_1491 | <code>&lt;number_of_updated_certs&gt;</code> certificates queued for bulk update.                                                                                        |
| AUDIT_1492 | New certificate issued by authority: <code>&lt;authority_name&gt;</code> . (Common Name: <code>&lt;cert_name&gt;</code> , Serial Number: <code>&lt;cert_sn &gt;</code> ) |
| AUDIT_1493 | Certificate <code>&lt;cert_name&gt;</code> (Serial Number: <code>&lt;cert_sn &gt;</code> ) updated                                                                       |
| AUDIT_1494 | Certificate <code>&lt;cert_name&gt;</code> (Serial Number: <code>&lt;decimal_cert_sn &gt;</code> ) imported                                                              |
| AUDIT_1498 | Certificate view <code>&lt;view_name&gt;</code> created.                                                                                                                 |
| AUDIT_1499 | Certificate view <code>&lt;view_name&gt;</code> updated.                                                                                                                 |
| AUDIT_1500 | Certificate view <code>&lt;view_name&gt;</code> deleted.                                                                                                                 |

#### Certificate policy logs

The following logs record Access Tags events.

| Audit Code | Log                                                                  |
|------------|----------------------------------------------------------------------|
| AUDIT_1481 | Certificate Access Tag <code>&lt;access_tag_name&gt;</code> created. |
| AUDIT_1482 | Certificate Access Tag <code>&lt;access_tag_name&gt;</code> updated. |
| AUDIT_1483 | Certificate Access Tag <code>&lt;access_tag_name&gt;</code> deleted. |

### Control logs

The following logs record events on authorities, key managers, and discovery scanners.

| Audit Code | Log                                                                                                                                                                                              |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUDIT_1301 | CA Gateway added: <code>&lt;cagw_name&gt;</code>                                                                                                                                                 |
| AUDIT_1302 | CA Gateway updated: <code>&lt;cagw_name&gt;</code>                                                                                                                                               |
| AUDIT_1303 | CA Gateway deleted: <code>&lt;cagw_name&gt;</code>                                                                                                                                               |
| AUDIT_1304 | Authority added: <code>&lt;auth_name&gt;</code>                                                                                                                                                  |
| AUDIT_1305 | Authority updated: <code>&lt;auth_name&gt;</code>                                                                                                                                                |
| AUDIT_1306 | Authority deleted: <code>&lt;auth_name&gt;</code>                                                                                                                                                |
| AUDIT_1371 | Successfully uploaded certificate with Private key Id: <code>&lt;priv_key_id&gt;</code> and Public key Id: <code>&lt;pub_key_id&gt;</code> to KMS using plugin: <code>&lt;plugin_name&gt;</code> |
| AUDIT_1375 | Key pair deactivated at Key Manager <code>&lt;plugin_name&gt;</code> , Private key id: <code>&lt;priv_key_id&gt;</code> , Public key id: <code>&lt;pub_key_id&gt;</code>                         |
| AUDIT_1376 | Verification request submitted for domain <code>&lt;domain_name&gt;</code> to authority <code>&lt;auth_name&gt;</code>                                                                           |



| Audit Code | Log                                                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| AUDIT_1377 | Key manager with plugin <code>&lt;plugin_name&gt;</code> created: <code>&lt;key_manager_name&gt;</code>                                           |
| AUDIT_1378 | Key manager updated: <code>&lt;key_manager_name&gt;</code>                                                                                        |
| AUDIT_1379 | Key manager deleted: <code>&lt;key_manager_name&gt;</code>                                                                                        |
| AUDIT_1382 | Status updated for domain <code>&lt;Domain name&gt;</code> from authority <code>&lt;auth_name&gt;</code>                                          |
| AUDIT_1383 | Re-verify request submitted for domain <code>&lt;domain_name&gt;</code> to authority <code>&lt;auth_name&gt;</code>                               |
| AUDIT_1384 | Discovery scanner added: <code>&lt;disco_agent_name&gt;</code>                                                                                    |
| AUDIT_1385 | Discovery scanner updated: <code>&lt;disco_agent_name&gt;</code>                                                                                  |
| AUDIT_1386 | Discovery scanner deleted: <code>&lt;disco_agent_name&gt;</code>                                                                                  |
| AUDIT_1387 | <code>&lt;num_of_disco_agent_scans&gt;</code> Scan configurations updated for discovery scanner <code>&lt;disco_agent_name&gt;</code>             |
| AUDIT_1388 | Discovery scanner <code>&lt;disco_agent_name&gt;</code> policy updated, new polling frequency: <code>&lt;disco_agent_poll_freq&gt;</code> seconds |

#### Destination logs

The following logs record destination events.

| Audit Code | Log                                                 |
|------------|-----------------------------------------------------|
| AUDIT_1495 | Destination <code>&lt;dest_name&gt;</code> created. |
| AUDIT_1496 | Destination <code>&lt;dest_name&gt;</code> updated. |

| Audit Code | Log                                                 |
|------------|-----------------------------------------------------|
| AUDIT_1497 | Destination <code>&lt;dest_name&gt;</code> deleted. |

#### Public form logs

The following logs record Public Enrollment Form events.

| Audit Code | Log                                                                                                                                                                    |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUDIT_1504 | Public form <code>&lt;pub_form_name&gt;</code> created.                                                                                                                |
| AUDIT_1505 | Public form <code>&lt;pub_form_name&gt;</code> updated.                                                                                                                |
| AUDIT_1506 | Public form <code>&lt;pub_form_name&gt;</code> deleted.                                                                                                                |
| AUDIT_1507 | Certificate request (ID: <code>&lt;cert_request_id&gt;</code> ) of requester <code>&lt;requester&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> ) is rejected.         |
| AUDIT_1508 | Certificate request (ID: <code>&lt;cert_request_id&gt;</code> ) of requester <code>&lt;requester&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> ) is approved.         |
| AUDIT_1509 | Certificate request (ID: <code>&lt;cert_request_id&gt;</code> ) of requester <code>&lt;requester&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> ) is already approved. |
| AUDIT_1510 | Certificate request (ID: <code>&lt;cert_request_id&gt;</code> ) of requester <code>&lt;requester&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> ) is already rejected. |
| AUDIT_1511 | Error rejecting certificate request (ID: <code>&lt;cert_request_id&gt;</code> ) of requester <code>&lt;requester&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> ).     |
| AUDIT_1512 | Error approving certificate request (ID: <code>&lt;cert_request_id&gt;</code> ) of requester <code>&lt;requester&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> ).     |
| AUDIT_1513 | New Certificate request created.                                                                                                                                       |

| Audit Code | Log                                                                                                                                                                                                                                           |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUDIT_1514 | Certificate request (ID: <code>&lt;cert_request_id&gt;</code> ) of requester <code>&lt;requester&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> ) is cancelled.                                                                               |
| AUDIT_1515 | New Certificate request created with key algorithm <code>&lt;key_alg&gt;</code> , key size <code>&lt;Key size&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> )                                                                                |
| AUDIT_1516 | New Certificate request created key algorithm <code>&lt;key_alg&gt;</code> , (IP: <code>&lt;remote_ip&gt;</code> )                                                                                                                            |
| AUDIT_1517 | New Certificate request created with key algorithm <code>&lt;key_alg&gt;</code> , OID <code>&lt;pub_key_info_alg&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> ).                                                                            |
| AUDIT_1518 | Deleted <code>&lt;num_cert_requests_deleted&gt;</code> certificate requests last modified <code>&lt;cert_request_retention&gt;</code> days ago.                                                                                               |
| AUDIT_1519 | Certificate request (ID: <code>&lt;cert_request_id&gt;</code> ) of requester <code>&lt;requester&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> ) with CA side key generation (profile: <code>&lt;profile_id&gt;</code> is marked approved.   |
| AUDIT_1520 | Certificate request (ID: <code>&lt;cert_request_id&gt;</code> ) of requester <code>&lt;requester&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> ) is already issued.                                                                          |
| AUDIT_1521 | Pkcs12 for Certificate Request (ID: <code>&lt;cert_request_id&gt;</code> ) of requester <code>&lt;requester&gt;</code> (IP: <code>&lt;remote_ip&gt;</code> ) with CA side key generation (profile: <code>&lt;profile_id&gt;</code> is issued. |

#### Source logs

The following logs record source events.

| Audit Code | Log                                                                                           |
|------------|-----------------------------------------------------------------------------------------------|
| AUDIT_1501 | Source deleted: <code>&lt;source_name&gt;</code>                                              |
| AUDIT_1502 | Source with plugin <code>&lt;plugin_name&gt;</code> created: <code>&lt;source_name&gt;</code> |
| AUDIT_1503 | Source updated: <code>&lt;source_name&gt;</code>                                              |

## 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.



Column headers display a sorting icon when the column values can be sorted with a click.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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                      | <code>&lt;ca&gt;_admin</code> 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           | The <code>&lt;ca&gt;</code> authority only. |
|              | Adding authorities             | ✗                                           |
|              | Editing an authority           | The <code>&lt;ca&gt;</code> authority only. |
|              | Deleting authorities           | The <code>&lt;ca&gt;</code> authority only. |
| Key Managers | Browsing key managers          | Only own-created.                           |
|              | Creating a key manager         | ✓                                           |

| Menu option             | Operation                               | <ca>_admin permissions                                    |
|-------------------------|-----------------------------------------|-----------------------------------------------------------|
|                         | 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. |
|                         | 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.           |

| Menu option         | Operation                         | <ca>_admin permissions                          |
|---------------------|-----------------------------------|-------------------------------------------------|
|                     | 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. |
|                     | 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          | ✗                                                                            |
|                   | 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 <code>&lt;ca&gt;</code> authority. |
|                   | Creating a rule            | Only rules for certificates issued by the <code>&lt;ca&gt;</code> authority. |
|                   | Editing a rule             | Only rules for certificates issued by the <code>&lt;ca&gt;</code> authority. |
|                   | Deleting rules and actions | Only rules for certificates issued by the <code>&lt;ca&gt;</code> 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 <code>&lt;ca&gt;</code> authority. |
|             | Creating a report | ✗                                                                             |

| Menu option      | Operation                     | <ca>_admin permissions                                     |
|------------------|-------------------------------|------------------------------------------------------------|
|                  | Editing a report              | Only reports on certificates issued by the <ca> authority. |
|                  | 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   | ✓                      |
|                | Creating an administrator | ✗                      |
|                | Editing an administrator  | ✗                      |
|                | Deleting administrators   | ✗                      |

| Menu option             | Operation                         | <ca>_admin permissions                                                                    |
|-------------------------|-----------------------------------|-------------------------------------------------------------------------------------------|
| 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 <a href="#">Certificate Roles</a> for issuing certificates with the <ca> authority.  |
|                         | Creating a role                   | Only a <a href="#">Certificate Role</a> for issuing certificates with the <ca> authority. |
|                         | Editing a role                    | Only <a href="#">Certificate Roles</a> for issuing certificates with the <ca> authority.  |
|                         | Deleting roles                    | Only <a href="#">Certificate Roles</a> for issuing certificates with the <ca> authority.  |

| Menu option | Operation         | <ca>_admin permissions |
|-------------|-------------------|------------------------|
| 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            | ✓                        |
|                         | 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 | ✗                        |



| Menu option             | Operation                               | global_admin permissions |
|-------------------------|-----------------------------------------|--------------------------|
|                         | 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            | ✓                        |
|                         | Revoking a certificate                  | ✗                        |
|                         | Releasing a certificate from hold       | ✗                        |
|                         | Exporting a certificate                 | ✓                        |
|                         | Importing certificates                  | ✓                        |
|                         | Archiving certificates                  | ✓                        |
| Endpoints               | Browsing Endpoints                      | ✓                        |

| Menu option         | Operation                        | global_admin permissions |
|---------------------|----------------------------------|--------------------------|
| 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       | ✓                        |
|                   | 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        | ✓                        |

| Menu option | Operation                  | global_admin permissions |
|-------------|----------------------------|--------------------------|
|             | 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      | ✓                        |
|                  | 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                | ✓                        |
|                         | 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                   | ✓                        |

| Menu option | Operation         | global_admin permissions |
|-------------|-------------------|--------------------------|
|             | 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 | ✗                    |

| Menu option             | Operation                               | Operator permissions |
|-------------------------|-----------------------------------------|----------------------|
|                         | 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.    |
| 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 | ✗                    |

| Menu option             | Operation                               | Operator permissions |
|-------------------------|-----------------------------------------|----------------------|
|                         | 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            | ✗                    |
|                         | 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                    | ✗                    |

| Menu option | Operation                | Operator permissions |
|-------------|--------------------------|----------------------|
|             | 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.    |
|                   | 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.    |
| 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   | ✗                    |

| Menu option             | Operation                         | Operator permissions |
|-------------------------|-----------------------------------|----------------------|
| 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                    | ✗                    |
|                         | Creating a role                   | ✗                    |
|                         | Editing a role                    | ✗                    |
| Settings                | General                           | ✗                    |
|                         | Identity Provider                 | ✗                    |
|                         | Reports                           | ✗                    |

| Menu option | Operation               | Operator permissions |
|-------------|-------------------------|----------------------|
|             | <a href="#">License</a> | ✗                    |
|             | <a href="#">Plugins</a> | ✗                    |

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

1. 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](#).
2. Go to **Administer > Roles**.
3. Click **Create**.
4. In the **Name** field, enter a unique name for the role.
5. In the **Description** field, enter an optional description of the role purpose.
6. 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 <a href="#">Certificates</a> .                                                                                                                                                             |
| Requestor | Create certificate requests as explained in <a href="#">Making a certificate request</a> .                                                                                                        |
| Approver  | Approve certificate requests as explained in <a href="#">Approving a pending certificate request</a> , or manage public forms as explained in <a href="#">Creating a public enrollment form</a> . |

### 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.

**i** 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.

 Column headers display a sorting icon when the column values can be sorted with a click.

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. |

| Field    | Application license                                                                                                                   | Plugin license                  |
|----------|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| 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 <a href="#">Creating a destination</a> .                       |
| Key Management | Integrate key managers, as explained in <a href="#">Creating a key manager</a> .                                               |
| Notification   | Send notifications triggered by <a href="#">Rules and Actions</a> , <a href="#">Report Schedules</a> and certificate requests. |
| Source         | Integrate certificate sources, as explained in <a href="#">Creating a source</a> .                                             |

## 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>&lt;Username&gt;</code> |

| Code         | Message                                                                                                                               |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------|
| ERR_101<br>0 | <code>hasPermission</code> unexpectedly invoked for <code>&lt;Permission&gt;</code>                                                   |
| ERR_101<br>1 | The util command must have a <code>--cmd</code> argument.                                                                             |
| ERR_101<br>2 | Unknown command <code>&lt;Command&gt;</code>                                                                                          |
| ERR_101<br>3 | <code>--username</code> , <code>--password</code> , and <code>--email</code> must be supplied to the <code>createUser</code> command. |
| ERR_101<br>4 | Unexpected crypto error:                                                                                                              |
| ERR_101<br>5 | Error creating default cert expiry rule for initial user:                                                                             |
| ERR_101<br>6 | <code>--username</code> and <code>--role</code> must be provided.                                                                     |
| ERR_101<br>7 | Unexpected crypto exception:                                                                                                          |
| ERR_104<br>0 | Unexpected parsing error while loading auth request:                                                                                  |
| ERR_104<br>1 | Unexpected parsing error while saving auth request:                                                                                   |
| ERR_104<br>2 | Unexpected parsing error while removing auth request:                                                                                 |
| ERR_104<br>6 | Could not find password auth provider entry.                                                                                          |
| ERR_104<br>7 | Failed to hash the password for user: <code>&lt;Username&gt;</code>                                                                   |
| ERR_104<br>8 | Cannot update non-existent user. User must have existing id.                                                                          |

| Code         | Message                                                                                                                                      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_104<br>9 | Login denied. Tenant id not found for user <code>&lt;Username&gt;</code> .                                                                   |
| ERR_105<br>6 | More than one LDAP auth provider registration found ( <code>&lt;Number of registrations&gt;</code> ).<br>Unexpected behavior may result!     |
| ERR_105<br>7 | More than one PASSWORD auth provider registration found ( <code>&lt;Number of registrations&gt;</code> ).<br>Unexpected behavior may result! |
| ERR_107<br>6 | Unable to create keystore: <code>&lt;CA&gt;</code>                                                                                           |
| ERR_107<br>7 | Cryptography issue when creating user.                                                                                                       |
| ERR_107<br>8 | Cryptographic error processing password.                                                                                                     |
| ERR_107<br>9 | Unable to initialize SSLContext for LDAPS                                                                                                    |
| ERR_108<br>0 | More that one LDAP auth provider registration present. Unexpected results may occur.                                                         |
| ERR_108<br>1 | LDAP authentication error.                                                                                                                   |
| ERR_108<br>2 | Unexpected exception during LDAP lookup.                                                                                                     |
| ERR_108<br>3 | Error closing LDAP context.                                                                                                                  |
| ERR_108<br>4 | Could not find Active Directory user.                                                                                                        |
| ERR_108<br>5 | Error creating the daemon user:                                                                                                              |

| Code         | Message                          |
|--------------|----------------------------------|
| ERR_108<br>6 | Error creating the initial user: |

## Certificate Manager administration errors

The application throws the following administration errors.

| Code         | Message                                                                                                            |
|--------------|--------------------------------------------------------------------------------------------------------------------|
| ERR_11<br>00 | Internal error occurred                                                                                            |
| ERR_11<br>01 | Error parsing license : <Error message>                                                                            |
| ERR_11<br>02 | Error parsing license: Epm client could not parse license                                                          |
| ERR_11<br>03 | Error parsing license : <Error message>                                                                            |
| ERR_11<br>04 | Error parsing license: Epm client could not parse license                                                          |
| ERR_11<br>05 | Order Number of <Order number> uploaded license doesn't match the existing license<br><Customer contact reference> |
| ERR_11<br>06 | License revision <Revision> already uploaded.                                                                      |
| ERR_11<br>07 | Uploaded license revision <Uploaded revision> is outdated. Current license revision :<br><Current revision>.       |
| ERR_11<br>08 | Failed to create the license expiry schedule                                                                       |
| ERR_11<br>09 | Failed to send email for license consumption                                                                       |

| Code         | Message                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------|
| ERR_11<br>10 | Failed to send email for license expiry                                                                                                |
| ERR_11<br>11 | Failed to check the license expiry schedule                                                                                            |
| ERR_11<br>12 | Failed to delete existing license expiry schedule                                                                                      |
| ERR_11<br>13 | Failed to create the license expiry schedule                                                                                           |
| ERR_11<br>14 | Invalid plugin name: <Plugin name>                                                                                                     |
| ERR_11<br>15 | Error executing plugin options for plugin: <Plugin name>                                                                               |
| ERR_11<br>16 | Error loading plugin jar <JAR file name> . Plugin will not be loaded!                                                                  |
| ERR_11<br>17 | Error loading plugin classloader.                                                                                                      |
| ERR_11<br>18 | Plugin <Canonical name> is missing a language bundle. Plugin will not be loaded!                                                       |
| ERR_11<br>19 | Plugin <Canonical name> has invalid language bundle. No messages section found. Plugin will not be loaded!                             |
| ERR_11<br>20 | Plugin <Canonical name> has invalid language bundle. No languages found. Plugin will not be loaded!                                    |
| ERR_11<br>21 | Plugin <Canonical name> has an invalid language bundle. Language <Key> is an invalid map. Plugin will not be loaded!                   |
| ERR_11<br>22 | Plugin <Canonical name> has an invalid language bundle. Language <Name> , key <Key> is invalid ( <Value> ). Plugin will not be loaded! |

| Code         | Message                                                                                                                                  |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_11<br>23 | Error initializing plugins! No <code>&lt;Plugin class name&gt;</code> plugins will be loaded until invalid plugin is removed!            |
| ERR_11<br>24 | updatePlugin: Error converting global options to Json string from list                                                                   |
| ERR_11<br>25 | validatePluginStateUpdate : cannot deactivate plugins that don't require license                                                         |
| ERR_11<br>26 | validatePluginStateUpdate : cannot deactivate plugin <code>&lt;Name&gt;</code> as its in use by destination : <code>&lt;Label&gt;</code> |
| ERR_11<br>27 | validatePluginStateUpdate : cannot deactivate plugin <code>&lt;Name&gt;</code> as its in use by source : <code>&lt;Label&gt;</code>      |
| ERR_11<br>28 | addPlugin: Error converting global options to Json string from list                                                                      |
| ERR_11<br>29 | Error converting global options to list from <code>Json byte[]</code>                                                                    |
| ERR_11<br>30 | addPlugin: Error converting global options to list from <code>Json byte[]</code>                                                         |
| ERR_11<br>31 | Error fetching language bundle, Plugin <code>&lt;Plugin name&gt;</code> not found                                                        |
| ERR_11<br>32 | Failed to add an entry to the keystore: <code>&lt;TBU&gt;</code>                                                                         |
| ERR_11<br>33 | Plugin update failed, plugin ID <code>&lt;Plugin ID&gt;</code>                                                                           |
| ERR_11<br>49 | Failed importing multiple addresses.                                                                                                     |
| ERR_11<br>50 | Failed importing single addresses.                                                                                                       |

| Code         | Message                                                 |
|--------------|---------------------------------------------------------|
| ERR_11<br>53 | Failed to check the events retention schedule: <Error>  |
| ERR_11<br>54 | Failed to create the events retention schedule: <Error> |
| ERR_11<br>99 | Unhandled exception caught                              |

## Certificate Manager automation errors

The application throws the following automation errors.

| Code         | Message                                                                             |
|--------------|-------------------------------------------------------------------------------------|
| ERR_12<br>07 | Failed to mapping existing source plugin options.                                   |
| ERR_12<br>08 | Failed to process existing source plugin options.                                   |
| ERR_12<br>09 | Failed to migrate existing source plugin options.                                   |
| ERR_12<br>14 | Failed to send email for report <Report name> , schedule id: <Schedule ID> . Error: |
| ERR_12<br>15 | Failed to generate missing report: <Report ID>                                      |
| ERR_12<br>16 | Failed to generate missing schedule: <Schedule ID>                                  |
| ERR_12<br>17 | Failed to return report: <Report ID> . Error: <Error>                               |
| ERR_12<br>18 | Error while retrieving report data:                                                 |
| ERR_12<br>19 | Error while generating report:                                                      |



| Code         | Message                                                                                                                                                                              |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_12<br>20 | User <code>&lt;Username&gt;</code> does not have permission to edit or delete report <code>&lt;Report name&gt;</code>                                                                |
| ERR_12<br>21 | Error while generating report: <code>&lt;Error&gt;</code>                                                                                                                            |
| ERR_12<br>22 | User <code>&lt;Username&gt;</code> does not have permission to access artifact <code>&lt;Artifact ID&gt;</code>                                                                      |
| ERR_12<br>23 | User <code>&lt;Username&gt;</code> does not have permission to access execution <code>&lt;Execution ID&gt;</code>                                                                    |
| ERR_12<br>24 | Failed to check the reports retention schedule: <code>&lt;Error&gt;</code>                                                                                                           |
| ERR_12<br>25 | Failed to create the reports retention schedule: <code>&lt;Error&gt;</code>                                                                                                          |
| ERR_12<br>30 | Field ' <code>&lt;Name&gt;</code> ' value ' <code>&lt;Value&gt;</code> ' cannot be parsed as <code>&lt;Type&gt;</code> . Field will be treated as a String.                          |
| ERR_12<br>31 | Unexpected exception while processing rule. RULE WILL BE SKIPPED!                                                                                                                    |
| ERR_12<br>32 | Expiry notification is dropped for certificate <code>&lt;Certificate name&gt;</code> . The address field <code>&lt;Address field&gt;</code> is empty.                                |
| ERR_12<br>33 | Expiry notification is dropped for certificate <code>&lt;Certificate name&gt;</code> . The address field <code>&lt;Address field&gt;</code> is not referring to a text custom field. |
| ERR_12<br>34 | Action plugins not currently supported. THIS ACTION WILL BE SKIPPED!                                                                                                                 |
| ERR_12<br>35 | Exception while executing rule. RULE WILL BE SKIPPED!                                                                                                                                |
| ERR_12<br>36 | Error running rules engine for certificate renewal rule.                                                                                                                             |

| Code         | Message                                                                                   |
|--------------|-------------------------------------------------------------------------------------------|
| ERR_12<br>37 | Execution of action failed.                                                               |
| ERR_12<br>38 | FAILED processing conditions. RULE WILL BE SKIPPED!                                       |
| ERR_12<br>39 | I/O issue while parsing conditions. RULE WILL BE SKIPPED!                                 |
| ERR_12<br>40 | Error running rules engine for event.                                                     |
| ERR_12<br>41 | Could not parse plugin config, ACTION WILL BE SKIPPED: <code>&lt;Plugin config&gt;</code> |
| ERR_12<br>42 | FAILED to create the expiration rules schedule! Expiry notifications will not be sent!    |
| ERR_12<br>43 | Error while processing event rule conditions. RULE WILL BE SKIPPED!                       |
| ERR_12<br>44 | Only NOTIFICATION actions are supported! ACTION WILL BE SKIPPED!                          |
| ERR_12<br>54 | Unexpected IOException while formatting the certificate. Error:                           |
| ERR_12<br>55 | Unexpected IOException while formatting the certificate chain. Error:                     |
| ERR_12<br>56 | Unexpected IOException while formatting the certificate. Error:                           |
| ERR_12<br>60 | FAILED to create the key manager scan schedule! Key managers will not be scanned!         |
| ERR_12<br>61 | Error encountered while scanning key manager.                                             |
| ERR_12<br>62 | Error encountered while scanning source.                                                  |

| Code     | Message                                                                                                                                               |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_1271 | User <code>&lt;User ID&gt;</code> does not have permission to view, edit or delete destination <code>&lt;Label&gt;</code>                             |
| ERR_1272 | Error verifying destination config <code>&lt;Label&gt;</code>                                                                                         |
| ERR_1273 | Error verifying destination config for plugin <code>&lt;Plugin name&gt;</code>                                                                        |
| ERR_1274 | Error while generating report.                                                                                                                        |
| ERR_1275 | Failed to retrieve schedule runtimes for <code>&lt;Schedule name&gt;</code>                                                                           |
| ERR_1276 | Failed to parse schedule runtimes for <code>&lt;Schedule name&gt;</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>&lt;Certificate name&gt;</code> . The address field <code>&lt;Address field&gt;</code> is empty. |
| ERR_1290 | Error running rules engine for certificate renewal rule.                                                                                              |
| ERR_1291 | Failed processing rule. RULE WILL BE SKIPPED!                                                                                                         |

| Code         | Message                                                                                                                                                                              |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_12<br>92 | I/O issue while running rule. RULE WILL BE SKIPPED!                                                                                                                                  |
| ERR_12<br>93 | Expiry notification is dropped for certificate <code>&lt;Certificate name&gt;</code> . The custom field <code>&lt;Custom field&gt;</code> is empty.                                  |
| ERR_12<br>94 | Expiry notification is dropped for certificate <code>&lt;Certificate name&gt;</code> . The address field <code>&lt;Address field&gt;</code> is not referring to a text custom field. |
| ERR_12<br>95 | Expiry notification is dropped for certificate <code>&lt;Certificate name&gt;</code> . The address field <code>&lt;Address field&gt;</code> is empty.                                |
| ERR_12<br>96 | Error running rules engine for certificate renewal rule.                                                                                                                             |
| ERR_12<br>99 | 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>&lt;Error&gt;</code> :\n <code>&lt;Response body&gt;</code> |

| Code     | Message                                                                                   |
|----------|-------------------------------------------------------------------------------------------|
| ERR_1309 | Error while uploading certificate: <Error>                                                |
| ERR_1310 | Unable to parse properties for domain: <Domain name>                                      |
| ERR_1311 | User <User ID> doesn't have access to authority <Authority ID>                            |
| 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: <Error>                                                 |
| ERR_1330 | User <User ID> does not have permission to view, edit or delete key manager <Key manager> |
| ERR_1331 | Error verifying key manager config <Key manager label>                                    |
| 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 <Plugin name>                               |
| ERR_1349 | Failed to sync domains, Error from CAGW: <Error>                                          |
| ERR_1350 | Unexpected response received from CAGW                                                    |
| ERR_1351 | Internal error contacting CAGW                                                            |
| ERR_1352 | Unexpected response received from CAGW: <Error>                                           |
| ERR_1353 | Unexpected response received from CAGW: <Error>                                           |

| Code     | Message                                                                            |
|----------|------------------------------------------------------------------------------------|
| ERR_1354 | Unexpected response received from CAGW: <Error>                                    |
| 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: <Certificate validity period> |
| ERR_1363 | Error parsing authority certificate validity period: <Certificate validity period> |
| 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> :                      |

| Code     | Message                                                                                                                                     |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_1384 | Error response from CAGW while getting domain: <code>&lt;Domain name&gt;</code>                                                             |
| ERR_1385 | Failed to get domain. Error from CAGW: <code>&lt;Error&gt;</code>                                                                           |
| ERR_1386 | Failed to submit domain, Error from CAGW: <code>&lt;Error&gt;</code>                                                                        |
| ERR_1387 | Unable to fetch whois record from server <code>&lt;Server name&gt;</code> . Error:                                                          |
| ERR_1388 | Unable to close whois client connection with server <code>&lt;Server name&gt;</code> . Error:                                               |
| ERR_1389 | Unable to fetch whois record from default host. Error:                                                                                      |
| ERR_1390 | Unable to close whois client connection with default server. Error:                                                                         |
| ERR_1392 | Error on DNS lookup : <code>&lt;Error&gt;</code>                                                                                            |
| ERR_1394 | Failed to submit domain, Error from CAGW: <code>&lt;Error&gt;</code>                                                                        |
| ERR_1397 | Certificate Authority <code>&lt;Authority ID&gt;</code> not found                                                                           |
| ERR_1398 | Unable to parse plugin options for authority <code>&lt;Authority ID&gt;</code>                                                              |
| ERR_1399 | Unable to import/update domain id <code>&lt;Domain ID&gt;</code> due to Json parsing error from authority <code>&lt;Authority ID&gt;</code> |

## 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 <code>&lt;Certificate ID&gt;</code> . |

| Code         | Message                                                                                                                                                                                          |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_1<br>428 | Automated renewal failed for certificate <code>&lt;Certificate ID&gt;</code> due to certificate processing error                                                                                 |
| ERR_1<br>430 | Automated renewal failed for certificate <code>&lt;Certificate ID&gt;</code> due to destination errors: <code>&lt;List of errors&gt;</code>                                                      |
| ERR_1<br>431 | Failed to find the renewal daemon user for auto renewal                                                                                                                                          |
| ERR_1<br>432 | Failed to create the renewal schedule for cert <code>&lt;Certificate serial&gt;</code> : <code>&lt;Error&gt;</code>                                                                              |
| ERR_1<br>433 | Failed to check the renewal schedule <code>&lt;Error&gt;</code>                                                                                                                                  |
| ERR_1<br>434 | Failed to create the renewal schedule <code>&lt;Error&gt;</code>                                                                                                                                 |
| ERR_1<br>435 | Adding definition for custom field with duplicate display order : <code>&lt;Label&gt;</code> of type <code>&lt;Type&gt;</code> at position <code>&lt;Display order&gt;</code>                    |
| ERR_1<br>436 | Deleting definition for custom field with Id : <code>&lt;Metadata ID&gt;</code> failed as it is in use by <code>&lt;Certificates using metadata&gt;</code> certificates                          |
| ERR_1<br>437 | Updating definition for custom field with duplicate display order : <code>&lt;Label&gt;</code> of type <code>&lt;Type&gt;</code> at position <code>&lt;Display order&gt;</code>                  |
| ERR_1<br>438 | Updating definition for custom field with Id : <code>&lt;Metadata ID&gt;</code> failed as it is in use by <code>&lt;Certificates using metadata&gt;</code> certificates                          |
| ERR_1<br>439 | Updating definition for custom field with duplicate display order : <code>&lt;Metadata values&gt;</code>                                                                                         |
| ERR_1<br>440 | Other certificate custom field definitions exists with same display order <code>&lt;List&gt;</code>                                                                                              |
| ERR_1<br>441 | Updating definition for custom field with Id : <code>&lt;Metadata ID&gt;</code> failed as one of its value <code>&lt;List&gt;</code> is in use by <code>&lt;Certificates&gt;</code> certificates |



| Code         | Message                                                                                                                                 |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| ERR_1<br>442 | Error parsing the value <code>&lt;Value&gt;</code> for custom field <code>&lt;Metadata ID&gt;</code>                                    |
| ERR_1<br>443 | Unsupported Operator <code>&lt;Operator&gt;</code> for custom field Id: <code>&lt;Metadata ID&gt;</code>                                |
| ERR_1<br>450 | Could not unarchive certificate because entitlement limit reached.                                                                      |
| ERR_1<br>452 | Error response from CAGW <code>&lt;Error&gt;</code>                                                                                     |
| ERR_1<br>453 | Error exporting a certificate: <code>&lt;Error&gt;</code>                                                                               |
| ERR_1<br>454 | Failed to parse certificate <code>&lt;Certificate name&gt;</code> stored in DB. Error: <code>&lt;Error&gt;</code>                       |
| ERR_1<br>455 | Certificate Chain is not available for export                                                                                           |
| ERR_1<br>456 | Error while exporting certificate: <code>&lt;Error&gt;</code>                                                                           |
| ERR_1<br>457 | Error saving chain to keystore for export of: <code>&lt;Certificate name&gt;</code>                                                     |
| ERR_1<br>458 | Error adding P12 to response stream                                                                                                     |
| ERR_1<br>459 | Unable to parse response from CAGW to export certificate for: <code>&lt;Certificate name&gt;</code> . Error: <code>&lt;Error&gt;</code> |
| ERR_1<br>460 | Certificate can not be exported since the issuing Authority is not known                                                                |
| ERR_1<br>461 | Certificate Authority not found                                                                                                         |

| Code         | Message                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_1<br>462 | Error adding P12 to response stream                                                                                                                                                                                                    |
| ERR_1<br>463 | Unexpected response received from CAGW when exporting a certificate                                                                                                                                                                    |
| ERR_1<br>464 | Internal error contacting CAGW                                                                                                                                                                                                         |
| ERR_1<br>465 | Failed to export certificate for <code>&lt;Certificate name&gt;</code> . Error from CAGW: <code>&lt;Error&gt;</code>                                                                                                                   |
| ERR_1<br>466 | Failed to export certificate for <code>&lt;Certificate name&gt;</code> with serial number <code>&lt;Certificate serial number&gt;</code> . Certificate key is not backed up.                                                           |
| ERR_1<br>467 | Unable to parse response from CAGW to export certificate for : <code>&lt;Certificate name&gt;</code> . Error: <code>&lt;Error&gt;</code>                                                                                               |
| ERR_1<br>468 | Export private key is not supported for export type <code>&lt;Type&gt;</code> You can uncheck <code>\\\\"Include Private Key\\\\"</code> and try again, however, your exported certificate will not have the private key               |
| ERR_1<br>469 | Export certificate chain is not supported for export type <code>&lt;Type&gt;</code> You can uncheck <code>\\\\"Include Certificate Chain\\\\"</code> and try again, however, your exported certificate will not have certificate chain |
| ERR_1<br>470 | Public certificate must be requested for export type <code>&lt;Type&gt;</code>                                                                                                                                                         |
| ERR_1<br>471 | At least one of public certificate, certificate chain or private key must be requested for export type <code>&lt;Type&gt;</code>                                                                                                       |
| ERR_1<br>472 | At least one of public certificate, certificate chain or private key must be requested for export type <code>&lt;Type&gt;</code>                                                                                                       |
| ERR_1<br>473 | Unable to revoke the authority <code>&lt;Authority name&gt;</code>                                                                                                                                                                     |
| ERR_1<br>474 | Unable to unhold the authority <code>&lt;Authority name&gt;</code>                                                                                                                                                                     |

| Code         | Message                                                                                                                                                  |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERR_1<br>477 | Error building certificate query with filter : <code>&lt;Filter&gt;</code> . Error <code>&lt;Error&gt;</code>                                            |
| ERR_1<br>478 | Error fetching certificates with predicate : <code>&lt;Predicate&gt;</code> . Error <code>&lt;Error&gt;</code>                                           |
| ERR_1<br>479 | Certificate Bulk Edit Error: 'certificatesFilter' missing from request body                                                                              |
| ERR_1<br>480 | Certificate Bulk Edit Error: If 'clearOutAccessTags' is set, 'accessTags' must be empty.                                                                 |
| ERR_1<br>481 | Certificate Bulk Edit Error: No updated values provided                                                                                                  |
| ERR_1<br>482 | Certificate Bulk Edit Error building certificate query with filter : <code>&lt;Filter&gt;</code> , Error : <code>&lt;Error&gt;</code> .                  |
| ERR_1<br>483 | Certificate Bulk Edit Error building certificate query with filter : <code>&lt;Filter&gt;</code> , Error : <code>&lt;Error&gt;</code> .                  |
| ERR_1<br>484 | Certificate Bulk Edit Error updating certificates with filter : <code>&lt;Filter&gt;</code> , Error : <code>&lt;Error&gt;</code>                         |
| ERR_1<br>486 | Certificate unhold error : Could not find certificate with id: <code>&lt;Certificate ID&gt;</code> .                                                     |
| ERR_1<br>487 | Certificate unhold error : No Authority Id associated with this certificate: <code>&lt;Certificate ID&gt;</code> .                                       |
| ERR_1<br>488 | Certificate unhold error : Cannot unhold certificate <code>&lt;Certificate ID&gt;</code> . Authority is not active : <code>&lt;Authority ID&gt;</code> . |
| ERR_1<br>489 | Certificate unhold error : Cannot unhold certificate <code>&lt;Certificate ID&gt;</code> . No external id found.                                         |
| ERR_1<br>490 | Issue certificate error : Subject DN is required for CSR.                                                                                                |

| Code         | Message                                                                                                         |
|--------------|-----------------------------------------------------------------------------------------------------------------|
| ERR_1<br>491 | Issue certificate error : CAGW failed to create certificate for authority <Authority ID>                        |
| ERR_1<br>492 | Issue certificate error : CAGW Failed to create certificate: <Key manager ID> .                                 |
| ERR_1<br>493 | Issue certificate error : Subject DN is required for CSR.                                                       |
| ERR_1<br>494 | Issue certificate error : Subject DN is required for CSR.                                                       |
| ERR_1<br>495 | Issue certificate error : Subject DN is required for CSR.                                                       |
| ERR_1<br>496 | Issue certificate error : Subject DN is required for CSR.                                                       |
| ERR_1<br>497 | Failed to save certificate: <Error>                                                                             |
| ERR_1<br>498 | Failed to upload certificate to the key manager <Key manager ID> . Error <Error>                                |
| ERR_1<br>499 | Certificate revoke error : No Authority Id associated with this certificate. <Certificate ID>                   |
| ERR_1<br>500 | Certificate revoke error : Cannot revoke certificate <Certificate ID> . Authority <Authority ID> is not active. |
| ERR_1<br>501 | Certificate revoke error : Cannot revoke certificate <Certificate ID> . No external id found.                   |
| ERR_1<br>502 | Failed to apply service-level filters on query <Filter>                                                         |
| ERR_1<br>503 | Failed to apply service-level filters on query <Filter>                                                         |
| ERR_1<br>504 | Failed to apply service-level filters on query <Filter>                                                         |

| Code         | Message                                                                                                            |
|--------------|--------------------------------------------------------------------------------------------------------------------|
| ERR_1<br>505 | Could not find certificate with id <Certificate ID>                                                                |
| ERR_1<br>506 | Could not find certificate with id <Certificate ID>                                                                |
| ERR_1<br>508 | Failed to issue a certificate from authority <Authority name> . Error <Error>                                      |
| ERR_1<br>509 | Failed to parse the X509 certificate <Certificate body> \n Message: <Error>                                        |
| ERR_1<br>510 | Unable to find certificate <Certificate ID>                                                                        |
| ERR_1<br>511 | Failed to process the certificate <Certificate import request body> \n Message: <Error>                            |
| ERR_1<br>512 | Failed to process the certificate <Certificate body> \n External ID: <Certificate External ID> \n Message: <Error> |
| ERR_1<br>513 | Failed to apply service-level filters on query <Filter>                                                            |
| ERR_1<br>514 | Failed to run the certificate count query: <Error>                                                                 |
| ERR_1<br>521 | Error verifying source config <Source Label>                                                                       |
| ERR_1<br>522 | Error verifying source config for plugin <Plugin name>                                                             |
| ERR_1<br>523 | addOrUpdateSource: Error converting plugin options to Json string from list                                        |
| ERR_1<br>524 | Error scheduling source sync, sources will not ne scanned!                                                         |

| Code         | Message                                                                                                            |
|--------------|--------------------------------------------------------------------------------------------------------------------|
| ERR_1<br>525 | Error creating certificate from certificate request                                                                |
| ERR_1<br>526 | Failed to send new external certificate request notification to approver(s). Error : <Notification message>        |
| ERR_1<br>527 | Failed to send external certificate request cancellation notification to requestor. Error : <Notification message> |
| ERR_1<br>528 | Failed to send certificate request approval notification to requestor. Error : <Notification message>              |
| ERR_1<br>529 | Failed to send certificate request rejection notification to requestor. Error : <Notification message>             |
| ERR_1<br>530 | Failed to send new certificate request notification to internal requestor. Error : <Notification message>          |
| ERR_1<br>531 | Failed to send new internal certificate request notification to approver(s). Error : <Notification message>        |
| ERR_1<br>533 | Failed to send new certificate request notification to external requestor. Error: <Notification message>           |
| ERR_1<br>534 | CSR key algorithm <CSR key algorithm> does not match the required key algorithm <Allowed key algorithm>            |
| ERR_1<br>536 | CSR key algorithm keysize <CSR key size> does not meet minimum public key size required : <Allowed key size>       |
| ERR_1<br>537 | Invalid certificate signing request provided                                                                       |
| ERR_1<br>540 | Failed to send new certificate request notification to external requestor. SMTP Notification Plugin not found      |

| Code         | Message                                                                                                                   |
|--------------|---------------------------------------------------------------------------------------------------------------------------|
| ERR_1<br>541 | Failed to send certificate request cancellation notification to external requestor. SMTP Notification Plugin not found    |
| ERR_1<br>542 | Failed to send new external certificate request notification to approver(s). SMTP Notification Plugin not found           |
| ERR_1<br>543 | Failed to send new certificate request notification to admin. SMTP Notification Plugin not found                          |
| ERR_1<br>544 | Failed to send new internal certificate request notification to approver(s). SMTP Notification Plugin not found           |
| ERR_1<br>545 | Failed to send notification for certificate request cancellation. SMTP Notification Plugin not found                      |
| ERR_1<br>546 | Failed to send notification for certificate request approval. SMTP Notification Plugin not found                          |
| ERR_2<br>010 | Found invalid certificate with name <code>&lt;Certificate name&gt;</code> .                                               |
| ERR_2<br>011 | Unexpected exception while processing certificate.                                                                        |
| ERR_2<br>012 | Error processing certificate.                                                                                             |
| ERR_2<br>013 | Error creating certificate factory.                                                                                       |
| ERR_2<br>015 | Failed to parse certificate <code>&lt;Certificate name&gt;</code> stored in DB. Error: <code>&lt;Error message&gt;</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       | <code>kubectl</code>                                                                                                                                |
| NAMESPACE     | <code>certhub</code>                                                                                                                                |
| POSTGRES_DB   | <code>certhub</code>                                                                                                                                |
| POSTGRES_PWD  | The value of the <b>Database User Password</b> configuration parameter described in <a href="#">Configuring and deploying Certificate Manager</a> . |
| POSTGRES_USER | The value of the <b>Database User Name</b> configuration parameter described in <a href="#">Configuring and deploying Certificate Manager</a> .     |

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.

## 11 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 <a href="#">Administrating nShield HSM integration</a> |
| 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.

- [Generating a timestamping key pair](#)
- [Issuing a timestamping certificate](#)

## 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 RSA3072 -s "CN=TSA" -o /tmp/certreq.txt -t mytoken -v
thales
Created key with id 4a00a4617d1afd5ad626955132dd0d396a69ed24
```

```
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIICqDCCAACAQAwMzExMC8GA1UEAxMoNGEwMGE0NjE3ZDFhZmQ1YWQ2MjY5NTUx
...
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.

## Issuing a timestaping 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 <a href="#">Generating a timestamping key pair</a> 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-----
MIIICDCCBliAwIBAgITMwEf/Fvr7NDwanyeRAAAAR/8WzANBgkqhkiG9w0BAQwF
ADBdMQswCQYDVQQGEwJVUzEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmlF0aW9u
...
Ud085g==
-----END CERTIFICATE-----
```

4. Use this certificate file as the [TSA certificate](#) when configuring the solution.

## Configuring and deploying Timestamping Authority

See below for configuring and deploying Timestamping Authority with the Management Console.

 Do not forget to also click **Deploy** after each update of the configuration or the license file.

### To configure and deploy Timestamping Authority with the Management Console

1. Open the following URL in a Web browser.

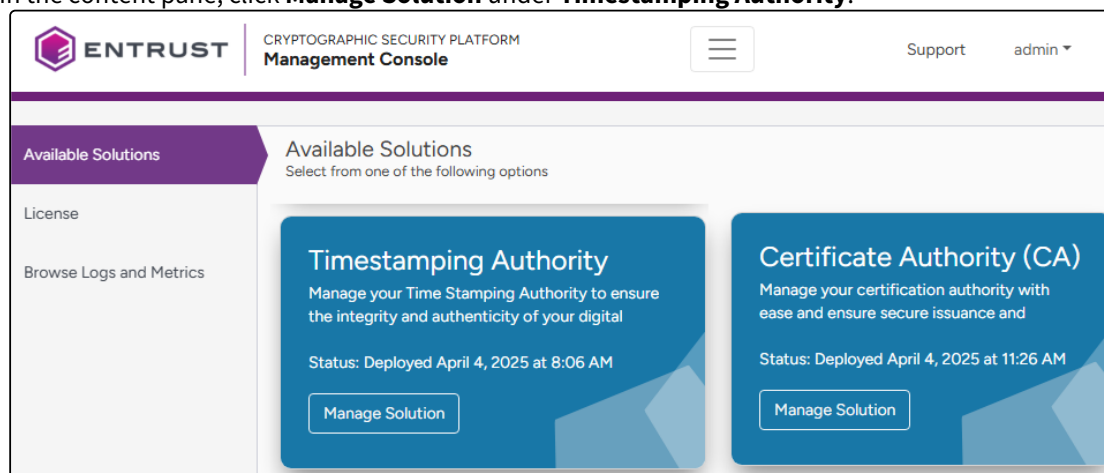
```
https://<machine>/management-console
```

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

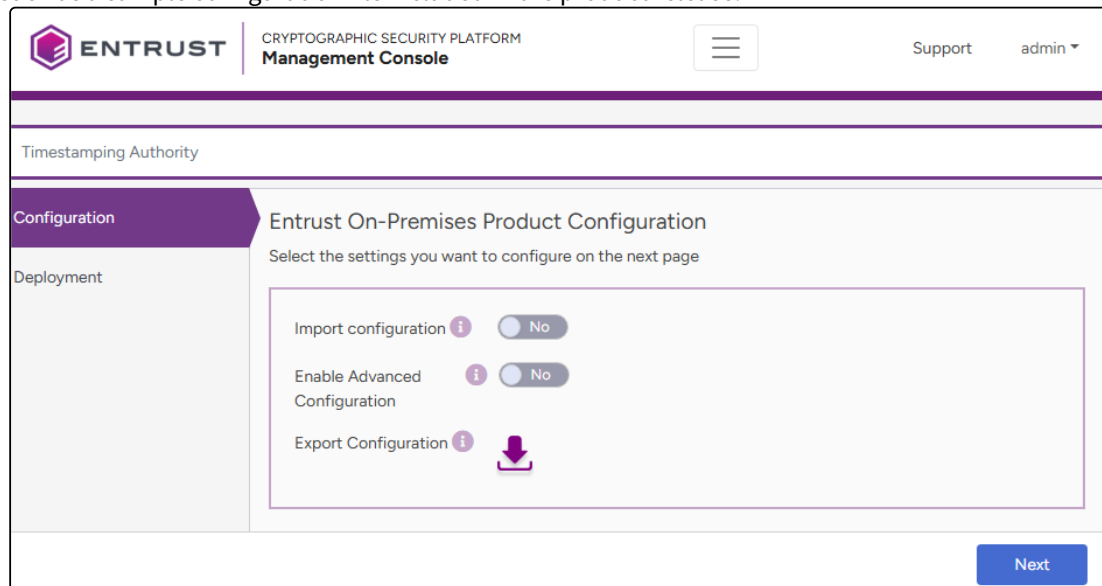
2. Log into the Management Console a user belonging to a role with Timestamping Authority management permissions – for example, the initial `admin` administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

3. In the content pane, click **Manage Solution** under **Timestamping 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.
  - [Hsm](#)
  - [Tsa Server](#)
  - [Clock service](#)
  - [Tsa issuers](#)
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**.

## 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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> for the supported models.  |

 It is recommended to select a Hardware Security Module (HSM).

**Mandatory:** Yes.

### 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`.

### 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`.

### Tsa Server

Select the **Tsa server** tab of the **Configuration** page to configure the below timestamping server settings.

- [Read timeout](#)
- [Write timeout](#)
- [Idle timeout](#)
- [Max header bytes](#)
- [Max body bytes](#)
- [Graceful timeout](#)
- [Listen limit](#)
- [Keep alive](#)

**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.

 This value must equal or exceed 4096.

**Mandatory:** No. This optional value defaults to 4096.

### 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.

## Clock service

Select the **Clock server** tab of the **Configuration** page to configure the clock service settings.

- [Maximum allowed error](#)
- [Poll interval](#)
- [Connection timeout](#)

**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.

### Poll interval

The period between successive connections to the [chrony](#) client for checking the clock health.

**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.

## Tsa issuers

Select the **TSA issuers** tab of the **Configuration** page to configure at least one timestamp issuer.

- [Issuer ID](#)
- [Log timestamp response](#)
- [TSA certificate](#)
- [CA chain](#)

- [TST profile](#)

**Mandatory:** Yes.

### 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.

### 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).

### 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.

### 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.

### TST profile

Configure the timestamping policy for generating timestamp responses.

- [Policy ID](#)
- [Allowed hash algorithms](#)
- [Accuracy](#)
- [Ordering](#)
- [Qualified timestamp extension](#)
- [Signature digest algorithm](#)
- [Serial number length](#)

**Mandatory:** Yes.

#### Policy ID

The identifier of the timestamping policy.

**Mandatory:** Yes.

#### 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

#### 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.

#### 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.

#### 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).

#### 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".

#### 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.

## 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>&lt;file&gt;</code> file.                        |
| -sha256      | Use the SHA256 algorithm to hash the data.                                                            |
| -cert        | Add to the response the certificate described in <a href="#">Issuing a timestamping certificate</a> . |
| -out <file>  | Save the generated request in the <code>&lt;file&gt;</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 tsaresp.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 `tsaresp.tsr` file.

## Parsing the timestamp response

Parse the timestamp response to validate the format.

```
openssl ts -reply -in tsaresp.tsr -text
```

## Verifying the response against the data

Verify the timestamp response against the original data.

```
openssl ts -verify -in tsaresp.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 tsaresp.tsr -CAfile ca.pem -queryfile tsareq.tsq
```

## 12 Managing Validation Authority

See below for configuring, deploying, and administering the Validation Authority solution.

- [Validation Authority overview](#)
- [Loading the HSM configuration on Validation Authority](#)
- [Initializing the Validation Authority database](#)
- [Configuring a certificate information source for CSP 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](#)

### 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](#)
- [Hardware Security Module](#)
- [Database](#)

**i** As explained in [Managing Certificate Authority](#), the Certificate Authority solution provides built-in CRL and OCSP services. Therefore, you do not need a Validation Authority for CAs created with this solution.

### 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). The following methods are supported for obtaining this information:

- The Entrust CA Gateway API.
- A full or "combined" CRL published in an LDAP or HTTP server. Validation Authority does not support partitioned CRLs.

**i** Entrust CA is currently the only issuing Certificate Authority supported by Validation Authority.

### 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](#).

**i** Skip this step if you use software cryptography (not recommended).

| HSM                 | Command                            | Additional steps                                          |
|---------------------|------------------------------------|-----------------------------------------------------------|
| Entrust nShield HSM | <code>evactl import-nshield</code> | See <a href="#">Adminstrating nShield HSM integration</a> |
| Thales HSM          | <code>evactl import-thales</code>  | —                                                         |

## 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](https://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 CSP 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](#), you will select the certificate information source using the [Certificates Source](#) parameter.

 For any of the supported information sources described below, Entrust CA is currently the only supported issuing Certificate Authority.

## 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-----
MIICqDCCAZACAQAwMzExMC8GA1UEAxMoNGEwMGE0NjE3ZDFhZmQ1YWQ2MjY5NTUx
...
etTv+pac+nJKW8fw
-----END CERTIFICATE REQUEST-----
```

 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.

 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 <a href="#">Generating a VA key pair</a> as a single line.           |
| 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-----
MIIIcDCCBliGAwIBAgITMwEf/Fvr7NDwanyeRAAAAR/8WzANBgkqhkiG9w0BAQwF
ADBdMQswCQYDVQQGEwJVUzEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmlF0aW9u
...
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.

 Do not forget to also click **Deploy** after each update of the configuration or the license file.

### To configure and deploy Validation Authority with the Management Console

1. Open the following URL in a Web browser.

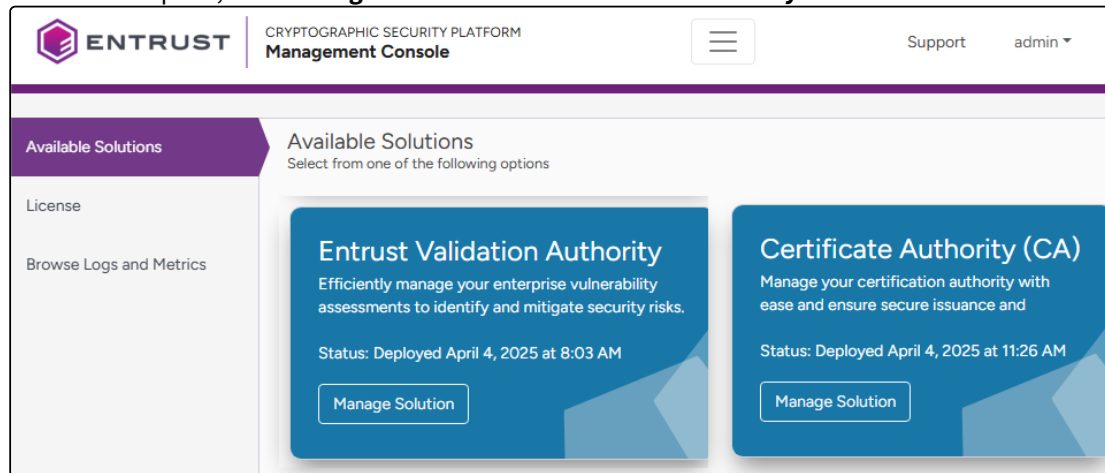
```
https://<machine>/management-console
```

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

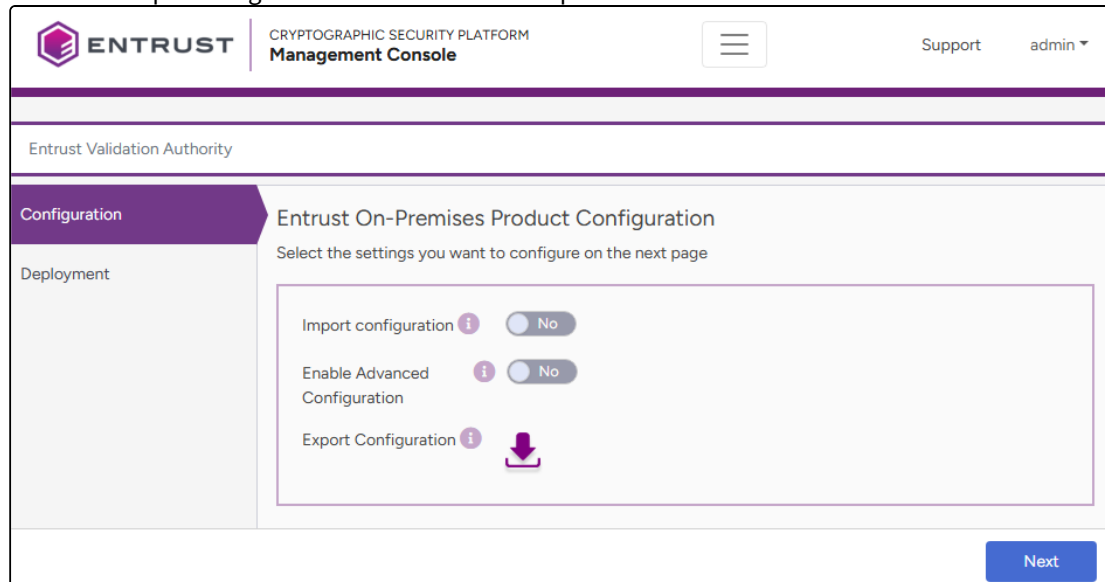
2. Log into the Management Console a user belonging to a role with Validation Authority management permissions – for example, the initial `admin` administrator user.

 See [Starting up the Management Console](#) for how to manage users and roles.

3. In the content pane, click **Manage Solution** under **Validation 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](#)
  - [OCSP 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 | ✗             | ✗    | ✗    | ✓        |

| Driver    | Database name | Host | Port | JDBC URL |
|-----------|---------------|------|------|----------|
| 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 requirements](#), 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 <b>Select Files</b> to import a file containing this certificate in PEM format and Base64 encoding. |
| oracle   | enabled  | Use the Oracle utilities to set this certificate.                                                         |

| Driver    | SSL mode | SSL validation certificate                                                                                |
|-----------|----------|-----------------------------------------------------------------------------------------------------------|
| sqlserver | enabled  | Click <b>Select Files</b> 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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> 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](#)
- [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.

 This value must equal or exceed 4096.

**Mandatory:** No. This optional value defaults to 4096.

### 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.

### 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               |                                     | <input checked="" type="checkbox"/> |
| revoked            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 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](#)
- [Response Hash Algorithm](#)

### VA certificate

The certificate described in [Generating a VA 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.

### CA certificate

Click **Select Files** to import the certificate of the CA that issues the certificates validated by Entrust Validation authority.

 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        |

| Profile identifier             | Certificates Source | Use SN Lists |
|--------------------------------|---------------------|--------------|
| CRLProfileWithArchiveCutOff    | CRL                 | False        |
| SNListProfile                  | CRL                 | True         |
| SNListProfileWithArchiveCutOff | CRL                 | True         |

**Mandatory:** Yes.

#### Response Hash Algorithm

The hash algorithm for the OCSP response signature algorithm. Supported values are the following.

- sha256
- sha384
- sha512

**Mandatory:** No. This optional value defaults to sha256.

## 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 ocp -issuer <ca_cert> -serial <sn> -url <url> -VAfile <va_cert>
```

For example:

```
$ openssl ocp -issuer issuer.pem -serial 0x000000002439fa8f5fe6370bb20ccb2556da6991
-url http://10.1.141.37/eva -VAfile ./VAFfile.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.

## 13 Managing Log Forwarder

Cryptographic Security Platform provides the Log Forwarder solution for forwarding logs to a SIEM (Security Information and Event Management) server.

### To configure and deploy the Log Forwarder solution

1. Open the following URL in a Web browser.

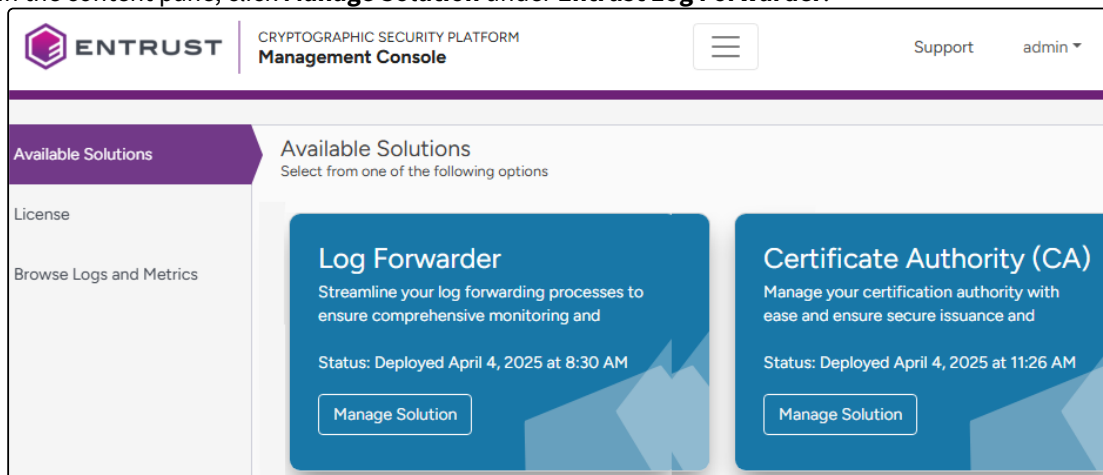
```
https://<machine>/management-console
```

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

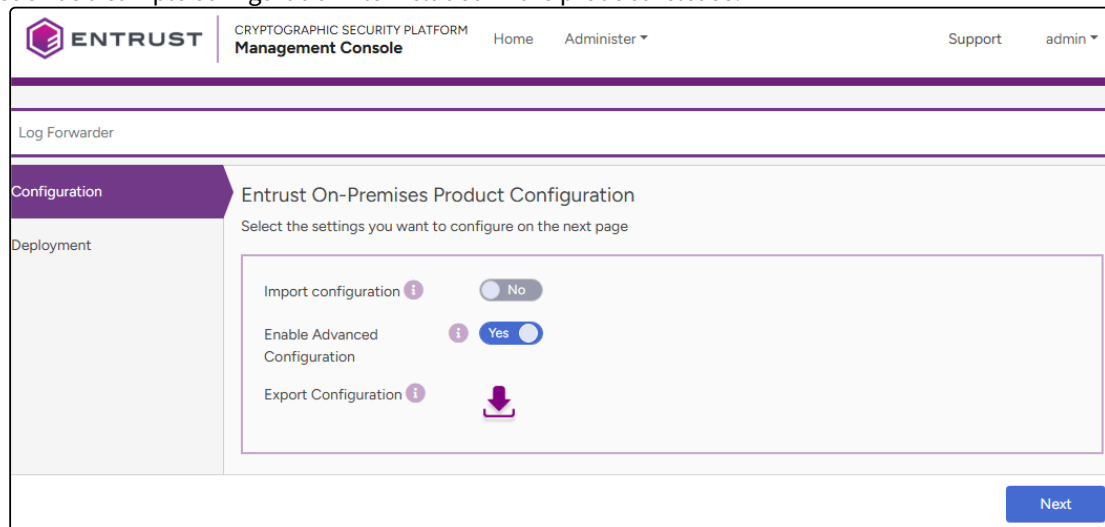
2. Log into the Management Console a user belonging to a role with Log Forwarder management permissions – for example, the initial `admin` administrator user.

 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](#)
- [Transport](#)
- [Syslog Format](#)

## Type

The type of SIEM server.

| Type   | SIEM server                              |
|--------|------------------------------------------|
| Splunk | Splunk Cloud to Splunk Enterprise server |
| Syslog | Syslog server                            |

 See [SIEM requirements](#) for the supported SIEM servers.

**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:** When [Type](#) is `Splunk`.

## Transport

The transport mode for connecting to the external SIEM service. Supported values are the following.

- TCP
- UDP

**Mandatory:** When [Type](#) is `Syslog`.

## Syslog Format

The Syslog protocol format for connecting to the external SIEM service. Supported values are the following.

- RFC3164
- RFC5424

**Mandatory:** When [Type](#) is `Syslog`.

## TLS

Configure the TLS security in communications with the external SIEM server.

- [Enabled](#)
- [Verify](#)
- [CA Certificate File](#)

**i** TLS security is not enabled for [Log Server](#) configurations with [Type](#) set to [Syslog](#) and [Transport](#) set to [UDP](#) .

### 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. When omitting this optional setting, the system certificates are used.

## 14 Upgrading

See below for how to upgrade your installation to Cryptographic Security Platform 1.1.0.

- [Upgrade requirements](#)
- [Upgrade process](#)
- [Supported commands during the upgrade](#)

### Upgrade requirements

Upgrading to Cryptographic Security Platform 1.1.0 requires the following installation.

| Version                               | Installation mode |
|---------------------------------------|-------------------|
| Cryptographic Security Platform 1.0.0 | prod_mode         |

**i** If you have a previous version, upgrade it to Cryptographic Security Platform 1.0.0 as explained in section **Upgrading** of the Cryptographic Security Platform 1.0.0 guide.

If the Validation Authority or Timestamp Authority solutions are already deployed in the upgraded installation, ensure the value of the following parameter equals or exceeds 4096.

| Solution               | Parameter        | Section                               |
|------------------------|------------------|---------------------------------------|
| Validation authority   | Max header bytes | <a href="#">OCSP Responder-Server</a> |
| Timestamping Authority | Max header bytes | <a href="#">Tsa Server</a>            |

### Upgrade process

See below for how to run the upgrade process.

#### To upgrade Cryptographic Security Platform 1.0.0 to 1.1.0

1. Follow the steps in [Downloading the installation files](#) to download the **PKI Hub 1.2.0 for VMWare vSphere, Hyper-V and Nutanix** file. You need this ISO image file to upgrade any installation, ISO-based or non-ISO-based.
2. Backup the installation state as explained in section [Backing up](#) of the Cryptographic Security Platform 1.0.0 guide.
3. Repeat the following steps on each Cryptographic Security Platform node.
  - a. Use an SFTP client to copy the Cryptographic Security Platform ISO image file to the `/home/sysadmin` node folder.
  - b. Run the `clusterctl upgrade` command and wait until completion (around 2 hours).
4. Reboot each node sequentially, with at least 15 minutes before each reboot.
5. Back up the installation state as explained in section [Backing up](#) of this guide.

## Supported commands during the upgrade

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`

## 15 Administrating

Cryptographic Security Platform supports the administration operations described below.

- [Administrating nShield HSM integration](#)
- [Checking the etcd database size](#)
- [Checking the node health](#)
- [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 node health

Run the following command to check the health of each node.

```
curl http://<ip>:15021/healthz/ready
```

Where:

- `<ip>` is the node IP address. See [clusterctl node info](#) for how to list the IP address of each node.
- 15021 is one of the ports listed in [Required ports for incoming traffic](#).

A response with the `HTTP 200 OK` code indicates the node is ready to receive incoming traffic.

## 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 ETCDCTL_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 ETCDCTL_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 ETCDCTL_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 ETCDCTL_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 |
| 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 <a href="#">Configuring the connection of an ISO installation</a> section of this guide.              |
| Amazon Web Services       | Refer to the <a href="https://docs.aws.amazon.com">docs.aws.amazon.com</a> product documentation.             |
| Azure                     | Refer to the <a href="https://learn.microsoft.com/azure">learn.microsoft.com/azure</a> 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
```

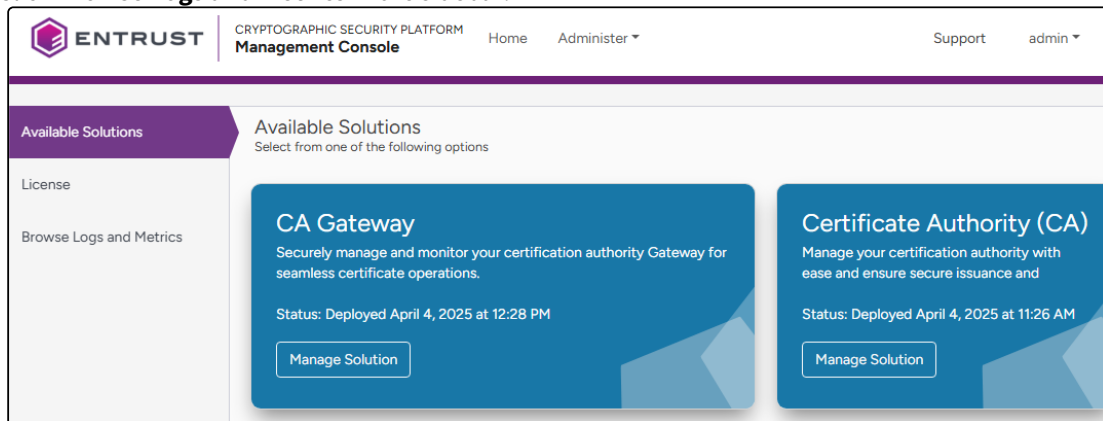
## 16 Browsing logs with Grafana

Cryptographic Security Platform provides a [Grafana](#) portal to browse logs and metrics on the internal services and the installed Entrust solutions.

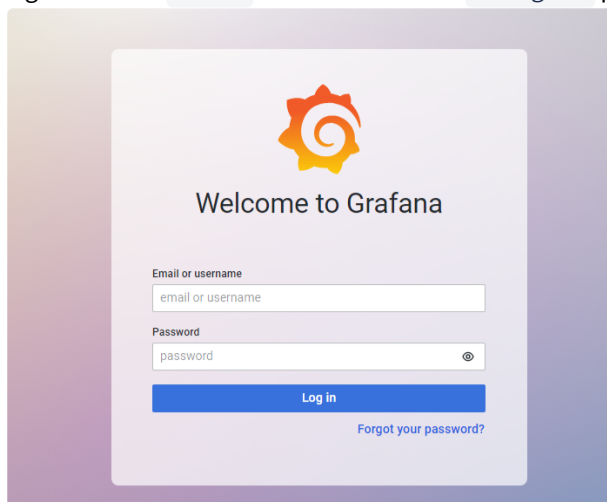
**i** See [Managing Log Forwarder](#) for how to forward logs to a SIEM (Security Information and Event Management) server.

### To manage logs with Grafana

1. Log in to 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/v12.0/administration/user-management>

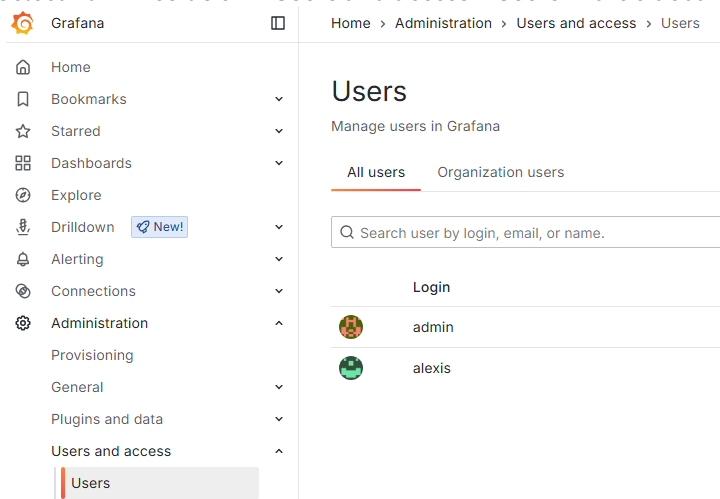
 The process described in [Backing up](#) does not include any Grafana configuration.

## 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 `changeme` password.
2. Select **Administration > Users and access > Users** in the sidebar.



3. Click on the pencil icon  of the **admin** user to edit the user details.
4. Click **Edit** in the **Password** row.
5. Type a new 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 `changeme` password.
2. Select **Administration > Users and access > Users** in the sidebar.
3. Click **New user**.
4. Fill in the **New user** form and click **Create User**.
5. In the user details view, click **Change** under **Permissions**.
6. Set **Grafana Admin** to **Yes**.
7. In the sidebar, select **Administration > Users and access > Users**.
8. In the **Users** grid, click the pencil icon  of the initial **admin** administrator.
9. In the user details view, click either:

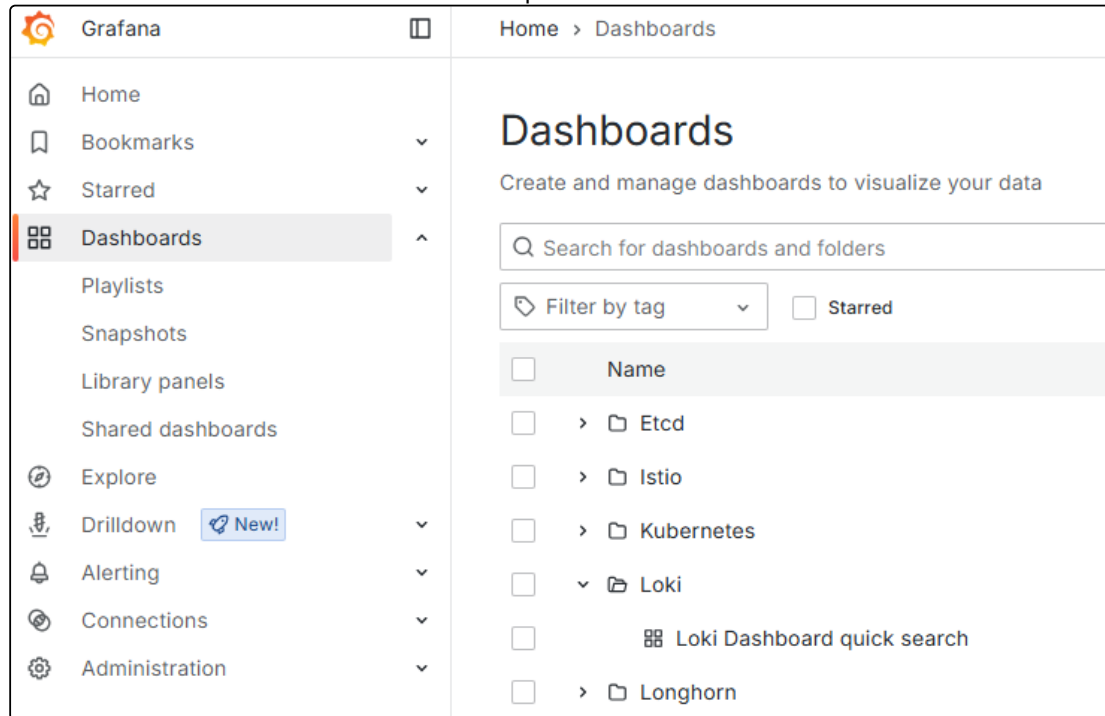
- **Delete user** to delete this initial administrator.
- **Disable user** to disable it.

## Browsing and exporting logs with the Grafana Loki Dashboard

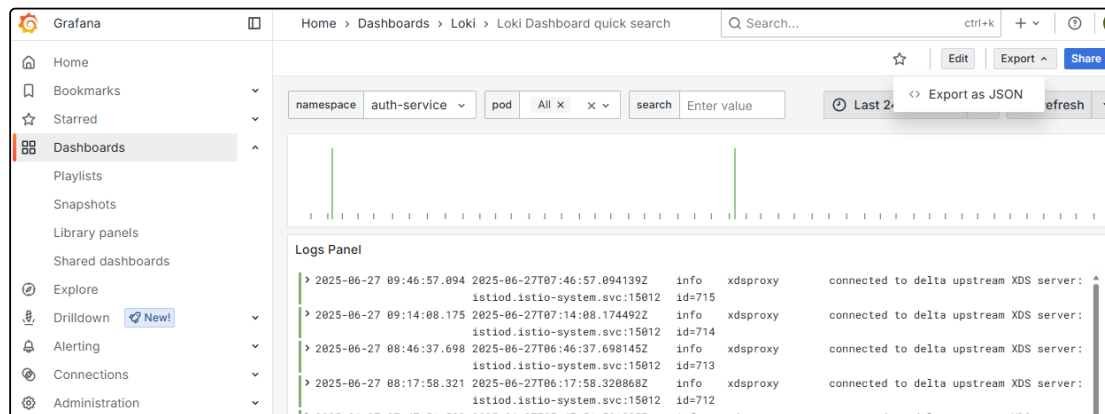
With the Grafana Loki Dashboard, users can browse and export logs of the Cryptographic Security Platform system and the deployed solutions.

### To browse and export logs with the Grafana Loki Dashboard

1. Click **Dashboards** in the sidebar of the Grafana portal.



2. Select **Loki > Loki Dashboard quick search** in the content pane.
3. Define a log query with the menu options.
  - [namespace](#)
  - [pod](#)
  - [search](#)
  - [Time range](#)



4. In the menu bar, select **Edit > Export as JSON**.
5. Click **Download 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.                                            |
| 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.                                     |

| Namespace          | Monitored service                                                             |
|--------------------|-------------------------------------------------------------------------------|
| 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

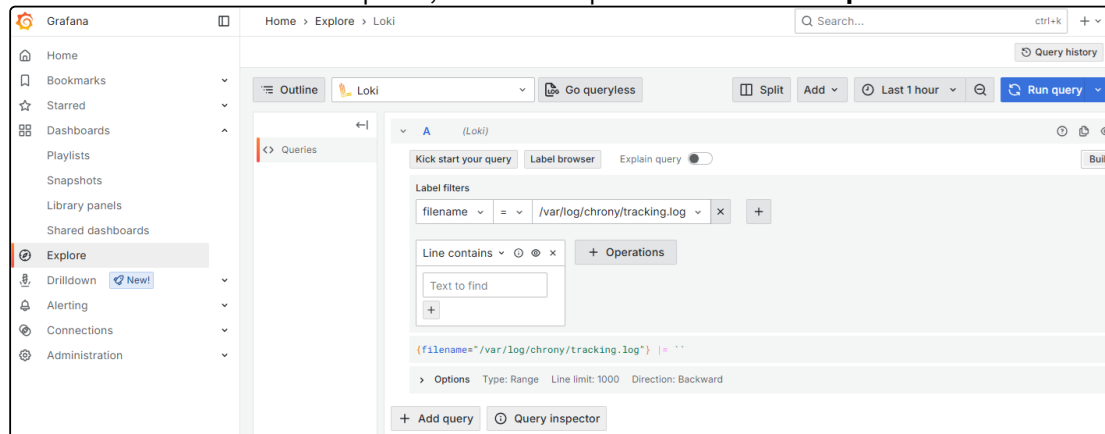
Click the clock icon in the top right menu and select the time range for querying logs.

## 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. |

| Select label | Select value      | Query output                         |
|--------------|-------------------|--------------------------------------|
| 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          | tts          | 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<br>" | Logs for failed timestamping requests.                                                                                                                          |
| "endpoint":"<issuerID>"              | Logs for timestamping requests received by the <issuerID> timestamp issuer, where <issuerID> is the value of the <a href="#">Issuer ID</a> 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 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
```

2. If the deployed solutions use databases, back up the database contents according to the instructions of the DBMS vendor.
3. 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.

4. 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 according to the instructions of the DBMS vendor.
5. 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.

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.

## 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 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 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.

3. If the solutions of the restored installation use databases, follow the instructions of the DBMS vendor to restore the database contents.
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 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.

3. If the solutions of the restored installation use databases, follow the instructions of the DBMS vendor to restore the database contents.
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**.

## 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
- clusterctl node user create
- clusterctl node user delete
- clusterctl node user info
- clusterctl node user modify
- 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 to a PEM file containing a private key. Supported key-generation algorithms are the following.

- RSA 2048 bits
- RSA 3072 bits
- RSA 4096 bits
- ECDSA curve NIST P-256

 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.                                                |
| Requirements              | Does not need the disk performance requirements described in <a href="#">Machine requirements</a> . Specifically, fsync latency is not an issue in this mode.                                             | All the <a href="#">Requirements</a> .                                 |
| Supported number of nodes | One                                                                                                                                                                                                       | One or more. See <a href="#">Required number of nodes</a> for details. |
| Supported operations      | You cannot perform the operations described in <a href="#">Joining nodes</a> , <a href="#">Backing up the state</a> , <a href="#">Recovering from disaster</a> , or <a href="#">Restoring the state</a> . | 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
```

 Each update of the license file requires redeploying the licensed solutions to be effective. You can use either the [clusterctl solution deploy](#) command or the management console to redeploy the solutions.

## 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 &lt;protocol&gt;</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 <user> and <pwd> as proxy basic authentication credentials |
| <user> |            | Prompt for the password of the <user> 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 --host <host> option only supports IP addresses |
| 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.

| --protocol | --certificate | Action                                                                       |
|------------|---------------|------------------------------------------------------------------------------|
| http       | <cert>        | Throw an error                                                               |
| http       |               | Set an HTTP connection                                                       |
| https      | <cert>        | Set an HTTPS connection with the <cert> 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.

 The root user owns the generated file, so you must change the file permissions to download it using SFTP.

**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.

 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.

i 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                            |
| 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.

 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>&lt;secret_id&gt;</code>    | The identifier of the secret | 3-128 characters in length, start with a letter, and contain only alphanumeric characters, underscores, and hyphens.                                                                                                                         |
| <code>&lt;secret_value&gt;</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.





| 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



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.



**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](https://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](#).

Upgrades a PKI Hub 1.1.0 installation to CSP 1.1.0.

```
clusterctl upgrade --iso-path <iso>
```

For example:

```
$ clusterctl upgrade --iso-path /home/sysadmin/pki-hub-1.1.0.iso
```

 If the installation meets all [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 1.1.0.

**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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> 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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> 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.

 The root user owns the generated file, so you must change the file permissions to download it using SFTP.

**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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> 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-----
MIICqDCCAACAQAwMzExMC8GA1UEAxMoNGEwMGE0NjE3ZDFhZmQ1YWQ2MjY5NTUx
...
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.

| <code>&lt;key_type&gt;</code> | Description            |
|-------------------------------|------------------------|
| RSA2048                       | RSA 2048 bits          |
| RSA3072                       | RSA 3072 bits          |
| RSA4096                       | RSA 4096 bits          |
| ECDSAP256                     | ECDSA curve NIST P-256 |
| ECDSAP384                     | ECDSA curve NIST P-384 |
| ECDSAP521                     | ECDSA curve NIST P-521 |

**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.

 The root user owns the generated file, so you must change the file permissions to download it using SFTP.

**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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> 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.

i 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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> 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.



The root user owns the generated file, so you must change the file permissions to download it using SFTP.

**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.



```
"DN": "subject=O = intcagwidp, OU = CAGW, serialNumber =
9979ec1454fe8dc70a78c77a1a1e78b6cfafde77"
},
{
 "ID": 2,
 "Cert":
"MIIEOjCCA4qgAwIBAgIQMVR8yW7+GCBca3lyRBSt3jANBgkqhkiG9w0BAQsFADBTMQswCQYDVQQGEwJFUzEc
MBoGA1UEChMTRW50cnVzdCBDb3Jwb3JhdGlvbWJlEiMCAGA1UECzMZQ2VydGlnaWNhdGlvb1BBdXRob3JpdGl1c
zEcMBoGA1UEAxMTSW50ZXJ1eWwgcQ0EgR2F0ZXdhcTAEFw0yMjA5MjMxNjU3MzBaFw0yNTA5MjMxNjU3MjlaMF
cxZzARBgNVBAoTCmludGNhZ3dpZHAxDTALBgNVBAsTBENBR1cxMTAvBgNVBAUTKDA3NzYyZW1MzdjYWJhYmY
1MGRiNTI3ODNhN2NmZU0N2EzYmYyYjMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvtsMW84yx
E5Ln6XMprAE6rvIApr0fevYqoaBI89gOdTyf6LSer0eSigVGr4TMvW6yhmfyZQKvBevP/
rK4pCB6mBoAiUTr5QF7HwBUJ0z4xbmiIxwhXIFcVNvXKnCekg3eHVS9DSHdjy4U/
Vt6tXSZmHkI1rZ1uEJweBWVlGp8MHU6Rot0mZFZ0ourxiHmRcD3s1DHXu6hADp54wHjGDET7V2WVPMKvcVAW
e+TgzAJcVpYBw07fj4kqER2Uml0T0PfjRtdTC9swxl30aC+UfmleAoBrSjWB+06lw60bp5oLlgPgIUD9R5fZ
osqPNbVfS5gs6/
Vo5BqfFcGIgmXVTAGMBAAGjggFSMIIBTjAMBGNVHRMBAf8EAjAAMB0GA1UdDgQWBBSk2b3+ZE3ZyIe4bTi3ph
Adv6jB0zAfBgNVHSMEGDAWgBQ4XuxK8LobB2x+dGs0jaQo0BHwzBLBggrBgEFBQcBAQQ/
MD0wOwYIKwYBBQUHMAAGGL2h0dHA6Ly9vY3NwLmRldi5wa2lodWlUy29tL29jc3AvZW50cnVzdC9pbmRjYWd3M
EYGA1UdHwQ/
MD0wO6A5oDeGNWh0dHA6Ly9jcmwuZGV2LnBraWh1Yi5jb20vY3JsL2VudHJ1c3QvaW50Y2Fndy9jcmwuY3JsM
EQGA1UdEQQ9MDuGOWlkcDovL2ludGNhZ3dpZHAxMDc3NjJlYzUzN2NhYmFiZjUwZGI1Mjc4M2E3Y2YzNTQ3YT
NiZjJiMzAoBgNVHQ8BAf8EBAMCB4AwEwYDVR0lBAwwCgYIKwYBBQUHAWIwDQYJKoZIhvcNAQELBQADggEBAFy
o2+QcxN4gN8XxhnErYQ3ET9kk5hrXUa+RGGctLiegINKX/
fxlG0V51QglvP4rFd12bnYCMqSQulq0H08m0E3U7wmKZem40Ml0Iffjp94RyDHaMnp0Wv9e4C6I6Q6nv4CX6nr
9TDmpIKG32c0kKu7veSZaLDBVA/Wg+W2ox6yf3W8PbPpUbf6Ld6UC/
gu0hzBMLqw8H+lq4WQs9KWcFFF5+XMm4y1Q38HIL0b0DBVpeib0QOono41mc9+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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> 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
```

 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.

```
pkc-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 1.1.0. See [Downloading the installation files](#) for how to download this file.

**Mandatory:** Yes.

### <license-path>

The path of the license file for CSP 1.1.0.

**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-----
MIIBIDCBxQIBADAzMTEwLwYDVQQDEyg3Y2U3OThjMTNhNDExYmMxZGE0YTlmOTgz
...
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.

 The root user owns the generated file, so you must change the file permissions to download it using SFTP.

**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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> 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 RSA3072 -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-----
MIICqDCCAACAQAwMzExMC8GA1UEAxMoNGEwMGE0NjE3ZDFhZmQ1YWQ2MjY5NTUx
...
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.

| <code>&lt;key_type&gt;</code> | Description            |
|-------------------------------|------------------------|
| RSA2048                       | RSA 2048 bits          |
| RSA3072                       | RSA 3072 bits          |
| RSA4096                       | RSA 4096 bits          |
| ECDSAP256                     | ECDSA curve NIST P-256 |
| ECDSAP384                     | ECDSA curve NIST P-384 |

| <key_type> | Description            |
|------------|------------------------|
| ECDSAP521  | ECDSA curve NIST P-521 |

**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.

 The root user owns the generated file, so you must change the file permissions to download it using SFTP.

**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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> 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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> 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.

## `clusterctl node user create`

Adds a user to the operating system of the node.

```
clusterctl node user create -u <username> [-p=<password>] [-k <authorized-keys>]
```

For example:

```
$ clusterctl node user create -u john -p='S!B*d$zDsb=' -k ~/.ssh/authorized_keys
User john created
```

Specifically:

- You can execute this command before [Installing CSP](#).
- You must repeat the command on all the installation nodes.
- The new user belongs to the same groups as the `sysadmin` user.

See below for a description of each parameter.

- `-u, --username <username>`
- `-p, --password=<password>`
- `-k, --authorized-keys <authorized-keys>`

**-u, --username <username>**

Set `<username>` as the name of the new operating system user.

**Exceptions:** The command throws an exception when an operating system user with the `<username>` name already exists on the node.

**Mandatory:** Yes.

**-p, --password=<password>**

Set `<password>` as the password of the new operating system user.

**Exceptions:** The command throws an exception when the password does not comply with the [Password policy CIS benchmarks](#).

❌ Enclose the password in quotes to escape special characters (such as `$`, `\`, `*`, `=`, and `!`) with a backlash ( `\` ) as in the above example.

**Mandatory:** No. When omitting this option, the command prompts for the password interactively.

**-k, --authorized-keys <authorized-keys>**

Import the user's public key for SSH authentication from the `<authorized-keys>` file path. For example:

```
~/ .ssh/authorized_keys
```

**Exceptions:** The command throws an exception when the key file has an invalid format.

**Mandatory:** No. When omitting this option, the user must use the password for SSH authentication.

## clusterctl node user delete

Deletes a user from the operating system of the node.

```
clusterctl node user delete -u <username> [--force]
```

For example:

```
$ clusterctl node user delete -u john
User john deleted
```

Specifically:

- You can only delete users created with the [clusterctl node user create](#) command.
- You can execute this command before [Installing CSP](#).
- You must repeat the command on all the installation nodes.
- Removed users can still run commands that do not require `sudo` if they have an ongoing session. However, once logged out, they are no longer authorized to re-login.

See below for a description of each parameter.

- `-u, --username <username>`
- `--force`

### `-u, --username <username>`

Delete the operating system user with the `<username>` name.

**Exceptions:** The command throws an error when:

- `<username>` corresponds to a user that cannot be deleted, like:
  - The `sysadmin` root user.
  - A system user created by the operating system to run services and daemons.
- No user with the `<username>` name exists in the node.

**Mandatory:** Yes.

### `--force`

Remove the user even if it has processes running (the processes continue until completion).

**Exceptions:** The command throws an exception when this flag is omitted and the user has running processes.

**Mandatory:** No.

## clusterctl node user info

List information on all operating system users in the node. That is:

- All users created with the `clusterctl node user create` command.
- All users created with the operating system tools.

For example:

```
$ sudo clusterctl node user info
Username: manually-user
Enabled: no
SSH password auth: no info
Authorized keys: not present

Username: cspadmin
Enabled: no
SSH password auth: yes
Authorized keys: Comment Type Fingerprint
 user-authentication ssh-rsa
LKBjXit1xwSHd7bHNHi3krGpkeD0kzT5P4BDYBlJlek=
 run-tests ssh-rsa
05ZQ4eETDaiHLMZVxc8cFIivYlsW1y2R1QDQuQf4ePU=

Username: sysadmin
Enabled: yes
SSH password auth: yes
Authorized keys: Comment Type Fingerprint
```



```

user-authentication ssh-rsa
tRdq4FmT1UUp3Ym0cY1lf6+IuvrJaN3gAgaxBNDufzY=
run-tests ssh-rsa
mGGT3xZTL8WKwQELPZlvgr4JHPwXo45AUaMHgsQq+LU=

```

See the table below for the listed information.

| User information  | Description                                                                                   | Available                                                                           |
|-------------------|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Username          | The name of the user                                                                          | On all types of users                                                               |
| Enabled           | <code>yes</code> if the user is enabled; <code>no</code> otherwise                            | On all types of users                                                               |
| SSH password auth | <code>yes</code> if the user has a password for SSH authentication; <code>no</code> otherwise | Only for users created with the <a href="#">clusterctl node user create</a> command |
| Authorized keys   | Details on the keys for SSH authentication, if any                                            | On all types of users                                                               |

## clusterctl node user modify

Modifies the settings of an operating system user.

```

clusterctl node modify -u <username> [-p=<password>] [-k <import-authorized-keys>] [-d] [-a <ssh-password-authentication>] [-e <enabled>]

```

For example:

```

$ clusterctl node user modify -u john -p='S!B*d$zDsb=' -k ~/.ssh/authorized_keys
User john modified

```

Specifically:

- You can only modify the initial `sysadmin` user, and users created with the [clusterctl node user create](#) command.
- You must repeat the command on all the installation nodes.

See below for a description of each parameter.

- `-u, --username <username>`
- `-p, --password =<password>`
- `-k, --import-authorized-keys <import-authorized-keys>`
- `-d, --delete-authorized-keys`
- `-a, --ssh-password-authentication <ssh-password-authentication>`
- `-e, --enabled <enabled>`

## **-u, --username <username>**

Modify the settings of the operating system user with the `<username>` name.

**Exceptions:** The command throws an exception when no operating system user with the `<username>` name exists on the node.

**Mandatory:** Yes.

## **-p, --password =<password>**

Set `<password>` as the new user password.

✗ Enclose the password in quotes to escape special characters (such as `$`, `\`, `*`, `=`, and `!`) with a backlash ( `\` ) as in the above example.

**Exceptions:** The command throws an exception when the password does not comply with the [Password policy CIS benchmarks](#).

**Mandatory:** No.

- When omitting the whole option, the password does not change
- When using the option without indicating the `<password>` value, the command prompts for the new password. For example:

```
sudo clusterctl node user modify --username john -p
Password:
Re-enter password:

User test modified
```

## **-k, --import-authorized-keys <import-authorized-keys>**

Replace the user's public key for SSH authentication with the key in the `<import-authorized-keys>` file path. For example:

```
~/ .ssh/authorized_keys
```

**Exceptions:** The command throws an exception when:

- The key file has an invalid format.
- The mutually exclusive `-d <delete-authorized-keys>` option is also used.

**Mandatory:** No. When omitting this option, the user key is not replaced.

## **-d, --delete-authorized-keys**

Delete the user's SSH authentication key and enable password SSH authentication.

**Exceptions:** The command throws an exception when using also the mutually exclusive `-k <import-authorized-keys>` option.

**Mandatory:** No. When omitting this option, the user key is not deleted.

## `-a, --ssh-password-authentication <ssh-password-authentication>`

Set the supported SSH authentication methods.

| <code>&lt;ssh-password-authentication&gt;</code> | Password      | Key                                                  |
|--------------------------------------------------|---------------|------------------------------------------------------|
| yes                                              | Supported     | Supported, if configured.                            |
| no                                               | Not supported | Supported, must be configured and cannot be deleted. |

**Exceptions:** The command throws an exception when using also the mutually exclusive `-d <delete-authorized-keys>` option.

**Mandatory:** No.

## `-e, --enabled <enabled>`

Set the user status.

| <code>&lt;enable&gt;</code> | Status                                                                                        |
|-----------------------------|-----------------------------------------------------------------------------------------------|
| yes                         | Enabled                                                                                       |
| no                          | Disabled: Cannot open shell sessions, either locally or via SSH, and cannot execute binaries. |

 Once disabled, you can still modify the user settings.

**Exceptions:** The command throws an exception when using this option alongside any other option. In other words, this option cannot be combined with others.

**Mandatory:** No.

## `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                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------|
| <code>&lt;clientKey&gt;</code>  | The file name of a PEM file containing the client's private key.                                   |
| <code>&lt;clientCert&gt;</code> | The file name of a PEM file containing the client's certificate.                                   |
| <code>&lt;caCert&gt;</code>     | 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 <a href="#">HSM requirements</a> for the supported models. |
| thales  | Thales HSM. See <a href="#">HSM requirements</a> 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 v1.1.0" 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 | ✓   | ✗   | ✗   |
| 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  | ✓   | ✗   | ✗   |



| CIS recommendation | Description                                                                    | ISO | Raw | VHD |
|--------------------|--------------------------------------------------------------------------------|-----|-----|-----|
| 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                                               | ✗   | ✗   | ✗   |
| 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 iptables firewall rules exist for all open ports                        | ✗   | ✗   | ✗   |
| 5.5.1              | Ensure password creation requirements are configured - minlen                  | ✗   | ✗   | ✗   |

| CIS recommendation | Description                                                | ISO | Raw | VHD |
|--------------------|------------------------------------------------------------|-----|-----|-----|
| 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 v1.1.0" 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                           |  |
| 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                     |  |

| CIS recommendation | Description                                                                                                     | Compliance |
|--------------------|-----------------------------------------------------------------------------------------------------------------|------------|
| 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                                 | ✓          |
| 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                                                     | ✓          |

| CIS recommendati<br>on | Description                                                                                          | Complia<br>nce |
|------------------------|------------------------------------------------------------------------------------------------------|----------------|
| 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                                     | ✗              |
| 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                               | ✓          |
| 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                                        | ✓          |

| CIS recommendati<br>on | Description                                                                                         | Complia<br>nce |
|------------------------|-----------------------------------------------------------------------------------------------------|----------------|
| 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                                           | ✗              |
| 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       | ✓              |

| CIS recommendation | Description                                                                                         | Compliance |
|--------------------|-----------------------------------------------------------------------------------------------------|------------|
| 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                                               | ✓          |
| 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                              | ✓          |



| CIS recommendation | Description                                                                         | Compliance |
|--------------------|-------------------------------------------------------------------------------------|------------|
| 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.                         | ✗          |
| 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                            | ✗          |

| CIS recommendati<br>on | Description                                                                      | Complia<br>nce |
|------------------------|----------------------------------------------------------------------------------|----------------|
| 5.4.1                  | Prefer using secrets as files over secrets as environment variables              | ✓              |
| 5.4.2                  | Consider external secret storage                                                 | ✗              |
| 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 [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](mailto: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 <pwd> password.                                 | No, When omitting this option, the script ciphers the file with a random password containing 13 <a href="#">OWAS special characters</a> and prints the password in the execution console. |
| -s, --logs-since <hours> | Collect the logs generated in the last <hour> hours, where <hour> 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.                                                                                                                          |
| --disk-perf              | Generate a disk performance report.                                                             | No. Do not use this option unless customer support indicates it.                                                                                                                          |

| Option        | Description                                          | Mandatory                                                        |
|---------------|------------------------------------------------------|------------------------------------------------------------------|
| --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](#)
- [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.

| Features                                                                                                                                                                                                                                         | Standard | Pro | Enterprise |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-----|------------|
| <b>Cryptographic Security Platform</b> <ul style="list-style-type: none"><li>• CSP Compliance Manager</li><li>• CSP Public Key Infrastructure</li><li>• CSP Certificate Manager (Discovery)</li><li>• CSP Key &amp; Secrets Management</li></ul> | ✓        | ✓   | ✓          |

| Features                                                                                                                                                                                                      | Standard | Pro | Enterprise |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-----|------------|
| <b>Enhanced PKI Services</b> <ul style="list-style-type: none"> <li>• CSP Certificate Enrollment Gateway</li> <li>• CSP CA Gateway</li> <li>• CSP Timestamping</li> <li>• CSP Validation Authority</li> </ul> |          | ✓   | ✓          |
| <b>Advanced Automation</b> <ul style="list-style-type: none"> <li>• CSP Certificate Manager (Control)</li> </ul>                                                                                              |          |     | ✓          |
| Certificates                                                                                                                                                                                                  | 50       | 200 | 1000       |
| Vault Clusters                                                                                                                                                                                                | 2        | 1   | 1          |
| Compliance Manager Clusters                                                                                                                                                                                   | 1        | 1   | 1          |
| Standard Compliance Pack for Keys & Secrets                                                                                                                                                                   | 2        | 1   | 1          |
| Standard Compliance Pack for Certificates                                                                                                                                                                     | 2        | 1   | 1          |
| Third-Party Objects Under Compliance                                                                                                                                                                          | 300      | 100 | 100        |

The following table shows the quantities of Standard Objects in each package. The quantities are shown distributed equally among three use cases; however, the license allows you to distribute them in any other way you wish, as long as the total number of Standard Objects remains the same.

For example, using the Standard package, a correct usage might be KMIP Objects: 0, Cloud Keys: 300, Secrets: 0, as the total would still add up to 300.

| Standard Objects | Standard | Pro | Enterprise |
|------------------|----------|-----|------------|
| KMIP Objects     | 100      | 16  | 16         |
| Cloud Keys       | 100      | 16  | 16         |
| Secrets          | 100      | 18  | 18         |

The following table shows the quantities of Enhanced Objects in each package. The quantities are shown distributed equally among three use cases; however, the license allows you to distribute them in any other way you wish, as long as the total number of Enhanced Objects remains the same.

For example, using the Standard package, a correct usage might be Application Security Keys: 50, DB TDE Keys: 50, VM Encryption Keys: 0, as the total would still add up to 100.



| Enhanced Objects          | Standard | Pro | Enterprise |
|---------------------------|----------|-----|------------|
| Application Security Keys | 33       | 8   | 8          |
| DB TDE Keys               | 33       | 8   | 8          |
| VM Encryption Keys        | 34       | 9   | 9          |

## 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 CSP Certificate Manager.

## 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.
- This product includes software developed by David Giffin <[david@giffin.org](mailto:david@giffin.org)>.
- 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](#)
- [Intermediate authority certificate profile](#)
- [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 |
| CRL Distribution Points  | Never present (not applicable) | Always present                                          | Always present                                          |

| Extension              | basic-ca-root                                                                                                                                  | basic-ca-subord                                                                                                                                | basic-ocsp                                                                                                                                     |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <a href="#">RFC 7093 section 2</a> | «The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in <a href="#">RFC 7093 section 2</a> | «The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in <a href="#">RFC 7093 section 2</a> |

## Intermediate authority certificate profile

Entrust provides the `intermediate-ca-subord` profile for intermediate Certificate Authorities.

 This profile is not exposed nor configurable. External root CAs are not covered by this profile.

See below a description of this profile.

- [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           | intermediate-ca-subord                                                                    |
|-----------------|-------------------------------------------------------------------------------------------|
| Issuer          | Customer's online root CA                                                                 |
| Subject         | No constraint                                                                             |
| Validity period | Less than or equal to 10 years. The subordinate expiry cannot exceed the parent validity. |

## Certificate critical extensions

The authority basic profiles set the following certificate critical extensions.

| Extension          | intermediate-ca-subord                 |
|--------------------|----------------------------------------|
| Basic Constraints  | cA=True, pathLenConstraint=None        |
| Extended Key Usage | Never present                          |
| Key Usage          | digitalSignature, keyCertSign, cRLSign |

## Certificate non-critical extensions

The authority basic profiles set the following non-critical certificate extensions.

| Extension                | intermediate-ca-subord                                  |
|--------------------------|---------------------------------------------------------|
| AIA                      | Supplied when the customer enables OCSP on CA creation  |
| Authority Key Identifier | Matches subjectKeyIdentifier of the signing certificate |
| CRL Distribution Points  | Always present                                          |
| OCSP                     | Never present                                           |

| Extension              | intermediate-ca-subord                                                                                                                         |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Subject Key Identifier | «The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in <a href="#">RFC 7093 section 2</a> |

## External subordinate CA certificate profiles

Entrust root Certificate Authorities support the following external subordinate Certificate Authority certificate profiles.

| Profile set                                                         | Profiles                 |
|---------------------------------------------------------------------|--------------------------|
| <a href="#">Azure Firewall Intermediate CA certificate profiles</a> | azure-firewall-ca-subord |
| <a href="#">TLS Proxy CA certificate profiles</a>                   | 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                                                                                                                                 |
| Subject Key Identifier   | No       | «The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in <a href="#">RFC 7093 section 2</a> |

## 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   |



| 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 |

**i** 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  |
| '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 |

| Alias                                            | OID                        |
|--------------------------------------------------|----------------------------|
| '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      |
| 'WordMark'                                       | 1.3.6.1.4.1.53087.1.6      |

| Alias                        | OID                    |
|------------------------------|------------------------|
| '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](#)

 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)                                                   |
| 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 <a href="#">RFC 7093 section 2</a> |

## 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 |

**i** 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  |
| '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  |

## Subscriber certificate profiles

Entrust provides the following certificate policies for end-entity subscribers

| Profile set                                    | Profiles                                                                                                                                                                                 |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">SCEP certificate profiles</a>      | scep-digital-signature<br>scep-digital-signature-key-encipherment<br>scep-key-encipherment<br>scep-non-repudiation                                                                       |
| <a href="#">Smartcard certificate profiles</a> | smartcard-card-authentication<br>smartcard-digital-signature<br>smartcard-domain-controller<br>smartcard-key-management<br>smartcard-piv-authentication<br>smartcard-piv-content-signing |
| <a href="#">EST certificate profiles</a>       | est-digital-signature<br>est-digital-signature-key-encipherment<br>est-key-encipherment<br>est-non-repudiation                                                                           |
| <a href="#">V2G certificate profiles</a>       | v2g-supply-equipment<br>v2g-user-identity                                                                                                                                                |
| <a href="#">Intune certificate profiles</a>    | intune-digital-signature<br>intune-digital-signature-key-encipherment<br>intune-digital-signature-key-encipherment-clientauth                                                            |

| Profile set                   | Profiles                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | intune-key-encipherment<br>intune-non-repudiation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| CMPv2 certificate profiles    | cmp-digital-signature<br>cmp-digital-signature-key-encipherment<br>cmp-key-encipherment<br>cmp-non-repudiation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| MDMWS certificate profiles    | mdmws-digital-signature<br>mdmws-digital-signature-key-encipherment<br>mdmws-digital-signature-key-encipherment-clientauth<br>mdmws-key-encipherment<br>mdmws-non-repudiation<br>mdmws-p12-digital-signature<br>mdmws-p12-digital-signature-key-encipherment<br>mdmws-p12-digital-signature-key-encipherment-clientauth<br>mdmws-p12-key-encipherment<br>mdmws-p12-non-repudiation                                                                                                                                                                                                                                                                                                                                                                  |
| S_MIME certificate profiles   | smime-digital-signature-key-encipherment<br>smime-key-encipherment<br>smime-non-repudiation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Multiuse certificate profiles | multiuse-p12-client<br>multiuse-p12-client-server<br>multiuse-p12-custom<br>multiuse-p12-key-data-encipherment-non-repudiation-client<br>multiuse-p12-key-data-encipherment-non-repudiation-client-server<br>multiuse-p12-key-encipherment-client<br>multiuse-p12-key-encipherment-client-server<br>multiuse-p12-key-encipherment-custom<br>multiuse-p12-key-encipherment-non-repudiation-client<br>multiuse-p12-key-encipherment-non-repudiation-client-server<br>multiuse-p12-key-encipherment-non-repudiation-custom<br>multiuse-p12-key-encipherment-non-repudiation-server<br>multiuse-p12-key-encipherment-server<br>multiuse-p12-non-repudiation-client<br>multiuse-p12-non-repudiation-client-server<br>multiuse-p12-non-repudiation-custom |



| Profile set                                   | Profiles                                                                                                                                                                                                        |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               | multiuse-p12-non-repudiation-server<br>multiuse-p12-server                                                                                                                                                      |
| Mobile device certificate profile             | mobile-device-p12-digital-signature-client-authentication                                                                                                                                                       |
| Private SSL (ACMEv2) certificate profiles     | privatessl-tls-client<br>privatessl-tls-client-server<br>privatessl-tls-client-server-data-encipherment<br>privatessl-tls-client-server-supply-san<br>privatessl-tls-server<br>privatessl-tls-server-supply-san |
| Code signing certificate profile              | codesigning-digital-signature                                                                                                                                                                                   |
| Active Directory (WSTEP) certificate profiles | wstep-digital-signature<br>wstep-digital-signature-key-encipherment<br>wstep-key-encipherment<br>wstep-non-repudiation<br>wstep-non-repudiation-key-encipherment                                                |

## 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             |
| 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                                                                                                                                       |
| 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 <a href="#">RFC 7093 section 2</a> |

### 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   |

| 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>

## 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  |
| '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 |

## 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                    |

| Profile             | Key Usage                          |
|---------------------|------------------------------------|
| 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 <a href="#">RFC 7093 section 2</a> |

### 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                   |
| '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    |

## 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. |
| 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                                             |

| 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 <a href="#">RFC 7093 section 2</a> |

## 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       |
| 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 |

| 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  |

## 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)   |
| 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                                                                                                                                 |
| Subject Key Identifier   | No       | «The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in <a href="#">RFC 7093 section 2</a> |

### 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                    |
| '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       |

| Alias                                            | OID                      |
|--------------------------------------------------|--------------------------|
| '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    |

## 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  |

| Extension name             | Extension OID        |
|----------------------------|----------------------|
| 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 <a href="#">RFC 7093 section 2</a> |

### 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       |
| 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>

## 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 |

| 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  |

## 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.                                                                      |
| 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 <a href="#">RFC 7093 section 2</a> |

### 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   |

| 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>

## 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 |

| 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 |

## 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                                                 | CS<br>R | P1<br>2 | Key Usage                           | Extended Key<br>Usage                         | Allows Extended Key<br>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 <a href="#">RFC 7093 section 2</a> |

## 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 |
| '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  |

## 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)<br>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)<br>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)<br>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                                                                                 | ✓                                    |
| 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)                                                  | ✗                                    |

| Profile Name                               | Key Usage                                          | Extended Key Usage                                                                             | Allows Extended Key Usage in request |
|--------------------------------------------|----------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------|
| 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-Repudation   | TLS client Authentication (1.3.6.1.5.5.7.3.2)                                                  | ✗                                    |
| multiuse-p12-non-repudiation-client-server | Digital Signature, Key Agreement, Non-Repudation   | TLS client Authentication (1.3.6.1.5.5.7.3.2)<br>TLS server authentication (1.3.6.1.5.5.7.3.1) | ✗                                    |
| multiuse-p12-non-repudiation-custom        | Digital Signature, Key Agreement, Non-Repudation   | No constraints                                                                                 | ✓                                    |
| multiuse-p12-non-repudiation-server        | Digital Signature, Key Agreement, Non-Repudation   | 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 <a href="#">RFC 7093 section 2</a> |

### 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   |

| Key algorithm | Signature algorithm     |
|---------------|-------------------------|
| 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>

## 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 |
| '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 |

## 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<br>(1.3.6.1.5.5.7.3.2)                                                     |
| privatessl-tls-client-server                   | Digital Signature                    | TLS client authentication<br>(1.3.6.1.5.5.7.3.2)<br>TLS server authentication<br>(1.3.6.1.5.5.7.3.1) |
| privatessl-tls-client-server-data-encipherment | Digital Signature, Data Encipherment | TLS client authentication<br>(1.3.6.1.5.5.7.3.2)<br>TLS server authentication<br>(1.3.6.1.5.5.7.3.1) |
| privatessl-tls-client-server-supply-san        | Digital Signature                    | TLS client authentication<br>(1.3.6.1.5.5.7.3.2)<br>TLS server authentication<br>(1.3.6.1.5.5.7.3.1) |
| privatessl-tls-server                          | Digital Signature                    | TLS server authentication<br>(1.3.6.1.5.5.7.3.1)                                                     |
| privatessl-tls-server-supply-san               | Digital Signature                    | TLS server authentication<br>(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 <a href="#">RFC 7093 section 2</a> |

### 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)<br>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 |

| Extension                | Critical | Value                                                                                                                                          |
|--------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <a href="#">RFC 7093 section 2</a> |

### 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 |

 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       |
| 'unstructuredName'                                     | 1.2.840.113549.1.9.2       |

| Alias                                            | OID                      |
|--------------------------------------------------|--------------------------|
| '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  |
| MSTemplateName       | 1.3.6.1.4.1.311.20.2  |

| Extension name             | Extension OID        |
|----------------------------|----------------------|
| 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 <a href="#">RFC 7093 section 2</a> |

## 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 |

**i** 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  |
| '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  |

## 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<br>(2.16.840.1.101.3.6.9.1)<br><br>Security ID<br>(1.3.6.1.4.1.311.25.2) |
| smartcard-digital-signature   | Digital Signature, Non-Repudiation  | No constraints                                                                                                                                                | PIV Interim Indicator<br>(2.16.840.1.101.3.6.9.1)<br><br>Security ID<br>(1.3.6.1.4.1.311.25.2) |
| smartcard-domain-controller   | Digital Signature, Key Encipherment | TLS server authentication<br>(1.3.6.1.5.5.7.3.1)<br><br>TLS client authentication<br>(1.3.6.1.5.5.7.3.2)                                                      | —                                                                                              |
| smartcard-key-management      | Key Encipherment                    | No constraints                                                                                                                                                | PIV Interim Indicator<br>(2.16.840.1.101.3.6.9.1)<br><br>Security ID<br>(1.3.6.1.4.1.311.25.2) |
| smartcard-piv-authentication  | Digital Signature                   | Any Extended Key Usage<br>(2.5.29.37.0)<br><br>Microsoft Smart Card Login<br>(1.3.6.1.4.1.311.20.2.2)<br><br>TLS client authentication<br>(1.3.6.1.5.5.7.3.2) | PIV Interim Indicator<br>(2.16.840.1.101.3.6.9.1)<br><br>Security ID<br>(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 <a href="#">RFC 7093 section 2</a> |

## 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 <a href="#">RFC 7093 section 2</a> |

## 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 |
| 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>

## 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 |
| '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 |

## 24 Post-quantum key types

When using software cryptography in a testing environment, the Certificate Authority solution supports the following post-quantum algorithms

- Pure post-quantum algorithms
  - SPHINCS+-SHA2-128f-simple (1.3.9999.6.4.13)
  - SPHINCS+-SHA2-128s-simple (1.3.9999.6.4.16)
  - SPHINCS+-SHA2-192f-simple (1.3.9999.6.5.10)
  - SPHINCS+-SHA2-192s-simple (1.3.9999.6.5.12)
  - SPHINCS+-SHA2-256f-simple (1.3.9999.6.6.10)
  - SPHINCS+-SHA2-256s-simple (1.3.9999.6.6.12)
  - Falcon-512 (1.3.9999.3.6)
  - Falcon-1024 (1.3.9999.3.9)
  - ML-DSA-44 (2.16.840.1.101.3.4.3.17)
  - ML-DSA-65 (2.16.840.1.101.3.4.3.18)
  - ML-DSA-87 (2.16.840.1.101.3.4.3.19)
- Explicit composite algorithms
  - MLDSA44-ECDSA-P256 (2.16.840.1.114027.80.8.1.24)
  - MLDSA44-RSA2048-PKCS15 (2.16.840.1.114027.80.8.1.22)
  - MLDSA65-ECDSA-P384 (2.16.840.1.114027.80.8.1.28)
  - MLDSA65-RSA3072-PKCS15 (2.16.840.1.114027.80.8.1.27)
  - MLDSA65-RSA4096-PKCS15 (2.16.840.1.114027.80.8.1.35)
  - MLDSA87-ECDSA-P384 (2.16.840.1.114027.80.8.1.31)

### Pure post-quantum algorithms

See below sample requests for the supported pure post-quantum algorithms.

- SPHINCS+-SHA2-128f-simple (1.3.9999.6.4.13)
- SPHINCS+-SHA2-128s-simple (1.3.9999.6.4.16)
- SPHINCS+-SHA2-192f-simple (1.3.9999.6.5.10)
- SPHINCS+-SHA2-192s-simple (1.3.9999.6.5.12)
- SPHINCS+-SHA2-256f-simple (1.3.9999.6.6.10)
- SPHINCS+-SHA2-256s-simple (1.3.9999.6.6.12)
- Falcon-512 (1.3.9999.3.6)
- Falcon-1024 (1.3.9999.3.9)
- ML-DSA-44 (2.16.840.1.101.3.4.3.17)
- ML-DSA-65 (2.16.840.1.101.3.4.3.18)
- ML-DSA-87 (2.16.840.1.101.3.4.3.19)

### SPHINCS+-SHA2-128f-simple (1.3.9999.6.4.13)

Use the following CSR and keys to test the SPHINCS+-SHA2-128f-simple post-quantum algorithm with the 1.3.9999.6.4.13 object identifier (OID).

- [Sample CSR to test the SPHINCS+-SHA2-128f-simple post-quantum algorithm](#)
- [Sample public key to test the SPHINCS+-SHA2-128f-simple post-quantum algorithm](#)
- [Sample private key to test the SPHINCS+-SHA2-128f-simple post-quantum algorithm](#)

### Sample CSR to test the SPHINCS+-SHA2-128f-simple post-quantum algorithm

Use the following CSR to test the SPHINCS+-SHA2-128f-simple post-quantum algorithm.

-----BEGIN CERTIFICATE REQUEST-----

MIJDWTCBhwIBADBMRRAwDgYDVQQKEwFbnRydXN0MQ8wDQYDVQQLEwZQS0lIdWIx  
LDAqBgNVBAMTI1NQSElOQ1N0bHVzLVNIQTItMTI4Zi1zaW1wbGUgU2FtcGxLMC0w  
CAYGK84PBgQNAyEA06644sgf45+BYFEyuQLej72GY8YWNQ2sHEKTYz515v+gADAI  
BgYrzg8GBA0DgkLBAB4LW908lqet6lCcYHVkj+5JmKPPMaoY3DNTgt3Vn5CIgrAB  
rxKraRX3TEBwJv/n2tMmvHSGzF9nucBjsEuof+syStM3j8f1hbc0h8Bnq3tJCDNx  
NuX8JnuXP3EywE+sDiYBQ5LcoEKCwnr3XNv1XZ2ZfOMy7DxcYxLRpRBbIIC5RQMX  
cQlRrVXnz8t4gJg1NmJNXfyFxb16kpeOmT4kl9ECMXLWjJEmgN1Fcz0nIqK43cHB  
nWVLzEhKQYRkTHNqnFEUqJHmr1XR/CyMwwk8uVHrSkTyOx2PWdVu6EpK7f7Hj51L  
QbqyJW3GycDr3pEJR36Dg80S3JUW6Td9/7aoGeLmVi+ZQVe+DAEtGADvyM/2HRC2  
so3M9zKJDufIwDexUqJ4UyYw9LHkBTkaC3E5Let0lgKr888b3tgkR5Uhz1C//Pq7  
7cTaYioY4fBp1V7dC3MwYZ10o02DZbxY76/2xZpU2DbuLQ6AzCbX20oLu9mKjLbL  
Zht3VEYKtKt9Yf5+Hdei8uEx+SBzV9dHNNuexHZd30ig/DAGwdHS96C3Q6RtNCFB  
TWQT2SAAfhVG4qpGVrUsp6aSF7GyaET5L0l6uZ0J0Dtus5+Ip0tP/gonuR64B/m  
6DUXqwtZPHKCJm49EjEz40Hbcs0IWexrLAS0/CiZzkv12MLXY7H2FpX22hXebMg5  
DWFIPkGvCHCqYd4cG8QevvtUq8/5SVH/p0oBMRQnBNCIIBvVTI4VfFDVEa5Uqmmk  
1B0DQg/KAo0tMRD/5Dt0Du9HYdRLaFvGT6uawrKDhtbP2y5H99X2Gd37XtyUf9LN  
Sk2jbGBvpAbeSpVZ1m32tfHw8ydQAFIz7dyMPGBASEVsneEb/5KaYjktVTlirvj3  
n32IC3EqAhEQMYV8qjV+edc+x0BSwyIYV9nJqWQSPMdQMBV7eTpdqT4UfGcssG9J  
TOAyA6gOpVVJUxtsaSF/t8S+BZ56wx1GZZSFYzU8Njcl/ffRVV3zYrYJFCKuZxVh  
z92eq0dTWp38k3BXcwaNar8zd77cesqdK0Fj/xsX2P0/z5fPxnfivnLCNfStz6KJ  
0XfBhS2l1lfJ9o7CsmQ/6lkk0rel3j0IXLGrCeumN/829JpgZyJvudciMhYaqYgn  
eMMN2uM/3edY3mX5+BzTqqt6GX5SpAf4rZ/FWQYkkzzyqg85N4GnhK7liU0eZXP  
AB/uWgU3MYpwQuS/TSzF2q0e2y7Ll88x07uVadtQ1+hodRJyNN3QFzRbCGAsU1SB  
EzUcWoXZQWdXxF/Ab9bLnl+KC/aJsRvV2gW2V0gtLBjEU4dZGhAVs6MEJj6Y5  
sntcX+7Ga7FFlJk336EFXDdUG12JeFhhuV8jIV+s26NT3A6H928hrfiWD8oTur5  
jb5mijSVHR4dSY2fjmR1n9tvQ8AwXgzl4oa08Uml00ZYEn/WBIjx5JRfiXifecep  
We68hTkCgq943Cei9BnDREYLLTJAz55BcJut8LiCj8emzzAopbBAaH0JyQbaaBb+  
w0FbFA5L+8N0GRnz9sJhvTOH+pv36MsP307CM4yDpKM38lHxQ1/CCjMQJ37ABtT  
HuMbVTLjgIrec36dRzF0Jxb3/jVMCjmbw5f9EL2078E0XzWvBsllfYKqqDqIJbJi  
N0BUMWd01rURM6g8sH9j5dHGowUCLxWI3PJGsBvRZDbgbfTafEQPmPhzELUXRhez  
5+X91+PZHcIZ/sc7TVwCl4EPdp6BLCP/XhvMyua0IT+5HtGTDtar38H3hRrZwz6b  
eYsouM2JPbIQB7ttRajl67gbDDtwNao00bERa/3BxvoY6Zk4d47J8JRHR2m+jnou  
liXs58mjNhZC9jAq7dVAoW3MX2hdBLl3HwS+Gdc2133Je05E/NLYENz2X7qctXM  
jmaACzAaVzVSMEL0npYHVPjRgFmI/MDD8YKbMeyqt2x8NTIGlQQeHQzcQxTiv3fs  
UX/9j258lyXtw63N5i6RFYfFAXAhXWV6B0cFqie63XKVbBiHTsAhLXTYs24A0aHZ  
Bju+eciFmzUSyTQKEW4pokIjPfmzhbpJAQ0DA/CKS64ow0uJpk+cipZbTws6FXsH  
dxv2esFPl8cnboH1t5LIMIPiaa/1grVZ5VFv6noZLBnPBbhfcc00MwRXZI+C++iE  
wC79AUxPAM6JiWuzaVVADpVNgTB1po43n37TwLHBD9eCcaKwtJIAatqyLB5mskYE  
LqRP1V22Pt0/MDZvQL6GYnF5ck3RSEmuLLmEFpD4Tf8G8D8jff8+BEw48nT851Nh  
X+2dd0nxuZGB4Yc5vOpX7ZVbpvWKeQtvFu+hCfcaMx6H1DYy8fh20BZQYLWeoyiY  
EG87MAVPAQamFDyqWTTToyIkdHqJcYzu8lz0pSXTVT8FpEmTC16pw64ZCjJh0hqGP  
w0Uqb57VqMXsR5luY/cPQlyWPrgsgeEixVmapRKzEUa5dyqMFP23dMS8obARTdVU  
r2xCATlzhLw2Rc/nYoQWSVTnfJAPvMjAan3GalDV9mvde+yjA1EFH2YBmTWwdjHk  
TcCCTxyzqRb1N/QPVeUhpPY4o1M2mDhtNSnPzEraS8uuTgKV6cTx9aayNKSrTJeb  
zh4r4C/yyshoMSd6HryOCKQTEllk64y00vLga6SN2ZsDYUy37CZtUmDsP2IiocVZ  
qT2Q22cqbcm0eRZ/S2lxsuRxr0f5YH9ROCYgpAFm2+WoYIN4+/CNYIAhwguKoX3r  
azlsT8ZvB+dtUA9hLqs27bWz497fXsE/PLiXuchqMlirBB3DxV0DbRnDTaRLmuLz  
l5Ziw0ab/XdrJ4jW6opaMi2zLRO0iszX1qs90dpTQ7R+vuJ9SDWQG1PP5sgYkq2a  
DcQG7kBZztixblMnAYlhRF6ctgMFLfyXzt3+oIM9WdByIz2e0G0uOnGqE+QNB29  
NawOrLzwR1Dts3ZH0E8opR9S/5INzw+VKsXSWEsZ+u5IxU5LkW4Im1f3Yu6z5y6p  
o3qWyZDlPgXTsLtGd0gKLWlWeiPnJ87XuxR7RYn4q7J+oHrICfu7zU0xi440jHEH

Dgj01qUH0rzF/a0986mXUxHcEcT307kvPLxmWxAUjGcnZ3AdgGbqpUPmwGJCuBCP  
8oWK4FiLufwp+SehaK0nZfKq4aGpRvoZpYP4sPsBkthDWKDS5Zt+f0ZjPqunMT+  
chl1dHqBuMdWsbUNE8aLYzD0/Y+1mWoE02NvAY3ByJfxBjiTP+jsPqyTo8t6aVpm  
q2W8ruqtCRNFiwP0cA+HacAwLZt79ff9bx9/QBTCvkDDW+QQQnYXhDnwXQHIwVO  
deDvbqAxXqMnrmLHiJthRMogyUAym1qDx5iYOUl fNCSDMDG5qZ1U6AVE6wKz0ED2  
PAFSBPBorYWya5TUh7qWiRkrPPSGxGn55JllMoZfyAPSkJoKbX1DlYdtDmgcw5f  
7LE3mK0b6fRtpr7S/rvoKJACt/eXCV4qMBxYcA4Edoicys39NoN7dJ+OFHv+bzkM  
0UTHmVL76zLSEQZEFHH/jxQSzR0kUxsgshZNoFMzjWMPR1qji0kbwb6sIA3uP76i  
a8q87RmV1clI8IEklczxg96mEXHLQT8kyGdoCIRWvKygdDbVrLOnpAUqVE6fq3at  
sfH2WXRBNuQNu02cPBUCqWhcjsUBLLe8ZwM+WOn5FnIM0rV6LA7/TLvPGWEwGH  
+W8G221HfMhGcIVrzB0Bmucp5oS/H0cfESnu9DuAuG2fhtxzoE2HX3aq/0oNpId+  
xygN4xZb74680gLPdlkf1td5ik0fyjB/Kni7VSzTrFFuX1/wvlhZ9hN3K/86o+UD  
/pJcnRPNiSL0crDkKfhdXexByxDdeAAxpa4bTuN7fzY817KuDoPcEaaj7H0ghkB  
qzIr4l/7ScGnFBjM7vUKipYbdPDZI3jrHxAlqzSDgeSZ/nzKryUvanEqm5VH1ud  
uj0IIVBvk2c/gFndzanT66TlIpj4ARnLLA/KRWNwbyFJdBeVsdrpZpEMecLOM0i3  
a8Knz4a0zdZD8wxP2oZQz7fBVliIRerZoLG8UP4vZfe0hebYRNgbgup6cbrcKKL  
ykVfTbEzPe9J4VZ0roZf5xqgdDLT24aa0ezokSLDLaN900ffGQmdcMQvua90y2sO  
oeDZ2cZD3AaB5QVcgjS92UnlP4URYDXhZ0qKfaMnVIBz/itKFqvdiCY6qTRTLJD2  
GtMxgm0BPEjUDyYoEj70rm8aeQRWdOopC0DH1/LZs2FaLvLCSCTPSewnyY7S2AN5  
idPPuOwW2+ts/QfeW7+PI29eXb6CUMTyqvgvgoJtXcBKW3nvP000B2CKqjFAC5Ek  
/LgangtvZi2sBy2351XIHGsBX3LWeHcCHjz06wfNw07dedJ6Ykj4bXl0ZjUHHTnv  
EwkyqEkW2Fs3UrWfMBLULf1HMLaQfgrYgoGXh+nDMHPM5MvMUzNM0o8JL1lhoy5  
PNZA4jVdHN4X4pvI6KPGfziUj7Ms9KH7MSjNPNTMISi37hzZ53SePl2Xo0ICyqDk  
/UBmIh6mpoKJ+sw459X1SS4aLV8L3UqUUD9gfnTp0uwajKwq9l6VQsUj30rHTKTC  
FXAW+qa3Ahjiqar+tm0lc35z+Zlp4ofdmY4x3cv6f1AR+hrxrUt8x2g0YNFcShMT  
UQK87eer+hrj0WpAL26dLhFq9ktw6NdsHJ0JzkVw7VhLSBCby2miljhBg8B9U1WZ  
i/tU84ett09s/DqM+SvHo0C99DInYEFjpy9+wGux1S3aLpyco/TgzInxVzhNrDyq  
78Z3umjlxXShD5C/s+B5qXkHUady24G6Z6Nuilf7jJxwVS4UJxE/jGuITAhzSLb5  
E0PRwNZoFb52Zg0ek0rR8V2jLDfKsavUuyyPxtOS5xWztxgm4IUNhd5pQtXMdvJ5  
8vdHOADCQ3MJ/NUKqa0alZw2d15LPWtdtkWn67ErV9E0t4meeWYjzyH2Ek3ERNc  
v8vmBGD9n8Pw7PKbBLHZjueFF6S1tg7sC3XeonaMV+3Iec+uQKzbOm066fq+5ffm  
mgv0M0gwL/BTD1KVDN6Xp4x3/41UzcPcPa1R6B40jt7tDzRY2XR5PTrLkORXJD72  
NvT6G1T/kZ3XnXw4L1o78KSkdxnht/9pwMXAtb8vrT98rTVEMIMUZFKqTqP7aLDk  
W20swEh8ruc+MDhwaJLWqM3DrkuKERBoevvMAQLftFGQia3nhjcprr/qX1W20zMK  
o94K2qs1TVwqxSYy/Gwb0Z9rNB1AzEMZm7VqmVYgfbFnAnISGbpLXotru/khM8c  
073+NV436xLABrIRudyvLbiTwqq9jXnNrpvHqpB3upGY7okUXlzPdDnlaXWQbsQc  
m4+QYAGYzB8YRYAIEzTLcULH5+TFYWO2xB8keSEtUrbGwY36IwIDpVGz6dD9mSVZ  
nEFmYQxcmZ0bSEbg1Et4pCJSPdJnS7dMuIj9MM8+M9L/pTmodJQ/KJ0AMXmtwbx8  
GdlfPJ3P5dePb6bNGgHaqhuyMPLSHEwrMH2+leR9ZyCvGX9Mu9RVYoTEX1FLVWkS  
0FRDclW2cGj19cPUD609gHeb0aY8TaGqhK/KbtsVpP0Cl2CE61CfJ7Y3FPh6HJKq  
dKLXuqDk6UF/i0egtQRUp5mywHDhMqGtPF8FRvFs0tp5URhYm/f2dlul3zEwfhe  
MeZGedSRGczYF76JJThzdJpAijQ3/hgI5c5mJv0gj6fAme3rtIzKpXrtbIQcpAhX  
pm0XnkhXt8V7EcDrREGTzJN87tTH/WN6d3JTzt5m/acKErMf1zhjgFI6ez7s3L3a  
64aw6SHA/qJ/Vk0cthpA6gtWmM7AgL7zh0m5Ib0vH3HRMbsnZ6JJKgbtBAS9qLbp  
oxw1eL0rdrtLh1MCEmb/ese01m4uU8qbYFU+nDDVE08DJEK6jmuAgfW1gMi+B8  
Y5sx5UJNYEe1D/44li2Xd6XZCgsigF2cI5L5+gNemg3J5s4pwPIT90SvbFnaZDqu  
uzLHTwLQXhXGj6kN2FKSE9agaHzEUaEUDWQXo3B35IEJx371m0fZgpbQ6UXpyIG1  
x4qWc2F0qOp7v1UfKP63iNjZGpodtz9mmi4Dnv+PXWlqBzc/oyI/B4GMy2EX1kaL  
uELXUEHyxBVlwTztHWNvzVfYTGLbvePh3k+CB5d01rakM+0i1e4VHHE960zsZTy  
pTAHI005AVCmVcodojHB3af7C/mLukZCJv0G0ZDMuX66/jcowbmoLm+KMfmSPYtT  
9V4VXTTnHeH6N7bI0esFx7ab7p9zf//1xk9quwBsKwnr40AoXG5mBE/sQz4Y1geV  
+NARfiwtbxfYiISPFqf82KhVnFbnczML10EJxnkfQsJAQHeHtFg86MaQVT6kN35L  
YwmI5PP3/zREhsTmT//sCWia1unJLcenPWlRGLSAB3LkTt06cs/+CQ5Lx/7RFTq6

1QrnQ3MdA9Q53zea1yh0KUwECP2P3Lvzo0AabamZeTujNn0VNJ+cekCIFTshX0Bu  
o539M5kaFf1twT+Iu3Jw/WKFnE8ZwASY19ZcYxppTwMw9HpJNYiTnJU0A2mMem9u  
S2fo8KYCazJYVsSo6lCupoglivnLeAmthjLnyeB4/ozIsTw6AVH4G8ctITSaqQCG  
Lg5PD0JXWWSwmM04ZQ7xNEt+LEX08jEuGHFXrDEwbBcdKzJPDHztj7Mw3BUTgU6n  
nXp9QgueJ+mZbWYRR33UZK9QWA2vUn1JxEjBDJ7vKemLXvm22mNJDlQ+yTKKCEgZ  
aL/MCq2yGN+pnVXtYsXw9R2Nan2CC37ZmuSDNTnv6ECMXRWad04Kdmo0lo/xuAfu  
pd7gQB/vaIgM7yHKwTymQ121iA4mlLrxu0ml6JmeyWtwWliSjFm3BJmPM00iIahV  
zIMCIF90e+64wmeuznx7YwdIuGx3PXUMmbq1uPBCcMRowokjNX0+I27Ig0zn0WvY  
PnHwoLJk2nA+mBAmSVgGkIUg+ygW2diS0Ud0j+iiJgIQ0/pARh0lvGVULYhxNNGE  
hAi3nHx/XV8IaW+5f8GuI0l0VBKy0JEk+Efp6lhZ3UVwK5HYV7fJCbf4rP4u1KG  
bS2AhcKHtXZ5INJIRonVQ6hmkr9jhgXV/E0V5nhZuA9HS9roZA4gSQKC421WkmJL  
kHTznM4s8qhYJsY+GYtkWQ/u2qWU+BNh1baeQnBhxhGtDjhGLBAiIEU7mckeP/O6  
8ji+JIFrYwAGDc/cMbKG0yrxppf8t/aS1SybS04hmVGqV1zZar5QXlTJ4r0wL8p  
Rb+0T5B0aVvAEbnoNsnuk7Gs4Eu+AYJp4PieydFlsWgfY+Afx7tju//SfUo63uQq  
vu0wWHZA7U7bgdiTSwLYGPaRtTjIXnXx8FtoyEUwAB/PhJBJaZk5SgncRq+I+EU  
fgCpDG90p3e6M/m39rv43VRvjgWzmfAytme1d0TkvlXtciolyCSzJ6Y0Yqcx7h0a  
n/CpXiiTqqUB6CDJgM2BpLp0VpgtYPRm0+gHmjuJp8X0Uoe9MMk5U+y1zkF35Saz  
PzoCSi5h0ICnWjYSfb+VFUMDEk8KEl/wznI09KTUZHhnlHX14suIKLesL/lSzAPk  
xwqZeCISgUuX9Ts5v5I9J6kYD0PLmoem91qo8FklY7ty1raTvlwR8ttzcAbNYngF  
e+ap6xgl29sayTKPgqTimpYWPrttrnK/LFch/HxSpg0ajy0BKcIDjluwLnsTtR7Qf  
cvBFa62RqJ5EqCSHj1a4MvKx9db78s9qa6+vnc5E8Gk7CyETVCmng5MoFEQdMpu  
Wq+sa0e075ejNdyAFrdtqThgvL+iGRDcVvd/EIU0gbkv0bQSPREjxJ6wTyII+w/P  
euBRH8kqgm+GMT/SWh0EQE+430mE1dE8AUcUqBtH05KsBZe7FM84EZGBR8cfILAm  
1W4YWB19y2D8PgZzAmePQ6JJft3GLdf++ayy3eDJVoGZfnh47myijqMm0JttvFND  
FZi0q0nYMYL8+l48RLp+dHxgQ0BNoMMYUws0pJFuNaP8H/CIndhC3wtHdqrFgXrk  
yb3tmGs570ue592wgTWA/GYTqZZWHPZCXnihvMzyGgvcZapxwP5o/5uwsKwmRLG3  
cvPBVs8HdVhjAEgX07dTNz/fjRK+zL8TBjYqgWydP37zxwdmJNQCzKq4dbjXYZs9  
MLHRM6Mu4klTpPTvvNdGnF90q0GBZeY7pXyHBnS5gKsGwDz4ESM6Lax9Gvs52ZLa  
PIke7D76yBXhvaYc4dGUMrIcTyABT99UWxtPMGqt5TaPJXJuGdZ0v3eNvyJg0j+Z  
hDMtW2bBH133pxwwEu7/QMkJ003iib0m5wCmp9b8lBPv8e2sH2zn5S1922iswAQT  
5k+QV/bY9XV2k7wFuq77G0mGt1c5pYWF7FVUR3BIU7Vtk0+fgvGwy6FwXQLXG62p  
gmfbFop12TeQuY9+Zvuvw1m70Dp6uZzSkHKUyd0eFYl/DOFSCEKB1T6DlKUGnL4Z  
8CfufWRJ2ReejUmCBq4hpTZu6QLJHP1xNb59KxqnLnwuFE5u+kpo1q4u7hVqQ5bT  
9jv8sKqddF9/pabWwrlB0p5ipFVv4os/bAR0XL45I/jdHK867iq6X75ZwTlv8LyN  
Sdx2ek0MFTld499m0KgrY8asya3JodTzbvMbTVRY2NW9Gxb+0LmG+a5u2JZ1gPPY  
XdxYW5/3wfGgP/n/J6tpVfu+UwLFmr5kqQElwAMa2Ss6v0GA6Zhu4GBKYNzl6K7u  
VE+7jxPYwwu0lbSATJD6sJgMHPsGgt0IEGyTKzcuHKuMsiG2q9rqd86V/qYYr6t7  
1kBq102ip17NAooLVbyxH7tpcuJVeXP0Uj0ZjVTHsFCEmipPPKUqgae4x5jWsr+  
9LuKS8lMuranGvmy1jky79N33HaT1zhGtgbbZbrG/9645m51+ay4Iuy9qDfEbjYS  
pP9/ULNIIf103peM8SePKeHPBQ1M9mLtuQiHSBHvR7Orqrg90hKjtL9ylA12TCX/+  
rJA1daW8EkGvCv/fqhZHFUf61c+fEUAbwfljLh+kXRG8RsBiKZrbmrEwRMh54NX3  
tXVeIAJcjNgLca9gAhJCWNxHLHgRssyLojJ+um+wqfAto+6FyBsBVo25d9icY0Gx  
YExnAhZmb6TeeFJK6pSTAUFxuGI45snuV18CkuDQw8vikf5W6oQW8nF/scTIqFa  
JJp+XxxgULuIZiUbWjtiw1+uhcNURdfdyOur3s40nM3U/vC3KNOWZx/1x/Ixy18  
NGBDtVV081K/CDM6bHwrD0kL8ofs/dmCjje6BvttzreghfsUGzWUtUEvoqSSRq3v  
9wHUFeeeb9InUy+8py3NZ8MknchYxo8MrRJV9e8PuCwn7X7sdtUWX480/xgkPMFH  
wPsFGQCozHXWctiTEcI4RGk18FU5HJNroSXBukl41JZ0GyQRvTVjt+/nZNSR+l7L  
82u2zIehBrHeuu+L4jgHR4LxEr8uYWeAMP26nSknylv0cQNFxjFg6eyjEc4Xw2Gf  
Z7yGmFusINumJfFs1NbFk63r+MePv+w933tB5ALIuswdUK6/J6x30f9eImNquKi5  
obPUcLg+GivgRMU7wEu+Zn8azh/l6iLikSat3Qb/zniUsy9QuS9dBpVtTJ/7jscu  
EntAhg9TYkFPxzSfmsFWx+Xj0Cw4ZLbSEZRtb4889JJNHUzjYkD4ZIC07TLmQ8dU  
zn56HLwr35ekPLZL39VLFsr0rc6CVUAdU0Gkb45AF1cKyCg0N+ZLroyxFEYQk16t  
b6b5sz8qzJ5e9egbmEhLBnFcF6W9i/rDsBXDX79wFw3HEaQFLg+lNmZb0d6h+y9X



GnoKp54r/qpesHGb1nvcYLPsS660SNAdtrtlQ4nd4CFGC2/NvUMEmwG9c9ULtIzQ  
cinfGzF4zwaJ01G+Bcg3hIGzTeGD4orgi3Qrjq3F2TRE3MOVlFSbcm8Rd02ZxJFF  
QF1tquVad3zFaEMAEI1aLzxAv2YYL4dfz2sVogLpsAMETUZN3TfMHQARZ6aLm+j  
d/YsHh4Nh85LkDAm9nKSXQ9dmi fZmZNMxqg/jUWn4VPzd+2wCojB3VYyHsJH/o5y  
1H0X9Q7NH1Z1SVRXiXcms962Jrf3SqD+hpt6JE9lVdAly4Hi00FrwvVmchAWBCr1  
rEXjdmPy8dnuJgkwcbZ29A7deT6gjRRKi28lsNKhb7fHAV0xTuNMsBPo+l0QvRBn  
fujyQT0t2ReZCSmSkWW8VeA/48/wNQZWcEMwGn8syku/RqeFPbL4uZ+s6n8cpGr3  
GqBGfKkFkL28quqYNR4YTVU9YieZ9hJvlQVaOpWAYyGLD+N9l8sl06rGBFes0PDi  
buPKF3UyximNUf5gLiK3R1oIUfKY90+WUFD8iHkjpVpI0v4VSc0m/cjEJb+vMJ6d  
vGMBcX1coNp0VDD17U8nZqftIBe13qEziXquLDjY1mKAPzV2cLgqpWxcPcISaFLd  
q6CsokUPnKqSCQzJz8rbGtndG9ZwvJ3Q/47/BpLfg0sq27Y0tLAWc5JYQZ58Lc6Y  
mbWfewIhV7lqWdzTQhD0y1NPjcdXtdYEwY6rQIpxiIAC7ztSU2VRKZwGaQDU4B4D  
V76PF2/qJER0hMJYgU6/Hn8ZViV4UNSAGZ+Ps/ZL7pNoWkq4d1SLNZcCWbSR6yGB  
iysohv4B0IJYz46FfQo3t0ypAvVQh8fdXPIp62Kv2Je9TJu4Sy+kL3yrLnW0myTe  
qqC05TDtARAX6ygg6L5Sg0dk7NQb0Gx4XwiPXbpfxDW52Dopd97xtxMb950gy2f  
ldsn6kkKnrY7eUka91T+QB2Zrds51wUYbBfUJQkdK+MSWRgjHGL0BZ6mvEbn74yd  
CralklyxgtiHsWqcS3Ze6b00L/QPfkmcR+JdBo54yQoKW3lcw7K0BR0FWSyKHfwp  
7KqzrzCtWYNU+IiQDKbo7hQV7nVr1EM22pCW+fKo7lpxygx14xBKRvo7IuPMYbcd  
w8lapKmpF55mN3Y2jbdwGzcJX+bkVDxfyeL4gKog8Vg35t0XSvmPrunu5FV5QMV+  
n69uqFM3VXX/oZY4rOYMC3hmd2sW0VvFCfJxpUq9CdV3sBLnC7X0N27aBFRg6aXD  
bG6Ypbyiy3ejJ0d04LJxlasoQYbTVtiIgvARbpeLWtB3qq5WJcxhghXywu03X9CW  
esGiyfkZ2kL9eVkuXg02iER+50wo6PHJ0KerLWD3iVVH4LqVuNtZpLI+2Rlh8sNw  
oZ7dgmZqcyhDdtf000tKADjBaLME0Z7ah13KEgJeSysTt86lLoQli4W1H0cTWJ/SV  
Kj160eohSK9DPns1o6EwwdRjh+IvB+Ord3jWnvmLc2E97PnsLE7XNffHq0oYhMo  
V0bUUWpIhWA9Pg+n4lyRCj+D04wZJFOUQv8MirUR8+RyOwiylBmvEKdKzxMIe+iq  
PV668dv3RKi/HQ61LYHg2KnZl7Usm0McB5PQG5vS71zH7jbQSf1jheQ00tpy6Uxf  
20qp1Z06NS49QeH8Yh2/OqvcfDBYDLNA0V0Tzs0Y6o4RAKmkoumzRAE5bUjq0Rz+  
1gF1rKfW4+EXiz85GveUN1BWeWrncb/Yl9Xd0aogDoAhaz/X2ZDW2ALGLi0QIJV  
uZmYEQQ5bjnKE/7lkY20pTmAahYKT7/jhJXEYsKBYwtFs/C90u2d9L3qKN3p0Akz  
2pZGDZ/2N0GEn2kMrweD4g55Xk18wwWpMqC62dydu1lfcRl35K//9xuuFDemkCF3  
pp6fWtmbZQmT889+B4DNLdPpo6mxCo8ELCOAzeLLh+rkwUwS5nqkvVMgohw7zS7  
/b40S0gt1ed5PqJF9l0WRZJc59oUd2LzKtAl36G7hp1GksH21Ed3G8rrMUWBtItX  
n7p+oBF0YWhjuz69qHfBA468sdHvVON2k0w3TQveSVL1vDeWGEklQ2Hk6SU40I6s  
4eyf5R9p1ipEii8aoC8a8p/yaPsHLEWrm9oIPNIW0q/1N98vNHQ7hoDypb0U4nv5  
cpxCwzZawwsKUFPLDMQTUSonVwJTFGqHKCo4v6XrKeM7eD2+gjVoDRAMvLRWEGR  
8DI fYVnIQkdZP+BPKlx8deuLTZg9ss3ggqzew6lnVuAs0v1B0mx/tbjLPg9syjZD  
pbTExS0LHKm0ynzEiLoaqjUY7yJ1oG51R5LAK1ADfRwuW0TomWJjTl/0FSqAAvQI  
/El6wcK3iq/B8dZTASeWdj7daey974vywQaN0ZG15z6D4QB9SV0oWgh8aiaPPpx  
cMFEu/6z7n5iXLLHp0zhFe4mRtFvF0vMuYI1qJLYoTyG5yJE47y3uw67ccA2Ftah  
NSyaPZ95Z3KHUanGSTxBPNds7jfjNNTs+9A1XlyX58aNjiwQ8sYfoGLPGr8n/qYj  
mpWY5GRB2S7/QrxvNMd0eHv/2ud4SEYmSzYxmT68RjybdLSKzA3nnXZiN33T+JGL  
YFCnS4Fy5TaryM9wByq+KfIS0CkloHc1fqaLJm02xAu19qwQ3kxc2sjdgrIRKrrb  
4Jj5Jt1TWsXnmUGL3B8IAdNb0XpsmAEO/YCeD7Q/g3GCTShzBQ05BGkpKb4YM8hO  
eE8v3qnJLAtuvYfFAnJL3Pf9qbXy0QAeF8xaoyQybnq5JyJLUvaamy0tPucvzzfJ  
Fb1oj1B2xrep1pfqBLXavxbS8JZTT4MbEWMo0U9CgISeS9UeP0rySCiDvVz3cH96  
5/QBC0xZLHU91+D5e7yollp0WGOlf4qzhyIneM4FJ8Z9Q49xyLkqISs2tS9EDttG  
bZH/E97aHiKubXc/4/uPnnBQ07Asn3ULrzcP8udMMD0Li2d0smtCw2svTT5nEt7i  
uiEU0AwpEppN0SLxV+4au4eCImjWnPCVcLwLDqYXhzbIReCmvQXWgaELHAAxWSdv  
c7VNcyKVjkioYs5/eqn04aIozg+yicDncbSaDyWv4gCXATnvK1Farjky/CHx90hh  
u7HDwrUevUpTAhej1bSFSZWNCAPxy2wYjSZUWty7sHQiLCu2BS7BPFwkpLJx3AaB  
+fRmXmSp1f/01FoZopoGK+X1JNK/PNmRTphxUTlioSr0iT+sFT1iMfebVgeBe80K  
0Fejd5/l+ObIcar81hljGfz+iYh2hmgbi6Nov2FSbAWUN0KmJFMGGvAfdYf1TBud  
xNGFMujqUSHq3KMD5Kj00EEh0UIM/4z10W/IjwGWjyVSdJDpKhLszYGSuDTvzv0B



gbxa3fVkrT8Hvhx7L5TOZkHe2fWm0ESYSgkcU7YbqpPlc4kYTn21CNjmdt5Gv7MY  
90TNqEsFn+CefJBmBsHfM6Qc8f39eGEbl0W71/hsIINwINEqlCnOZZWBcPB1gC86  
XJxCIE0tbd+7V7vxMFtm2vxpV67EXwPBcPRpYziBfMJR7HQ1S6SC02iZA/st0sxM  
TmAwd0CdLplEylsDP1b5VTe1Kw3K4/wyZzUDG0BiX5NEsNsxbUbAlpapoT4vr/K  
rnpHBYazsko/4SNI5tSVba6bBgq10gNI/P+1Z3J6i8n420hYE+kiuuVZl0JRdnvL  
fZngAhdXdP+txjp8x+wJ0H06ECF8weegefByciOu+IUhXZhhbRcLn8cD1+X28pRi  
Iu0D72BtaQtFBAiRUwJ5vvNNbP+93Ppy0taztZ+OALA8uwSfFiXtZJAzSrhJpQUw  
7u5egWZm0q2UYbL5FygB7MNFvSy8X8wuLnGzYR1D18L7zVYXXRxlzqm+Dt0ZR6yt  
tvdgWdJDCnjmuvmr4D5sooEnnTAoV5IFgPunrkKEPhfLEa96dK4frICYF8+sI716  
4BxEX6Lyyw0N2kVKSNOIG0g7j0qovm8VL6WD2c5MrgLFkzrdEz5pMwdQezORPJ  
6of6JgxUBQVGYqa7wMNTfKw5dsFePax38VbctwMq+EI0ZYyQDTF0ue1Cpboo9EEj  
jcC2fCV0TOYMPnjT2rJnZLSJyVSoqlUqz3MimbWhujdhCA98X6Ge7pI8bWSHC08t  
0xV4D/VtednzBEZzmNFBTLQ5YJOnia+b02qYX8HxF4l60iyI9BnFScDnLNvKLlyi  
UuLpLtU7v61dWEL8VWn4LmQohH7KqKqJfi6/MhZFLcwUgprG+kUCyFH7nt88+TSb  
in6JfjuRwuygd0XEDufkLT+I0laJWe6d/598WVPs3ceevuvvSF/Z1X7E0uqJ+mg3  
4GS2+mrg2Wg1y48r/oV9Grf695xPqqS3eC2KKejJkUBZ1GTL43Nm20e9QvFrJKaC  
uklxrgrtVYEQ4UNjXpisHkRsoEqy0myFKTCTbYJ++rT+l4eQipdP8A14fNZ7sP3Q  
SLQV8f7Lm/s0gbcu7bJeGDJbDTtEq1SvHVQGRXve64kwU2ugdNix/ftCR1XpUR5T  
fNoU7J+gxMS/086qyb8KTLVpw9WkYQ6nRiAn7D/WtCo3e2pXnfvpaFyTr1xmQRZ0  
BbxPAnCkNsDdrvAzu2VBKXv2tqpaS22ePDh/d0hzZtLJs51+hXkWebtmqCAR28f7  
L5sAWLXfL02eYecUSwLaSZKGbQYYC8pKgFRTWH2sBc3VJ83y02BC5HiEXb6KyR5/  
Mdz0o+61XYIgGDY1cPjB2nZndhiDxDtLssDW+rIiC8poCyDh+SWKS58H2dyrzDJS  
eM/mhIN42j3nxfS2WL9xjlqAr59hBGT00ZoDJNXq1UwPAUPQg/bHbjtdlmmxDgUG  
FmjYVSc5hKTX1DjUqFEuyK4USZSoM30zjYeVYT7bmo2APIp2xyAKYq6fL8GQCioS  
DJQV6AuSQHRLGjpdIc7cc6KrLnt3AIXZPT5z5o3Y5vAL0rD02AnZ43Yl7CXK+tYE  
oUc7nRaHfVLqqlzJTINC4Mh70LmA+7sToM0Zpdj0g7hUFsUI/GfhE3cgvyY7T4iE  
0VhLgHZo2VKTevDjwlyH5Tg5C4nqSI7oE8u3UMgbwe8Igu+PHjf1to0o8DNAE6Dc  
TKArqNPWC6GjfyntPsdMnS5FJ/FzcOVHs1ExZ4e5pbn3Ssn+qvsxo6pdPNUdf9ij  
uuXZE+SMkoj6B2fWYFP1VLV8D/FRF6BcboNTy8lR55zg6Pff8GDVE6MULDTuLq/c  
RjkiufMtoCezd+gwWyyQqilGcp9Jwx+AD2vwmAQWgYSLq3HmEyAUZeqbi8IEcFt  
lZpNx92uftfurbSioSnfPCaugNT+3oS4pQ0siNt+O+4YuE0LI5Ug81XIY9qePqH  
f1SJrxJWddd1G7u05zkAcKFSPvH6kWIB5rt9nk2NhOHly9H5tDTa5Ku+KldSdUrG  
3+4h0UpIirZeBrnF4SrZK9X39IPLuk410+AbudRvB4McaINFDZyFD+JN+hpa6+43  
SoXDsdR6Q2U+RVrdLEYcUfhJo2ruSck7PmyRRIwh/P7tUfKHkUPXpx6eBds08Udj  
L+ewktAqbHlhdry40MhL4rBD8g+x1dqf/UBy61t/P0p5yaFttgroueXnq+XBh0Li  
loxlaHH0cm2KFYON55sfHHMSAyIsP/PW5igV2RtiQPpf40gqsk7GgUkM9UX+34TM  
hvT8JE80Y7SKODEtoMQS4nAHPwRY1eqa5uBpJr6JxHZefjFvEyfkXgixvG8UE5qe  
p05P0ypV8Up9N95MuaAvJ49Np2XH9rmsgerHujb4/8cSIA2Yanp1j3EvKa0l6HoW  
isfBi0n55b37YH5cDjSo/J1SL3/ILfCt+tsWPY9gqQfHLY+sK/BeXGKuXwIkSAot  
fteHLSnRVKd6G3K396c2JkTdAZnvCSg1G8C6rF5yW2fbYzqiwk/zNSpU1fBcWBm7  
a/ghDmcJrVdheisVut9ujMyqjmU2HUdrUHaQplvjW6BK0gdDRmZXgQRpU/QN1OD  
uUUF8Mocp9PJ30ujSW4im6C8616E0e5A+yBbjbKmg6f+6z9zyWbH+B1HjG8IcrHA  
3ys0J5PMgsCZkYD8Fk+Bhdof3ZzUykrysNBCf4N7VXLXSHWoWsDxx7YL/aHLan5c  
h05H/scsK/gNHQWRBvb8bRXLlBFLphLmNh/sqrbbUFhFcD/7qkiMbM9/OBIyBq/w  
+57+z92bxTjnX2B5nVhl7wks00uk9o+9ZhsHG2wwbqh11TCnMt6898n0HzpMNF  
lySve4w0Bcr/j9u01SCoyTP8yp7RXJkiPdHlDAdd1D1cX/5MMWHOCUDMHTDYxyTV  
QCBx1Sca0ZzJHKZdj66orSkzvZCxorOQrFaCZS70rLr+0eBtzS7rLJ9mnkCQYdJI  
uAKVpVMTr8cS/chXo36zS6BB4x0b1DAP1X3nXJA0uvl7JrBt+H3iRzXBrHzwvly  
dxxd9lx0tj+BbB0zA6FUQAUjpWx9B+a+t3N6zYr30AhwRha2n69TPZrciNch4ELE  
yMdIiqoSgph4w3PxxrgsrCkbrsFkCCq0IY/XKfFZDV7ijIQkTjsh0Fak4kv0KZf3  
KyYUuHAX5uv0N6r8HWIjW5acyM2xg82rlyWU2CvI+fcNCulw1AVBNyElfH5LUTN+m  
vp6wZabhz7yge0JgUuuf0s3j7GnlVVL7Um+A3q+l9+jjFXesmbqjhCdPWZ0fI57  
oLthQ+2sCBl+MIvw0c1GL0DsAwPApShxI2LaUXo00X2tKxZhTVcAUfX5Z1iK343j

YFJakkvefQ6k6iS3RczcvebjJBfZkeDh4+PN51xTqkF79fS/2qBpzi8gTaoPKP90  
mT0grkHRRhyfF8QESSR+jnoZ5IvrolEWpAdih/Ynlz3lyRqBr1XuUzHAoTalP9C2  
otlRFkreAchXl0XZPNjUZDfRno7HgjswdyBbatiFKJkQK9PLKrZZEutfrKj0sg+A  
Ju09DaEVIYXQE5yLj39u0Q10m0xw0obJ7PetqVoF9DhxiU/MzmXCpNw0RYAy2fh0  
q5uF8/3t46ud8Dv5Sdn59IGw+aWidc0+JNJXv9KJHYAU3wync8F051S+m6tc1IKb  
JdFow74R0Gy90383q4vGU1ZBmxV6p2e70WQqX7dCG8pybSL6o7GAtvXo2BLXRSF  
yQh86a0gTLJZHpJ6oQTRfL3/9duM8S3t8KHpytPkAaC9LfQMyg6EN6WDsNcecGw  
c9+XTDZEy1tSjw69CouHiDdIHeORB14inoMXLXyRhyqJkYzkIRn4yAgdZ6Rv0r0r  
KHf4bWZNTJ6VUtYxYTj8CWTla5px0msLMHct3fQdF9S+Xxmdut8nD1J6X6wnfa2J  
Hq5zXFLOfY94XF/pC9LZHgFL0XCpu0eyF1ZnkYl9wWwNm0NEWBUgHRyxMBG4cS2  
hoRRzniiL7Sh3eLuwG71RUEff+uEzjx6MnVNfroBayMPJ20a4YQMBXsdfLV8f+UG  
CZ4s04k7dK+/0aQhHp9AEKta6ciRzXsSGdLS0pLzu2typjabD3zjHxpko3FPrfm+  
KgjGpRDP00jKPH0nXbC4afBkbLqnQESQ/uFPtdHLP8JxRbejhtOCgs+kFHPt1JCa  
6oxW83+y4/tzN/dDWDmud5Jv/kgmQODTLb317mSNnB1r9ntiXhSffLmKdgriuxXL  
wjqDbG3TqQlLEBbxllBRNpCX2bavKsd3XR+at3csbzB5COMDZ/VbeTurvX7Jd1n  
T4YJulKbw9bj1v0q4MLPBdt/YKf5e1MhwXmf9JnNgzcqGwplRQvs5IrYcEIGZmUt  
znDCP8bfSKmPx+per6mzK664tkLQqehZIm722hlT9IN2P0zjcDOChWk+g0hV/Mam  
tn0ssxkWAIVHD3/KVlo0jZY0Pr6sM63Ic7ekRPSHPXN0zpRfcNjXoYXAQNG48gUX  
XC2LS60gdyIHLiH4I5LqQlLpWnQyCPV8w9qen8LkWLJe/WE7eGR45PGJcEJeoQ2+  
tLx7U/Jdz6aifLUovaLEmpupdlc/QVEoI+npicbfz5ksSSZ10SYPyShGvdWw0p  
cKE2DGR+K8MET4+FvAn9RPBUZfT0mqCpvK+dfX53+J5swL4jxdrGLTx3UnlUAAue  
snAg+QIqno0qvYLUctn4WDALkrG4gvkZ/P10/bHzjh26IG0yr9IJzADENVfZhnB4  
n3N9Cv8nHY6Tx60FCJ6wpCtONTY/XTPJG4HkrERTguouzN2sRbB61IhS5ioVJjT  
HN3T1nA4wPXEEf3qoFRT/qcZzAe/SDF2kmpG8ExdT3A0kDY1TSN++UWHWEWEr406  
4y+L0E+dY/aLuLmr+iI25GHAQUa7nQg6iL2UE5VQ3fDer+MVaILopyTce8q11NvP  
f6HLJvfy77B8rRIJgLv9dGDUTzmP2Y/2v3fS5nqWV2NGJpn29U3HlFgHbYgPh0w0  
GtlFAkQkEiYTawB6FeZ02XABv4xX5bG0uPEAGK+7zbG4GqTbcxxBL5xVv05JG0Wv  
Ad0eEM+YoXxhSMHIeFGcK4pszRYa9q2RNSuru3p3KF4b8Y5cfXp7MLsI0Shlqbkw  
w7nZwfdTwsDuWx3jABATrck3N5ifQ7Eb6HNEiZLJOAncCvr3CEsOZH2WKI+CuKB  
thsj/uCKtdr2L8k2gmwTzp589LLapDXIgrGy1CzSSz6CDQMhWtenqRoqNzwVXsBw  
osBC1vUyktMe0R1V6TQl6bIUK8xN0loJkp4ps/+d7f6Kc6r2XnE/PTzP3HwSRv53  
tuB+U/JtmnzaWioFC3ZmLvme1hKtDAOQBmBASihGjmah00lw/iP0f0z0T9+Dwun  
SUSceS09kOK/CbFNpmJsOcTDzXD2hpP9oSkoXidmYcfyLL+fxH6XMPvQ7K7pKgf+  
YK1YbrfBqH9qnEn4+21Z1FFcKDqLd1cJvabG8K7LZdu0KffrsLUygI1zR0b5Ch3q  
0gGPv/Bn2h2/yAV6moYsK+7XCoM2sez1PvX0WkfK1jE5K6gffXxJb6bs6m0MpIIP  
p29p1evt8SURK1hM0+Cvqznub9q8r/oYrLF0U0Tt7I386R2RZLKdqGni2JR76i6V  
2lBOU0WhlXtC6QvCD/5E2dhi6/3s7o63SadWGuW5CUcXKPjuytmR+jFMARpT0zMc  
Va0qAC9I90NAeJ13eTLFmNWJ+o0MY5Xj40NXT4iGICetcv75iZujmPs9ThrIQU/k  
+Ct+VWnQYXSTz0+Gx5zMtqiWY7nSgkHxdHdaRLtkrxI8MkF2Ee0hPIGdrM5RuC5k  
LTD0ANv0uuwvA9erNG699JQR3Km5d9kfz62a1lmmIAo5hStScLbRqK9Dt36fQgCJ  
CrugEo+SkpMyC5VjzS/FvaqutZlDyeND0+l1fXL5Kg0aytBtAyIX7ndtxuoy8r9f  
DhjVb1UnKLFBVIiMyGenIkTcdghoxQprWZvRIKIO7BKiuV0fR2t6gZuoLerc1wCb  
MULE9R5ty8RwgJ1mwvIw6KlpnwK0p/ZrBNCA2H251ZMdKngHGP8IOP8i0p5DFOEk  
DTAw3f5+5r/pC/3cpD4wxa49c1U8DCLJyjEJO/8oLc0oqTdH58N8/tlynLxQUHHA  
41hqCKQ3xqfzj+QBQ1mypoMocfgHCwoLy+8r8ikNk9HXhYB15fr38/zFBfQ1QQka  
YajusDSGMVbLPiYjTYDedqDrbzCr0qIlsF9GNmXRF2hfEZZppl/AJ83Jh/02/FvO  
cuv09TAjS5dYY5rUgokyhFAEpDjS5/Ikn1AXPL4CH1iD0941AAt/c6CK8leJrLd1  
IrU5AV0zQ3M6QNExpNpOtF0Yd3DUMRHx5tbaXIdRfEZx8kM1c0BxKfif6z+7ZL6e  
u0VdRyMkPPOKD0hyPFk+UndhVFPzVpVP5AwPwDn8sBCTM9QCJQhgf+5RccK0aB7Z  
LI1eR09iqnNIEeUNhAjtRG7HUe3P+HUDGxIWZkBq8CAoLY98AXh1IM/5V1j8JMtL  
00+keTi4RZBe/st+hG0Hf5dLGiCA5GyHC8bu9PgYLPcu6/BZvEOHPTWbQV7I5PWu  
D7mLRTxDL8/Z9t660TDVC5Y0fnN+3FkL1wJLWKvq4h2qj4V6VaFe6wi2n9E9ir5  
GKFxwXrppNtaFFL07/8Jpoh0L4AoSWvuGOJNBMAduWdvwG0+DNbWBqAAId03WJDf

```
wTbcucZr88UjSWoc1xZipSmLnrrj0dw/2cB0ry9XPYkL3YSJhrADRCnbsfn9478F
7P1XZtXvD5XGmNx3bbYu10z4cFt6tsMc0CpPRjnkEbc3yEV0r6HVj50zYMBHwd1l
8XRHKJr01yVpmMqdHt4V7890ubaRcRtraE6KXwtjCZDkQQA3rjc6LmkaX3CLpJ2v
e3gAtWNoHI+r7j37iBBAstpvmfwXGwX9v/TpH34hiI0eB2WdPIIoLugbZic0qrQQ
WkfxqmpBUse2teBo4bAJLF2WtbB1sXbqdL5bJ7j1PK0wl6GDIUs65K21EJLHKxuB
WRFLL2x6PMG3eBJNGdC/e6pDqjRBueCA/R+WoxET4EJhCsUwEzjoxhI5qrF2l8kPz
zFl8ocqrX0FB0Ye0bPPnu/skDw/Y8rJJ3ttRlaQ9qzeJ9U8mv2Lk+X86a2Gbd5HD
oSzkt7LNsB/43deK3uE9GYzHIprZoL6XGhk1NRU9MddFAzOCMIx0/pvWgNpwH0q2
9/gjJkV0TJDYdMYzJw2G92729ocYVzW7WJELiuVMXvsfYog2kRcQ5iRid6ehiMFP
dP/ANWv1eJnyGepkK9sU1WWFu2MTJ8uVbwfhger0tdKTHcbl0kB8D/rLJAXp4A78
sM2mTIHE/bzeC1sHstrG0T/V7r7iZZIP1Fa69MD7UVyJPawbiAIRsFixA/BLHS0/
RwhvPoRUZSPE/5qNa/Yk5AH1osdoo9pVNJ25ef4AIVT4zwhrSinfbwCerrsnPo7T
awzQ8XM3838t5KcZzd2VdPhMWXD4EwnVRxYncVqvWfWwyZKDJ1iAfDScpDrknFXJ
uEMhlKCGFB0pLU2C2WB1iG097uxdWaYI61V0nCIkloYB2KtIMYPeRs3ANmHelTzc
70an8hGkJR6rs0nWXgt2ORQWW/rrTs1CE4+dqsxwccYiCQqxsV+fBhFA0woJKo9B
LeFKfE6JE7e2s6ChfxwsRFLJVjK2jNGG5D0vqHhRpljSsyAiMwq0hyUyNA+JmnaPs
DGUEEYqcDsZpTy4SyiGk2Yn1Tkebqx91LEQMVx9HsGa4m9dqlrYFL0e5v0wuJn9v
u7j+NWqk09rHxBzfEB5wtCR3Whvr21jLuuyfIQReeAQCEFWclq4fs9KhXM9BmaWF
iojvckGL1dXPcjBvZ8pFyykm4Ae6J5hfVvRq1vVLXnm6TRq/fFjLBxI1aB+yk
0vuBTUBnyvW/ZJ0HoE5fPL1Pb3AxbYsf1h5Ll8zNFVnISfpEEE0CcBsR1a7bjg
KYq7arS40y3HBex8SEIUPPQVJzXFbMI2kBUUnSHZto172My9xAcjXVh6xA/xlyIuB
Bdf3tHUGEGcvyJSEFVjwmAdOHFoMMNj/quDYutosct/Sx4+f2dwexM40BjACG5Ig
ph3uI8LEN+yHJNLhavadl9yJvdTLuQmcNJse2b9TMn0e2Ra1BGMWVOY0zurtT7WT
HA4YcdHAYEcumedBkLUC8btkDs4/kX9LDuocsSYV92Bm7DrIOqk3UKxv4fha9aNB
aaxCeri9FCzLwsf9jas5ek4+jzi3nFQp05LxPT0mYJJ1HVTc0uZxhDGAIPoWhC7R
B0f5hCD5CgOmZUnh7Z06LIHLS0ZHBQHR4+Uf/E5JpycF7M09Tn9scYy0cqaDG9o
3vwhsPVE4xpxK0GD60ECR5JMA+GgfXOTW6fgdIoaFD06BdIPwcc4c0oBxj7ebQoy
tAu5XCJpuJLH0UtkT86fBTGD76JrVxU072Mrz/hLNI4nHc1gkSF9brfaAqWDMCdy
wxvgtaiR4v6Zl6otCde549GCTaU1KNqnYXULWlgu/B6Pf6nNwE5JzZDHy+9upcmg
DrPlwinb+rdvNC8veGI7gWdfQG/YZfAN77hM5rfd2XQIsu/bKSYgnM0qhd4+drU9
HtFmeAjsonKmc00o0w0Ex8fvEIF8QiW30jJzixsVqvdy7n0rTjoS6fd1K0AIETbD
ThFEg7kEf5hK7Q67WlryQVE71bMpVb3Nt7jR0g7yXIawZGD2rZxluaK+C1L7ZULC
TR+j2HmSu+r7fjC3LcLymWBhSPTapr02sQ0jVMXdeWZuK3VhuB5e0pe8v5+suEuF
Dy2PBGf7fYTPslRW7zv2ZhnFeNYJ/mW1PQRIe583qQQ6PxtkwLFOpF76kksMCJrC
Tx1hCBrfVaILU1r0kIYMHjgYL1SSZdV/KW1xWfkgcD1JC0HIvC8jdo3S9D6Blc/s
ETi4HDwDDbH240i4WwtsNxnyE0w8K6Z/zb77WEVUOmKQiH5qSycjrQdKyKUhxvM
RRNbWCbhoDnhWd5Iws2g9+dSD/vFJ9RuEh5cmqagiMVYmyUWhJU+33aBAUcFbZ+g
Otg9K9mRFE13vDnYzTD3Ja5UwMMtSDyE28fXXvmgbijffaiJZ5FmeAsZ9HIkUNU
akK+FII+LNZs7RfuQL2tBoChex12ZjLtvBioy5skPfwuCRX47g6D9oGpejE071+2
mqkzCBSf9PbQV95j41h/yhwFT1B0emYpcI+hzVJaMOKcXptNyDQ6XP+ZhD7rlcQD
FwwJLr17ELZ03U9iHdub1dP0DU/E2oFwEJ844RvNVl7RbE+KBCHD9+W1GhvuAh04
AbsnEw68CdMhsA5Jfgt+A1VHdMjgziA/cvpVEhKqdWtReUS/2PQ9S0icuBwh87Ts
tAjsRMq/Oqyl0LSmdi01yBtdfaVa08J9ydVjB26jNsLk+qpV55Q6I+NMx7oZLDjf
vo8450yxw0zB7xQuog==
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the SPHINCS+-SHA2-128f-simple post-quantum algorithm

Use the following public key to test the SPHINCS+-SHA2-128f-simple post-quantum algorithm.

```
-----BEGIN PUBLIC KEY-----
```

```
MC0wCAYGK84PBgQNAyEA06644sgf45+BYFEyuQLej72GY8YWNQ2sHEKTYz515v8=
-----END PUBLIC KEY-----
```

## Sample private key to test the SPHINCS+-SHA2-128f-simple post-quantum algorithm

Use the following private key to test the SPHINCS+-SHA2-128f-simple post-quantum algorithm.

```
-----BEGIN PRIVATE KEY-----
MHECAQAwCAYGK84PBgQNBGIEYEgzEWffewdd8BZUPj7Dkt6gU1kqbc81gccq3y58
AqR706644sgf45+BYFEyuQLej72GY8YWNQ2sHEKTYz515v87rrjiyB/jn4FgUTK5
At6PvYZjxhY1DawcQpNjPnXm/w==
-----END PRIVATE KEY-----
```

## SPHINCS+-SHA2-128s-simple (1.3.9999.6.4.16)

Use the following CSR and keys to test the SPHINCS+-SHA2-128s-simple post-quantum algorithm with the 1.3.9999.6.4.16 object identifier (OID).

- [Sample CSR to test the SPHINCS+-SHA2-128s-simple post-quantum algorithm](#)
- [Sample public key to test the SPHINCS+-SHA2-128s-simple post-quantum algorithm](#)
- [Sample private key to test the SPHINCS+-SHA2-128s-simple post-quantum algorithm](#)

## Sample CSR to test the SPHINCS+-SHA2-128s-simple post-quantum algorithm

Use the following CSR to test the SPHINCS+-SHA2-128s-simple post-quantum algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIFSTCBhwIBADBRMRAwDgYDVQQKEwdFbnRydXN0MQ8wDQYDVQQLEwZQS0lIdWIX
LDAqBgNVBAMTI1NQSElQINQbHVzLVNIQTIiMTI4cy1zaWwGUgU2FtcGxlcMC0w
CAYGK84PBgQQAYEAXndonwKmcHFM0uQUWLz2ib7+RmWyKljkb4Em6J2pnN2gADAI
BgYrzg8GBBADgh6xAAIf/u7Qv+W6YN2b4HIj4Zwf4uYhaob7DcTv1xG/1lIcMXuI
o/vxDIfUAaSu09wzXVibK7a+RRcB6BdDnQ3VQdVkr/wTaLJdv0PGquja6gBamRp
75TyDaD5dQ4EMkWSBf3NsRHKtnri+47w3Sg6kQUp3Zd7vwE+qKESAXPFVUetUIPQ
7EYlHg/tt+Hv2Yw34SJIC1GBkzDTv1teatkKi3IYtrcnfn4WdKbYhQgWBu5p5F50
mJ1rVGUXARKUdIbL0Z7PaXMqM2v2A5XatbIYq00MnwUUGittZQ9N8k8hhpKx0CU3
mpsUChcXvFyt7l3MVCUFtALYxndUNuRRebD00HM98wCttIo4/jxB+uWkCZBMWvxe
G95WsVjPh6dfeKwjU3oUhl+YSe2dyjTj0YVd/HAFb0/A1WdV5g3f1Qre1XS7+UJO
NZxRFT+UjiS7jaRjVdiISSTA6kgAz0S6PznG96fpVpk06tIzCqmxJbJnt0aXS+z+
Qpj4QD/wta8rpUx7nTGA1HDZrXjjorgTddGVAXriqYX83wRJOMPwAYp5fFX1nff
AYQznUJWGfNzsSPlzLEVXWz1GCDaUDTbd043u7GtYCXpNjsQkgMeydcWCchl1sLA
cqpYpYaQ8xlwzv0eOKB7vQKdMQKXPG5qfDYz+rQfoUlx2239qoCJZIxWJKzmbS
OrDPqWmT+q3draHiMmCt09tASkd1zEOftAqpGKlkjqtqQPMIHYu00s20AEVUM7XOp
CDBFHallY9fd9pDxxTEBjLKnYvUBnDejE9Hy/kl8+vHzqrR064Kr2ivMIoYrj0wz
yLmWbo4GGoruD+LXwphKkCEQIAPO76QFO/iPG5iH1xkfQFUXA2BgeXfBYB66QujL
k09VUTwT5BFS1sCFI0lpMyz8bCsQQi8QAYLGg0ooCd3p/muk5MYjk/85PiDE6E5E
uBIeqX4Kf+x+eiV8LdRZCJOSjFtyfWNHPTQxjyfJ4WLwLm9fKuCcQrEEYy2dCuJd
5Mx+grf/t4FsrEGNFrabdPd50JwIwNX7vi1oev3kSXNlHPaMns/026rYih9DUC4U
nPFVMSn39DW6AI8CPndLhPVALL6aKbq0rIvt9Gx9z9VY0c2PFyGIR/1nHZMlunGc
+8RjXrm0fp8Vp53sPl1VhKLirclMd3qAa9bsxxAMedzetrVZt8ftU3676oEAaiZt
```



3WbEup03LhL3zyDnmvr0wBKJDwA3/1RJshCnWaPQb9RN+bkDvy/13Wtgi8FKXExX  
GTwgINbxYDNyxAg6I/siSoLuvMZL6L3BN+ghexPznCraUvhE9YoSTROQDruTTqY  
76bpnjzv0/SkojarptmmYsltKsB9NF6DEWpfEJ9IVMv4oMbI8UpqzYGgLP1WB7V5  
t0GLaXTZfSy3sFDTog+gEvKFVHJL4rWkWT5bZ0iNsMYshicrq90qqMR3Lwu/MgO2  
pTOyiRlCCSTofk0bcSmdCwp2jg+7fjWTCWLz13G7NeElkbtjtjKp+270AefTD57M  
+IcV260sIww1fnF91yzZxMoHDKRy1h0CVBSFKhHQ0hjp4ffdgJtyzCdgi3pVCSxA  
xza8xvuKza/F44zhLWLjRxR85UTz02AyI7N7pGtYgp/hugbULmi1CE3aYmS/ZtrL  
W44rXJcSL+Ztw0gjgAqjL2ZYi6UWtUbHizq19WPAq+l7YM7AU8KU05VJjmdurL4O  
MLUX/MaY7Vuh8y9FKfPHQq6wK2eSxIH2N1mh1XfwY3nCzpztuQi3i/VWoY2wNL2V  
B9rupFY4a44q3lbVt6yefvciJuNYWvMrOVJekVBPzZqLWQ/1jKH80j3QzdHYujNT  
ySR0lJQq88add9oEglwiTicmmHwb0oLfZ0WwaocE1Zy4K0RHCPf5jwaSGI0cLaa  
g5hT2QD1G+PzgzN6wjn306d6XnNTHD07+f/yS6znf3L5YVN8Ik4LWFKHbI8bycx  
oiUVQIBhbkoFVkboucGPVz00iWzA0bRGiJBImdMCMerbY1SpieaqPVJBHS62th9  
82ldfQ0iFVmuFi0fvZgarogPS5lgkMe2uEQImS9Ev/pixpFL1pwij0CG4ADldkN  
yu4+YeYmUjKZBFsTB4mFRTWU/8GrT9EhElm0cAM0IgbGwbJJWLzw8Y2JKnIhWqE  
YY3948TW5nKXCV70Vbj0aKDZZtRDsMQPI39NmbIz5pwbJapxEYRrmDt3R/gwBo4L  
KMdycn753XQ+Rehy4cpwXMNPVpfnPZxbnteeATHwpHZN7JCmnCNo1uUrQd+gtzJv  
HTc/Apx4y01ZqFKzMuS02Uj6swGQJmdXLtI+chULKTEgYJKk2F75Sfg0wECgH05  
1LTzjB5hXe1THRQNQ23rsNYpCBpUrUzhnqI2yVLzmgjiSMQ9Kx53pUHD99eQ+1c1  
TJnUq2hyyKWqjeEW43beqqk7YQudmSgLPBb/6mc/jyXI6dF5Y/Iu7Pr4jFVG2HRB  
+rkaNN0ruORTDM001sCW5ZEmudf/Jn21RFkzMw5jqLZceRGvrtjnhNrFrXir5VVn  
t2CY+SK5n8QRWGb+CsPh2rQ/h46InGavNfNi2Cjj8zwSs3EHCEStpdjryA01HrGt  
P3oEhWr51GEnozLbMb9/myL+uArJ1J67Cazl2C+hEvP50/0X4JQTqxGxbzqVnqvX  
6uRlFharmNiLj0ZyT5Q0dJkR4wD3BemtevjBpvgHjjXQHtyiutkFjeI464y2cjJ5  
XywdffAw60PdB8W2ToE9iqrgAdkfJUzAlFm1K3sgKgGF0Hwyxe4igQUghlzoZzpd  
BQDLtS7CNA3DY6Nl4XQ8ZKbDvGL0HCghgjgz0wWc/yTK59K6JHixe+JK/qdJUXYw  
ADr+FxIkFuzK+zipoHm9UsViSG0ElrWUuD9yNGUo7A5P1u47sUs9ykaiQfD0icMv  
2gR+w5Y0bmZ/DFImL23J7d7PQD/rh8vHzkAKM1SxIYFICJCMvEo/F4CqhMtzt3mX  
/sx7Td5Lq2oLCbmk23dfSPXxI7JSu5p/XyWJWe7SoUonK8eX+r0bplalRl6IirrW  
6vDjuehuakPi8mbslQab0zri6FhZjNvM+8MmxI+U5EHRXg2lHnKvoia+gIXRXmD  
TgVtkzKyrotRetcHCWevJVxYK1CDeCN0TZRkuJuo4CoSTfp3Vo3AAHsC140sMKCh  
78YeTvlCwtUKu0biNMOP/L8x3URfadae5EY0q0nmrb1jA7tl4gTVRUBTdU7d0z3q  
M57wpkL8RlgZQgTNo+Rt+4arYk8MK5PdMP8XFDR41Xyjq15rlJppHjdzuk+SrH8M  
FRVs6evkaom6Yzj/FQ27Et+Y2uXPNqQFt3uVIufAacCfaUSTi5Rcqx+bCwqFZtA1  
kqLTjciyHSVBC5kbWp3D8e6LCPxJ2szV6CdQYVMTYdIH3tVkJ03nxksy8jVAX6GN  
lh+hGgzhl9X0RTKUK9jh6jE8ursS90XkVMLwQr2Grsqa/k42D75U9rw7fVdtEG5S  
1yZEhUADhXpRfzf40g8cEgw6u6Ouxh2akI7+EXITdiyS63yBqNiSIAH81CvutXx  
N7PDwBuufI5ziSK/PyD69Eq2Y94K2hzLaCKstaTnNroaXmRETMdT/AZhHGDjdQ7o  
RT8kslWBeLTZ0ppBkFCcYcI2I80+LQu/U2YkaBr8M6o2a3LMyZTUSbvXZ1GCQye6  
6Hc1zCPI4QRjmbm5LnHh087nAYpjbS1dQ9jITYNARYYRIhTG5D2S/zt70NdnPDGi  
QMa/6vCwCLKn5QXgBowUVH/xoTMpiOW7fWsf+suxXqqSiD0jVChURcgE/VBuhu6L  
A4safMy+k6ZRbSVJ0Fh4y2lXVM/zYhXA+LgSz2DQlMuxhbYP2U+2N9o259CkhW5p  
ruysIu0ZHTG1hMkg8GuN52hDzBKMctIZ0d71lGMdzBql/nqn/37czJeY1mMunB9Y  
ccx0MLDN6txWAa8/JABQsLVh2pPiEoYvC7FjMkTK7YQX2K5ghuL4BiQ7q+q6Hk6  
8maba+FpxWI321D/dQeBKPiq3KHFivd17567mpquspDwT8gHwkhapA58o2ORMbV3  
DQu4AAEW8AAoxS9utqvV0VMauwjcd2CBYBy13WvTMQ8du0VnLziIztSz8wAW14aL  
3Xu5yGTlwoaPqrFk86y21jfn83e0tgNtKe9FvVq0yGbPS6V+bE/MgxyhtVYtwYx  
YasNlL1Cwx/DrH/U5WcQ1mC2Q6L5sXsbbLdP/7gImNKJD0fjG0TV/9KrQpKRkJ2T  
XRiT2RG6ba7d0Cy8jq88VRxR3gyvHLm6jb7SaaDS49mYG91aF/lEjj7EnEeKo0Xp  
5Xx1KnVm/PncNgXgw77sYS75sdPMxMTVFud0RoGb495JyCZbru427xYrQiXRHtYd  
fPT2EuAYr1m18H2xJWX7ipKrLhNaMyjIwWc5G62gRWcNuKVF5bLiURVz82mdfop  
N7AcN+n2DQfuHy5fGEk8r9ep+B3Wte2L9KS80qpn9k2Mu/rKnnqp9dPDzl7P0vn6  
7Ih0k5A9uE7m3fJtAaUWLpCqsxnysTTkV4sVC8mJABiqHLZEijT0vHcSwq8N1maA

JbxXVALXmVLP8a44zggYZ29AQpgIq5cvpphMywzTdT38HhxYwOYrTq0SL9gfpqA  
Yq/SVb55S3SADjX8Q0qSwur5ssDCtvlvRZ5CsABpekcaF7rdGznrgjpkx7x38pig  
/70NlmhnFvMtuPIIYLOZLcTghoJkT7nAl20sz89RJ2HgUHIEK094xK/vr1m1/054  
+s6F4QavUaJjoYDyVyONSJiCqT9NbJzGwMKRtw9kQmKRad8wWhuenhMpXBjGthj7  
ImdkFPhJ28vVi0FU0GT0Y4MEJChs0GPK8wLyzYxDhBq8i4eW7FuFu/WPF0AmnT+  
uXqA5KI0+1NjtWoyFEms2Ckz4NeEmS4WXfz669pq62AsDdNywqGH1e1Qfz610npK  
a4zntScNDl1d1PTmyVoQIm41x0bqPh0pLnagLGjR/PE/5dRCDlR0itzRaXHYALed  
OgcFnf0V/oI+MVSyHyQmtEDX+/HXR0sZ1utYtfqUBmJMcLtruyDt8za9A8W2Inbs  
SMkh7KPN0EBn5dx3ejuhLDga/Pp59NZLzf1cUmMLZQLjEAEGVqjuUXoUZk00zymQ  
i/3HQqctXkZsgDTa6aywPHpuxG9uyhprXXLxlzMJwrJifelpkZpnLzFnhTWXjaH  
cTkfS0vHWGjywg6lsWxkter+3w90yACyAYVWkYCD0NMG5LiIrxik9iFCnYaxY  
gxqqCkBOGVAHJEZh/V/Z4n7C9CgaXeI1hc8/R0zffujDtw43+Sk3hpS96+f4sgXx  
XsBX900L03ZIItnSfrKiUvZvGusZ3VP9+roUJk625h/h/03oAEj2oaML2F+03KD  
u2SQUusJ5Ag6bp4qN1hWbJmMfC4bGsax6MIXNALhIpnWhQAsjqzqZH6I17EtwUjKp  
1o3EjUD3BTV9a8051k0IquuqFNufiLe1RHTrlrAd5Mxt507s1c20rOERNRqrqwGI  
PMPsKpLUuvPyowCNWkVIXj8+ZGAumVQ9nqwF5nZovAcwuArn7o/LhuUN7rjShUD/  
2Qfnh8nCUJ9FjDtQCIoYmoVXn/nsRGPnU4kj860rd8Ne974Dpv+jHlm7z5ivNGqh  
PRq0kvEBB4HQ+SjLxf9xfLe7M9A10hKIZEhHjmqPFd3ACTgLDKKs0PMhjz8i0SW  
oV00NY6fM9e736C5ZF0iE010U4ckGp1q9cqjmQ9rWHiV8KLme/XTo2QRR5QEXvFo  
Ii3Ek/UcrmoR0sv2wLCVU1xYX9PXRHe+/AXuVF842u0VeKVFT7/GJ1fgSueTSD7Y  
ID9ynTVhl23cYbLpciFiCvRzNxEmah/9U8tYwLGH7HxU3C+sD30syUVc/hnGP6G7  
+TR6C7c1MKKKmYw6ZzKYySIFW5eyfgI6+WMRufdMkvHr19VELCEZLeGaT4X7NKWt  
oWMQfFWCYugP7yHq4PPvvNR/H+NjYlE/yXUtM5GBnDZD77XnQH+n/U2hPowtm5Yp  
4VnBI9/VprluxW3RETEhPF0TlMquutVaSRQAcdy5lx6/P+zkIpnFrjMRImqezhTe  
Hbki f0CKbgxGws/hEncp9Tt+kLXMf2QovU7SLD5/GTWO7EqWYbqTqZ8tYwSZFAhy  
k09hDRGFSwLFR1ILEprOrPiP1nafYhH0odZbECKCb2DCp4/jzFBE2BeWMoiEUJmW  
X2zCD2Qz/FgaC34MyTccY2DdIiTBdXRoTpT+6MBW8NFqKY0ofHDSn76oy6xamhNk  
Oz76vfMSdikiZyUZLVtZurZ4SyXcMyD245jgitX3LTbc0EiqEiJ+S6mxuXmzDVfM  
yU3oaggrGrh7BDmboBL1s300ib61pAWuim11lCerbua181/kFUXxieAFs0Epb0/q  
OQob+zzotpuVALcz7UqSm0h156iAy7j3WBezrWhJLZHIiXvfvq/bnX2T/XLX7Lo  
wC1UHNyKHCBwjTvhYF8c+G3ekVFRBCXHXuCson8la2LIGAfvbUrtDsH2ed4+P6+h  
lBaXISvZAKUp+QprctXS1C5SB2a5VYIwt102wxCuJpzhMcqVxalngmtRiy44gnOK  
MGL7UK6TmDjJrJvcinY5P1FBdQLnEmvKQ/5NrRE7W0hMpBqBN0p6FI0GBji+RBAO  
MozxITIiVcNUwmoGm6/jMcwRfs9JsAjJfMfMf0tUDfuN927G5Rf+zaIjqM4+m+gw  
IoaY50S/Gv4WbsBY+Kce2DL/c7tEE781v53yP0mKMxR2boJx3NfL6G1XCoHHA6c  
W9Tw2M+04kt+a8+zIJI0KwLzWj4v+7WzUWQ8405tdaxwisMkgaXJV9vGq00RWXGk  
0sLUXSqfu52t4J29iwdR181JYMeD1x1GwqscoVdD0sXE+1FUCJ703BvCL/20uKDd  
ldDspjH++Lm0jneHCT02bYnTonDvUvBNwwjahN3kPxkk4MztGqX9G4wcmhoGy1Ff  
p3SjBiEA59kTMgZpGNa2UVEPSxxH0q0V8uE2NUIdPHz4fBxftQFQHaGFC6TL/Pa2  
wLmyzM1UREp3LGI8AuAU6IBHwkPDeBNLHW7Et4ovI1skHMBavYqi2trGtRWDz01J  
ndv5xwg19M0jpMYawfMOCyYmGE22PyaDe/55IROXBZB5oAxD9mozn6mTp9thyZLc  
aUE6Dj1UmQDEKx8zXN5ND2PGwN4em1b7/YHePvNxxmPX0hUSWNS5/nM80EqYL/r  
Oxaucebel+blbh3rZe78cOWLQHm5K00ncq+yBxw5NHYxyNbrgciAFYew0XIPiIom  
e6Fq8cg5/X/zQA7EB2T92oTMDKQXd3Q/CkbEzdLAOExXluX3D0BHFeirW8PUkVFL  
+R+6Ztua0t3bVqqVmQ+cyb1woStmnMh9tx0g/neGkR0Swfw8T9sF+LVlaaqes0lq  
0xIbunZat6czCFB7IriBRABQ4HM9ImUoccUbLCEm+IxImvACQA3jEgY8EkRYzwAy  
z5m0G2AAAt5+mIpTbN6b9w9iBu5FekEkH7rjDemDseHoFIFYMeLbnHdeTY8BMxSW1  
5o29tug4ubLBRUexD4/T0sLCHXrpAfXB1PVv0XkaCOaiA47Xga4zLbD0efcxvYjy  
/SxqHaNUCVSWpdHvpjw+2/quJMyd4iLYyjMqg2lut9GfrHpe1kDDM3BKyhABmv8n  
QrQCjEiQY3H5dglp0BD+Q65njB8oIya13Du4DGKeLmQd65dZRRERdENG7shvUfp6L  
rkfbl8mdkByQhFn2HZrcIUfpoiLhzLxOmUYJs5FyR4i8QDtsroysYv0XgYRGTFc  
cQDQwImyGuKlRwpsHIIiVUwQ1iInkF1Sa0u87+3+Gve4RCEDxmIcSKzS3kt1AsLX  
JNBQ4s9i2KQGb1uVE0/wu6PQAxIjxycgx/FvCmw7oxGDgRiFmAiLeoDU4XNZLnVv

```
4j0P7e3g9sP09qp0F0TZSagfhk0kJ3iNWfQ/vY72u7DQ2pd0ojDzYPjPMmjRxUom
2It0nSzhn3ZUFxN9jahjCQd3JFaQu/06Yn9vqAceeREipFGz8s/D4V7FH8vb6gWt
fxuSGICqLC0c3faMbPzm03zF6G6djjQMzWx//hqiR+J7Ku2Ma/QX308uxvPZWwGP
NrlCtvlPtPpd1sL0qoiJ6vxPiJGnrMCQ8ABD9Vpbytl0eUr63j5BaQv62r0W3nWZ
hh1lEA63iPf8p6yezPkU7pCctu/3q9/6baWZhn447wlJ20H0L+OLza6A2SyxnQid
0w5Z8+ByK9l6A0FJ+I52WG1FoocX4THUnztRppF+CwzIjATs3TfT1X6Wi2aY84a
qkdwwut56bqSMI/lqI35s0D4MgIaUJUttCYRAX05W49R6y4bYH97X/nQPNu0j2Vt
2iBtET/CYZLnnC1Qt2D3IFXUyyyG7lpBKSqQV50YJU67bd20/hdjpnRtyZvMKt0k
RwMYZPtIb0L6dSIqXusbLZnJ6zMlaBnYQy8mToIVJxdiaXrQIZNJhrKbs34Nk3Mz
chS1tUS5FqAFNknZ85CcZBftSU9cHmGwu1rDD7UWSPtEQ2EivuyoG+nGVZXugZ92
lbPN1DLK7lKGzDpRzdDsBhkggiIIUqJQkA7aIBwBTm6j1K9i+7+tamdJXhgMgJI7
86lRmRuakTPlz14P/exGkxPnLC5Dvp+dK4nojw68mzT+6oZPwAhL1+DM6E0GJRzS
cBnReY30q9aLiwcIdFB1hel1WLKaXAcvGCgVScGHRRihZrhQRxv36ZuHQMvjQIdt
R5Fmor6GK6UbXemtvi/WSx/LcixT2qUC0NXea0QtDiBEhw9N/7UfqLUY7IoIio/8
0H6lpvx7eTdcLvXnKfZk0HdTh0F19TiLJRLuHzYtDhznwGsDsC5WAb5DcYMBnk+
DmFR5gn0T3t5DqXxR50hNGrZnCGps0k7+LXL7ETZwayF7KlsXaDmB9A2ZoFI2F4
W8VFFVJpF15ExfZE3EHsvhh4xdAzshQlaIpWwUHeYccSZnZPvTgvDJ2M4KD3kaVc
TaIa3fbT9CiEDLqb/6L5BpT1LVkkMKy6QYm5hxnespY+c+P3J01Vwe2iU94+HG5c
AfDaKt27VTXAmk97LcX/uVavxA6QDfZnyn5ac3DjEd1oJM3VxcEMz36iK0IeB/if
Fw0bU8aTrjYbVXNa0fIUJtXFnk/7Yu0jmbIwtMDXXXtgsMtBhV8IZJU7nqVf/Uh
u37psbzNzZ7cdez0FvKRRK50+tysbUz6FGx0joiPF0k7a8hSm4571h4dhxMtvuhjF
K3ymBac18Gcuu9+oBfMAIpD7w3x0bk3aw9oh1VQbYVqVLOVN0+2gZQfda2H6KDKI
PimnA9VxTS9kvdVY1hLEQP2EGONqOvMi/5+4wUM/0coJ8ktGxBQq1e+PVhFrvwR
80cDwi9B7JIQZF9zG9dp8mIuJRS0SaEWcTeAhtbI/eCTl8hVN47Vbt+/EnE+QccL
7shcoGJCPJ5y2n6gTy3F8AbmkdSZncFXwFZ0bl8KR7sXyAajRYtEzhvEIk1+Ca2p
SvEqzKS71T88726PX8c8WFCdMoPh+K6bY5DSOD/R4ohd4gRNY1saqNey1ZniED19
RF90oDX10LbttHrupk1+yXjy7t8hLGY6hX3ybkTh4N93dmoN68uytM88ZAN/1ww4
0MxeL1jv6abkDN3PpmshLvTq/ertZddqS4siGEI6TLCiQpTyOCXlwJFagHIoY007
5GpeS+EJTC2DZSAX1exnBGx4Z9pjVTpet9YlguHymjGB1K2CuNSfFNoa1zubI5mK
55tyD/iYxtf2IcrQV5QI0uE5BoTA5sPjv/N8Mob8I1ekKsuXmyAYr45A53pCLBu8
c5Na3xpcF1geQFOMMeLMSGV4wGYdfQAJL3HbI3CRZrynafoBhjY+JooyuNrVN5EF
od+axkrBWlJJoSJOy30AXnZM5ecMgriWxQWxKxWP+EdCZbuqumN9wZtnP0eh5+hY
Yl5Kz0u9gfsWJPb29RElj0T3PkSx1nkYQz4nM5iesVpQzHJx0g/0IpU6IUtc8N3n
mAQVmo1N9QxbpmLcpl2PJJuJidYGehI9hOPfZ4JXRvN/It0TKeFMJEM0Xdr6FYFs+
+CrBMeBoJSw/MWgKo0WmP5vJx4QdQwYRM3c0CjeKcomFsY4fLP7quY96Cc9NlxS+
cP0WwmlY209wEu0SdsL+kC8ngtA8itw7YanGDxW3VtcdQieHGXL8qGAa11+b5/l6
LdvCS82SpVglGnzLeR9+Y63BtHMJggUp8kMwsUUM5giRnfvEIvNzAA9DRTISpezH
SVNaRL8DdaZqNRKd7/4XiJ4W/y2knA4Ui1FGfsPK1dnFiBzGz/ddl9zLRIT5eWS5
HIbPYDAKFUuDtqts+6T7nM1fH1fcmmnLaDkxPHo43+LMnC4SM4IeYow6eRHX1
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the SPHINCS+-SHA2-128s-simple post-quantum algorithm

Use the following public key to test the SPHINCS+-SHA2-128s-simple post-quantum algorithm.

```
-----BEGIN PUBLIC KEY-----
MC0wCAYGK84PBgQQAYEAXndonwKmcHFM0uQUWLz2ib7+RmWyKljkb4Em6J2pnN0=
-----END PUBLIC KEY-----
```

## Sample private key to test the SPHINCS+-SHA2-128s-simple post-quantum algorithm

Use the following private key to test the SPHINCS+-SHA2-128s-simple post-quantum algorithm.

```
-----BEGIN PRIVATE KEY-----
MHECAQAwCAYGK84PBgQQBGIEYBciTYZpFSPQ3Dm1MmkODG8YoTDTHfTu4JMxWg3q
beonXndonwKmchFM0uQUWLz2ib7+RmWyKljkb4Em6J2pnN1ed2ifAqZyEUw65BRY
vPaJvv5GZbIqW0RvgSbonamc3Q==
-----END PRIVATE KEY-----
```

## SPHINCS+-SHA2-192f-simple (1.3.9999.6.5.10)

Use the following CSR and keys to test the SPHINCS+-SHA2-192f-simple post-quantum algorithm with the 1.3.9999.6.5.10 object identifier (OID).

- [Sample CSR to test the SPHINCS+-SHA2-192f-simple post-quantum algorithm](#)
- [Sample public key to test the SPHINCS+-SHA2-192f-simple post-quantum algorithm](#)
- [Sample private key to test the SPHINCS+-SHA2-192f-simple post-quantum algorithm](#)

## Sample CSR to test the SPHINCS+-SHA2-192f-simple post-quantum algorithm

Use the following CSR to test the SPHINCS+-SHA2-192f-simple post-quantum algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIKL+TCBlwIBADBRMAwDgYDVQQKEwFbnRydXN0MQ8wDQYDVQQLEwZQS0lIdWIX
LDAqBgNVBAMTI1NQSElOQ1NqbHVzLVNIQTItMTkyZi1zaW1wbGUU2FtcGxLMd0w
CAYGK84PBgUKAaZEA3C9KtQNnTZRINo1ueM9SpptZbq/8Y839YR/JhjnsxFV0m1H
HN8ZZC5rfPHvYA/koAAwCAYGK84PBgUKA4KLUQCYa7+cJPCu2c5M6scrS0QVb5i8
Jp9LqC5Q6/+HSCgvFT4X2Vn8K9P2beTKuGN2sV0iTEp+biB1PbPDIC3hhtzUVFvV
ygPoXQ+aHa2dSFBxSIDTNmj8GLryabMUTmtHSyNAcjYNEZ0410kZnKB0qtrKxUG6
KbEa0fEsRXgay07fh29Wc/Y0rLSkzWmuHjyBfozZW63hs0KmlC0e4T6daj7oiD/r
QnGxgvV1/IRDQ5/1NAWnVJ5412zlrEUwIlPCNhDu+rmr/of3Ahv8EnGZXuJL5c+
sWu2bLkBMUQbwBrq8yoJ86E0mmPR43qdn2SI8nFdJv/1/TULWVEItEqoxJJA1Ea4
ESSaoJVnmOuB7AUfbimNVP78+2ZNUVRoY0IZYq+GFgwPb1u37ErqqtJh5KSNMRw
XqGsvm4gIUq+4iMm8Ya1Pu0cr1q96T7Ug6HE7shTSi+IfSt2ci3274xXG0wIvQR1
vwt9rcYi5NQtnF6hwGeAb+5q8sr+ZhQh5fWQ6IyGb7IuH7BB5YgHOLz4HZmWZMRn
tMd25cytsB6JPd/5gjPtJ44Tr0ZF0Fwo6z2u3TtyYs0h4vbFU0q3DHCim/eL6za
dk10rCzaXJLQvhpeykSWqB0LaA8f3p2woIZiJR+cgWkCxgm1shms25NlW1kj3TdG
pR35Q/uE0dePkZvF0q+9/MzBzPt5a0bAoJB00p6ptLLQk/BzZ8qQWLL+LHPoJrew
h7pYrKQcuNIFGn8tfdFqEuzft9LGBZjKhqtFZCjGbZMZg1IOaAuVbKfHL9qXhZOL
S5S2Ds8IqxbgI1I4YfAfKMcDrX6NQVw0n3Apg9ZLun8USXjHB0XOGCKYEMJ3fR0h
/kgC84T48NSZeI+ZNIDaZmMBtg1+UnAkuJPRyj8zB0hKDOWcafelWDPoCD9mMVaU
qF6JUvL4QRu0J7CDh1NzNc2xbv+6I4dPwtisPgE06LH5ltLD9SffXL3SR2PcWlJH
UCKU0NGPXtWVBZM6Lj95Hr033vKUQwEaLRTzgti5l4xhjYM4LiQQB0tRwT90KXI/
2uiB90QLqx/ZdIzng4v8juMrAH4p87AU5lMaBLDH7cIn+leKp1YSvRrLnt0wgJmi
VLIqAFr6QfNG1us8o6BMJK1oLKdbbwWu2HEexdRwnYuhdP+aPU68p077tDKvNh40
FH3CyPaVv/DGU0Q2WScoLJ0EEoXhX+3ob8N8xZxWptgJzklCUPQ9YGIk1heyYTU
xYCiRhtj1ikatPwwDZqPHpWnmLz8VAdTuvNJoXffsKIKrDI5nvYE9LXvGKt4b0Y
Rz0Qfp3fuHEa59+LFrzHSmN02EZq8ehKXjW+UIC/yptpZINTlQE+JSz/NyQ4Q7XA
/a/KU8XRRG3/j8J/JhdLFy4kpGCI3gVhAZmVQs8xLSk88ZEupThZukYiy0zusg1/
YNw8hx8ziRmMJt4UJplxuE5F40MZUXmXP5JcYCq+CTebareT3zze8AqAfE2K/1z
```



+tbqLdh/GUEhBM4xpBtJLAIvVNDF7s3nYCQGIYGQ3xhggaKhvtc6vNt1WcSnjLzC  
miZPScvFP8+SQCEWQts4vCS5PSwu4iYp3MHhjXMrRRhTGvCTv60f7Wpx0UbX+na  
2L/IBCC7ez+9VXMLN53+NnU4VZqtXuD+CT53ArIxcnmz7n7LnAqfJM5ebKT2ntF  
yW0Jd2Q3piPzNzDKT5razcpLFLnlwV78KcPx4S5likKV6J4gaTOP2Vu1j8g0ZkJC  
2t8zLzA/T3NZs2o6j3x7uMivnLWd68HwMAwxLAVBZW006SFL11qP/aUCNNy2VLzw  
v40CIReHe417finR+xjn6P24/aknLuBeHJeVUzufpdVx261hsG/syEIQpMu5zNw  
CJqCtaz5jTXJMUKzRDpveY2bgG5AqaDUKWYgWuxBKfAOeizDgmBBRyCyFh5bPUXV  
PIK5comNf2f26q1dFQlUYjDFHjdwznk8Q3f4ZfLn0vP0PBAsfsn3oLJxDS5VHouu  
ET88sceoG7yRlgl/w0rAC+8ga+SD8RZMProJKAVvAH9WMPBNxxAFTrGnljvI4f35  
2Urb7jA24ioHJde6Z1e1s7tac7cGDYApHxone5RF5sjYy8AohI8ZMGnWLC HHUlxu  
Qmzh77CQwUCaga2Y0XmswNDiBe5w8kULfTmezTVesA/SDkbV0RNzSglqgoPZYciB  
nmGRaIPL//srzQTtBu4vHbWS3yVffM2rvp54hMD90poMvHEtNP2bQQ100q18vu3b  
OghUr9j0jdFJ9004icyU/33FGDgdIy5dX/KlyxQqhyH8wRHQRpswJs/f3Nce2dGo  
zq27h3BURJKZ/TgKjD51mt29v8YMDWhs5ukkyG3EKT2MEIAivDN1TV7SGEm57Hi3  
8tL0voVV89V2PhpuEFKK1TriGMx0upO4zkQpYATH0bepzSN+bVx38GFsK8BLyRx  
yYHiSll6JNpI2H83aVAvX6tlywnfMKGajr8uha90AdUeTvXHXsqVd1ntbykPU/tj  
sxIufDXQRtXAYwDro2n/larx/P4Fv9mDV+UxTivGmHuHm+kB2HK1tyD09TnfpfKR  
KjeweDsfrn8q7KdTLs//G7/cB25RWhVmpyYh4zFVf+H7uNHEbxoPo0ZH100HvaeY  
2eqwqSJd716q0bXhRedWuWP/QGfIvSt78xNz5m9QVY4EouMBLV2poRcFbeFKGAg0  
nYGxFAQ1gzTBKIBDCw0QYe5B30ZP8e3MPsb6K+SdauD5iAlz0fXLluzLFJ7YVgx2v  
hn/QPzKKB2Er7PG4nBxAhLGCY0ANaIsrAvEvVhAkWuWqu/fTgyB/LhbtCGvXnIej  
yrVfhjvfa2iMfXB3QJXKoD9NpLFEf33B4hwQImSA00zzfMpbS16ljztop9wnx25i  
Mejl9h7+HjDIA27fql0zUjcy7s3FEqy9vBERgh6rUXjLxL5KCXUwyGtV2wr70A9  
DACxZ9yJNe874Kzdn0sjw5S4LCFKxzaTBnwmw8fpo0J4uUIeMymHHqQ0QsR9eICT  
Iz+0PSZ20ipAG+06R9JfxXpdA6Jfz8Q1ZYZI4tDs1qoxQTg/X31VVewTs9FseCt9  
D2CyUknP1vzFJfs4RjYwW4TnrILtpu0b/njH4N7gTrNhLMwbY0lzN4PDV5/6798/  
pPZ6bGkURqMDPo88AI7P+TDX3N34Kpt/N4ygs/2Ua8+9314QqfboLkfgThl1AgpF  
0i0bG1Pbea6JiPfXwHf0BBi3RkbZmmHj2Y0fkIIVKMihACQVev+whWyVic2FdMeH  
Mc1Kwx9d13v/N0pxFWaHt0UrrKDywydxn5Mqxlyom54y46+kKBhFKafJzLuRShI5  
YysEzAFkGVAe2E23TsAz0oQ2u12yFuCrW7Xn8MVRTVuYbodGuMpm/8BxduhqU9Rt  
IcCMEAMs1UrSp4pYddeDhGrr2ARKQvL+HQXvD2wd10UXV/0ce+mSy9z4zn78Pac4  
kk18SXrl2qGqvdyntfuemc2IAPrzByw9Co9vqHn8SHHyvmrbJdHKad36PavoVqv2g  
qBwXfxVGN092jygdntcd5y8k8trouoqViFBdD2Q0BAmn0rC2WFuVtQesXDH/E21ah  
s8BHd63gIaq1hKw0irD+kjGPZveFZrpyEzZmVQnE6ZRTqfb4TbZk14H8qjD4K3R  
2yka4XzonQzqnyYqRQCxpJ7UHxtyt10B1gPcaG+ks4yfyjKZHIslWc78NbGPJDgd4  
ufHvkYUgobyN0rTcoVR00c0A7uqf6i2neqbasy+10HwB+uclqpUx/Hv2sb4KPESw  
70jaBOB0uGJCN7KgGNGBXIsTfd2R4/V5XyJyTyEwXKC/oT9lWrurKw9zLwlyIVGJ  
u0IyFPMayvWNph7eLqU8wZruQYUCUlyyqTkm43EiomR8W0AlFsQ2H3d0yKVmn3Wo  
xG0hcy6PykXAEDUjbrhiEqUy45SpPZyF7nQ2W/xqE+weILSJfhyRon6Ikyvhjt0  
rfmndjP4ix9DSeHvKR2B6P440mynRXZpCDUCEcOVdcMM/wqp1ZT56gY0AjBoboX  
gmKvNmncgW5r0raQHjTd31yj9Hg3tH+IsgptlJ8hc0378t8wXdlmvzBB6Be2U0hB  
2hqR8bP5jY4ZTaf2ae00dQler3z7QmPw8/8x/76Wh77dABRJfmbU7iw5yS5LHPjJ  
qzmHILZqY8QSbs7dYM8RwHqBRThFwwAlbMSRNP3TLoDDt5Q9M0KMPGYbbJya/n8V  
eZC0FeEkd3qbfzWMBzPNCodBVI0nBsVRMGZAUw5wP6F+Hh07Cman9CKKtXbm09ek  
cly1HBERmJZh94SGQNkn1aa1vcllfjXAEQ1MUBsYDDKH7N642LHNzEAUpaB9c7T1  
cyu8jNM89wPJS5EpqVWX+ny7yTQT0MK1Py5ZBwHpc0EdJ8EBGD09yagXhsBdijc  
1aw4ZMacQb5AyXymbzEt7MstgWvxdkTTG3nXz4op37Gk0337RXzjY72MmvqBmnok  
E0JkuTnl7xveeP+WqSeeinqf500r3/1QbcdGzftImGvN8Ey3zIyVyAiKTRhZWXFf  
dvCsV9HAv/6tJRuI5Q3EMoCwEjZqZ8ue32DkzWG72aZc/qKM3PT0Ch/YopQf9/V0  
zq16jQ3mrBU0T3oQGLYLCL5Na+UEhXF0sirn9adBjeWeVa2TGcwkrL8ZVTuFxlKh  
5MATsFVvuur0n7KmyfDKN0cdvgfKcLZf32R3N8qNytYY0vX/ACsuyb0yVAPA73g  
KFSeviuYAGlG3bLwLHnv3LpX00FwM1PVSDIREaX4I1//0GxQ8btIwcZ8btEu/+5  
ViUEA+cK24H0+ez5TJxPsVRQ+r8C3suGr9Hb5sYBmNPRj9r4Wclm50C038liNljn

T+bbx3QXkiu/E9t3wByEp7j1kW61X1nL28xdXhnG0sAseTeh2fLjaSDAhIIdX8RC  
r3Ve1qZiPyRruwjek3s+rhl8GYGLEa3axwrlDm4ffEGqIBlgT+F9BDS0zuHdAbQu  
nAotPOS2jRp5uAV7s0YaxzYfIa5Zp3oFKCzoMeOnLmrctjaVQLdPnObVqoU/2sw  
sJ9tQLu1E05riHb5dvJ52wLbNNcgzBYrduX18aT8UppS0aKFJfoLiZC5Km7dGtO4  
NrZETXetqRMLBM4aABqoljlgqyYebwx7D+calKLvgNJzSF10I0lp0/LM9PZz5G9f  
whYPRCebZ+ny60hh7IVFF7iGcKeejdZQGbsiVbrhK6w9hBFTT/qpSJ5gf+0y1qc+  
2cx4sh0h4ET/Cx9gYzGXo00/lljZdejoo00rw9ZWXlx625AvrYR/gSGieGxyyg  
ssKi11WT6LvJ+0MyKz1ySQX7YTqNP/o83TpdF1Y7Get9McG2HZSy4Vvov2lYqSgk  
9wM2HaCBSm7METOvy4H/o+uaVYnyPULdf4yMu0LCxJDQ206/lFikHefMPj/52tVq  
1NWMj8fzET5X5ZYW9QVsSewYBORuy39ZU0t2yabIn5+0C3xBN+1wzMcsxQXbv1nc  
WiNccvod1JGVBbvUpcu2NCFrm/hcnytbMBEtrAmK1D7GfHJudswWE3t4EzS8zLm2  
txmVpPbuKZj6b6t6FYEn9jQEi1ee0/Q99BaYQM/lLHftWYmwwuB/DdKaRAJfkTXg  
akJV1mUrF50A2jCAoSItJokkKoHoIj4/lxv0CQM6qd7T7yupOK8+VhNSJkg6peNP  
ZilnsZcJj1ujYfLACbIWhq2roAk6gUmFRw6BsZfTs/BtonwflWuvpwKyBe0BVbvK  
uclXnW8270mvMAfiy+sEordvZNQsxw9bZJXdoT0yTwsLH51EUDfM6RAtVyuzxqs  
p7CaadFuq3j942eq2tQ4+G9GQ21DXZ+ZnSQKXbSR9S1UYT20p0l/WD5qs6ZNNP3  
uPWgUpVgK8uHtmHISig+s/ofPGFeYhHcAoAfjCFfsSKA8qj60BjyzPXctSwrq+/K  
yUpBQ4B1786MkpSAMfRUTBiGC+G67AXpXmkHo/xFivuZT7V2Xzm6sv0BTN30ko+s  
le5/koicURbw3xtJB5/A3h/0fPpyuKpgB5eU/c3nS4urmMzimJE3qMhdI7s4c4ta  
95kbVDXlbETHzTG0uS6JoIvfmtTVrDxnVmSkMRFu2jp0fq4MUJn4JPgxTeJQidzH  
qTHJygzF69q2eLzPgZ290jFZPEd/67g6AHK3QCw3MgUIzex2lhbN+o5PjN/z+BuD  
3EDk0U5S3NbDELZR1IcItw7/7+p+eu5LpMa9/uManVBMrw5YKj3yEdu9DWYF4PG  
tuUKi+fjtl0s/BDEcWrrlgZcpss9IY0caVaqR7Znk+JpUA1vyP3/tMk8PAQ/Ou/i  
utPwS+fhnEOxgjKUvdJQqZvWCc75niE4XchXLSnuARiP0JzWP3zjvEOZmRJj32iA  
ls0dcaHFRbwkGw5ieKwuCj7+CwpH1s49m0m8iEjgInmlCf0Rud9KxIxJ0ZBvvR2R  
zawfVWD0ioDy/ULrM1HqPcxxdiZWU1DV6Hw/4SM22KEXqPiYU2ls/xgYv3FUNwi  
Bduv4NZ51XXrz9apU1cEBTU1qzaCAE6uSt+4xx3BHMNsViv+X+XSs9/mYS2H9BKz  
giqt4BIly840gbFbSvUH8f2GBEnuv2SCBdVzqSGEVEfpF1/6zbhJ8teqBa6yjmLm  
k9XldJZEB3VHBd6XBJZHsvXzuEG0RIjFCqu/QBiycr8fz8fyXRnwG66rGamN7FNB  
uNcArOEJ5VE21kdnocTldSDN2nd3ew4pMKiTB6m6z413VBG/IJDPqD9npZCacXRp  
008T2td97a9oRPN7WZ+hdQlbhMQJdqibmTwzJ4woFoyzf1ULvgCMc+aMV5289evyk  
zzGdAbSUKTVL8P2FrmlkoS0/btsZaMyWYfdDHw6Y8aGtz6A/bTbSA9uWMctgSaNT  
mIO9b8LxfHF0VmgXSPutAkg5fJsqs0ie6SyTWP6Yvy3plbQXpSQArY+0V9j1yDp  
he1bHmKsBbUSCnJKmhWHQwVmaGw40J4UER2kF7E9FHL3tB3mGdqZTRp0rEsz34d  
jMrfGg1LmEAsWbfq5xtU23G/aTD0bJJRY/ZuNGCkVyEraorJTPiY1mRPpAB1uxdC  
Jxgg0b+P2XYvqY0yaDsoJodakHpWbsqeENMshLEr3aLCLUVKgPGLeguQkuWYScrU  
8N69R3rfr784ImT3Zcqxy3+8TJ/zs9s7GYccChXcu+yORdxcRghbnxBYnJcEOZso  
K+5VqQlZ6NKnSxpNxR9U92WJHwhfDE2XtqIyrFEuBkCiuhnuxe/9AvE4xUUREuDB  
L06PtWuXDbp7SR32GL/jvt5vIktFJLYyAQdxT/P4aLAszfDuoRQ4Z6k7jMXIhAtK  
nyd8kfkbeKHt8qeanGa9nuntblygGDVLtiwHmbVm9Bjl87M12rE+QZLo34tlv00l  
r/GIn1WPPS3m5l/vliWtyeHRbH9fesW0b7jKq/xzQgAJS+xBp8CTD7jqHhM7Ic0S  
fB4qDEReHYjL1SgBRitBxjNG99ZLQTIxS19UHqU63FLJfTWfM6BzrSvM9HY+JM  
iIQX0+UV16N2SW7VkcJ5mjxH51TDIGUIcpTT0Wcq/FbXh4WvBYVdQnoP89H+pnIj  
tJgA55FPV9wQLWI4wCOQ1wAR7SiV5wkcwk+3SUMxyN0D8R5aL2p9AboKxTUUInuP  
M6wyIKthDpyi82oCdSpz1+YlgyOH6k4ml11bly+Z/4iy4Vf69MufyP+HrXDtala5  
oS5hfkHMD0+FBJZC4/YOXs7rjFx2xKn3aAr0cD8YJsrkzc3+yKNbbWIce9zSbTam  
XVQb4LvVcxHIF0vybbHwF6FtcPnyqlTqd042yeZDEiAjvJCPS+dJIjF9eE5s00+  
VWGQ8mjNJCP3rfwUUHFzdfqJ/F3m/CB1xruUIUke21ifGM1cio35x6Ggs6S8W3t+  
EHat3i7ZVT9v3MP3D/uIOyhx5bqq5NsJf8k77MOK1Vgb1VA9EigLVZQsSrtcL0k+  
Lz6cYMVYlMj3E14v9z6VmTE0X60S2HVQ/lQJ11g7Q4tv6zdUI3siqwWZ0DPGT+MW  
19LoU2frSN0J05THwdGv0CLSjCaMxnHVOZVj/FHmjPQ9tJuzo4mTDUSElqKMyIEW  
H40cyrLyfAG1JM+Vd7RBkLfIrVCGu537+EPw0ztIOitFCoY9H15fWmcMHVwvBdS  
ax2KGrTTUlfLBFwnP9QUPEbAvbDzxFhq40AtfU+ztAW5aSi/4/qwD/6fwSTf7f37

7+49vNh2G5QHMBclqmT/ueIpgxs5vaEtpcbjASirhDqE9GVReoBh4HWk+0lcHuLz  
uHxGhkFIfeB8XxIpYC//tf7+jRfWRZr6hrHe/sTB6LVrjXCRmfSX1My1veNWqlbR  
LXLf55oLqLYGevDwBWMTVql8y2XC4KIa5sUmQBQhraI8jVzkFRq7f7T1vJvhwNbN  
U+t60+JA+H1recqh+nmkq0c+FGQHAjIwg/w20oLxLFHR/7gusb2MFpDeUz+Tmegw  
R1i0bwXyYHNDCLhWU3b5Rk9/AHbwnxvdVZgec2owo9ATSJsyyRmRv7/HwQInwQ34  
ViEl6kabs0dz1yLCc+7ZAWCow3sia+oaM+1r3kzq0f201qML2vqieUFxswkeP10s  
w4nUTZ0JpU66GsXaKQA94T+MxCZeiv7klTRFZT+eaLQlW8LyTNR9gP06UjSb+teT  
NEiciblMg4qY0am3W+Z21A0z2kwzfiRLPY6Rla5EP5eEdd9gX+Uvzg1TtPutpa0i  
6rqarQzYtv8jNs61vvKbCdcQs4YXcYD+DEfNI+gyJI+B7ep6b74Vx2btmBHi7hCq  
3IOW5YxtalFkq0I7s70o/b+HoZHp4FfaVZQsCgYaCPyR4YwNQju6WC4sbADnwjUH  
q5KxvhMsj7Y3REV2LNQjBer/0P2of7p0LHC67hJeXGr8qPAsKZUzCVf7xUFKUukd  
U4mHSiAl6aIz+7up6qx3P4jLJDYx4PogZwF34BqH320F9yqbWUwwLaGzxGMiOcLY  
u1sljE75C9pvDKmh6nkatfrLzXWfdjGYyx8+YDMgveOZf58HNwgl4T7fxdMM77dq  
6r7KsrQAZPelQSYiv6A3A/ipAehJlwjJPT08I26x/KXY4y8jOXN3mvB1hXt6g4ls  
dGQX0RWS9qGijjwavaxvYF7UFRTPeKobqjU1ocUSGnFZw+j4z7EWQLLoe0dGzLE5  
INZ93uzTjz0qLRleg+APSnifgWX42KVEtep9FoW6La214az/qY+mN0hk9jbiTrJR  
frtdxSAqJEMXeamaF/AuNuY4M19innNVbfnKKqvfhZoefeK8tFbhmRA1iVsLW46K  
//4E5svp0ks60zSEHWKdSIG8RGZlvwW7U8hVT52BkfwQ85/V5hewXTkZE7hmVry+  
uPk15mXLt4i0mLLR190r2SFwskBf5tVG4G4f5yenChKUE2ZM0gPRp0nk05YyoYkK  
34erdiv45ktYVNUPj5p47bnibZYRyW0CXW1p1a4rxQ7JV6sT7n7tVtE91RFG8gDP  
R4AxqtGTGTARTef9wd0VVZ+3C6tABN/xoQ0wWByPLPv5MlCT4ELXpoyQVpP2Q6vW  
qfvY6N5WeJVBbKJRqiacquTwc57pl3Llr5PfPIX+HtF40W0EtXu4L0DZyTM0pJuJ  
65pK04cfPBQ6tKvfErr+edMk7x80+dQo9UFBgikaiJE0+A27OWNZonPqnvWeQtAt  
z20An8BuWFBZbbaKmy2arYVqfuV4BS+jwHHG9bf8xbU01YFr6LYbCDHwP6hz3g5e  
M+vMZ+fet/BkIjXkcMZZfeqMKMkN66+cM/pDJB2NkfXTFZrbpuR+mn7+5+UK1MrI  
t35I+pJmDU+NDjGZbBDR0N2w0b2HtB+yhCu1rgRBEX40aNVpwYYtyhucw1PtrJxP  
pJiYyPcV/1miKHMdLBAZ29qawG1Uc+6P3faTDkP1o/rexvQHb4hPGZD84rtREGqu  
74rkzlkK06qhZw8BYKaBwaX/GqFF4oR7tIdliwNz3RcVhvgiIZ2smQMryF1xjHPr  
PcngdBc2lu8eWPraU8sPSd0AmQCG/Vm+0cFvBje4aeH+JcOUY/ZJaDuMkyC3b03Z  
nLEfckil0b++zfd30MVLfe2yAufVcIcoHAMtjry9AUwTpp2WkZ0pF6KSY4Jben3K  
05Tmiy8Z36tNqGW/wSKD+19y0hXFT9ZbmbGXAi2UMB/DaMeBsI/5aXUuLprl9oBx  
7j0FIMvkIFam055bJcNG2UVRlbQbJqk4jvyZg0gMlJFDCMYh3Pu4jDvGaRnqd1u9  
aN005r3WIJ0vUkAC+SexvRSCiK9YUUR4LgCDNac9b1ng3+Axp6gkFVhvMfRgN3TG  
csnsXeDDVJI61/+JhlnBa3GwvYtJsHzdIdZ9H5EoitV4pvmuTdfd9xaWfmar1Ltt  
xthwoptMHPqhfgpYHARLGedtTntRfjTqHx9F3P1e52xNNp8XUr7nqJa7wQb2ovAS  
1VuzfsNa/170SAXjx72Pk2meiBw9icASwdIzkc0g8G0gsNwIncGkkoUxQqULrmDp  
q11fEGYGcUP2bnhjblKNXWEuVx034UVBrbIWxFMhmnS1cZSLAJSPHGaouB+mB4gz  
fs1D9aVltueCJhtILD48avL71HnKqSiqKForftqBBjAmnlEVptI7t10yXSrUwhsG  
+1gy0W0rBZcIqvU2x0/k/4STXoYao/IrW/P4IB20EDi4yo0tIhL3BswPFwX0M3Y/  
SXR5FSauKqr7T2cr6t3CkWNPlazGhXfox3VTNqCLECWJpGevJjG9mEq9DGxQIoZn  
TGNLwCISX8m3HpLfwxN7j4VeswtJtrDNu/MdhC3oyvOwpdai0qn8GF3luEK7YQK  
4N9aWT4//M9ruP/aAQv2K6vxtJex0betyK2WuNmTKkyIIM0Mlbcaw3YJ2eyfIceS  
LWjsrCx78q70AUcK0f9dhDI9n9kuepkq/igk8sSwijruKJPXXc6ZwbhFdjT/XcBN  
Gns5S0EJlmjqI7+UjdqAyRwM+j/K/MtR+xMkDPrmEnq/lTide/sYrzCLHiv8BD8r  
V5IIPUrkg0Axv6Iix98ehUHGDx+JsbZg8eIctpVoQ2C08oM7ipX0xgpxKz8eKKTL  
JApyMMWyp4VZA7WWW4HTQP14IGw/21uw0WKcnQtEhIqjCay+7igAFDagLttCLi8K  
V1g56cPB9mbrnMBpN2jv06HPVw6LgeGh/vHebTA0IGeq+znjKT34FSKB0/Ukz3BA  
Wef0w0/7V0GiP1nFrDjIBxBxA0ssyefpXtsz6BurT+asPGu+V9QI8TVcSkB3MZph/  
QELQuKph34L6w1tdvzt08iNNQv6F2N8HkRx1Sa/z4mficvD8ylpaPQcqoIKmJyi5  
N0Ii3DAU/OAJCb3Qs3HOADBN4UOKFuY8pMM1elMaILglJ34a0+GvHNS9IF/U1hTY  
30pFTb7+s/d+lm52vj5LMkaST/x1BTy2o5/LenDNbNwpT4TjLDIEsterRPhf8Tjt  
vm1lyP2Sxo9nRZXo3I6hZohYsAh5+ixbogxx0Gd2BG916z9KdEhRCfrzqN15/fKs  
Z/wSTqIy4l2JgkSUzh7h4J4tEuBpDWqew2ew55C/fJ5QUzIwyCRxc1h10TJIr83V

EGFdb+rUCsB42MXnDn6LhCsJk4rjWZt8hwQ3z1UqctJTSkNohzxgdzUqyV/y2bAv  
93rC+AIi12N6cINVzeJW13Ce5jgEki+MnlXtoM0ihdq/hL/DMWw4FSwAibFA/Dt+  
B0xm4eKpS3yxSd2IZ/EeTBJAqaUZCn68UQFb6Q5uZDD+74A/ocIAk3wx11B6W3i8  
K20+ThY9m1/5SiA672/Xnp99HV9jnV3ZMZuGyYPraS/NrwGYLBKYU+LZwHQRJ1iC  
oaX8btDsp+lVTIv6q2iM3u0ZFRqYl2WVKLqz/0hLGy/sMxVpRZkNy95E/9d74YjL  
2RotfE5ZjgXt+x3UdtgzsoADfvS9GyMMQOPgyo5IhdFHHq/5xwJrhvaibdtaowmQ  
oTCSam6xAj1t/KiNnDl7Lw9r/75XJG0ZftrRvm6gk1Jlzt3KsZl4WwbN04JN2+6  
h0Hnbck5K08hxm5wNNkxR0bbPGU1E1eAysTjZCT7E15DhUyb7Q62LWQPd09x2Xa  
U8AlNRULcHphavUyD7l4jfs1Lawphf6CaAXbI3AmlqvV0weWNE5NMP2U7SDHP8jW  
SycehxczghG/V7/imQU3e7ZJresKp+U/5J5EF39BEg/4/ly0ResAzdXqNyYu/j  
E01trlz+VQXhD7pVSiwM1EaGCEsvddoa0qHbtKWrE60EefMjKSzm8OG9d9WwuAip+  
UnrkJNxyLBWP4Zj351NwuJmc0JVGrm5PhK3D+w0RDq0yG+fvUmYK6/n5Eyqq9V+  
t7koJBVeedXbMLGgGBEWYfCjREHiC1tHx7QYesqlSF866ZTL0Kl0sw9+gLKuYEsW  
F1j+vZDGN43gcuFw4Yzi+jbwkHRxcQ9aaPn0mT0+R1Wn1G2mQTy4zGBJCTb69Xu  
0208w2A1WW5R7GQ8AYRbnR2ZyPzMyXNjyNwZjoGYWF0GNVDOQRuH0IyORSaH8LFz  
s63qI0lkyoXfX+NBYeYLXpyTSZH4E88TbYQG+bl9WW18+eTvIBGbuCkdijMg3kDp  
GkDL33grYoFvdxrsgXxovjGYMuBZbERqbTguTgqfTR+p53XqimK6LWRDEMe+D1g  
93ptLN1pX61fvhC6r2efENHeSvINHm2u9Cay5eGXE3NPEjZ+3L1HH6gPmHtFBKQT  
KLCBIQuSwsrWT9Cld9Gg19CRyURyZ6t4wCaSBmK9lKGBt0DmCVVgBblijs6JxVRV  
/jkvcV/Gi7wDJcWnBZNVpArAXD9xlmkYlLxLHf9LNheJokqACBfdEvRkiQhPCR  
7myDs2Q2m1JKw0huV//n6a0bVCR9GWEqg2HN5Cvfr4EkSudcI5Xl1TntWuLnz0  
PA7za4rqFSeVG12I5mOLDXiFIAZd7AlCg+WReFlJGNG/GBZBQu0TP+cVtA798aR6  
4kLE+gaCNbR/sS01+RGtaBAds4irl0xRZtGsdJR8D3d5/f926pKRq/RJ40NF4J+m  
zBcURd2iYstXutz9yPkk0ifvIvMg0SxZCia2BI85CPiFWt2bb5ezQveIxjIaoqcd  
vDUzrVMDT6ewgVKG0EaxjkAmpfZgKx0gXFwHTdV2e9ZKfmWwm1azG0KL89EXDLt1  
l2u/td7uHff+plTVZ2Mt0lKkex/jbNVJbBMHWZt7TdNjm51ZtUyV/5qvFXC9RajF  
jFX9hg1euA93SgeXL3MthhB8GLFIsx660B/6VgTU7FRuXFEQwPrwz/ya3en+k9AF  
f0pyGDkA/gLGWJZUJICz4ATypVXs4/W2QNpKgLo0zd8ddKogomA516z2SKihp27E  
r0hV2jeJofFenSNGTKezQEub0TeIaXjQn6dlgyqrDcr5eZM+9iwag+EIUNRHv5wm  
bzcdMMAZpcx3lKJsLnJmS0arDFwI6GDcvN0hJ3Um3dz//tc+7y7ZG-i2Dht04fEna  
DvlbFtiUNFOWKKNxky9McmnX+9SxLnsbpCIIRIWNcVkrT+VRvN43ipB9tFzjHa/  
0o/7x0j1oiYnBoNCmnNNrhg1IzNA/u12o3zpm40PEEY5VB/F0vDqSjyMbvbWdvKy  
65hX2grB03VGycq41903rC0W0uu0TADz1F7tSWHF/YTckT8ABCTpH9AZKwssE52n  
OQAQ9581RFLGYNSPFVsbx6K/2uV8XNPwTwbknu+0Ddm3YXhl72irA9woXaWvhPzC  
+kYBrkVvKTHR0hpJVBnZ6Lr/W4Hhv9QMBtddkRult6TnBHsojV5QKKDXi8WcyGBtn  
t7pz2FSJxFXDAi7+WeU0MsIJIA/DXlZ+u3VRuB0hhJ8GniEqW8YgZkz7m97+1XdE  
bSsvCjfIWPYf17YX4KESrrdnWrtuCvrad2YJfIovkLLpQTcghL/EsYDHTqVyHN3  
sc0orojQ0qyCq1Razlih493bJILZKa8sckyt15l7ElvRvhmASxvnGfMr0tmY6qHX  
QL/uEbFiRf79m3JJvJBLi1dLj8tPHIWNdKsaluqK9eiYtlnPS7pP/3qFVric2FXz  
+v5W/Tc+rg4N7ZXYBc5EAnbKFZoxEWhLJw1j8QSJA1zsn4hIl1poy5zy9ZAxWnbq  
dpdXDRay6PTZQZi0aa+3Vt15rEWX0kjrMLZZwBnVaIXtm/mAG5/SssA2N4h1GELl  
emm4m9tDNyvv+PRXONEYVT/vITjTlkhM04z9pg5V0lWumzNYS6hGposIMU0uTj8lX  
q+TirzCZJIDSv0aA1yYePU6xI4uq91dawQusd5b/vky+TIVg3uHiZU+t4HFus+dH  
Px28BGyIYZNRggb+h8cyBAYTu1f6ejp0J1StoC/C+23JhtrqYZunKvr8d/mjh0j  
eUbjJibfNzPwt397HAp1OnUKt3Sz7ArfDmvogcTH0J9W7Z3a86wSIOuCz9m03gXK  
rLkYuYsGcT4CRKyxpUrNQHWfhygl+4b5KrxevC2PtSX+2dJdzx0lCI5IzBJum0S  
z2+KBPNE7S+fv770IAGN0Z/d6Dj0NCi6uE+pcro07eGSH/yJqhsnn0EcwZa0UWYj  
15uYaPiTl2WLF6AD2ABaPcI5VhXuL/sTSf8RUHPZNL7EMqvVZYg2GFUDem329Ju9  
4rWtqcMweM6j0vL3g88vRpkFNjHSiaHYze87gdi5PgEpfLoewEVIQKgsQs6HejI  
lE5mWHUNTa/EdVh3AK3ooLIadwpHeqrMhBB30+uf8SkqQEdlI1EMeKSMXqs4xvEl  
YfFnH3KKuTiUJGaaJ3PiHne3+NViytJvrLXzRatQl6jCdjq3CyyDmqpe8GyJoM4  
X1U0hL9WWEfycBUdtiysn+E3bSKqd+VnpLzbDoWvgU20HY1CUoi3SSH00AnuVFF6  
dzTh8wF8ja8mGd+8u2wlmgic990djP3jGR9qcww/04v9Xf89z9sm2+yi09YvQdxE



ydVDCdjWXD1F0q5J9ghSiCm8ZjGEV4h+ntL5diRWAD5C/IKoePL9LFIgvzJvNhiO  
xOEOpnm0UHFU+0o2xGXaND1kwCwNN5PFkkm/LawkNI3m70UCPkQcRYyL2LBGcgMB  
dKC/oYhhw1U8oueRiXFSbIJ7Z25bCIJfa4CSe3DasGdiscqQex9IzEmhMTRwqIeD  
PtA1dELX61GyTNI1dl8oLWdnZshdg2HaM8sYWEgthF0rb+9ILH3UetH0XTAmYLHr  
6m+gdJ0efrNifbj8F8xv0FMoJz/eqUqywkYRM8IyPRClkRszvrHxS/cXiXVdal16  
M/vIPsrW0ipoCyyVKS7iijPFsloZv6EGyBqMziJCA5jMDrIk6zsHj0Q1VK1jG+2C  
kViV874CncpFG12yHXsZKTgbDA4+YEkrur3zBzqH8GMrjALse/dEHibpLZYMBZgq  
8iuxvmCkxInkwEoJzUI+Ixzzyx6/u5uwekdu0ECmdivCy29TcV6UPSoMf3zzp32a  
u/3LRMGu2lo/yUDvxFnwlcS41V8if9+zJCTm1baP0xH5IQdA2qs8h+U5WkWWAmJx  
7LP13IGtA2SDBoRWqjrsq9Nq4uEtK6V0dnvcJoZC9dNte8Bp4dYB+k4zLTm2G6/  
XzeG098+E00yoYafkopSMmmq0zroFiMGZVLyB06dR6z2TCVZktUxI+VPgmFr1BXu  
4LmXPSMH2FK8G/ufsyqdcgsSNrKZrDXAQA+sXjmK83qtnroDufRiN339FQUa7zxS  
nxG4YKAWnCseSp1uX7FVgplHGRgT3nyPupMq0SMfnsyaJDBLNWXf54VUJxOGVwsE  
DE4vtQhB4wedMbQftgIwnLRGNAL0DezouztH80wYwRE0fy80jgtSCasd7ehcXfIM  
S8Dc/v67HpZry4u87GU3/X7JgyEmLlxMdVIUXjZxp3rQqran211NwZk0UkdKM/YE  
Zd6A8qYTutdhmPqmUSSucwAGA4ZPK6UoLHJyHGaw8JwsPjPMAF06HzEHUbob4/yn  
saNTt6xeQ/2rDprcHJIAM9CcLklp6C/mSYBby9AjwGYJ85DgmpYq1SSkrD+sY/pS  
hiVEzLH2VIKH5k7T0rzyjHn1sGn8BkL5kq259Dz4IHeXl1TJnYatCiV4oyo1zgeD  
ULUMX9fSJ+LzIQswkIHBKLDIPU4ePhp+XmuXZKkrleVmQxOC/YC5tuvEbIwdleh9  
UAJcfrUuSgEhs59v2Gns8NrNHAgYjNmV6WdfJSSzETdD4qfgQ7fXOTzk05N0me/H  
xNzB7OWPqUf1ll4fZPNTN0vSTKffUTRFLaAuj/4kBoBXF3U4KZtmigc9+2JcMNBD  
UYqNZ1i3omEgpdBgZg+F9wmxA7as4a95j2/tnSUf49PjSpGoPRQU7T2WPFNAHr3  
96wCYvUbbH55QAHAkQ9XXK87oyWFawpeR/cqswe6JLi8nv0dAj695XUj9t0AqmRe  
AjoTniTBCS1CbYgXUNhRjZMrTlSJbKWz19V0v83UNKmJm9sIH1DyDp/Nj+rHJSF8  
NZw8WygQ9GM+XGTWtbR9TBxcML690sFT5kfQaxYv+d9VW/M6tqng3KXBbWwmG0ym  
ZRPINP6UYtr8lvWN/CMo5ULAhD0jA6pJ0Jzcmc7uK0S0Zom4wxz8TsGABrNtXH4tM  
c5WmoDWbwk37dsqjepBrZdTuVlT70XCPrGGe4jUqTSul5x5KltQnB8zf+BlK3Ex6  
c08rV0sG+v/fBs4YV8CGMo860VDZzhS20r4tTQ/efb0wuv2q+u0VtFHGEEgNqHCv  
28JyqK55j2t+9DNXS2ylmvioEpXDVn+jMKuAjfEV9QPPJ8Y7FLbk08Juf/0X8zW  
NH0om3WYjGiKbsocak2CvMiRjL6MPRUEx9vrNC+Nmy01deb/BNg49G401hBG3iUY  
a+Y8b4fxCmJvJAL/PffKA8DTQG5anS0s6xBWGGs34G51lp1L5mPjww0XoR8viJHi  
XhF0rGskjVJiqw79QkILbewvf+N8sVqyt4N8GCaeTeU+fpk9VzBVRE1vi6PMoar6  
dMWrZUMIsPu1DbyPwzUjimmC0ntvHp2fGuWxDm2aZrGfXqc7uLa/RBIU5tmYa/kt  
Vsz6sZMIdjkiB5rLhA83UDNRu/Olk84mW/gMi6SjT9ji9y+SDqB9t0f2uEDQipsH  
8nYsjVeS4kPZW4pIDZ0+mP2Q9R1aP587KXh0m5nALVLzUDoAKnwtDbhFII8LVcbB  
3MH9K3Ct6oJEB04QXeEk0raFQQUpYjD+pB2Ms/xtUMoLC+/S8zPFetqhTTXpsmwu  
1RB0D4Sjw/e/w/b5DECKLxPjz4fRwwORvc90RcN0rG4wwMbQStV7QJR2LDTSid07  
i8j0mgA+c5N+6yULC8qf4KVdlOCqm127u/tTZYUeEWWL0r6iZMA3kte07G5wfSf  
naImpEPv5EyVUGAuCIioLaE3Z4Q00egQy+QFKQEXglfRDzVwLRqie/UsbFymaAsH  
y23QpeKFDWVbdDwvs0rPhvtKG3B0ESXjQ7LS/oS4Bp2ztsF5b0K6PZFb0dgU8CO  
qF71ocpZeR1dekWCHu10XxndNQipLwUWnjQgUfjQxUmLCVSSljE9lv1s1riI/UHD  
zqfcUSPF7Wn3Z+SIQSDehR7euHJ0SSujdsrBM7uI2fsRhZxhQU6EV9R0np6zR/d  
tA0og8zrjWpt//CeXE36Z3wBtFeKtfguY/COJ00HL+67+MHHwitaZu9LIiFzfW86  
bmJbt6/fa+pdX5hP00VqAX1wbvbEltyNV8zmPeVz4V9yKl7mhfiH0N9t4YctivMB  
1UsSMkj6ZJpg/bEvAIW3fd3qyUXgswLoCtUL0DsJajSZCbJFUCPMKwx0j4ftlc2J  
baQPL01Dy20vrmKWGucHir4yEFJLhR7ii+3ZvrKcAreLKfQ0pbnL4fzr4ZInVios  
KhKIUt4sjV7r7m3kpkG0t2hhgQvX4I/E8tcgu4XnoTfgXREXQWuVTmqpSica87wW  
JVdNenX0qUpb/z4oE71MBkV0KsV5iIS70LDS1/I69CRLAXSsvkF3nTLAlbIe0vhg  
+fGeAIuncdg9gaDLwrZBhs0GbZPJ9P2ChB7qng74CWvw598rydaJgLSARR9SEIR  
vJQyTCrj29IpWVeSeew2qGQ9xV/KLSMZGeR42zFS4Ezi+YEWDTDKnyHe+P/lvxzj  
Q0t0YJek0ojc0ZCK/kDsHC5VG1DhJK8FIEqLq2zz0JGwiJWEKRixysBka+/soAL  
fjNacFuQoWgCl/chOnRiu17x02UKjPNv/KvfNgCOP3qFWDgUHUoiaXbojXwd9IgN  
CKzYPMnjqFo0zD08b2urpyu7dybgmvzk3PuSlKNPUucV7/7nJovZw9xLCcPIDDmR

BBLvUF/tPf7me0sLWzT01uSnP2FALFvnm09c/075imHxX8b7uLUtIJcraX8ay8n  
1wT7PypT4nYsL2GuMsGCz/xew9ZbZ7GuhtfBkyfthHBGGj f9+UMoB6Ep8G/WbVfFn  
L0v71oHkTq8XxetePSjIdC6m4LBwwShPIU6kj0qYzPBMZvUz48wbhWLHZGbvqLL  
RdHIwTJRyKToC3JxXn+6P5KhyMK3oSJfy0S1qmC0eyhQ24oXE2p4OzCmLiz6RktW  
mLPLTpTDksYjgQrQ9LgpCPsV+W6G3LzCIEqjGXAKSJZT/M2wR/KVZz0Y3NUPiudz  
6BnaSKu5Rbs1lI8WT1j5QzEVass+YGBpBp35cQ0fbSbNwrnTC30VNkwtSKVIQe8p  
uLbyh3ZaT2ZGAYPMKECYkC7QMplSMI/1PB+/fv96pDZRJIzTWdFONi8JLHP1AoTL  
xCz0CxtYUDzKj2GwZRuCLZT2SAOM95EpceZJeo8/vmUSHCFSDv4nRjMxc30Hy1nn  
rAVM/2tqftkfcE8GgPL6aUsvXUawF4Ncwe3B4crzVWmfR8hdjeFqKhpScSvAnUR4  
N2D8G3d+G7UcmzuPVQIzKn9v/9d+qjAzoZIBBkvQmG2Xbx2obGUKR8onxMGPgIhq  
8sq8h01ta3Q6yCZvt9JL8w4dMdpDupB1haEbkVeQm7t8l6m8lViCunyov5faDBiG  
G4mgvWwL6fFIRqANzZODMi0CvoavFY0sKgQLE29qFRE0DVC4+ZmTVXLCp3AKB91e  
D2vnlkqI30kuXzSGwp2sAJFeLYDnnq+gb0t1kQW43sB8kHhH8K+EHdCwaThVaBGd  
tHd0G/n3Ib0z4+ufBXc6pVFbw6/lypGTpmBxJk9c3QrDdyaVxJDpDc4jQVRUkt2h  
pMjJEA6RxpHPZ0DKY1RQYNw6AP2Cta3pIZP0Z9hXOpM3wVYrrkc686krYkP90E6ad  
6+zrkGxILj//pOdFvJwBkp/gX4GPqQACkGxhUDwX0DEZNnQKavTFsIL9TMmwq5t  
LBDT6FJNWqOrzT93pXg0s5SahcG9gjjg9R0udq+J7uztmQVftOUohN+CTTzvmcFBI  
0YbwPB01QRBCWcHshpY0T0fmH3+TmtR02qm+BL4ydzjJarzi/wwwkue1f902xnqZy  
r2IGfzZ+kwY8b3gZgRYod6AI3f5vxKE1z2pYthSWQyVOAQQRKk72rDxXsSuwx3M  
FCY7wDwKE3D8dUPWDUvZLre7fpuI+sKiVCf3fd88v0ldsPxxztL0kUmvEwImEHn  
EpU3fLDxcYxWigYQYzYRZiY9goL6uJQhc6tjLvnDnQw/xIi3LIfBiBSFjj7Lea/I  
Whq0gzuyzwXds8/akZzPQhdHq79aCM2onXFK6K9aMjYhSoBCAq9gGQpfU3yq417  
cuqx7IMRKSJUnPw4L+0H4bbt7ZKkp7nYMNPE3ah07KnCnSu185PLK5+FONITTFXV  
LMPy3gostDe1cv/OceBP/101SeBrfOPokTcQaaCFddZuM0Qdfj70VIt0eAU09yye  
/xdJzWKHjovMrp2QgMEkWGnl5ItmdP5a5P+BDZYyrGv8yGlgTaV/FkiS66QF8bVU  
zLAWed0Fzvyw9ZQ9eVsEjQ00Cko16YTAVS3VzavCrip2BYA0ni5wtpQQ701xSLb  
D0opKo/auXH9RyWiXkZ0kvYtpqmFLUdzFqrqUJOVu55hlFQwH6fT3fve2k9PYzk  
sDg55VFUuQ7LVIJ/DE3hDD4KJEs6gr45gf+U//kIxujxWtCgwBn/qBW99WjuJMKV  
jUhK90u0BxZDSV3pFRf2drvSnuZ3RZbm/nIJ+R9mC5HhjXE2e20IjTLIdbUcrSn9  
qd/3LRRuIT7ymh0mHaHxCgB2KGqRxyjz5z0k5mMiZWe+PpknabIyQ6fHHLUEY+Qa+  
0ILAJEZvONd2ilbeYAM6oY0SD6Rg7py/NeSn4/ua3UpEDh7fj7jKRY9nFMV0vy6W  
b9bcBIp91xKITjpmbxYhmrZqhMyvaUQ1/wbrre4YD/YVx4/EsV3LnnVvcD3kHedZ  
vBbLevKhGJYxRacBSYAuD2KqyguMF1azMR5o3dvWNdz1LHe/JTNANCC9P9qSRIrN  
Xr0q2yVortMff1YzGtXgD2ICw5/pusoN4QnGuM00PF/tbEXadmlL9CzqHmHR7gaJc  
t14jLyj0c90Q10pBfu7dI5WLXTx0AyLZjvbDhdo0iFVF9KKwztYkr30CZDRx0qj2  
AUz4y6NgxRhCf0LFY3gnWk0HKhRlz7IybWEnppm2b8j5tJiaCMazNVFdPl6k7jG/  
BUoP3bVB0foN33/B/v4TdeHK0cuaYudd3sCWnE18NVNaVHk4HGLEK2KhtASI5mh0  
0DlrTa4WhD31idGqk1LJkFU7wGgKf+3toB6MmOuA6Sw+wD4BYuX40E1xrWnTATNw  
8WAVAjSSN9pTlmyrxC6lqyep4MGcGb/vKJvqKurJF4wVLBrp/42qYv2IAqfipsqG  
MLA8dd0udFYQFYb0Nds/WHeKZ/4ICFLH2hGPptzJIU3N9j5yYpV4jAceGzC9/xVj  
jx3hT8mVxxF8ISCZwGS10DVMHc1fzn+ipWJNzvBtZgq0jRxs2a1dTVRFYd4T1Q  
NjtwBKZfjVotqV0LEYSRQ8grFYhcNpOhqp3d5P4ExjJLYQFe7zBfA4xbWdgbzyiU  
cK8RRV9v9NT4KbUVsk7MNqBkcy1Sd64cq7peSRTb7w353XvSBekL7LTaLCHK/fhq  
DPvWb+/c/gVFtIKBYIzmeCuI9wh2xkLA64PJHQPYP0QpfMw8WtZkdEjGeK0mbtd  
jVoxhsRyb0BWC9yVu+Uqy+bHpjwuya/HhcweqnUsiMmh0Qe7MEbbFbsTZNQDXsNL  
WLQFXsNE0+ONRoLwRQprM/dZcjI00Fa1atoA92TCjYMiBQqN7vp8D/7t35QYuicc  
vMc/pPK5k0WMDtRdf3w+3AHsng3LbICynDMqGsdbM8XOP6xYj5NmDRGKLX6L7h+  
cAw0NVmPhcv3CVHHxYRXtzuyd6ThQdr4mwCXxYglxBMJCH/Xip0wgC76itcrXRPa  
0PKPxc4Ci4Wfa2STuqWgyqZIWgPOYowRRPIyntFE2jGLcK5j+fW4YMQ0jPJLTB6S  
YPuk9Fy+EtssZwe2byBya1zZ8xVu4XUcHSRh5plkb/t++djrcX7/4uAlKI+8lGJp  
/hWnAayieX/i0p8ay52dd+RhaQ8QBo4ES8Do3b6H9bZp+27JLR8JQNlFk4EMMu7X  
odCXAfn/7iDPvAS/u0dqkK54bg9DRmK14bTsNVjp238hbUohy6wPdXSguR+f5wXr  
VyJ2Q0E1Uj5Pr7l9HiddaoBBZ5GH80K4YV1ajprb0XtU0VbAoYaqv3aPlpVWoAnN

Zni1slrQ5oo1Lfn0CId5P/+hz/d1PWoTbu4p3GvZir3TcNkn4zuWCdut45VQV+zM  
m67fLnnRtNfa/YEWosCvEbZFo6A4LABPWV4ESfrUQoJMyBPpy4gDnRBETZF917bL  
JevRnhSnn1QMjDrMaDs+02D6ZcCzrNpk2nGYwV2BX/skN3BrBe4za0KD4RSDvox9  
C0cuuLhw9jmz6FN6eFVdVR9bqcAXWECuk3QangD/36CD3adCNDI5ZsTmN7w+FYl2  
0eeEgXQ0iqSzLq474W5zGVYUP/mFGJAXq5oqoWRzKXFW2Uo5LdQxaoGQ5VXMVvLb  
06xHWyUGqyQQyiqn7Z02S5bkbP8FFI1M4PPxqa2o/uLBSgsY6CzBeOYLJx3vw3CG  
KAj06VtNr4EB0pkgQa0h76rwbWPizoaEtxR18GiNFCzuskuJFFtixbkH0Lnbpmmp  
UiEFws0h98N1qGoRCr52IVxN1iheZR7BT1YIgUl1gjeaHZHtQPMU6pGpeKirhzIk  
5USGvKszszqZNFxHi/3gOX6qqIfpPPRBiaXaYawQI5q62/lhuPkYcubhTShKRxHw  
kcbJDPvdOKND2KTe9F9yto3aWLCN515XYwQHgYQH4T09x6npww3FKKjptD6nP6P  
pAJ1z+QUHY7MLDd/+HnhGm2ZG2yYoPTA/zJg4+/TunESDveMcGs5Pp7cJ71f+ldL  
rEZKDYys+gRn1Bgs8G+oC5gNy/fFy0ZtKsl+trwOV1fe0WShBBNn31GJxc0+9gxd  
CroBEoB/QKc7cmUNZukYhP73nRw/Ndm4uX7iuQ4YZ0hPnt8QAQuQ1VzsqLk3bYY9  
4wr+kb9vX3T0x3+YPEJ6vQYx/Rcpjjv7BaAE/QR/R0ngw6/5laSxRJiNYk/EuBiI  
zFshaVFFy5YsVfMiP3eFFzptJ29l0wv9rCFNV0muH6TYtrLJ1rUZvRJRYxe0EAwy  
IDFZwg9d6NDwCs900eeFsPagx4HHl0wFeOFI3BwmK1xGHIH90G2/01d0gK0pR9yZ  
zFLyZr/Dvtq6F1ahB/yLXcRyQeLC/wLmKfIPrPre961v9bnxXy5/M6gujiPZ1YDq  
moB8Zc5o6VrvXIT/c3Xa627p+v0anzUYIaGsvNSTHvalZXjdEAtfpgG5t4Kn3GdX  
VV8t2LlYaK5yQz6PkjoZj+eeTho+rv+nyn0qATLTq+kbHV0HsW1fxF1NXD3FUoNx  
XCSvNBUGSrWUpQ32BASmDW9wurk2n4mG4fU/q2bsf0ZNhBXg5+YpIR0PLeBH/VHZ  
VCM7j0z69R5V5PBTuARpN0kTEWrUJuRLMUWu0/Ur4kK/YYTUuHsF9P6Jsgwv690R  
QuLDbFAfUVWm9IkvuCARubTxG9bL4WhTWSFCeUxPv/Ccaq341yEJ4RVRehcIw6v  
53ZrG5sxHSYSycWVf9B8RwajnedYWMLERlwdBztRmVrxc0MKvLTFMC/QQ09yfsd/  
oyN0t0f0R4q8DyXYm5xhsvGTcWH73BKmwrSnuJNIm7D4+TJghnTyDaBmG70FKpaX  
bAVwyuixI9BmgvWc0N0/bLn9MrLQJMVAm1ZGNZV5HPvpYcxDQWcacvr1B5wRMtVQ  
N+FsfkxSDPzEiXK7tswz/Y3cFg08XTrCyDl6qAMQvwvDvJr90gFjWUf8ozpKejBa  
1g7TVjR19kktokTvRbGsqEEH7nUogq+nyorm7Sdka3VwL+S0oqx6xbfw/v+n001Q  
XUL/MAVH7xktkDmEz7Mw0e9GdosN3K3IYUy8youKP7HwdiqzQi7oCorc+15cX/6t  
J3uEBJRHLw6DFRPhb6Ez0YLMG8k+Ee7DG6ootFAhKPZINMku0iM9ccJNL0FJB3UV  
1QVes4YXvddW9GGBuaizbGMumjE4PKLoTyTi+07rsCiRMF50fi22Hg+/ykccP4wN  
R0d4ZVz1i5JwZi0CwJK7A51wlncKdGBsgveLOGBZRLA/UMxuAzWRMbrfTE6BjzPo  
fc9ByhC7U0DpB8PISjgJicSQV0kVyrq/PiFOUE0bZfgcSyORgZbzlj1Q6AC6rZls  
caJaMRtt8JcYuiDtrsMLMP+wBsCv7Luwo5H09ezuJyELr53+FNvVzZFKr4DY167A  
UN8vK3TxI/nVCw1/GU+QF/LjbCFmGxjC1LFtRhXvuScS5E8Ex1pM9RI0ljCndxul  
FZnL7tsQDwxgdNiPqpcWn/sk3QJgHCBh/bNm6ITmE8jHBMQqv389EGZQ9+EaL6Px  
Xi1vJuCuUwXf1j4G4l8etETa/GeeR35HN+f1w2D6Ex2qFjFo6zHnZL544zRZZY+a  
dE8H7yBN3Yftt0uZdQUaTyQDrEgIvW8msGur7IFA8dR4nwqWf0/46wQDrn7XhacS  
z96AGW1WlUyHEHBtx3+JbLx48DEbxRho5yaWKILstLrKHhuLnPK1/K6vvQ1KA0u1  
gDr2HR+/clafasivLZPhSiJSElFIPhfV0Bs+JFbGwzHnG3/BmtZkubjLugeJLCHI  
0NxvX7/fEe2sHPWQVPn5Ishv7rD1a408LL5xdRDxP5bMW1/25sd+I46gKwmUWy5h  
rq0DZfaKyETHYt56xshx4X8F3VrsRhfq+yKndkGiH3gnYv03C0cI0hWyRvfpzr  
yb8ie/+AON4jCJSLmh7c+SjtUrXP+MUULi8HZfXugzVhoIp4JynbBYBuZ9N9N29D  
f9XmkCn1Mkj0Guz0aLWD4cMu4nk6VESa+dkdTWX0jqhFuaZanwgGoueMViluKmB2  
gb1XL/oB2twsEYhYlwjpc0Jrh3zAH30qan/MKXU5DeeVn+aAu54TvmEoNI77LEjc  
8sq3Ms2mZwXNw+8jwYw4U7Ih5dFwcezoFwyPJYXGs2XgCN1zGWHuEZANiOd/S1Vb  
sn9LFeN2JNeIp0nK+YFvArtSx0Yo5oT1J75QfWipExHjUkvsFQ42Cf1XfvHj08hp  
uPltjh1qnRjLm50EmTOInZ/e5BQju45Il1EJuVnBOKqEec3Hp1+Gq6X0XlrQdYDf  
0Ba1CBXr5z0UL2xBEWAaKg2fAHpJ4u0mTqdY4TZF7QiMoENpjvkZlMkQNwBH0Se1  
+eYlx6ML7sQapuo8LrP71cAXpYmWvS1WGw037mfeBVb8/biOP2zpC7QLmp7bIQxJ  
Fj0TMbJ56A/MJKzUzZvOMCWSjL/bL8atlap94rXEZ/K5uidf1l6tAQBBfvdPN0t7  
y/WAIA2A86x7fm9X9EW+yOUB9EJAQi/kjLMtj/vfzIVngyhvrBvcf06G7PNCmdz7  
t7Y0iNLWuVsS8x326Hbjf/cSWGJJ0w8Z4kKvPZDH3e5LLRN/04jDI12hYJ42D6q1  
U55VB4AJ0lsJXM4W9aNUu6uB26en1+23t7Z/G05EPKY6LKjNxUwXJ/f7+y1p/64v

kVF6ZpKYXKSw/RarkCQ32J0SsGgMC9an8JED1f7RBP4VLxL6aiusuWE7qqcHEvpg  
e9xZzDm/HKnEGBgr/ZJU53zE7ZdAdRdbtqg86j6E3Y4mGPhl0Ep2YelQcngZBDKN  
F0v/6HviFaLaTLn+xwvZ83UA1iQo7C8XH/nerqlXgoJX0mB7zh80ydQDdkHzwVLN  
JSdhZ8M6FFIdcLWEJa8xnXfuEMPeImTqXew2/e1TbwARins5T2q/8cyAlrbx5LLT  
SGs5nq0Sg/H1Ujh1MIxT1azVYXUpMQIgiGjCteSmSR3a6h9pWzxrirCZmMvxHM9i  
D47dsN9NbGc0q/YikS5AnMricLBLOhH0ey9BgVu48r9YLLjC67iB0PXp+eVQ/Od/  
7ujYBb+h8uVGbDSr6++jZmsTMkePcdPd0TDY/3broOzhzVzAuAZWxYYrd5FuYoqk  
EK5EwC53ZmIyAAYRuCiYA0RutFrm0zndNbNDZ7VPLam9w+TUEnl6bD7jdoQH+50T  
qEbeuH0wL5KlgiQoKIOzn5Mma4MxNTkI7Av5z6Qwt68+uBk65GPQ1FA8Awyfwzw9  
/97DfVCyX057sLMPYchM5pIXYy0PkDvyX3InESdH2VsT4nfGMIFE9LPUtiwwNlZw  
mqxqtZ7q+dr4sT8DMAUKmZ3zkC9n5s/F6Xqx33yKus0QLEqvPtC/9rTesTC3U1My  
tyX7G66Gx+FMmy9a7xXsyKcrbWxMIMhQiVVvibyx3FDznUW9nNdYgKNl9aBJzW1l  
sf0XafZ8VCwmAphLHSR1akBMGHSSAhT8Mr3878IaUKa2aSSRN/9d/Xy1FqFsmV  
nhqjML0orCE6P09cscvBXUJq3dpx6+qGMX//QFpIkimGB0GctfAk/oLNYKkGMQst2  
iePNps7Gx+A8LqDe1QB7lpQ3aKjIjxAvXKUTtZz4w+sFvAtPYnrKfLra+DiYdcn  
W84YBxHYpSXbQAvLue9qJUGEDDD2i5tqTmxgmT7K6wNRHvdqi44NUwvHLoHD7BQG  
Aoc0m4fQ57B6D/It08sQobTXMqo2lrrPrAko0x8YYdczSYBe7kRwZLLcA6kGZ9/g  
YvDUo58ksNtK/Goa2/exZ7gDu99z9butU3xvCZWMUNmrX6PIVsrVonLhr63yBiV/  
q0pDpSBahFuHktpL0sJgU0aKdqgLNxFuko9hT/4TQ9HL2pMyd/PXroQuS7Du7X1k  
YEXYcGmN1riEXJuACJJ+lbn0YedDk7MGcAvZ6UPYsfnHY07/4d+3b+c0w23xUIy9  
D6Pkj4EiYk48WKKmuDp+jj2ARsS81/HkC/cB0jcm2FFSKaKHfV2BoK1vSs93qw7n  
TIUdpNbXNYU05AKzzQp91KFbogDTpxZKnYPvujBlOtJbFEQsPocEM2ZCw6mtmdoP  
JJCw2D7RXeRpAUT+JFdXVy70F0FFT15oGk4ybArCUf+9JzvLZZk3+ddsQvB2MgUP  
s9hujNBmwDcUlk5SgZvvBzbSqsjB0zzOpjs4Pcu6CcbFtC9ipdENkmcddcVMmG+/  
Qkz9/wE7UNCE3dfwmjyCpjP653awA+KVVxPXIHthCv9gwn1MuJF2keprLtXfb06w  
KiR20catmAPYCzhnzLcKWwpWUka74pYaxiri4VF8PYkdJEKAU4gWEY3MbDjnk/g  
jwhfrymJappT/t4FgggttZsg3RoLJtTsCve9K2G7ihNPgxfEomS8czeDgFqhIEU9  
YBeElKj1rDUDTGqnvbwUVY3ccH3quawNGJ0MftvQ+yxGhXL/PVUCTlZGG+b3B0OT  
dcR48N2GS1M6y1cQQEntU+DgzPcQ/Do8v0gsYt1Dvo/BOBj1hkMdC7R726ySxq3Y  
r2R03F90BsWtAfKSTL+vBxFOUfr8ksWEBGlcgp5ZHfVlyIub5MSdaZQnuDJMF+3L  
3EMWPxCVKkWXkt9qhSn0KKpW6mtxUC5hLwtY0p22hh22aKXXWNfYB4J8SDlvSfIv  
V5swE05QZp1bzyR87K74x0m8sbF3/yU9jRy1Ak0o0iRHLtKUK9JqhL08RT7L9mLb1  
Piq+AmrydWSLhh6DDPXp2LbHw2DuLlnp60fDQ+vafms+eWKGxRfzKiUph95Ky44Q  
ZqTa+CuvjcmZ9eWgoClt350qRqNtXXnAAM6PhAXoD/D66mMiFD0eAm9ojqgSp9bV  
uvVMJ9fZ3S2iz2zHvykhCdkxV0FdCqFREvLw4NHocA8/aSpp4iyE/YqYRN6N0hBb  
G0EK2EosGYA46MLPhkICE1a3qdxLq6KvDPIvgT4TN1Csp/s09VH4RW42WfYJIX5l  
tF4S6wdi0Lh1+IDBVD1xC7ocA4ym0PWV7PnwZfJEKXUZ3ahBbkHVjkau4Bi1QQN1  
Qmu69/D58oFyJOQmMDPEH2cRPu6BE30c7VpHY98U+2MktH9X4xtdb131G8ah5NJy  
3dfTqWl/YhVhaEcFVm0UAaSrYgnrvwKPGNvrJef9rMYu+B0V7pHQW04m6FOU5tkK  
I1Hjk7rLDo6PPLlgugIAM094d3Kk28B1QENv2pjcygs3xuCTwy4qpy/FpRGMt4k8  
TWC0vramLPBNAoY0+d2vPCjzxJTnHlpxm0EuNvP/JyG6KD7+we9CavugGBLZ2rw  
h0ye+RNYKLndtbUrrRuVgIzCEQK5gxZBktp+2IpzITwKiRhWr2rye3W6DvluCuA8  
Zb2dulYf1CTs30t/NNNFHMUYEL7p1Bfgp+cFxtvdJKajvuZUpoUm+NvF7sL87hx7  
6rDsIl/DOIBV0xAjMfQBtLUY439IgNv4SBvbLSDV/96Chi2UTPQ2Y+csTC7rUqdd  
ErMKy0gyQkLVQp99XsjB4QNKjblS6RL90aG1aT7a0AjPVcg4z40/koBJ6BAdhr4Y  
5k/MoCVVLp4F/vS08zmfZLXzYs9H/aJME6xcHGmmVU8gf5zxbkm8F31gLixxt3J8  
4Q0qtNA1Ih2iVEF/AnH5zViD0C+lKp9cQUiEpCU7Vb9fqkh9UyxrOzpRr65Dr5AT  
N07npVfExTWpjUIEFvDpKj5MPcAimOtKugZPVmxa3HtvaZW30Ev3xar4JH8jt8uG  
seG1MT2QKFGSUIuYwF/iRbUVyS4FC7T8UNBRHqoFNzF/F+n8rebb5RYUcSFgibHR  
T+dIeC8EX7CCW/Vy0z2cSPq5dWgsJCHJvXxHBP04IB/IQnjYxfQQfC/QkArD/xT  
xUXwFRcOouM9g+m81QcfzhJ6RvaJTz0ZWNu/gaRsHjVhXqdmB++B2089QsCLdyTB  
hTn9xr9n4M8l5Vo36SFCFPITuAoI3VtMR1nMRmh0sojyGGyDRs3etWtu7/oeKTO  
rQJ6IIsIXc90HMG0FYMPat50zIM75x6S04iXbd4ve2aYZ2xXVBNLPR6L9lmML2bc



ChvLnLh0YhUvk8qtsndwEhLbnfi9tTH0e0qZ1ySjgNvvZh0+v2zk93u2YU0m1J5B  
JoHMAuhcFggIkz690z90jdsdn4awrXSG0iB44jDX2j2YwiPKMSZwNZ10u13nvbI+  
W6eVAiks048Sp/DLQd5g+k05G7SVziHR39mxXmzkARwFKlMa/tgej4ACK61VDjBp  
6qQDeioSCKMfwUc7zdzzRJ5MTPmFjSLTW422GxTPk8FCrVX0fxLtKQJihMXrJs69  
4iUIBvRM+t1gSjv2fNf2bHA9vyT95t+17a3K5ww0t+WfewM1yXoFlq5Xf9WTXdq  
JkxCbriYSCNRmc0EAS/zgR+WgvTWdCjw86FFz43UX5TXyEYfwGmk4Aqbo9HUA8wh  
0H6NMkyh+Z6peJ/ju0x+VVaf88oLd1F8uZ0MeiEPYZ0dCUolpd7m0zLu8wX6VBRe  
A50ypsxz3RfD/2oBQzk7zWl/BdF2+mhbnt1QVf4qQKtx41eItCZLdoS9II8tcxwr  
YJdeDKWh/8p1UjMPLHKsR3d9jLwZhrOAmjTYespAp1xmQE6FXhC8ADFqPmqSCoJG  
5x8WsWdcYt6qCPgzNtIWjzoxXkMT+JNbpuouT2zcSmd0ZuWLYH0Cgpytyze8HSQm  
Lcnu0TpvkqG7eBENouIECNwTWkm7J08hVJG+a19vkUIQ1C6Ef8Q37dE/HVGJTQ5  
RsMYhN16fL7f9p0xvQsLXA6RGNiki8agzdz1NdJiKdWZt070bFNl6kn6h+/fCPN  
WDXWH8CtZXwVRft6ypKgeRA08dCGNoMZl8YEGlUM920IVALpq1XBPNvRG/qZyb6  
Ay0LfytInxcBlguAG5eUct0UdBgtJLf6nvhtLc+2BK6+9X/i8iMY4YJR9jZoxV  
pZ0jKZJVQs0JWaYruhVle1b1+HplTDbMBZpVtNsLTWEqvIPBsM43Gi4SIgn8EnCI  
CbE7CHFRIO2FtL4wGPncWjSZ1TjV1zojRNI6hLzMMij2fLCZ7VSzLl0ejUZfuo6Y  
006iHG2zmFTUGwas7wLhx6cNcBeCmGEALRBfcdd2mvHUuf0NMkKaTd2FIXU586NS  
TgDcSitejJVZI1pGwYBgLdrVpZxtAKpOU+z9ZRuvdo0KJKr9qYgbDKyxcekABpS  
CNpRf2ULWwq4+DzeC2hiiv+yKZy1re583SiKfv3mXGmG1U2p0ZQXktv6iZlb1nst  
okp0dBREQUofH1zrBnHa3BKJV6TOrsARK+Df1KHR/JJdf0o74JKm7eMYMDvK+XNL  
ne2Q+eyIf7FQKLQH6TR2YkjiXWYc7e5nmuiXX4d3IdxtUbsSoJAKdSvP1AixvCMn  
1/PbhKGWZMKBEpPXPexFjajPB0ZNV0NTjoKHUC2Jzew6mAPR7jZi6rptTiPW/mGv  
L09fhQhrBrIV+iR3VjrkctMpVvSx5NQU7R1Zj+Y/6KldLSLqbZ0jKgAp56jnDLWA  
/kl0Xw1IaQlKhKWXeyL5VlyMg5k6MUuIzpoi2rRpj8zAu0v2Zqt4x/hMfxMt20hw  
OVQvvVvoT0XwdMnaXTuBX7dWhgsf83xsZc5XoRSL40GiXQMqdiTVfa9wpAbHlDyU  
p5tpWayCb6ipXftz7vLHUxyuFHZ9uGaR7q1HXMjYxlcCmSYgcGYsdccKG1rqHHxp  
9JLPnJZ2bm06d8SmoD3axiJirLQYSy7C+4bZ7YwdTelisZF32jG/vVB/Dzlh92ws  
HrjLCvL/T9QHpsQva4WE79+75/5eZeq5rfc7hH903qpUmmr1UA0QjxndkADZz4mh  
5I/Q30Z4lxbqHRayyVsZrZSKvgOGVxWI3sMmZu1LAyxPI18hHiuQsdeyHgGVJJQH  
JzZ6+3cyaLqHidCRg4Sxs4wg6zuUtdPheFEdBCpc47v91N6tFwoWc96KYXg4dmH  
ZRw0JstQTTEEJD+kwKdTRwka6CE95iu1/ejGFOGpNHRbJcEKiaIekuPbniUw5FERQ  
4pohdxQ1QNKtG/ixr1w0Tg6UQ+k4fRZYrKGqUcV5XqLjgKX4HpUPZiqzBsXwNSE+  
8pjC32Pe+06qom84wUbcH787J++sYT5rAjwQnccTooq0w3XLCeohz9uF6Nuu3fSZ  
RhhVUvqsfy++2DhPtvjgSTOEIEFfNkdNfxEhj9bjDOrPzgckjK6oZ8P+F5Zw8AAO  
z8DABVAe/WQQq3EuGIKfTG80BpfHm9P4Bv5TvcNTVLN/GZsCRBC4UOqFxFWyMK31U  
lLA3ZTfPKjKHo2e4cNpQSVyBL8gxeUW8qQVx4PpGBYX7duM708LrMEisC0kyYy0Z  
5grpXYfYa+VLB6rAf6liVcIr5/w+fTK4k67//iTrLuwbjEifQPjA7mA0iPoQnJ3v  
ukD60bb21D5Gzxkf8Hig8/35Be8Xhlwr7SvhWWWetOaLnIK8dvE7OHRl7CZ+cPHB  
sBJIIX0fakiwmnCdh8UL+UWH4YYviMLySfGD930FioG5dqYv37iwJMiBG778pj1a  
1pdmRfvhwGUowuLyZwwAGnyUfU7w6U4wUzNpvEelouvTC68UG03oNgBRNoIwe0pw  
RPBZe9uD/x+i1nS6imAJ43FLKXjPTV9CGg/YOsHy9uiaNln6t9jHq5CrS7bdpt9E  
ycIS8zgI6v8bgx0vo9tA7XPgGB/JMLkkqD33b4r3vLiPpn2hnBn63VUVP20VcLdh  
9oejg92aGxekh0Y+jMQCnPLT9vPUjJ00Xdx05jPe+362C5aC0fVcegVveuvuIbM  
nHVah1CqVGOTLbE+NcA/GLcSkpQv9+auaBk0eN4RgQFhKMAVR68haeqKkJWjApBP  
JkevmS2412J82Ih4hrp4z56c0xSvzp3e+ybsKp0+YuzBQJpkv10GXUGF8QRC/Lh  
GHXJiFKTn9Pt8YOGVdSB4VMjhmoToIyF7Ct02rmDs3et6iFj/+w9rZTM3oYajdpi  
TOP8Z250nbuv7xbaIFLCWnUqpM/XEHhWPUEIk1PWBkUxR7rg4GrQWCxvRu0g6zwB  
eJINE4Z11XIBu+/l9xMDy5EPDFyvtvLoi0mWbfiLc0ILLXGDJy1rPk8XAmjabEoL2  
WD0F7wXwXWij0euSZD1P3HX2VPWDnzH7fLZKbgZTFghhEGn//SYewlEnfLUTI5h  
fStDAPgavWjNvrzn0Pf4BmjNR0xkx2/Jc6nMZTyAVOqmm4aDraE7rqlVKwAii0Nq  
l4wrKbLLWQrSotzNKSCQZ9rRdl0QdWwbYJldqI8lrJYXX11EvtcvHyhLWEKssWMO  
T2QXhx8XigEChXRQ98tiEAZcLy5U/04/Yn16hPBIVyXLCpjuadnFXl9yRULQvv2  
c6RUAxtcjLCfQ043hTZRZ9wPVvVKZq467bSB1zLx2BLJBRdXGR8YkGUHjp7HZ2Vu

RSuDA1rUyJOM7Dhw/j8lmHBN2pU1zx04iEpmvCRDmGxoYNZwBAu4G01BYLXPjr0f  
6jagKEK0vAleF7QONITAUvWSB8+tIicTC+iznZm0oIPvuVi8RT8Zpi4nGowcC5MN  
+DuLqkRfWsZdgNucdA7PD/J+5BQt5nLwz9+ApfQwLtBAzKBt1joz20hF/685ytuX  
1BmtQ/I5cVmbN0nUsLANLqEQbCxg64LYuLwuVfmwYjddNn4pDtONEWWMsmc8RfxK  
NVRAZ8xJveSfXxL1xL0I5DhjTHKUnxWbmFwdg/EOWVJZyhQMPrwMxwmnlUZ8+P1s  
A7Bz51ebp58em7LoVgKocnRnKt0jrtchNxoZ7stu4fImgl0iZHNfgVeHpzo0XG+U  
UWZGoJAj1ru8xSfl4AHeEM8J/FwYLVAtIyvkB+Hb3MY+Hp19ZM8F3Z4nPyBSfdeg  
u/Bjr5VykBwn8ZrUYOvXPvg1VEtY9NnqmIqb3Yhg7oXpoqJ6A16L9KXxaj+/bjhT  
ZYxu9AlnpgTeRoKog4AFiBWRnGknaUqKwDpyMh6QpzusbbmInFqswJlN2KIbH3K  
ZWnPt1aGcqsghJlLJ/nNqvgHlZ7ZL15DycrkHRub7Yy7Z4B7Pq3Y5XU3501i0S  
Thwv/42cdenQCj3zLBHntF/IBHk5jJEBgiwITioh4jZ6p82W49Y7YHcVCSAWfumv  
Hqea+5+4GPr/DTFYVct1vKcCDsEQrhKjWY01S7QZfz7sG4gktUQVC68245g9L5Z  
U72fo17v3eKgF5G2RcTs+RnRDHE0PWyXwe1030Rvo0773T0atY9VJXD/1rPDdPys  
fX5ZVxu+IE5X+Xavd1BjTGMZ0EFx5qt9jrIrk98kkyGMAE4Mx97nojJj/uH0+TkI  
UaVo0hd5NHtVjUsCElAlYKyU2y9Ey+ZT2G1CQpLZ2VQ652VtNtZowSndq+1LsPRE  
LdRqmEp2hIqJ2Th17dI9NWdp6lBrSmkJ8/XTYPONIX08xBV9GEXRgZa+f0R04m0YD  
veivs/wG9NjKwLMZygZCzLRT11M0jSrWc/xLU5QyUwxQIbjFWayUhiwSsXuTkj9K  
GLqvDu78TCviD/nWgzDMIMN+B+MsBdiv9Sc7EbSBQus6abn397u40LGkTjwbPPtr  
rF6IRsSZ4EGcnWTQcuXWTD0ugmNbpLT9/CUqVql0r4EikLXHuWKcso7KUalWp11  
riLSz2BYzk8WB4FGjLabXJKXjT1FpK6HpoBa3v2Zvr6pMEin1jqFZih4aiIOU0Jk  
4PLWkTpgDJ0w0DnVaFSpAQZpA3lfGhHv/NQVib+GirjUniBhCvvqru0FelbqVb2q  
Kok+vdkIufl88kKumtVjUupB2oDd0pLn0jeTf2itdsuJUK/Jb0pkibAUp/8V0Inl  
iqhScEL4u5bPvrY0VHjK1bl9V+0WkweeLSGf9y5304+tcC61HIE57dQWCjqX6e6E  
44fPanMZvx03bFOcdouBAxK9duyxIXhSkA3++t2pHm2/REb6YmMwovLcZZxWwS0t  
Uvgfw1L6fXzYI5C+oz/STVOCIOxPN9ZukZlKchZ1+wWZTKBj0X6vNK2pla1vzY09  
B24dcX5i6AdiIFf1cbzPxjyNfPZrZRLU4hm/R6e3+80IhXazy1yYmaKGRpzfS+Uu  
WIYbIVCBp0o1Vj5vzl+KrH+SbCRHP8DZnSVicCZLnNwWvCiQ8cnwwjLNK9kS+C1y  
CmQ3+kTlvCgi8Tr6uw7xyRMNXwTTMKe0po+qXSz93EdauDYGm4stLJNmb3kqhe5Y  
e6npPCDHMMW0+XdfN9dQfGfRCvb/qDNYt0GyG0nSWHqHje7KaelY3ajIRrrfJJGo  
J2+sXg7rxyFn8pps3+PQKfTebm21UGU/f4yIwPORwwLCpTTJ9ZZBhb5Y+nTDHAL  
XVgP+tmf1moS1WiCKmEm73RJ2Z2b2agc862uuSoIbG+j3BRDQ9KGUYUxN+X02eLF  
l8v0kVfyl+GrSDgVoUG4JJkm1C1WXtrYmUjXjHsF4rfy+YiCaTXttzY5DQScZ90o  
WQwQAPv0kroX+e6fYic6xSHlR0hayNT0pBXDHDBDo/H+WiM6GASyVIigVdSeVRoe  
gzT1aZnuWj+G7SS54hcz4hFypp0lph8FWeUTjEXVj4dwacvLsY0IQ/9ei3bLL0JV  
BsmAobkxA/DGFMtpdsS4IasH0VeM3/GG3nDLZFnVXVv8q1Cus7LC0vxKL4wp3ZLx  
MmagxqxYr4hsC6kcj8ZETZ4zjidi85Q8zn0pYV7089yqffFdXHzcV2/5wEPozMU3  
uzmjbMURNwNy9QUZFd0EQV+BoyBNli45u2JWeMpFStkJJZR+3jJrJHlMJlpvzPNi  
EnU65QZTktHq8xbGJYsnMbZBwaQfqT/mEbWw1/FdrDa+dgCbquQjChAAXdBfDQC  
L5dEGEc7u0Mvm2zGAnidxXf02Ix/1QZsKEmWiyyhpGiSy8kbKapAULG09z6nC1nt  
6ZL5q8zS5b30FBv+0wpuzebDxsIc7iG/zg1cMI5Gz/jDLuzxieUaFai9dJe6s/NH  
9AG3qoS2u8lAwKa3nG9DhzT5NYt20t0gY1f5mPFuIH6NWMnTavEXnyr5GkD88rvv  
RIg5It9rwqy1h/7fvhQBzI6gHc5rzSSEgwoPd5hZKrbmPpVl28UAT0aYZ8HcSX2B  
UvKvJF3244j0LJzswxJ43FL5c9Uc05a06S7bPJPq7oKn5QgwJesa/+1K0DKZ42NO  
boCn+PSXD5tjSx30os5goiCrRS2k2YC592UXCqWCh4po5b3Y2KEvSBw1h85XxkZC  
sxioDDcHL0IqSRIwttVnK0B5QDFDrTtfY+TDDJ7qC8zmrFQQLNsBYQnAz4QgtIPO  
TvFiTOSbh9s/Wo/Ze9UztXUVff+BVSzFvLdkJ5k653y+T4N851Hu8sXk+SmG/6p  
t4SJM0g0QaqRk7p5lHA0F/UWdQPL3lnfwig0fQIjRiLW2+Uva//UfH3BJfMgP91  
NJIMz16CJha4L3jIIV6CPJy1u1Z2SWEWQ0Tae5Atld1YfGS3E2/miLtYhqu0jERKR  
yqX5ZDvjLAggyqZSMTOPUYkT0wpJ2uzt2dw64bVZG5+Gv21PUT25ysvNGxFd5Ps8  
hjTv12NR52GCWQJgEikBXZIne1IZoJt8Tiu3/6wLJyLMqJ6PSluL4SG4LqbnQZea  
jhLE9XoxlL/hLIu2fLUIfcQD0pNJ5Nu7fMTajJ44ebK5fj/yb5RlGjjxdJ2G476  
uJjWcyI0aEIqjmRKKak93dx2QkrC+LX4gvhaX1kDH+pkwWY9MIzn1m1RlgFRs/t5  
ABvs490P8Xut1ZPzFiCKpsy78WEzm+kN2l9YdK3hjbQUPaMwxsMV1U/0Bib0+Jo

qL0irRlv9xrenpskqD7/E3suUvnKICa5jAjjn1q4Jcu7S0neVSPXMDivpJBQfEQo  
FuKwCwhtoXnPjj+XRVcClpS3yj6tfaMY0i80ukhfkKrTgBl5dhVI36o+WFo3MDLV  
uvs6yEVYvA81Jy4lgkZIBa7HjUhmQdUzK7NQYxAQxEaw1oNaqxvRpYcxIRsUYDIg  
dIvVN0u0+jxkgP6XrSSRgjfbssHg8/peAJkj3IbXyqiQqDVF7kUftGSLDuIgUqg  
ax5yZ6IJFcj+Mwt5cY01u4f9dVmSNEKLFybnPo9C0r4cbosE+tNowrvkU9r8Kvwb  
U98jjqbJ0c7BIRGLJXSPzT4pSlMpAIOVfoewINLv9QJlYiksE2AixHmCxtUaYvS5  
EAgirV5juATgnay5T/V58u3RnNcLvfs2oPwZKGHTZnDEE2PRgHi7Q+HLCG+0hrVB  
wSZb9f9dSpwsRWJV+52dX9RCTX9kolBjtiWonlEb3CL6uchJ/FcrJj6IDdT4+zof  
V5C7ers60j6A6vom0hpdMCPH24fBPDjN+SuJH61bETMoDuSUjRREmj9gMB2oITjE  
bEAiLuAp6zN8kljmFKkgMwvFINFphjvFxqVbj8GW/zvJGHnVo+V6Ap3Wjm7kImd  
6oXc1i/gyeT9IF5dMpgbImuTDgQJ2hYlMaSjiEv6FIcj2I2N8BKKbHvohNt5KQK  
6qsvWVK4pTwxJFQ0nVPXPy2RoeUgqKj918Kqu4cm5WMMhx9pkc+OI6KINmJAsfq  
nrAqoNDAq/usWsJFjv27wGeFu90N5z51NxyKlyyp3sG52x5qmDpwjAQ027LWhf5m  
bKw/qnixtYUTv7JaxI55RtjRvXbDH9UGIfUf0jiMmvkDURgidBoSPDnZnVRQJvFE  
ja/fxIYbKoFBRxAqtKQJeVqPXS3MgcJCP4ovqFvWey+BBaC2BlNlLvF2cH01EvLr  
byLfkj0Fr/bHQeJPKc6UsU/TWmTMbzyQXexPuWdg9eI0x2jtfY5KrWuMoUCCEQCZ  
cXD63ccYJ9ZSxopF0u9jbPs6eWKKX4qLMNIU9akMT2ePxCtIdHECTaIQJhIu0tPn6  
KmrwWC610WgIWswPSKczXqjGhx39uNZAiejMDXWjzMRJcp+1nxgXQi+ZgTw2Jpk  
1bQnHtoBV9uAmx+tx2ipjYNB2uj3A1FxsQBS6/oGgA6pSy7ANVTvLKdiccoA2Evr  
EvjH6tYS0k1vLudyspDAGLYI6ANcYWGfFKqKWHU5gC0RbAs5dTqzywXhKU2ej5HA  
23eS8fLB2+eVVw0beG0XHmtZuHLA3YiIksKdRajA4DxvSA9ehPS125ZQKgZP3sT  
DeglmnmkGSGJDG6z/HPx/Ksdhsq86+n5YfyLtX93pfvht006/AW8cY60o42jqxBH  
GX0/1wc4YwBNZl8Y50YhdLRQc1H5wgwEpYi7enoeM88NqoEE45SrpYiv5GgC0IFp  
+SYuMM66Cd0pJCVSsr9H9+Bzsbwqcwy9NiWvmnoz250dvRh24qCLLza0J6Fu1zkv  
YnEOGsnCwKXWuCMooIkMJVBHTUueYyHsgEWH71TSGlNmGQihQUk7xrb1cLP9oCD8  
eLQ6srr4QVMZl4/c+s2gEsyw5+LyQR/jj0s3fqWJlW1bT+7y0qTNk0T0b7RKdezW  
8dpeK/T1z6GE2rchN0i560DDlNzVLiSEwz7II2jPf60q/ePZDfew4xrFR0tnUXmh  
5GZ4l9W+LJGIIx+aBJT3ChrDdPutqrj5fu54YV/lPMGlnzwv2KQ5Kg+MgUu23Q9g  
1kvG6Vr3AAVF5jhtDyEvrgCjIc2HfzP3uGATtC/dQHtd0/WH1BIeVXUA97c0mc8g  
z0hLEk0Yncx53a0InjzWmkqqR5R1pVWzBU6m2q3ri/O/dzqbnXP6DB+g+F9Twsz4  
6rQEECLUlbRMD+LS9Z0mF0t5csjTuJ9Ahvez0FGSkdQ7MLnm8vPXLVV1qtptu/sWa  
psrMioJRRcWlqgr/UYqo7132A/8qsN7HWPQRQaq89ZdAemRqh36ZnJEdTp02Gx7z  
VtW8XPHLS37/fzSW9U9A4hr9PuQ9Agv6Ssf9M0dvWkqiF2kvUtdq9PQ+b6J0zCb  
UrTp+qgtq1MPm3fcWcmQzYdHi6BUTrSzEbE/L4m+qEUh72R8aHLWRfTCV5QHAvPP  
+A4+aK9uexuMKS27pAObCp+WZJfvlbMxtTifm+i7NQvC1Wigfq00xndraqLyK3PS  
ypHc/5+SuJngeAiU2ixyKmnVFCmq3FYDUGseuN960E/LvZY4dFfrzLmApKJJUwV5  
/LBx4QpP+fffbLSCgT6xLB+kYwdwNt4wc9Qv55CB9uyrb+PFemT7RGacX/mz7z1e  
ANTY9UucLc5pTanL0eVDdcnwqG1C6UIC8LcPyM20V6EfcvUGe9GUDDLQuPHx9m9X  
F3qH0Aj8Pc3ZAGpIM4RvTxZm3uq/Oef7FBZ0ovEI940bBB/R+ntUSa5yWyzI16Xy  
IZthd5pzDmnA1tY9rintqxpRTBWmAfbjThvKprDzLHX0hI9cMrY25CH83AB0dVKG  
cJjAsDe0nJ46H+ArkbGSrXNJ2f+l+P8ifbPAmH7ZBb+LaQMuS3ZICqU4DxnZc2mG  
u3606GTTFFYiic0yagxpBhjTPWkbG8wkGiu05x0iWkbdx5AkSJ4imq1IiPs1l9Co0  
MVWLXJ+yb/xZ9Zja9FhYlIDZJ7SL4s0p8JbFBjM4z0wI8ZtTXMLL3wS+L2hJ12zq  
kyhUWoWZM1DBBWjsoeu3ToGuZ2Wd42qNVH83FqG3wkS7Fz0g3i0FZlylnl2+jRm  
OpjP46Noe6VoJf7+8ZNJaAa+V35TLXbjV8XRsjJItNBxu7SOH0YaKv5XNY0E4LbB  
XugpKtvOWQWDF6WqS9F00dUdS5+OGhR9HSNXnou66kGm+XVC53NezxFI1D0/SDy+  
Mu8nPRJEK6j/pic/sfMVjXc1dlr+C7r4IafRi+xg/j5ChiEFQaYTuz0zWW078fr4  
i9a0EzBISwZLlnQj042RHfyBt+VE484P/c2lemFXIxStMXhC/ySoOMYw3h0LUSv+  
L/a98cYn5JpQMqFbNwV9bz8pH1L1VrA+zhHKGTS3yLSjez6yR/6wyakzeHdsEZbR  
OVl7VMXdQjU2HkpjxRVs9Qax0e6s2QXLr6u5AhSR/ABrjWPs5r/4hfJoqoyxHCPV  
inWAL7cF3sHhMBB5hwivBZH9CFXYxAA6fvbGmfEz9pn6IO7CtiRtqzNbCzsBN3oQ  
Rjq0aLM+SZLEZGhe0RactLnRhXWz80JcVK9ANvVvah0x6q4PISHdQALHCiimbNE  
sHtxeGBfcfAk6q3ETM0nYX+iDcMSm9eFCwxI+wImjh5Tsr0yUnfyDPWIZkj6Jb1A

g7WY2+/AtXRJNYFTKK3cvB9feUQTlA+O/dnSBgvckB2Xltyw68AyIw1vB7vVhHWS  
CxBnGkoBieYzyXofZ560E05Kd0ig0/MscAShRwFS2XtzlX9YLZWvIhr1/W9wk4z9  
BKZkF/FplcwygtQ09t34pkez/SQh0wsLcBM87NjnpB20sZMLhBKAaLM8XIJFcEe  
328olwA9EhAAJTkt0jnuzEy5TT4JmAiJ6LZG1IG+IimsVrJXdxFx6h16Wqx4hjQk  
vf7L8rYfG7cQYsXImI6LjRh0odnxtW2z4crWLCsb30CERGo+LfKwF8RNRLGuyB  
fzBNUPeRFZVuG935L7DwoxM02Fw/tb8IluZ1at8UInSfY9DMzJm6XnkSB0ifLxDx  
F8QkLq/c0Xxpkzm5mJSDTB0DJw0TugF8XqVdX9DdbFKl/De1JuJk9CsFzbpyvH4o  
Jloh6T5qNp7P7cA90MZbqa0+0vt3sjFK3R0Wlk0GBoY9RhhGCmtug1EA8T958oVQ  
2Vaoz+a0+mCjGZ5TMkhU6T1nd/nTygbntjmGzrkj7JluMbqu9ZD1fAX80hiPmpon  
qQxdzuD4asYS1J+NElKcJ/P4w2W8jAtWPm2I1nQmB6AbY1AuNAq2s3a/9B45/Lcy  
JIq/FCFP2I07vML2CcEQUtxULfIz97N7b1zpz+xjkkWv9VYYeKtiX/gFpAjpgnp  
eI6vrOSPfD4IEyn460fuJxYYixFfE3AqF/4DwcxUJghNzWVcfGdcyHQ0wwwce6K6  
gvc7MF5HBLv6NAvgG0DAwXRqK43ZFBscF/DG6fUqVozehAgcesEnjDgxIEjctLH  
GfKM7ljbteIjCSKl058GndQ4vIAw4mTny/Am1b5T8wXyzAh/T6zZup0goz73MeON  
G245da2d9KCZ9AaNE6A479YdY3q3dmPK2XM1mPbb9qgF2fqPmJJvCT/LPydkh/uTY  
vvp2l123atJcR43mvf12u1jS9/lztMPXM06u3NdAyan+St3+p7E30deLECr0s4m5  
wfNu5r/HmIgj8EYWyZwV3G926Uenk5wQdNKI6FEc35Qx8kQ+M1j0hvLBEIvFknkb  
NTG8EMN64oaQ00DU6yQ4uX1EPXXb/fXiCJfiyPSC0qIew22wUEmIMljCfBQ1IKbzB  
tBmXTt66wA7+0f2uVtZB0ls5VhPlFV0+OquwLZ20nVvQf06Nw9MLAHpHWA6SSu1V  
pg7/FT7ah4IOf+9WECotaoAR5ISEmZBfiTij6I3zmsz5d1zXkvBYfqYoLwY4Qum  
qaP8AH15zqMhG0cbv/VqI7kFx/UJHhEYgJtZ/2RPm050oqDFqT++H32nptjbjbfa3  
HEzf7yLi9G34iLD9AZY4dPFED6neBuonI2MftGV581cPbRh5BxNZcnUuv0qMEzg  
OuocwvJZyqjUsZhzt+yBIpkmuRRlwjiJnmnpKQ2HAtuInnNaQjDXpEe2UkQqGcsF  
HYhPQvs3Bj23KJCIOERVE+MLEK6VRVr88pWCNFH6pXT40gw2KIYdDqbi+AcVhWBZ  
YrecEEZP5DmJdHKVxQ4jB2ohLGAe6hV3rF735u+Z+4mxI4BT55L0VjGBzxn/zPmf  
9Sn1MnRYZZZqlgKRYb2ZsQBtd8ZCCi500asW8cqpVU/KmSeXZ008PUjLBxNEcPrr  
PXRb0zHaBq6/jbqpkun8Q/gazM9euNtEzfp5fY22AxmqFSqa2wv8aquYFX04aIY8  
hLsbw/G2iZFlakZRzt+hRiDdGKo0yrmAiKgQH7I6yq9lqbYKRdTNLx/JBkrdEmw  
dsUZxVNNIEsTrsLM6xNFWqpFdpWewEjz9vIliTwN3zRwClqItovhJlxbvVcHtqd  
hKq9ay0YoGBCgWNIjex2NE8srktmTQAMrirr0EHlg/hlWsZk2uYHfFohDRlYkMQg  
01UM6XAij/fbzeBBXahJdKd2mrCOyk/F7Roh6ifxf20gTxmS0+HWLku4KThEvGX0  
3n4bnxC1dBbIm8u0o5tH4oYvDJyQ08a4q/H3Z+LCfWlRtNLdBztZCbHkWdn3ic0f  
c5Ub+ODT7tyoYNMQUuXBizSM/DRH5bzHpTtLRtmuUOCg1U0TtrKbTJV0LZ3MhfsQ  
EhQI82f5u1fF5JbeqmhtbI1QK/5NCCTWskJc+QDUvY8wPEyLDsS5ptuKDxqNp0Ms  
Te9riT4gjMC3gxIxMhDN/FNXpBks5hyLtIAi/H0bCepZrcrf65Nezw7r8oVD45gz  
7GChSF+dFkqRL/7ormCCySDisj5SxylJGGIrTqesG8QmXhZNR0BCpCyk5MuZVCQw  
YhMHWBccZB09aD0Af/SaUZ+KkouoLWlv9IED5FjSWK3S1qVrQ8Bpaw4X0aN2TnFG  
wwskl0RtnagUeJGx1n4rbZbZzlsTN8+NVxZjqKP21RkoX7e2vW6yMrbULDRIX3ZR  
thHSS31gRNxozhxKg6NTTwxZQotdy0Ckt2wkvcalkQ50ZPaj5bpLWBPazGzP3hMb  
Vou2nYo1FTXWVx+kf3t26edITEg17is7ZdbaD0hGL246LY40iIAHOJtdbyACsoa0  
IgLUqaVNElyoJ6Ix40ls+UxeBmCEKFJcskEQv/KZ9YNaFq24nv9Tw1mTNEfONFQi  
laqaqKckLmEB8Wa8C3WuHG19Nc1VnA29HMPRGjDo9W3fTI/D5wvh+iZaxqZKpq0V  
VtMX3YqjbYUSUJ7ASLD5aNX0ZzPdjhY83lj8qtR20GF5gSAnx95uxSgzUR2tUFsv  
9Xrh3w0drePMk2tr5BrAP75iUFJXt8eaeYH5P+JeXzm6sH2WzQbbKu58kC8PHJ04  
4Cw1fmgNP10HcnrBrDeOCwBELKwL4CwQ1S6SU2pzUtT+J2MrX1+rAw6as7fnz2MO  
TAjNhsF6yjGjU9+/a6GrPHir/dkS8IFBVR0ixa0dnXPkCyrG5WdA5GRYQ14FHYn3  
YHP2BWF49+kEJPQbh4yh0tdiNJ5DWJ5tdzYRGg+hS/Y7hIwv2l944zwnPT2hExOB  
pmfL6mAkeCBu3CiLD/0UBc0ABxeWmCEc7yTijrqXC2bDEqPPcNf6gWcR2f860mRu  
uE7AeXt3UgB4xqsNfmp6RcM4pQARDo8S/RJzykToodLqdJtLKKMovMoQuzBLFWkh  
iJmwESUAFtFB0s8EKtakTmZVFifs9+d5JanfEv0tIXZLv5WTCVDBECOS22pJMG13  
OoTzi+ehg6ChVjRUEQZOn8Y2Z2NIDAF8xQAiePJR2hqeQaNv9xIVkp3ICeyBaILXn  
rzaW/LeN4yFCF5UTJSHrFfPRtaGvFePtpeIDtxTQopXy940FIERN3Udv1wf/Hhfy  
Kflni75cmOVQfnwoXARbnleNkZRUnuyeJ6c0w7NSibTxfUxXGS3MMtEa0D0ht4Vb



gTsx0L5QecZRF8qEC08VHGtnxfZEnof1nSsBimUKLkxUxWoQmnHsLw3FuWqCetF  
ks1LAKYp+Pa2aVE4vHsvGSoLVuxlQyyBcZC6t1a4Nf/BPPaNHFSJ6z0Trwj3V03f  
vJ2AK4muv95XghnDyy4qsa6ogiXbdBntA91utPCW7PGeLKpT08tVFA255RKX07wZ  
Z3Wx3vZ/CkA8ttsW0fPaBs91wuiexYHhamxIJbigqHaJZ0n8hcjeISkMYqCfUbaZ  
hYUERl9LlIe3UDS505BvWJ71F1NGQmvLC9qfAoa4pUBDDpRB4j2/Sc38sSTamZfZ  
nSuHs1W9v9Qypzndpv0Bgwqax9GeGLcBvsZEw2svScLwqj6vQbgUZMPAinzn01yw  
CQc9V3ruXbH2NfMVL1gj9doUR7mQc0Q532f9wJTOYFjY7raIdbBUknajRvin1roZ  
AMsAIPbpJ2jo1bREJbeOKUnzdGSzBEn87rZ7QWdVGsw96aUbVpQjTLYBOKD9l2OK  
p1Bq9NPEXUcK3Y4jzxzBgcMKewu8BTtLEtc07LcSuwnmt/AQvtrYbmeSPvtzW0qT  
FiSlVeG6Yft2E57BYwRA4knJQNU7wryyC1/MqPCn0ybZDpIi3m55jMrESi7BiSm  
ojrCPvy0hne2iQw/yhLFVGHrYpJS9Vgu7CwTeNi8XZJQ/GvnphhcwGCAo9BVpNLI  
EBP+JrFJ1b8cBbBMwC3x9vBDjipQd4q3z8qXJ6rJBzxKRsZwCBEiv30q63piSyJl  
lJBlWwbXcrrABFwG/Jd05p3Vb9/ZTzhIfIPqUtRdn75VjafGSAoS2+ryS5W74tu/  
C7PZzQJESNPm52pac8uvuD/RIGxPTEkAepCCbt2Pw11tiApuXvVg+L79b6hvvXMn  
YlqBYn9k/Bghw/Y1lSkBmbKkor50V2eKdfqJoCpPwBhEkpkznipqxV9y7Z3iezQn  
UVpdGxorpM0pwoC6w5VgbTFeGvU7XwgNPUAfu6tpr5fmm/a0pl/rGxSpzZiLf++F  
1q3elUwLTruMwCo7G13/YbtzErEiZ002ii163XF6akG51fdBMNqjMALVHdmx40Wt  
6VnZ9UXdFgZHHwN3PPVGuJDphSmBI2ciHL39uDW5AczPLP1uUFbHt8bR0TLJuSD  
z1+TP6URxJLFLAQCY0JwZob/Tc8CU2tPcptT/mT4Y/Ebc6Md/rjz6R/mCV3r5pb6  
XHY3x0wae1hvISQLaEKA+eivetwzL4LvVqQ3oxGi0sYYNsZZ7INC6kUAJqTzfNCT  
HGC0Yui/KLV5S4CegSPgw9yIp5WxXgwxU7kFyPu86LKjc3c1zUd8DM25+zS6B/63  
69scBKfOfZwM7Fq8JPM64psQtghgqRP0pPs7ym0Pjlf+9oaXvN4+hYtraCtIpeGN  
J25hxINC9y7D2Uivp7s3jCY3ykJZ5VAbvEPzLVw041upT25z4yMhTD3g/TGMKwXf  
vEsxVEIKGY/dVGEoJ00ndaqV0Y08Nk3oUurmSLFQlUSfk6t18zqL+Yt1YzEhEb1p  
TmeKBvNf7mSwb5AZn2/ZAVA4pKoj3B19Lwh6giidSAZvv42a2jbgI+t2cx2PrFVX  
3r+46G5BEtTHjrfsUWJRuf8ggLZMNzEQPAsLxpCvQ1YowS7VhPHMrg+rw4w+Mp8Y  
7HzR+P2HLv+uT2SX4InH5VDzZCe1ssz7bbrdPKR33wknzJ4weBagpf4JAv+JCwiD  
/JmJp9uWzebKzZn9GVHuzKvNA64bcAyTrM0ZJr537mPGN89/3NsRKDTDa10hdC+X  
2A8sbk8V1Qfs54qsVSzkmX8XlTaZ0wEQKWFPxXhPcqE5Z4d3n+i8fL/BzPyPLD7a  
vR0utzS4M7J/ozWMgQGo+KrYtYNR5gy9kXUsYaEN6mByjUqVct6vwaVS+cfvlz4C  
rrZzKut3uaWuNxxJ/7LVT3UsDTgNSjhegtq0jAiAFiNdXFhHJ8BGMNDVCvdbE6g0  
gHwgReWYjBrk/kCUmtPP0iJmCGetWUwsNzlsqsm/TjgoKApuhFX86qkB401Np319  
tQtsJuzOPSUFV4KcG1QPEAsVmHQKfCY90R5qEKst12owNmcVDMNT01RckX/86Reg  
PXSfUCd8JfXxPEVXAAXsUSUCFZdxE6BWR8w4RrvC4U/y8rDv2l/www/pmPYmxC4mE  
BA1rXQWdglEzcxpCEaZzVqsBw14SSmjFQABYgBApD09unQnfxUBmu3+EvM4d7n  
n6a8Luo0IjsV7wn9fU8OUqDoig/sJlty+oGSK0IgkA3Rgd/Cnc0PeCS0+VkJZdjPM  
FGuJYzKZNCtG7TdltPeFw10Q70yt/qLJK1jGgHlZgIKY0Ca0YFPTdbCItwNi/ot  
RfrRciviCusfIRGdX7T3uPgC/uQLNV4Ep3IDBerqfiudx2bMDhSZ7EuQJdGdsZ6B  
xRrWg/JnHh3fYah1Rnw/iuQ2J/KQ6Q3uiQn2ExF/ORw5UsHUsu6buVY7Q2zXX/X6  
4A5RfPy8F1MyhFX/U3hklDennxECiBIM6ZjoFjb0M00a5Yx0aZtrb0ULGW3ApfTH  
HPJT1T5bD52BujtZHsHbmT+hKFu02omYfMLWsA1GFRNndipkaE6fUZdPZCSMTHUQ  
ZjGSJBhPL4Lz+hCJ0dAC2adbPk4A4JYX3ZT6QKEL97yZb7NU+zQeW551xtLQt6T3  
WQaN9zZ52343wzBFSplJIE495e16/U18YVMFJWTCv9ew6zdTDk7RaTq/EC+s0vhU  
06qe6lGagvExvot3NDzj3P/Xn7eUokAHhmPiHM0FwdQFoS/13k/FNpeS+jQLoC0R  
+njhMMrb5VCn+BWykm/TCDl5ojmFrLPlbhc/kt0TkPZz6wzqTY/YFP22heyw0u9J  
j0C9dQJ99H7XXs7jcosjJJtMV0IJog0+Q30LA2cfBxyI/htC5eEErJXbLgrMUA5U  
KI/UNOU0xh6bagnX/aTdPHDAS487CLj61IgMKj0qQXlBecVxZIRDD/XUqt9+eLG2  
MZdcW3lengBFs7oJGRWlMyALsHXzkDZmDxYx52nQQbrJZS8S2a74ffxUwIv40u1W  
l3d06FxlWB3A8mEh1WZVP+NdL/zMIVWpdJIS5BL0vuuVScYNXDfU4wgQH0jmtgq  
kr6ZXdxkVNQ7tydnsciVW0lsyAWg36S8guBqkYfGv7AdI7wg6hoUiDaxhNicAJqY  
UXtF1CbNuZRHV4aExHfVK9TXmNG1/sYvDaf+uWqEUBZVFfy5y9lByLZ7F/otfyQL  
TEIMcu0t2wgCgWw4eQQZ7tiuchLIi7bTJBumfhiFhbny8cEjTQnfs9G4i36pfQVj  
gy+d442giQRvh6HIDB0AyZZCC7gD+7xiw0TQ4afYrIILvDo6PIklQkdqeoibsgWA

```
6L+ga9Xc8Iwcf7Y6aWUAW0pWgdVCt20si0cGJPxto0jZbmhBM0SFTK1Qs7qyDiJE
fB53KTIVGgc0FuQJ1kqkXB0vcLm2cEGFhcbvHQkgKJfjXrimAccJc5GuSct/rAlp
mD7iLDHc1a0unLVM2vGYmXNBKv+m6aIs2yZGmaIetOWRvN04ZnJsF7t0XVXv1LMd
EUB5JFsoumg90cqVHOQgbcRM4MJr/sA6yjFySg/TzqWZ0R+Jjo5WqA61lwJjZ5zK
9ZhQRjy/w6ptWByridB6Rsazqbz9ea/kLQIzoHtIrY26lCszPCgnpawKqPKP0zVk
qZQ+mRfY02KsTivth9oQKLMCybh0fFOU0x7xPTDKW+5ML+kxbj30+84dzobInPFx
pL/TySGfFHxv3SQ9F1FFLnEfZf0wjfPD4yH4VSA//a7JUq49Nb3pxewc4hcrQbDx
b2+0VTr+gzxs/k0r4D9MFdeApaGsBMYN/z+mm5NG2pFjMn9uIS+b+/c07Y602r8C
TyD76D0nC1VGyB2ea0T6G+989PjEahgsYd1fpuBwZCJ7y+hx2+RHqcCUEnbjUC5/
WD4hzzEC6iId5N2WXYJbSgZzeYDPXMwVsKjjDbHraNeZYofzoAHoLuNFLw7wbLg1
5EMJNPBpe/OHBYLUNuPYM5XIQK42xPS5FlizykTarLWvsqS9j5L5QkK6rh6ft2Rb
C20kxUoSwo10qktKbwxoLJAeZVAgYe+BLkKzq20BLxZAF0NJAak0H/pwIKZKFALn
TGWWD1vFoVN+3KAlV7sAo1VgxJaste4dRrax7DlvJTnmqcART2fMbrWhYPz1IMfd
7wwNgoeQ9iAMx8Bz4BpNldJyXlMGYkMjdSPFJZ78QDZ9FIQKUw7svyF6wnk/cIWL
IwUzrHCp0LJrfoBK0N4oybjcn6tBXcScvimbhvGMKqQrG2yDQKAqdJiLuAajZI81
y3eu16TxcLszFp/nkSkPXBQ8bAv6DzIDbV2bYVM7dGFz4sa5LwLJo0MiDF3GtfW
Yzj2eIeP6PDDcE54wRdkP0lnU8fo2NDEym03b0TUPVeaIG+fEy9XHhbwI1hirtqr
bPQBJ8txb2Rg4UjoBDLvcPaNHytPbH20a/HLdyofD6eB6qnTmSHyQaeKIOlk+lwq
alw/mURGHazQXHby9343AcBqQfxmdXbnZGTtl13Qh2a1sVTgvW1LmBCKUS3dnZB
r0kaY20JSMw87fU2r78hwdtgJI954wv6vNybjdYn53xPAAjyXxtnVtIDrh2b9fjk
Fll1u6SFgf+8/DKvtlwcx2hWkbbJ5qc0U6STYXko38Bp8DpuygTZ2011Ld+5+tjYt
QTWdUaP0FmiBpkI7f5U3xy0R5EwAbFftuBImfq5qTjEwgAm3Q//vMQ8JVLk/jtf
5PAGaVf+/hcGew0yItbilmI3sdd6o6hT+mjqnJtAdLxIJ2iFCLY0yM4M/ssaRCY
b2K9DTxfsoxEjh7tR6KEs3ZDPQ/rJqIwd9pWgVgriBAB87SV80rYrLn3TYQ0Mc8u
17F8ZQ69icKc+9EnBEz6RpsfrC6Kgw9ljIRc0a8nIDCsQsqCp8R0xmwpga6N2Ak
ChFG+Z4GwHq6NA2AqyPGKzYi+YSgXNnDvGJyQKEQF4pHVl91liVrz/NssYbSTPL/
YlWlojyOXVSowDz6yakwALV1T7NHumfSTU7GcGYyXtFiNIXDxgBnF5jz1TeSisL4
q9sxSVQdlCwME+dJMYfze0jvTYEsuZTffq7v15uLTUGsL8s1BhFbkVo/q4MN8mwy
woVIDvTt3AYDJ0ijt40ST/wl5+ulXh7hZJJJs0DedgKhRejqZ0KiCgxBS+CIzRVsF
pvZt0KUNceZTUGC7HLGWekNhx/VrbYlqGGCZjDk7dH/waDaNb7RhNeMZDdM8gBPD
6VGOpND01A9so+5hjyeB0hEkF0+RIFgxXaYn7wU=
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the SPHINCS+-SHA2-192f-simple post-quantum algorithm

Use the following public key to test the SPHINCS+-SHA2-192f-simple post-quantum algorithm.

```
-----BEGIN PUBLIC KEY-----
MD0wCAYGK84PBgUKAZeA3C9QKtQNnTZRINo1ueM9SpptZbq/8Y839YR/JhjnSxFV
Om1HhN8ZZC5rfPhvYA/k
-----END PUBLIC KEY-----
```

## Sample private key to test the SPHINCS+-SHA2-192f-simple post-quantum algorithm

Use the following private key to test the SPHINCS+-SHA2-192f-simple post-quantum algorithm.

```
-----BEGIN PRIVATE KEY-----
MIGjAgEAMAgBivODwYFCgSBkwSBkA5u7nnDNrqioeDXfJzLEf88oIaM6XuHhPoT
SBCuL50WmNkYguFhh4pvxP0PKFbH59wvUCrUDZ02USDaNBnjPUqabWW6v/GPN/WE
```

```
fyYY50sRVTptRxzfGWQua3zx72AP5NwvUCrUDZ02USDaNbnjPUqabWW6v/GPN/WE
fyYY50sRVTptRxzfGWQua3zx72AP5A==
-----END PRIVATE KEY-----
```

## SPHINCS+-SHA2-192s-simple (1.3.9999.6.5.12)

Use the following CSR and keys to test the SPHINCS+-SHA2-256f-simple post-quantum algorithm with the 1.3.9999.6.5.12 object identifier (OID).

- [Sample CSR to test the SPHINCS+-SHA2-256f-simple post-quantum algorithm](#)
- [Sample public key to test the SPHINCS+-SHA2-256f-simple post-quantum algorithm](#)
- [Sample private key to test the SPHINCS+-SHA2-256f-simple post-quantum algorithm](#)

## Sample CSR to test the SPHINCS+-SHA2-256f-simple post-quantum algorithm

Use the following CSR to test the SPHINCS+-SHA2-256f-simple post-quantum algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIJACTCBlwIBADBRMAwDgYDVQQKEwFbnRydXN0MQ8wDQYDVQQLEwZQS0lIdWIX
LDAqBgNVBAMTI1NQSElOQ1NQbHVzLVNIQTItMTkycy1zaW1wbGUgU2FtcGxlMD0w
CAYGK84PBgUMAZEA5M7gViQs5zFAommoRgv00d6C0g1dJYIycRl3UND7SWMi fydo
knPaAj6VT9/kYwuPoAAwCAYGK84PBgUMA4I/YQBXEfp/euxg0msmfCiXbnweOC0p
fSGTCYHajyt3VGWmpFott60P3fv8Q4B6UYBxiHfD5IJVdhkiKEA5CMNK1E1/Gueg
+HbAEdxIB86wU7eDNgxPIdaDmTkzwnyks28rTYdwVyEiY9257AphDy7AM1Je59ge
HGzXKonP1Hqhzf6I+rzv7Sy06qvg2N6FvLD7KaKgu+FpbZufki+fMJWSdg1LQq07
cxGhr7NUQU1YEjtVomGwOI/3otdjnpLQDX+s+99Z7ajgADgE4BhpZlj3BZz0Ln2/
AFy6Vp/7sk1EpFctMxVAiM3so9nfeVUvGptuAWzdH7MQHaiu6PDY2lkqchmc/yCy
xFdFjNH0+0fgENGTVFM6hBan0vytZ5pDwpFIX4xbtk8pi7Pxi++fn/PaNFZHoRRZ
OQmX62cqe0yqBgC0VcdEcK4rQRED+5KrsbGVmv15fDqDRfdirIlzkZld6WcwokAM
Swn44Z4KnAxsYHahSHznQWqixjhjqP527oYMjycxrdpGV0vQY7+fogiQtS0p9/I
pno0oLzMTymBk3R0fsZauCxdyPfbyyz+aJM9XnMG5i/cfuLuGZBD3w52zc9bxddp
aJbJDuPqGs60/aZCdKwGUC/GACMrSGO6oaLqpYSU8bLRn/3NsHlu2tRUlj8u3QI
pdt+CSQB9QEfzgbNQHxxuHQaYjL7g15vsBWCuFrY0yrEjANXB3B170fZc6PM82A5
Z+ARkiF/+h9sBh3RnQrtQk2loSjv5a/+t57HfcoWhyQQzi5KDtqVU+BhuIzVWD1U
JVESniPXtPRpuSIaDM132f2LI0j0fyskwKI3gx0CmjQMg4KsvT7oYb+om4GjDZzc
bDB1waXbEshNGENMaHVi12XUVNDdFunFawFNFUaZ0fuKVU9fLJddRHRcQdZqIoYI
YXu8K11yGjX6gnegcEe4XDlr9VbtPwECOSvz1ahmG9YKSUTA1pml3tf1M4QfGhln
x5GZWPkMJABnmxmSVsFR7T77IqRGcOBUTuDMVZDRxwNzcsNJo1aNT40wyCuON3M2
RSt0qHV+UV/c3MF1w5IMjZ0Dc2ZWJoEPBkEh41oGNS7w7arx601KpIq9d05J4aXi
WYALFJi2Nsmc4sYWD+bbijcHpgY8tJh3yKALYubYtnQRILMM5i+qFloBHXfAEq4I
fNaXnZZLE+A/Dy0VEspkqC7RhMXALwdbRsyh6ovT+j4o0ao2BXowSwQIrx1eBuZR
fvSF7WkRzVs67VNCy8XrilGvvLcf/j0Tyy0zi06H7nNSrBRNknaXzLKUJz0l74fV
1DOMYYDoWL6AZ0athE1r5IlSo2T42ACWEEVvBA+gbuDmJIah2MIJddMwofm8pBRe
T8ep0ggd/06A2zh1sHY0KUpLRlJ1VMoo0iIFcblduY0qCwQyui0T8NGjzQBSJJ7W
RabUMs4a0hCwASrmviJ7hDaR6FEWx+cvi2g3ig4kpku4X5Qotn/iEDZ6BJht+BKh
MnqoWiopkUqBGoAYSa2f2JrQzNQD4pVAPaDJ4SM4SbjDMHsU0dcWo24n0XqRoBug
Ev7h9Q8tccpgjJTqtksLvY8lYyThEh864+yuY0LnuGid+M1NblsELGIzH11B+BpW0
jKsYReKUFwG6MgNKpK2b1I34rJvRkuSznNkwLRS2Gbnnc2LWGqS4nPyFxtvnt+E
Gp8bJfBLs2cWxexCX540PeX2DQHuoEevqVF4eK5LxKy7uZX3wrjPz57xN5RH+Ko
mSdXL7UTB+h49RyW0d/Piey09TCSx71Ix9AvKhGkv1Ur12caQZb0vAQevujCw3Y6
gL9wLMCzhB0hkxmTge21RQMn0a/6T+tewQwv0SiNmawaB4rnT8nY4BZubGa+eOR0
```

hNU+F3uTmsdpeVvQFDQ/fqpL0Ji4qBmYszAmN+HPRvHHRB03JC8l6jh3LbF/ozTb  
SxTmkIF37VVTbtJHvmpqSpBwwMOYAy+nZrOYgpyVF09RyvWS1d4He7IKJ5MMBz7C  
BMVVvHISTyizeJVX/5daFddjEiJFS1bF54Ybm/mlFpD5YkkacwEexgCMCb1mnTo/  
DjSCp+zWUDxabBcUNXai3UWnHrUUZl+SuL/ztMM2Sfdx5NST42IpkvMi4efFvBGC  
c33KHLCKJuuNC7vHkVJLg/eRjh+8kvTJAc7oeL/HhPHXHGWUY1gHgAUYSBJZqUX3  
067UTtBowjsXAg3LSUxvFAcezygVAZZD69CRuPKBRYXWIsDXNdWG7EShX2WrwmcY  
YsrglExexShYUQ6FLqa4XSXFMAn5JnzjRtWLC6D+EA2FUZjc5qPrA9vq/CykNP90  
/gFczf2st9qPrbkZa0Vb8MfDRRDosePHQL7cpjDQ2iYC3vDjsLqLSKIZmz4FogGk  
eXmp/vrAiewlcXI5/2q6hUXok8yB8oAnzB9377F7WhSMoeS0E4IEhTY5GFmM7W4G  
JeBbtB8fhBswWtsKxZGkbwGP1MEJ9WZdMUHRdagZ6TjVW/hVfLwj0OTfjZj0F09m  
qAenzSQWoYUn73xWMkgFOXDEeiCBGTxfb21KAu17CGJ0VMe50Vxv2D3mEhloU5GCz  
b1Zd888taLu36xQNHOMXFrA3rUmD6seAGjB7SmskXJX1CWWVTkjtHrtM30WW81qX  
wIagM8deGBXid+Zhy6s/YLqvufYgmo/NBT0PVT85ZSqI/nF9C2zggA1v0S1V6G931  
4k0SGWL90Ih0fCooRtVxSQ2rnUSZw95C0apGj+any+PUZy48ZUXOX2ftaXPYkUvk  
SCY1XzsFAftVYJwAtpnYZN7+pVSv1tMni95RfETmF/OAmqDERPz2cUJH6XLZXAJo  
6ScULXtQ+KoWpZQ1ZNfHU5BUSKdFJUVLQlQjoRjiMLE0FchupP45Nz5+nsmCx++1  
Spm9stJTRqNNKwLCXR4DwPIiRtP71E0AEACiIhSF2iIXXEk/GfSIYuS+Hrn15+/Y  
riEnnwj+AopxIOLeZEPXLlsANotMi5cDBt0ZoUfhMBER/gzIa1c20PvxQMRWQ4Ik  
sLnBY9f0v6401NQL7bdW9c3KS0b9PJ60cm+gd4SyGDnn+L07TFEFDVH2LcRbUmv  
NKmPBA6dteBmyEzjuCTJfH0KjLuLQCdfuql0OT5+JJVNYcfGUZV2ouBITT5jtgVJ  
QpW3KaV90LztzTKDy4GpC9Ay5iT2oa23hlFMHQ/Ybmx30CC/eZjR0hRyY7t7/Xt  
sdkAyU00sDa4Mrsgpe33IuipgjAD12kVqBvg1PUsFh2ZQoPFZZ5ga2n13g2C7RAJ  
9UYLPLgxuYg9mejPfnmqG3HphhttpFacLMUvgbjrIjKB5+Ho0vITPBQSoAiX/a1K+1  
IjjX06YbE9g8PkLkcVbX0+vjyICrOyzUhrI8mGg2zKHs1tsYMPUFzaAzTwB9/DEe  
L+sBGMWqUJ2a0z7bxrrrg6uA022b0aZjJQ7M8M0K8FuvqPsBV0XHI90Ry80PYRvhk  
jCEmh7GZFWsSiCuthIzocvneTKG7JnSWSR62Aa0FyCUHQ2/KlQqDDpG8yP1MqrUQ  
Xzt0tdFBSsSk3foFyBqBzeVyrPgaDztCIiwJzfcxS7/Uk5K7FtpMIVmD88P1KwyT  
I+Z10s/fy0nTwcqTQoEELS9pfPwMiY++HIFxDeN9+AsOrHR2kISXzacDHnfvoE+U  
/m2HXyevSGhjNCD5A6sw7E/mawnCnJx/iuhty7HVnAier4EJ9IpZbzBkAkRxAFHf  
g/8uUYxl+Kka4L7i3f6TPHricdbig7n6C1Vq5PirOZ9zC8ZXjZSusNz384utKeBJ  
NTNAoiaGRU3DBIPSoL9EW644AVjItMrZb3C91z1SVunkoGLVnsYGVx8bjScE6t+1  
YdyzWCTxjaIVVnEXh5FISQ0kDy3Cv5BRuZt10mXHCyPQN0m0o+t5gTHf3ocIa+b  
MGg0YWIF6mtYpXnRZRnHRUPUjmfCwWwgNn5nfxtdUKEghrBrtspxu6h43TIsyIWT  
Xd3CNRRVqcyay0LJPust4Jbody3z4ELniIL8S40aDYlZw20ak2njpyCVi3G3zPke  
YC8+NMx40025SV3eihYrVlSIwrWwNlHASbD+uiqddI8pNHqclb0Snfk9SeFtWFOU  
8JjLB0VdCdYvkkADnFB4tCKVJuPRbYXgtrXiFMJJXw9GJZioYhxx++Me9AX2ndJz  
mI2gVhpZaIq7wY3XIk6lBJTCTQbpXqbXhFkqi1gq1ccabMt5JLcoZjGewpN/C2yF  
wLXq7Gja8rxK12LUU+tvkNT8pTEEWgB2GAGLvCW0SGNNupbpX0CbztHzbZW04cti  
o6qsg6+XV5a1p/2Q27om1UC+WYXT2L+/tgynLw1KsNJ2k003FYM5HuyRTqIsPXfa  
e/CD8pbYtq3ZCS5QBZgzl46sYkIw5pAwMZpk3meYNJH1XnkC1L0iygiP40VMLH1a  
L0HRPL+hehVl5wMuy/xufmrUI2i6zEbfXQDAhCnNEXpFQJyZ9zH00sTv6Wlm2ywy  
L1rBm3rBznbskgTK4G0+zp54A2z4u1UKPUC8DZNCC2FNiPDY7gdDar195LHNPf7x  
IKis18WvEAM6d23Tp+ud3kPy1WikqfwdjWQvw69U5j0LgEFxXtgIUPbRk71mBasz  
l1btpGxU71UqarVKvUx3J/p1+atFXrt074gHDdydHer/zGQBtSbInYgEjL0PZBiZ  
Wa9TsS8Fmzsz986Fn0co67qzXbS7cFonJqbNdp3ilycV2MHySyjuZWh4XrLWxfNk  
K3JDaARxpPhuAwDjI3lhRC5SdS9BvAXom8rgbybhdGMn2Dumt06xdGZ6XBF5P4t  
Kxy4qmV/oYc0M9I+vflXDDR9tBbvtLsbCjwTw0rXGjusvbZ5DaM5FQsgjSaKZNkL  
Avte1Qo+ksT3QqE49mp1LwXIOHBGYA6vFO0YFrbrmr4GBICqh+2hLBm4/gMn5XuGa  
DoiWMN4ef2eF0MXoPF96fzm+kjUKA66LYI5eoxD7l2lhxv0BNo4fzp20djNuKPx9  
UmxJ7EwEakZm6gaep6PmvB2YPf0oSAZCi1EKn7LOyf/XgcGTWg1z+CVCuZ0NDpFO  
ZiJKS2VR8FdeoGoRwCc4s5Zs02f9wVZukteE+ZzyEaZe3Kdzehra1G5AEMjIPVnk  
lzVZb+xy0U0I6XiYyglTcRaYNvztA/Z9+o0MLlUrjIM+AL8GVCq2UlwBUskQZEEI  
F3jBPsyIDrUV1+J/pP3FpFP2yhmjaLAHCFvZaD2nhsxs1NVYGEY9jw328+wqKE5x



3XMkQ8KbnzyTXy8p+J9KU0dkHa0lGAXXNKN8qZJ3Tb2NuYbNEbfCUuP5sW80jMa8  
IqwKdBx+pMA5JUcW0fDssu2Xi/3QurTKaws04+T1VCuKD/8cf8c9LJb999zeS7gC  
VvruwkgVlc7w6Rd4nZd3U2XjQJB2tgXZkfCR32nXE4a+PINWpgRq94gXv4zjkPu9  
feDNgA3QWlqGXIZ914YbuH5bd87C+c6aQjy8yj5HjzT0cBuE4HzgVJ92+TEZ+2na  
fbXiDzbGwv5VKu5xk0SROWGLuEteLfDht6ocMmsSIZiLQehF6oxcwHRt7ZZGJpG0  
4DrXpi5NRVmRgN34SqBAbbeDEDPc1C6RSLxonUqt7Bexar1uqIs5lbBxplvb3mdJ  
P5KdgbYdnM3Km8KaK8pdHoZrttTnEq08XLRjmAPj+HZiL5uQFRu5FMeFL9D8LCo5  
pMNZCLH4C6FTq2/9pjXUOwsFbyKQ0kK6oR8WfPRRMYGWjDYbQGkF+7WxasEGe7jI  
KopJKAokzHrA09Q1QuvWSICvDqF8y8hMVOZHsOKcjCWmzvKYDAX0fKPGDwx2PqmA  
aaC4R0GRsAWH+5tPXzxirFsp5inz2JGD+L3P7WhM9QnT+PN2W9bJbFKi8f/ITHLL  
Df9Dk4Sh2Zdf6056x6A1adXbGGL0ABQjldLmKSpLdSbgzuJ3+4uwFsuVCuJeuzCY  
NYppAZjx5/bpo2+Xh/USpi4hTCNHDLeB20EsMwLeGGQ8vlfhFEJLUpwildadaF1  
7EzZ1M95EJswF3mrL6IDEuQ/Jxi9y22j4aYuWgRmUIFFNvCvU1fQgmbq0sZfhfLw  
uTPVatkVgNv8ziKyckD1mJbgGoEK4tk3mnpXLoEwoBpoxhbibQNGR7Gqtwj66Rke  
B7zgjYgFRgtH6SaolHdslddAg1ZD4jrAHLef222d5I+8eZcQ0rgoIg90EUcxNwr  
lwGKVvRd8za/FrmmSR5JJJaafJhU8ZCuLHWvKWQpCc0JECxjP7qza7Z0XBBq5An/k  
qw5EXSbFELdgP37xR7RVQKaMXbGUKhqDEWMIfxQQc1zE92K3AFJrx1lV6G5b569Y  
NB33Ns4yHbiv3h7zRLkLgjyGfswGwZ/L/11zdLJDP07DXie81jVC6VYs2CmbJnh0  
R1uRiytWYC301KjYTOuyER5SEysy9KXrg4//oNN2hIk80z2BFq2ldUtWDj7WFLZj  
5w6LBXwDak1iBGJTMGPfTnBA1bkg7ALTdGnHql0iRA1ozxAS2AwNPbl7Uvr5AVB  
8g9MIYvWyojTslhsxNLnsGo4fff9FNLPcOcqfzonzj0OnialT1nXx2/XduuSGaYpw  
2bxnoNyZDjowDIn33seMdfMlntVG4HROeMQvchy1Ce08ajdYtmhdaGx24CQ2sq32  
CMmqeTYmREJT0vNV0dQAaqS8EfhLsR0e7WuSj2hqU+SbMIG/EuuuB5Asv6Ri1dxC  
i/9tu6+gbrymuV60IHVSgMZyaUNVUiojjjY6sUTTfNONZeEciYvc+diw+lgyQNDc  
U2Z3IY7SxC0rYAK+b6+ocgc2JgdANEHUIUcHa4ZCQqfjKwq6UfB4gGnncBhgpW5K  
D18IJFLi5cZYwgXh8pOHkuam6Vpa5ka9f6xGY0YP7REg+U3pS7tMq3hs3SHRs1+K  
jnsi4f/Ftw6uWDDJOA+8K98piNefv1TNUDftyLrgEeGRNX9yZkXjojqZLIi8c028T  
9qDqxpomBit1fh8NLIJWQjNYWUB7UbTSylBCdv0EF6MCV6EwhfSsjqd3KjH/fCEzZ  
Dq+VCx0WnkV0t1yktvKcJjnFRCKPYAYAsATonq+6BRKohTqNPCDyLdsN8Y1YFpKS  
OLG0dBycB5TS4wBgZwaaEmmExPa3F52bRspYpuxNbbiE6dtKnyLGCK3phuywBBV1  
DuI2i7CEN0CsgxEL5UUGNMYQK2U+5eS0pLhedmx0zs7Htf2Yme4I2Vg/zk0RTv1a  
vUWwow6zIV4mJPEBDSgTDdE729DJeejaFcRhFrzn91velhIYPyw7E33fap+LfGA2  
8N430RgNvghiWCj/F4tne08kFxFe04fOquD/92aynLcWNHjuuGKXzqXKTPGvyADS  
LLIfNuNwrgBiDv9tPcBNcdQL/wTPGRE0WbBcviKcIr22Vz+7LoSqNqjbd7jkNTmF  
CkEszQoT88RLnGd+htNVu+NIID2A0JillCJicAJ8qk938pkKnr/h7gcBfIQrmJc5  
jX/xb6IVft0qGItZ9rfZ5Afht19gBWxtokXnBMMcjqozhir5c+1ZRBfgoBpmc0vb  
yBQu0ZhN5i7PKmjDPVK3dyXNu3IBEQox2BQMStTNR75NUCEHK9liniGca3pz28cV  
hd4+mMf4KX8TzAVX/j9zoysiSzz+49wtPGJHs0EmlbGwRfxQG8sr9nbT0Bet+Zpa  
9eCCzWdC6fSeY8DHUIJA85weJGpr90KFUGl8n0Bk92ld3MFifchGEZ6CNLeZ6JKj  
qs8eAXfbKJNFyPAUX31qVr2aDdbyoAthvA/aAp0WzNCgkzceMD2EQ5fLeXVleNtI  
aZe2rs7C/z31cAE0C5GrismxnRMmV1GN3sWizol3MUT708xmvFPE9natM54nnEUa  
ph6q4/RdSP8ptv2NdYWC0mAf90MgDvMY+gEUvReOCBmDLS2xt6n4vW7HpDMV5dDz  
EMnSPyNVzsW0on0WmbcYCLMFvHgza9asgaAi7Rr20Sf0D4IF1EtLBDS1lnRdMezM  
iHfxqMzrXR0dTT0IcUCeH/BIBYUqrFpBwUXu+TYlvKMoij4F0EkTcfpDU5n6aB2E  
lIAYDxJ/FJ3BT1mV/SVgsAW6vrF6XPTyI5y8q9U7gIZc90DMP2cgkNMuCYagkhsU  
cop6IWC0Xa7zyQJ5WHAA6APiX3gmb03mamCYt/Nqcqtos437VQvUrlwqItxPXpT  
Pz1UuKjMJ2ZZHixU6pvjdsew6Ezp5/znRP4BjhUen6H0b6NEXt8cvpXic0BfmG4P  
/sqYCaUS94PQEfth00LtajfUvbhiD+fNHR0c0UtDHubDriBw6M99KZpuSaQb8Sv  
7S+wf2bdP/2616wSjL8xQCZt0nJ+GE1gjEerV9omEw3d9LSuRLOWpN3dpLnX0egL  
yy2rUkxfAXQu+TRoC0jG0RLG4AqibDuR0s9lvk6/0dX1y2jP1iPAD20Bp3qufJme  
H8jwXRfDjAOAiIRtKaRedikNvkjFY0ryd7w1tOC5mhDj/a94D/083ewESu95qn  
IW8j6869nmXgj4vBUD6kUx419gT1zo9uhMsgGXpGARGdgwdSXPY6xDFLIRgjjKn/  
giqlj5CGuPlnv5iY8GiK/Z6kEKShlqS9lFnIkuxD+a9KJ6hqezeZJRGNkvCvxWS

1n8VnWyjGcKkXLPfKFFhUQONiqtVLyBckTbVpQ6E1g8c13htXXoh0+sUHxIwmK/c  
oPtKNVxDJRkGokMtQXF72YwQceHoSC4WPM2cKMKcG28QvRuoz3SkilGqTJEN00CI  
6kJlcBezduH7vuab9hacfmnC8GieG0G2pNQYODrEcFRVieR0nsFEDKbuK/M6fksj  
No48V1etDxe4n021Fv+jdvD8Lc57+3wsDP27nTLkKpSeztmkkCuCYD1YtCThxMaw  
DnZftcwwHICNhsrMmkGvmsVa6J8N5eXFBnW0h1tq0TQM+/3XgaZEiBAYdjvzeqe  
3IiBDheQ7LJIB4AZj+tJq12hGko4nfJjiMRW/zdA8gj6AfBe5QzcfxlXBFLaYsbj  
tjt3+F0qXj+DNwbSmM/71g5WKFjNHMrBIqw2K2vishdPqt3cc6KBWfIdTYT0P+aj  
agCvgl0TyK0v0ot3mcrQkvaFi4Ftjm7Sv3vxdI+uNc2YYPWXIcHcaG7z4V+xQ3g0  
ZZUhS5rRhmc7EVHxe0WX40mYlDcd/PucWz4AwN00LSZH5pd++yudIoqCDAPAd3X  
qFIPhxxd9RywETMHBe6HYgqWaoFhVGeOxrnJ7w65EnLVfM22dcFOT8Qkh84mCN/  
Zxp8kowHPqc6A0lg5if901w9acPn9Z9bJZEQDPM2Ay8JmLpQJ75mwgAQ/IyaR2CX  
zCwPfEapw10iMrrZdBFBVjDT6DL6Ydsbma1wMta+dzMSj90kLWkAPA9jqedmi0  
18uMtC5CCgwaKXRetywKXBQyKRuHUu1Uh0hACNSx3CimT3PcGo0Y8izuEELuGkfk  
ut3XZVVK8jv4309PRm+xQjr9y2vKL6BbDyImXFHD6+Y1iSrEas11jbGggmBNmE3L  
cm7Z8KSbsDKIZdVni9m35MhLCG0y7SAX8IgE90j7f1VlRgRft/oAndTP5vWpCXz+  
RRKseKZ+/00jw7hmRUT90TXAXBSXj7dLiMxygoL7IqDw6+FvcZwRXnKnGVyb0m8a  
gkrmYSw9lmMjpg17WoRuMJZvSSpfd1B1UgWnRJAx1xivv4UDaefaDdf+Z/3FAue  
puwcC25/Fpj3VsqH1wngcJwm6t0w09L0GZHU0oP2kB0ads4TzB+6Unb72bfvWv9  
jbJLibgTT1BlaCkuC4Xh0RCC2DrEtckfqiUsYjmNTYpsk4dc64AtEkV0Di9gJNph  
ISMHzboakEmsm4xlyhumU8vAvjh6wP1ajL4D3AhVkiuSn939BuXPurTgKh2yjlJr  
BsWl1oAWKUspmL2R9Sv7tHonNS4b1v2gMoVswWUtLhPQ6YtAzHJmT+gQSzbG5XK  
aNoVTlrOxqiFBURlv1i5JLPYPH9e0iStshtPa8iVeoH/7fBCgkHFjhTEd/2v2piZ  
kwgdQGQBOYs50XNsn7sUeLEcSTXjzQoMTXgfoNdMDLAdZwYBRp0dHJg44qXB5C+2  
LCf0d69JBDL+hPMBLt/V3J+hhsVJOYATi1p5Ycl6rQ+PHCzDYfqvIcKPLR92ecUY  
Mw+cAi/X1+L0P0+stLrjx0XkaKrziqbgnjqNA4YGJlheydtmHxohYb5b+oYrcDAT  
4+5oKAN50CIwCX0c8QbytoJ5NMEKm71lSX0c5DB0/TniyrylmzEJIhQ9cjjdCVDX  
mzYFkCdNkVfLR1QftS3k2Ld0CMPZs+snBYLUdcInJ/8x/xrXEqu4JJ8qaW84A6W0  
VxwUF/SLbSVCWC+5LrcLn9eVWH5fA9M81IFwdt5GgSiQf9y9TMtDyTobyQ68IM8t  
1pIQWkfZFy1fdopUIZWCxfgFkvAuF1g5DjAB7PHH+mUDHnyESXa4D329JC3iE5  
whAq3d7mdj0byyK4jM5e1LZD30m3RSbQHPsnFpX1NvZb3Rot+BT9E+6S2atIIUgc  
3zTLrLTxmV65hSHPNlyLno6rreB5T0GweH5NPZluzr3t0hat93ps0AqkRwrfG8G  
isKPzL7B44uFBj2fNa08YpoRXmRSJ24CLwa0HoWR8N0hVd1MT6A9zznV2irHFasp  
JbR9aNximhkBXFvu90uDEM4cBVj/YNmufXLQ9ANcIWmwDMKRwfIvklQ06jakRt2N  
pNgT26HEHxzFvUYks2KJ1qWzhUig1gkK98iV6h+uwoPscA83H7IEMxtvZXafLNxO  
keJlWAKG1C7GTAi4ePfx3agGrvpM8i0s4uMhpx9vYaSM01QIOYeGrJLakG+eo4H0  
hsMp0+8W7uF3JA2Nu2NjP88x9KFHJXQcvmBHGyUztNaRcuypLevropM7h7Uu9MEA  
Qjk6anE42IpfrFRXquyhTRCgVc+5D2nPUd6pAFwX1ujftdCFjSz1JRqjfZJqbitW  
+Zf3thHbChCD3qQwhR1gCrDxjuD4YrqNJ26ua5oarVQnd1C+riZ0Ufwbbaw8joX  
uI0/CDBLES5T5qGHFwyeHNhxqdoQB12d2cWEMIRKdRaj9dF9MXkzNx5LQfyYCp4A  
+LKKqPENz1NURNl4U3ZiqU5W+ReZfPuPyODp20GuJUURtrMXp0asFwwgAzplmePs  
50k6bxd+Q4kfFrVuxM5skh0g1DLhI66ByP91CAB5HQouXQINypr/q/zPLOMGtsf/  
9R97V20/vS301Z031nTMDLZoabMvB6zK9umZabAu5VUC8zXgraLu8w4xGvePpKIM  
Cy8m9WWcodM6d0WEv01baDzzvz9DfuzNoTU+KIvMCZLFMo0G5Qz5RMqCdVquzAee  
uZZH5MDIS+sGb806S/Vkxy5L2J8N+KiPQj+Rtr2LPn/6NZt0RCWaeUNkZH110GrL  
Q1mZIB2Wo64hyK2TWR0HldncYyMwUxdANNfTE0Zfk9Xg45VqF+vAfAUZgTHz/K1f  
V3E07XkE5vtLxhvUBUICAEUWheWff8/zgJ5ci4uj8gIaGFIEzu0h3NRsMPMLP9Nh  
IUUVwqiuT6+jrq/P/1zZyGFjTYX0iBOTyuU0otSQ3ghVyuaVptph6MwcCwodu0nj  
Vm6GlucucOC6snzWLVtHT0i+IUsf2dmOp19aMGWe6JeDdY09U0RFTHgq/DF21K9z  
0iSnxeAj2GxE7QRmdwdGPExedwficpr1NQS7cHJWA69Xq+Gy97Ayflyz9FDOBMSO  
78kwpjUKzi/yV9UPBGTCTP61//Eh0ukD7+XeJE6T0p5CkGSdXyffU2/JQaktunLI  
r04dciv93FstY8zLZkji9S61WMrtrNza5JUQk0dpj01RJTF4yLjoBNI7TRp5wLTj  
mBhxiLU786BXuB3VR+G2ZVABFmr3N/M1fyOLWFDDlvRKu0jjaYxH5jCBW8ueblwy  
20K/S+UhgCB4d5INqo9FGc3P8Y/LUMV+1KD1h1wWMyKu+I2wLgD/a2uJ1/swXz9S

k0e9IZAl8u3gMD4aSPCQJc08MYbWcohH7Kj0DzuPJUDkrEvTHgpAmxHpPr2SDmDz  
E8udlrH9Jbaxvf1rp+vCYusAFLguWVN/9JuKp9q0cIsBIU5kjKCLE7o+JN8CjGqz  
dca9CTNeMnZfMiEJAoz6+Y57V1Nq+FzRnXxlDesp1ks5P2vUuyrEOrfrjYJ8S22o  
qPH6dstyK8FY/wRtHb3oaGAZVrn10a2/Gp42d1/WCI+a5eJM+s2EfpLjgDtYFQUA  
t/p3L90vBbkDqBzSQUQBfVo++w/0C0iz2ZzJMq6HXDaxdLTWsl1xcpV0HC/m1ioX  
bSky21HSUEK3D/h6alzaq5r0TE0eXIiNK9UeFwSwwUr+UY6gZl0/Cir7rtSAlkd  
FWaTulb5hU4AsSMTljA7LirHrDbHEmGlq0z0gttDUBVKzkdvk+7U057n+2Gp0Cjj  
rXvF9p+mcthZPwIjKxBaEGCMHHYsfYWiVqKNmn1l7vtRc1bZR+xRwTL2t6RVW8eE  
ha5ujQzYwxthxoznktQ2PQ2fuHGM1/DxNNJgVv/MnqhCQsocGU4wtFG9fxyqMq  
Q03d4myLkK6Kpa3LoaH00X6koWpD1sc8Q3QTqxWqF4Zs7jRQExzBNiem8pmxexqs  
7eDrojEjrImFXR2KixfBiUJOSt/2gb0RVm0ByImhLWwWFS67ckRrOdbSQRusESU  
RnMZRVnK1VCjySwIr/dCOVHVT9XNDNUFEaUcIr40WnXyA6sJgqQXmmFxfMKGuRDg  
cZWJSk6t7oVpRGly/8bMmhUyC1qKEpNmSe0pIxE6Azq9e45mpQMfK+0JMez4BWui  
QGGJCyKioD04ATBbFPUNfk+LR/C1kec77g3aAMKuCPxkCU4gTnbpZY1M2KI8yLQ  
j/Wm+3YZLRnPz1rQPQEHY3lpTnNynSLYC+3Evc0RobZQJSJsa5QFLWX4/d3LRteR  
tScSiXf04Pt7mjZo0Y0HfOghmKZist3PBTt9XK0YdGW3QEzuh/pDFMjzKUSSU3vQ  
/LSX5I2gY2csGKeq0lkwR20/oEwZk3QKFfP68/nv+BBs6wo1ncadTDklr2XLMAd8  
xpMW+UBUsVdwoXAA1lvkNeKlJeJuHawN88IkHA8d4p470Ig+zyFZcpk50N8SsVqy  
+1YhLlFevkH6bhx7zHoxiCT9oXAPLaqsR1LNLx0US5RSqestlLC5DZvelXYrHhj  
jRRjvuzHuV3pJHyo3ii+Qn/AAfneeVG+e7N0zw/9cW/gAoL6pWRqFUB9zWhUYR9k  
Ulm0S0DgkbYnLL7kTYOmcq4FhVLzNM0QaSGo/FvTGJRQIyNGAFiQvk1xYZP+nSe1  
zvFmZJRjuNmsZi8902h9OnFqeIIkofkbcogWhTM50B0QZPTS5fDDA/nIDQZ1TN+i  
FSuB1npjyoAHNCHM35/ugxRr5Mwck/E6YF+Gu3rh/y0laoFTVr04mwAamgPdRPtg  
+kgExx6vy34t0Ex8gDwIctHf4Y7y4pJq12F0vafcMuVnIiEa8+dbPKXE0hKa0XkJ  
dy8xuyNFBcyiIMlS28QaSBn/D5s0qgNx/IPRokWF06m4Ry4ANcpP3/vJnDVKbMPm  
yJb1pF5hJRnslzYS9yWnIH0ZHN+bgnMhIdJ/R845xSrEEGc7HGhyfiwzTgV6tQU3  
g0pZCmHvRWKJW3N8y3FBKPx9knzv0Yhr+K5RR4F2aaAJBf9xMXhtKkKwVWBUTFlp  
uUADmX0pKSeXg9sfIBxiDaCeZ1ocX9RQ/XbvIV52uJP6wP0/c/eQNZL6VCSpcg9E  
t35Ep/j3rid0o5pt7T6GUyT9fLP7AZAPYyt/JkJ6GnLlEU6R080QU4p1yYswvKBL  
ZtZ5U6ZKomhRiHa/ioYqg/jK7l72x8TzC61vHe1XxLBew6CYJ7rYsd4Bwr5T/kau  
6Jhd2l02atFDkuyNuIIBHujVpCMZcpilt1M6I3aiPIcBRY5A0/zSLdU3KrCTVeg9  
aFNpT48FUzC0gkCqeAVjuQ49pp7Ew0/xJE/ZgClVpZbjFw0G7r4diqPC79neMgqWb  
3iArHv7T+p2w5SJP87+0+Jy7U1gMI84eUle03A/YyEJjlREvRFxp9qs5brD60B+  
S0X7MTQwxSfMjM+hrxHnPFtqqCK7bgWYwcj+R8qMCbbRQW53qxmy+SwGY/0qGlti  
KvFUARj4DrNdBUQ0ZVenXB9rwb+IKnqD2F5PUqY5/ryY2wofCfnLOaI7N9+ww6PK  
y+f6iJCK1pNg7c0GniYzguG1ZbvTqodm44DHdno0H3PBCVYDtC0rpy3tBEU9oIu  
6iezIozgVlgi7HuPIFprM4ePGM1a17F6SrzeZiv0uvCGM6n0LdPemwwGyC9ktAk  
v6hk2iLJnwQ8R4sGAZqLJrtYpQxdDnghzzyWhdeU2nG+gLSedAm8FchX7LXQc/L  
x+JRDj8RseywQwku3iAGGxUNBoTVRQoujyR8i0eYRpYFZoD6ic8Wnag1/asAt6wV  
95kzEqCnZMVCsh3wy4xRy24F0xw0BLYkXjYFXTsIN5FzxHcBavQxtewMc54RhwT2  
k/SL80jFrqYPr0tv86uP7GJpMTRxZ72fLaTJJ4VIsuvcttM2umcN/kAUjUVFyHIE  
ML29PxdVzDyxWY8FeNvqSX3IWUHX7BLDrqHV4uJ2QkFDBTPvvpTbdScxqdE/WgB  
ojT901PCzkEW24z2bL043EaaoQpfoHV8F4r0op3V9tpDLcn19Sagd1ez3v8p7l49  
GnpL4kkGA/VETDjttRnTz9FTEYpPGcnFolNm/eZKHx9zv3i/2ard5rTMx7f+HsZx  
AHir5E7eC/qHyXApMOYCTXc8I4NcEX78W4GFVzuzuXgK5eUGrDDRQWLY5B19zy5U  
DXw4eUMRbrmyxp3DtZSTMh2Vf62Z9uCMw3XgVwU3CveibaQ5vLRYWsRw5ojzoLQM  
GhoTxr9yRf0g2kjj/IyOu1MGMZlrRxtzFh680euchnNxZH3VVMlHuTxD5JlPOUNh  
5pT4iS6l3NYPZFOGFfH6NUkfPp/1GmwMHigZGIzvxjHq7hX0bZK+5BtE1BQbTS  
QyB/qxBnfk+MQ1IGHMH03Rlm7S+mMXtuIoWmQvPk1rumLyQIP/MrXijpKGxnGnLu  
qArIA0zkmNkI2yr6n45lvwYMXE9gvTdTf5KzLG7ETHq1cli9vi0ogu95/dqcBnAo  
hDGDeYy9/NXGveJ/4joR/QnAeyohnHNix+mbSgwBmCLJeoM6tvKNtYodE2rBCa4Q  
LR90X04CfodsmJadOMN88oKG6sEyx0YefI1VYD6+6YNN+nRmTnnSJzJXD/k+lgme  
uzDDBpyLPhasNTEMTs5Y6LQf+moyY9Fx/M8K5GUBXM7DVLkxYHceJZSwwUvTbM8i

0vc0tIKdarnZm0ayEAEimtd7Pgl29Fuxmv5FjgH8Kadfn0eetNlMzEz0UryERwIh  
/4RE7u+HSwLdLHD0zDWrtLErN80ujdy8726YvgWJp63VhD/1UKUnAw3J9HLCJUcJ  
ja8HgQ1YTz50Jhmbu651+z3MyNbWAty6wTwxKC268oJ/HGnt2QZjp5kYwaI1jq7J  
7qoT0amLF0n5W7Env937LDiZEjNzzphTGbdhevM12W1mNbU1uZXz1cPjWqnage90  
K9d2pMmlryoq13ba0XuLGdik6+yVhjxxXe4qhI7BjWvNgYlOV1yrtUb5mkWq2+PS  
RW8+uJP28KqQA02jqK68KgY1d33ffuid9uPKU6HWBnP33feIAGx+zP6IAJQ/i860  
6tVwn7ng5G55cL6zrddvHXz0y7ZT8e0emhzeKdKfpDnS8XswD9/oczq6LFxM37Ts  
tw+YdEeKBNRQ7crq3VoupmmwiUiCVrXvtZksQLjDx0AcfQUG8PPCGyZrtUUioGFF  
2gvK/by5rFf3zlszSx6/dyzMkGPiufL8GDJUoWiC7aEcQ2D0XfrxjLLXrbPrbxvC  
/WoeGX1u986EZsVIBIW4uqeFgdNeAtleq+1Bo4QFR7Uh4zoPaWRqMW56W0lfXf7y  
fFwREu+JyEDNLnaUVW5JNYg0QP0hUaiIG2eL72Gss3PCTQ18FqvYU70qQ5xGP7BD  
uERWxy7qdm5yvD3IGEavW4FwezPS7Y7iOP7h7GpWj2Eh/b3PFZGKfq6tYDACQtYs  
pZ84X7rwrzAmhesa2cGDN0SAK7dhW8bmsbK0ZB/GuXeCO0I4UnPEymYcSdnkVqCV  
HXAn/XillyAMmFRzga9LUgcCIoIFDnzxMi+tKpuzZQjJD7WySTlyG0TPyrI3KBo+  
JeVjF2aZmYCP0t3JrRpK302LsR+qFhAy2ZCmid8wPZhbGwUu54pqBq4vfvNDRCaY  
MzC6kXLqiMfDRZojQDaFaiQc9RqvjbYkBaTEylmyNzRzTzrujEI+nOpDULCVQx  
JPOIRtH0QDX6bvqaE7sDHK6fRWIuuFxBY7n1IbM6/PjVJeeasQo+o/g9i2hbfzgzq  
uLH/KNFHF65jJ80pR35sk1i2hfYQSpVYr1GL/PKK0E0SkdcrcK/eXDtKFvKIvsYK  
i/RzlhN5NUj6nmAVd30mYYBWhxZWtbsn+gBqfq0Z0ahLx+VHLMQM7Icnt0De0/8Q  
Ehj5/ONvshmr2y5LfgmC7D+J5zRadfIOKzPpcYRGgYFPKxYG2bTnVLKcULpInakF  
3QoKxrDRKl307SYZr+/JyEkteLGNyh/nsgsE/S2kz7kMfdUALB5fhE0qI9AS67pY  
ZJgKrhGKlas7aQp3D7ZGgVrs6GiBLUnfD49JHqiFdYdTixr6T7Hgs3ufuQ5rSQZ  
eCjt/2br3Q3ttkWTJD43MXHR9PMNGIEBJ/RehN08Gy+Nft0Y2Tb274DdQK/tZqqk  
FXH2G0zpmEUSEup0vNP+8yF7MaMuDAkgbio1F4UpycxhJVRs2P8bLJxrMnYfqXla  
adSnkFQigcGUHgwfu0Qr6pB7Q7zS6Aepyv6rvM95RwC19h2r8/9UEh9cu6NEFHaj  
rXxDcPpYqng9AIj2U10VE90bDAZZtXd3+aS/i9aq6n8Ly6GVNyuv4htd04YWGZdk  
HEJ7YzdgxSiLDoTIXKi0172R1ix00EBBAirv5VJCdj4rCgfhHtaizRMEyiBw7dl  
wymBibj5ssw5dn1haue3WKFa/IaPv3YwjFa5SQKy3ivQq5stNhp5IyUIXseU0czs  
y/t1aAuiigxGUs5gj8Q1KqI0AKjvJCfdisiPDjlnNckxCqy7lgWMDGmPz/hpr+a+S  
5Xx4rxBQ2t2k4mb84Fa5BzUFRPgFjWASucSc/ACrdwb2EtoidiwSW4C2MXdR/pOY  
JpYS29LP1QqWoLC4AHNs/soNL46DzYBCCn79qruVdBdCYScOuUa3qPavq99950uR  
ymVZOyXCgZi1scGqLRdFa4gF/HCqKM8E/7uoNFMHwZwSZ9UGjEzizEr8KDS1xoxDi  
mXsV7rrovL+ThgD04bywC/XILTvhL1yEGLdIImfzPcnsEig1UUAKuC7WNQMjBHM  
Myxy8Pr33pvLuJ8IE6CmBp3HNPw3gwUWghNvR2LKDANLcYrAQ3RUCWBvSnbsba1G  
oDQVP7qNB0d/NDx/FpKY0k3guyizgKZS9z2HTvtTW4qvHY5UGzpep5apDCsC86e  
lmIqM03NRD0xfus8T1Z7bbkb0yKBbX6mjuKmkQVOrvQ/jVlwSiwC+CGtJ7nHbsU  
kkBoPw26eGSCW0FMcJZCS+sB+FKX0vSL59AehVm1EE+lrqc2YMCbVSCYfR1mIjIm  
07/AiUva5pLwy0vVHvEgx7Y1+4uBhs11z5SKGSSwykGFHAaY954vT2fmmmpfE5EF  
0zrd5tSzrosW61FYszWFHOUKPG053R7C1nLI5aDgvb+UWYhXSQC0BRQNAPSoPS04  
ts4X9CsZp8lCy0ApivZqmuDJHJ6zV02wbHxw4gumvwwr834pziTntpcFPAzL4zZV  
e+wRnPr5/wmmd98qrWEdc3fFEv/ETPNQXPK4t+WRGVNtUyrs/Uh0DWv+Anga2Usp  
a6v7gPqe86P+d7LL0zsHkjPpBDwrmdD/Gt8UnFaRfK6yMnE2sbAXTm0U9Dt1UIp  
a5RNFjPvKTvnnPF/07GJAWV1qSRRRjVw1b+Ag+Pk82TooxKdNb70Vjo3ijpa+rmP  
sVrW2RnWQKrLmWiqY41w1h0Ud9IFaQ7NJYv9YpEle+zcLshRJSMPsfl5i0V7QNhz  
kNtfl9sGrED7HhMug0hYlbezMGCrjyyzVIB020DhzflXnXASsu4URRw+0v5HMPRb  
gSRR9Po1p0/CrXLZJKpv+donQbM7YTTA4xDZ0sPcN7M+bMG/t7MhrtjjYOGCu7Ym  
RaVlaJs/QP6WtG0r8HqhxJ2tHDChGoYbIesAft55mxEaIJP5XD01/R+aLpscG+  
5bWp5qHfjugUz5dGicWacjJTDW4XePCZ/UIAVb0EocQYuhfYhXJL0N4ZpcA4j0A2  
YVOD+dSqdZLDX7twQcFe7Ixma+5s/wgs6tfZWZiJoqn7S0dooHo98hi8dd1ZnC68  
URqwpI/HRox18+xjV264L4gLT3PRx5RmKmczIE4QDB0Ij7BDJeZEr/jK+KyEwX  
X1NhUatmG+ndrMRc2CdU5lMyi0Bx/legCQjDvVtSigfe01I/dGr4m9Wn6tf0gJTE  
YBk0dgo/5DXt0nXmZio9rVFYuRbhKjhhWPJWcUBptg3epzwntiPHwA3U3fiP8Xhs  
Mg9HLQ8ppxw8X0/+wfJL4TLZcdkGw8osmy2capjNvjP7QrQr0TtLbvw273B7Dbao



```
Ae7ySgN4Kv2uCS8thfDbeiL4EDkklNepvhdcTSvwjZySbptQhj87tpxZnJsPDo/O
X1kJpvyRPNqcIjrrHHWgf/m0ajNkHsK3I0pCXcz501LRhhjTxVQMmF5abMPngi0Uj
qNbog72ShxedFjdJpD6KsynMTiB+sCmjgJo2Z+aNazVLe7LrAn/wTAo6VgaP7TR8
DnctSfKXQTrp043uLgkn3DJo3MvJBkNt8JP/6zNaU/FQ+TMPTvt0m2pipvbqQZ6C
vEt7KPU45+ZDSV44ULaGcEPH4WUXLgKNAQ9PGH8VexF6U+v9npVHDM0PUSXwrbsi
G0ZDHmFamJv9z6vo62yMGqZxYnV0xRvYltCXrlgr9cSJG9G/ln2hVC0POQyx9NdG
yTm0eDLQ8e1/6ioSYR88/9LxXLNjGZcaY1/o4S05b6zbiP2Y+aag7DX+cbJKYX0X
hBWLX1lEzLAqKbGEUX1lEmyVVzqjPKSeiaVl+izXW93KrrkYeyGuYmy0uyqm6Ykh
UUyf7CEi4GMgWYy4mCjeqyY+4efcfG4lx7uF05MX5AtShY1QRdiIqSeoltWemsqU
rgZowqMVKv083Kk8iQo0pz/+XtltkqpVn+vCg9c/ynX44PLsI/lVb/v4SJ5lkoyJ
0PKPU2U13qE018XdxSyTAMVFQp2iuROTQPy1+bM4pmfL/N1T+fw5Am0fWRXcvljz
GCKDGOEW00/nZT/J++jJV2EasEj9Sxh0Zaar9s+j6h91hIGELMRyzGqUyiSLveo+
KQ+oDTfBsK0/IfBbvNHM4m/l2vG3o1STMnHxu7Lrn6Aonr3lWbBAfEjW7CGnkoGU
jx5Nw3GFvR7Ks7J/m0GLRfQNDNkXk17enoSA52ifvAzH8C+0AynG+c+luC2T6urK
6o79/ZDH5U7KtfgveQLjfy0XwofVC7gFrPaNtIzL/ZffJR00NG6iNjGqfVc0Ktw7Q
AuZm/FI1Ief3hN2gz5w0akfcjQZSLLSWQI97Qwm88fD3i9XsPSJ008XhlpFT0qoc
yXGiYye07ZHS+cHhYepK3Uv0Iq5b8ik86sWwyesSdAFuUkrOmVmYrbDs14WbrbZU
TOcuULN2X/pbVcIB3CaKfSZZ1bAe8RfNc7gWCY7Y+JV3qgDA8kQtLGdzIE3W8NGm
pL8umQcszXzKcCryEkfCtByAHJRGtZke4J+/C4Vos3TSD86IdSR/X0aR6ngl+HQy
q0rWx8buz1Fq6WePbkV0/fHvzuSdGG0o9Hfa6KgzrRYZawiAa9ItwlCLgoo/CTL3
+gWMTBgxzhNBRBkhgH+S1/wExzSjXryeci+o08+oxq22avc0zCTdNsolEUIafsZn
F2GXEzP6p4fCWdvcYmN+/VR3/ed+oTxV1m2ql1DZa6VlspiCbP0nd4N1JQ/m6RgQ
PYUuNqmwvpYAs440qUt9Dhfc8MGAIUdQomMLEckpNGFmECQb7nM1ZjixpEa5UQgy
9r7oB2Z0g43ynPuIt8e7z0TFPTXrEOuWp6wSfoqRLS0YFflpJOD31aH+okuTtnC8c
m/BvnsTr2oKMTbmlzHuV+KfURc76iVKXGcRj2Vjb5ad70jFOPX4tSMT1LzTGT22q
Vy/14wHPZLUBbwbTlh5iQfWk1QLSZvLcnVqIUBA/E9QffN9PQ0n1ktR3BfboT0Sp
F48jYYsgyqw/STiZVZSEUyu0bRgjIA2uAgxUsf7mc3t7rIbGFfNvFW0At+zVp+O
4MvCKPpKyAqUxqi7nNEQtwuUnYVXaw5wSJlznVFLGU7sK0AIAmg5cqBsMf4vUGj
7+Ml+Kqcm0Uj7XJ00s/T2dPb1U5kix932/z5xMFHuhwMdhvHVtHhKw847G0k3GKt
Djdb46LWl0rza7ZaenPQAS+TYJK3I/u/0Xp30SZcV770NJ1CG7xVxnm2kQkCsWv
rMJocxuRG4dzWET9X7L982rG3dcZofNjIHCwHBBmG61mBRfoIiTDPrLghJzQLKC
4N4p9N0cDyUuUHJnPP57MULK46JgQvXKAq4n4djJlEffhySR6UET0SX6emo1s09h
fFIoHT9W8fxxbYKfvWhxppq4tjk6d7Q79RVZ0KKto0LR2hubeCetucuJxFLzoqgv
PDwjNH45EXfrN0/aeTyQ8NJayXKKeCxBj7/igqTydX64k880Bawy5ngGTXvEf5J+
PDn5UpWD6Q4IakEp5i+DX5H6t7WAPWOMj8t8dzJWUyPSvomlkhRLz87w0XkZY8Z
+c0YxgCu0miryEJoa+Wz2pvxguXtTigc++g9wURsQxnfxlzdS9mTNEbT3ShplyhPu
ESVLM4MNu72Laf6dr6mH9TVWPQWAKxE9+TgQp+l6nCa0DLieiuL/rkxrs6+AfwS
JkBXUwSpQ9gwG+YHXTsFzDWW1MWiGwIgyFe73FmcGqcR4rWkx/8gBfoznSWYqmCW
xo7eygtBERm+QKQy7ycQYgXEkLDTSmRBvi2lCah920I9T+ve5sXz+0lFed7abKRQ
iFBgbArJGAV6UN8puwkiSiv6PDoB9/X4/08DBPOZF5JwjmZ+aoJel12ovUMIHKcm
mZlemcfiGiRxdQDH7juZ8BrHIKk0wOtDjPZUNFEjwqUwAOXxjmq/pCc9fPmG1Wd
RWZ8Gm/fvohw8Z7ngJX83Ah88oQK8nIajwkKRFyz/stpHwANq0BsggBb1kf9qvLZ
CNLC5ZnhTaMnsxHMLZGIoxV4ZLYXJh+5LLRqPs2UFTDlT/sa0JAZ2ac80rXhbbby9
7NX5Y90qRwMuryi3DMOFp94PipAjjyg2V2Q80xc=
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the SPHINCS+-SHA2-256f-simple post-quantum algorithm

Use the following public key to test the SPHINCS+-SHA2-256f-simple post-quantum algorithm.

```
-----BEGIN PUBLIC KEY-----
```

```
MD0wCAYGK84PBgUMAE5M7gViQs5zFAommoRgv00d6C0g1dJYIycRl3UNd7SWMi
fydoknPaAj6VT9/kYwuP
-----END PUBLIC KEY-----
```

## Sample private key to test the SPHINCS+-SHA2-256f-simple post-quantum algorithm

Use the following private key to test the SPHINCS+-SHA2-256f-simple post-quantum algorithm.

```
-----BEGIN PRIVATE KEY-----
MIGjAgEAMAgGBiVODwYFDASBkwSBkLIVJ0Ly/zucZpnWwhktAFUZrPA2fLaQPtCv
hsZyra1MXeQ+q0yW8r/2AE0mRromZeT04FYkL0cxQKJpqEYLztHegtINXSWCMnEZ
d1DXe0ljIn8naJJz2gI+LU/f5GMLj+T04FYkL0cxQKJpqEYLztHegtINXSWCMnEZ
d1DXe0ljIn8naJJz2gI+LU/f5GMLjw==
-----END PRIVATE KEY-----
```

## SPHINCS+-SHA2-256f-simple (1.3.9999.6.6.10)

Use the following CSR and keys to test the SPHINCS+-SHA256-128f-simple post-quantum algorithm with the 1.3.9999.6.4.13 object identifier (OID).

- [Sample CSR to test the SPHINCS+-SHA256-128f-simple post-quantum algorithm](#)
- [Sample public key to test the SPHINCS+-SHA256-128f-simple post-quantum algorithm](#)
- [Sample private key to test the SPHINCS+-SHA256-128f-simple post-quantum algorithm](#)

## Sample CSR to test the SPHINCS+-SHA256-128f-simple post-quantum algorithm

Use the following CSR to test the SPHINCS+-SHA256-128f-simple post-quantum algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MILDeTCBpwIBADBRMRAwDgYDVQQKEwdFbnRydXN0MQ8wDQYDVQQLEwZQS0lIdWIX
LDAqBgNVBAMTI1NQSElQINQbHVzLVNIQTItMjU2Zi1zaW1wbGUuU2FtcGxlME0w
CAYGK84PBgYKA0EARx6qL5/SCS1BkE/R6nr2q1a4TrsEJfEQdER277IRvZl3WPPx
y7jSJ+z9XbFCVc7pYv185Dk1f53xYmhB43710qAAMAgGBiVODwYGCgOCwsEApz76
Z2zpJ7y39dSgHUjW9LFSNB0J5fAsSjtabIGmUw9/FT58W5xGXqMXaCzg0vzXi5
+m82L8WD9kdFX5bd12ocGTsc4A+s07JB+09raxZRv9CCveJupBoLIv0+PM/aF1hG
jFd3r6bY+mJDtM03yFbAAgJkQUrH/F56D5rBWgxXvtgRxjzubbFbNeYV9ekyZbu9
QBikM9o3JbuwB3lGlq1iXpWYoikIuBqZmamLZI6TT61mQB8kWDmJ2tHoqTklzns+
kxGWqvy3M80MILJmnl8CbXqp4cbulB1Rs4qd4II93YYENpy9cE6QNZB074Go/cf/
WrkPCPRCWGsY5kjni8nutbqvqf7BBA3lUyD7Drb1KQbYVvL6bw+0/d1Bcps7lG9Q
FDeHeHj3sxhv0hFF0PVzqg8Er9Tk44zJ4fFctLYLc9B1DYyX4q1lS08BGlztzkVhX
ng26xerdbbLEky0Xefw8ITQpEF0YXb2JxyUUUeTbehSv+ZmEdSM4dEAPjJEZXq/n
dEvglB2Jaa1QfXCxx4V52MMAKkdfESJl8B83QXf5akfyMfsYbYgxaLbD/kilcKX6
5MAfhdt9cKmyzTwvgGU8szJUqaUGPyMVJOEtZum00gfSmK21/Y5XjPkoFAgoNtXq
yt1FfIf+Uc5R4DAKUWKus/BjdJTfI4dxSMKTJVZ6Yyne86PvcUK1mTJxmvwgWHvt
17Vc1xAXGxZZI4vxFB1NIWa0U2sGnhC0DIS+pF7/l0YYzhD3sXNOZiE4CS6Zx3eh
kKtLxK4a9lt0U+JXU7gD9DKnwqILIMwpEeqbdq0GfAbhpQm/bBmS17G0rfKtZ+20
N2f0mtXEhhwgZ30fbwIZRqCL34UStrKxe7qpGRFjh7guQFrp6bUfHgc+cntD/rjT
Atj9eF0Kku10vahBmiWocBqMal5ddoRFX2nwjBDXtCoazv+Y3y3u2DJt+kCNM0vj
WlWnug3+A7ZwBvklpWS730/9kS4A0yFmPMY9GLTZGLq6aMhJ81pv18cmmB/DKebx
```

RqIgBcNa0qIQMXQ0Ko/ZpPZPFafwrFPhcvqrwxWBuwGqv07dEtzPznr+1I4Gae+g  
7Gi74/DYxIrw1lfi99pZpLaF3wo30lR44clh/S0cxrw03BsmHub12a0tkFKpqkLX  
sR3zgT/y05cE4Qy0qUuARXi+yc5zbkLPpUlln3KCJun7mjYBzVb+mQpXIZ59W8Ji  
Skj0hwGLDrGb8aE9Tn5ZBEfcWCE/K+6NnENTro32PPur4qM/fYgWYaPYVge4fSaR  
sm5vFRqw+SfzJUuu/4+oihLJkhZgejQYvjmbfhSNhPopwLzGhD32vA0Zl7xkl8BN  
/5RrymCDRq0t/4Cn11soYb+lE0qunLMWmdMRQiXNhejU1ZgxA7e2u6zQE8upM0IJ  
zpLNCw5QH9LFX+EgmQRyS9Rz8xUa+5QryHZ73+DFmn+/oHBeiyGCwwaQ0SdtZgAj  
l6xjiRDvcKCy1FfsLwCPbdCS4DfoumcTGZW/kumAkVs6lFlcRdeoXwoblihk5H3u  
ZtnMi+QN0dUmknzwpF6jW22VJR053ArTgBR9lg7+vpvBVBr7KwwZMk2gbAHE+5Wb  
2h7+P+Ud04jd7MEuuCrAT4fCLduLPjOPZTGs5Uq+qVM/VEdasM0vvgg9dMtcVaG0C  
L7tWvd393hliN1p+A2WJFSt0K9LMX+amt/QpiJAvamIJSQj9+X8twG+60SuH9USS  
qjLZTSv7fbkT2FUaTF0zaLTdmM5MQbzwdE5COXlxMNP9cuqucT16wcGSs3J9bv4  
7zNyjVbNr4M1KBS/6zhk60em6nID8CnstCzagOCRkh/19SSmpSvpvLgKtP0sDaJ8  
jhhybU30BuIh0kzbYUu1nDWeEV+werdsFmma9b/JR3MIzmW/XqgUvgAbhVgYn7re  
L3UtQH00y9P0EUYI0HW9R35wb80beP1gYY/mC3rdSC3U4Tw87y1YtYMHKp3S66YAn  
f/6Tn3+lync2H0v0Y9Nk3LVWdXw3gWHDC5NC+WkZ1r5jyoLwz06JWGo8LATfTdI9  
3/wVxhaV+XPgD3V3JzT/WMUq96vU3jCQo9ikSBkX54NfR/ZwBGqLtf/awX2ku01A  
NB+RkNLM5XW5y5J/Hkm32V0jsAyyfIqV7QNoCZWjxavgTZTdu7t9KrszUSxBs34R  
wkdJ9Brc9Iiz2NooqBWzDFikvF5Zz0TD3dkiquezjRoW/4L8cr3zvo8VIMrTAF115  
/tBeo245hLQSQ67VoWMPH+XSs5PpR6eH0x1Ro1FQTUvp7obXr0Wna30Q4qycvZPZ  
qH4CBriAgjh3rNYL/+DfsvZiKrxwM05/0YSfo7DG03I1rAil/pZQZdeNZWgyDrYM  
Sh2cDQ79jx85E/FvFPoj5Ykff/u0GDJvXAnajs8lTtDvr4DitH2Zb0bWdpYnANhB  
baf76Ee+aaIwCKnFXIog0ZGI3y0Zhwkrwdc1MoT+zz0Hih/7nIJFsWy+gd3DmSD1  
zF+5hVl3U+6e0bKpvMctPEMyt3Rs+Jyf+ddmqQE fGEr1ZLHs2ECRbadE5X8/DtFA  
AFHBcXF2Ic2Gh9tqDFBTiVHH8dFZZA7Ys3hQGxmG1M4+g+eHgvz10nlFmIAFnbgk  
50PIk/TA5EZknij1jYjCSIq3YYVT/rVVIKbCFeu+hyRtCFYa/tZ3gZTi7bmvcmoM  
9D0StjXc+d8q+FHPYCy6oQGUQ8yDSq3l6mY/VFDXVH3FJ3kGJk4GtfAbRlg7AUli  
Zrq0UHWq7C5Bwfp7Yw3rgZi5g/PJAm2p3vn0DJ1Zg/7vM0GjaTFQW8PBanCsCePb  
hzcvlP3sSawZ7G8ekIsnhlCBeg7uQbP981o/jFKzapB+vL+0cqZo080QUaneYvuH  
o07gLA1PD6/kUd1e0uDSH6oL1HQVxNJERd9vJAVYmg0gcrqrtozBb/71r6K6Bd9q  
DSkWHGs0S2S8s8JKLV1Q6Q6epzQMsprFzT54IzLzRcu5bsUgNxtH0sdZoCmDFh4  
ILFRjb0AdjG+Ux/SVx0aVhWhYgLvWgH/qQn0KWDIV32cJ/hbFXcUz2hnCKlW9bw0  
63PJc+ZBBLdoI6TlVNAKbPrEYWepIi3KGyt5odsctMqf8jEnRBy+8KZLBA0wLF+b  
RFu3iCTYYl5fu2rYwZInQWV/UTg1RV0e2geEpRbYRnbk8Kh54o/pzrFvxnlzLbuq  
efPqtQRVpjpV00qtxqigqijGvAr72AiW5K21t/4M/OuVcDX0+pc2M76A3i6j4tdjh  
uGia4oECnQqWV/NJ0fZ49fDnC/rJu8IHk2RWimUQBv5yl2a8Iems5xyQl1i/Cs2f  
o+JRDtCtn7hxdSjZMDs62gIy5v56y63ewUYpP3swfEkJhrWa6jntt+yvVuDsUDVq  
GORE8tGkmdXSLaXX+R50ealgGlpScYfs6impPtFzpKr5ckIYaku4yE9abtTXMRrk  
du6c15VfGWHGepZV1PAC3RJI6MpBluDxq6h6GFf2sEGlc6eI4Q4v13RMFqce/aVG  
82Q6nZQXcF72GMeIL7udlLflLwDtgjTe0lmdkSsEtyNA0pgKommhx/MjZ8blhM+  
abzc0f2An//wwfeboNcgAz5DEftfYS5A3Q4oHYctH2BSDIcKSDPwBZ9GSix3+nS6  
Mrw8Xk05iK3PUcT/getEBWTiqbph8LFBvwwKhVyyGicTl+pB5jLmL0LwVYF9WS/B  
al0vVEA0IpKs9RSTxluoGxMHP+8+1NmQ7QvFZBNj7A2d6rJMqfDRSmdYaYe0sLbn  
8ShYCNLzbaCzzlRe0h5wIcweH9CvN8t8op1qGw3ybWmqx8VGH7KnRXnJ4SGm7Owl  
TsQGxTLh0i8opk2Wa5B29X1RG4lWsSCVvoRsbZpjH2YhckYC8Ke890vxsYnEVm/d  
9eNfEU/brj/LZJ0KVSvpMjx6gsuufJJY8XVeBEuIUgNLx0UaX+Vs4mGVtoXr75vf  
9LgS8rT1uUse8ezasgPzQDm6a0DrK0khKJUY6T5Sz5a4gXkRl6gfoN6/uRgApMLR  
cm7YxER3n0Y858n3ZoGib8SSPvn4R06WWIXf/96/LRi/b228u0nvZnTxVF7+Q08F  
k0FjR22bZE/yIbmWS89rsKPZKIb1axKq+yR6X0P0fqPbu2/o1W6PLobZBT6IjSAp  
0KtJVkm+GcpSTtkl1+7V/cEN3G/bx1nqrqDCfTFPaFP01TLrkjx5DY5Bzs45Zd6n  
8G/iijbXd3TfIOfkFMqk7mIjHCEXhrUKdbqhw8Qdf/QlbivnuAPm4nYayIXZvd1c  
GpmGDcJu0n/pqZ04Jw460djhkE0gcAAC0ojFzM6fcmamj2ZQgUI986q53m/59B  
f7CYBZHk4o4kcmLitbBUCHSUcoNGufJdGnpqZ8Ljruj0ouyDbzIjDqBsg0lQpQpT

hUscKwX5gZRRwZk5ueiB6AdD9G4T6eSxtltldafS3b7bpYQWrdiQPcTckz334/gIV  
NK2K5+IPT9jKj2F/H5fweBtNzCVPRPHMWE0h0sA5pcbMf1rd+w1BE0BSm6fT8upz  
13WVJ5hoWUVpm8BYqRfNsJhgCjEZGtrneXTJqPwIaoDPsRGob13mGPTKD/PxLz8f  
QSN6k0/oVKXGkYeh48S39kzxQrQajCIvrhTLxB+DK8/TTNuYf4H/F+uNH5Bi7+00  
4QH9C9M+FHs2BID6MHYPFRw/TFFvw3Ss5FvV7S64L3uPH2w2WwyovkuVx3eZiIYw  
H8DcC1MQ0J+VD60DP9t/afx9pwq0i0fPyy6PMuD0GKeWMAd8Ebg/B3lfCwi9f2w1  
21HYoD7HLID3TVmeGKUu6Cpy0jMfTKzqL2GxUbfjHIHs+VG6EYxcCbYm0Yk/8unu  
LF+P+TR/eNJerOQGTzIOYr3nuawis6dh3M7+kxjBtv+Ud0Lpnuk6+Pxo63W55puw  
wwr25rJangHQIua3WnKyn04JE+RBwCVhPZ0rwHuEG6RUUpUD9V+Jx5Ano4QV4wSwI  
Sjy/f0rtSWb+RFpfY1f1u3QSR/M1JnUgFXfbAVBPmzogmcpqfXyKlDg3ayevz7jR  
BdZOMXICmcTbRREcChWnFSNTJh7vksVbN/nGXifl4UNzI8PlWVY0R/+ywjTajzdv  
jjTmVJl7maQHLc0L4kD2xzhoFHZFLFRKacVe+2BZu2K/TEFWwgXLAuySE7FtUZK+  
iSQ9gYuMGdWZBPHs17k4s9FNMKbgsoYpKXyWZxPWLlGEx4M7e7or26wogSYCy1ka  
yC3LEPOULuHQVocS9t2gGmYwLWQj50P+piRGWti4Up/RqrY8G5oyrcchtQ5p9Pg  
Na0ITJlRw/PFPg9CQvQ0t0b1kG1pa13yK7LVLSKc4aJ80qPWe7S+OdxJpu9ktht  
LkBZAl80q60cN+oRSZ51gwyCIOob7nj0uby6+YJyUmItwwKXlnPIpLKiBxENQPuN  
dgxtbswY5vKP8XZR/tn6P1oTCjeaVLSrujRIDzBfoP2hpJD2iLM2+JTHbqbRqYp1  
FjSkwodsJE9NIAZlQEw3Y27H3b8k6P27mXmUIM78EOtMHfv8QpFizvxen+ehuncW  
/j9EOav4ssl7yjn4v8VnjIARjmiS+MMKwVcQ8GUmyLX/NmNvrFubZFIDIhBgyP5  
HVS/Nkm/qGvY8Q206URPCDH+q6mqB5PjBzXUqWfQC4ZMJ5s8D5J5tUcKx3MJ1Zabu  
Qk6tll88JUm738WLvrsW5KU64dlCuvl4l2vJ3XfcM8sAxlQPKE8GHbSpUayQab  
ER1r47fTKHEdU/XDIpoB2qdLxhEhtZjtsjzRbRta2r8AN+S9UJF5Acsvb+i128bN  
IkPfjv2E8D0ts6T1ijDqq07PpIiVBGMwh25grFDI4pLoRB02GyddLD/NfyD+q3o  
x8R6JRCxcGaD6jRNsx5/8BaXHzjgYK2W6X5i7r2smNAE6l1dHd+Sfm6D3Kvi5JZs  
z2ascKQLBUG8/TfxBVBI79KtRq00kJNSbo99/BURIV8R7/c4f2W1b0QhXdzvvJsF  
HKo4oPc5phpXH0HVN+LcV8AqTLunkUQfufbwrNB/zgh0s9Im5e14ZTKtVmyU0yc  
Os4h0TxUoIwNJEmXJ2axj5IcEZAR7hV7VvMm7eF9sbLj3v54o0Prs+oDUUmWNgh+  
JAP7FyoZZ4/q+q+eI90lQREa/XbEjkmWf85HLtmgwtHcQ4PufZ0VfzpIMV3Z95s0P  
LLVbpUIfb22oCJbVFnQHKj/lf+8avvNDoE9kqvAAfEh0GVbVxBJLdM8EJbuNYMeG  
/gzSnggofg7YgyXlrg2RpwfK/FXlArhVCHN7pJU9C7l9bptpPAbEF88fJQLiXAO  
tH5xZpR8h9wRiv16ADY0HSOpTQjw6rEj/YduUwMGEG2gzjz+bEEyA20zyWYx/NYUQ  
Rkw10CdJ/KwBY164bPcZ4a2byHRQPXRBfRhrtNPL7l/09ci+VBAIoR2X1Lp5JR7  
ciu4WwlZnTqVXWNXuRogALLdtHh7FroRETq0iVVI2d1eHsuQEEGvLRnj+Qee/LVQ  
Lo3itj+ZoE1oGZTE0gjUWztjcEMcBQdDGsW3akICamMc4DxN2bmEbTBgmhLP2zzh  
1zzz2kYzjd4GBXDWH0FIjRcXNlARH++bh55FGENTFh/KtWj5IW7sgDHP7cr8uVLq  
wZF9Pq7v7peNRpwjMD0ksN24qT+Q+ckl1qibVw1ZTBe9XAASIq2xHvborMz/RIrY  
kVR8HGHAM9s7EDJ/Xm52KiZ9FG4/RA8G0EJLL+YbHJNZb99JS0Z9Ja7vWqkk574e  
n7+mAf5WUROVffswmYHrJAQE6GrnDk2VhGefXvEOV3+IOsEEMtXi9gcPFY6QLCMu  
8f0sUzrmtaJqYw3AVj4r7RF5R91vEILTtqCNboDmvI9eOph4WQ9swwanYUa8BS4M  
airNYJ2k9A60Fl0bF0s3RRVRBxtL83xJ1nq1wkvLb8bjqmD/aIOlIh+f3irWfp6/  
xYc0VEaBxWGoTUvmAGehLzA0wq+G/e+/fDLwfZiy6bn2f07R052CSV0Fok9knltw  
c3UXTEfQwJ5iEGxLOmVxWLYW4xp7xodyUtwgPOG43kYX86DKt9Bb/4tDeGDFHcWc  
Q/lkxqI/dfX+ukhKwXsa2398Sugicv0eh1E1InKcvzGLYJsMTXyswuE1sgbFHN/N  
WPAsAqOnWHGW3iNiH6Hu+W/X38wl3FoTyPcv7u2WNIIf+cLCNd3f6AtFzitDg39lV  
RQH46z0Ubtcf5Yck7436V+cqKrtc8EAqrhJQgE8Et5ptkBKlyA99V4zaHGHbQjr  
TP5kMoso5SCBxvCg/rDWCdMwSaGzLg8yMdEgjkMPy9Yiws5IxS49sUILFY1yo7/  
hKTQZw4oC5s4c43v7+s+qmtzXsev8XueLy7Nooytaa7RxVThjk75vXhiQh3cS+Q  
Hil1chuoEB1/R4Rb418sgz7rZumhLSz4kIeeYKr8x5xmNR5Zm9io/JrcK8nvZ076  
djV8QfRh4vs6MvmFF0bBhtggrQ/da48DtSxC4E36qyYWDqC6vHws7/yIQYLgSPk  
mhMeJK00LZX7T47I/erjWySCoTVgJAEC1Lyk49bS4LIdAW9PXIeuhC3an3PGrEm  
WDx4b+a46Yo8CFc8Mm7Z/SOYYPB09146RNUfXHs0Y1JE0rFEpbWz0aT0jsyVWcyU  
GpCvUiRwq9z05JoBm588u0/Z3SMffFZPG14HGRc2LBE8zmEyrIP7JM1hvaLj2u5  
5DQznMSmWqh2zJRxjUVw+QEe5Lsz+Iq8f+q80ehtwknghQb85PuN54UZKRDSheAS



/00PV0aveDx5RN0J9FHITbZqto6MZz7DF9Yceo7zw7LAvKN658kpmDFI6z10s6yb  
GhPTTB0JN8AXcolpjIZftmw3V/Pj03APGGqZM2JX4b0xapTJZeDDYYATFRxYUkR2  
ZPaleKIVfR1vfUoKDLxMZVzDX00GhmnDWKDTgMu04+EeRD8js5gqCyMXc4PAMP9W  
9djKa/jeM4Lcjf+AY7pBeoqpybkVz4jXqd60g9YdGKU0FScKHieBpyZ0f16JUg/E  
RABWMU8XfdJXbxf8AwGI55WMJLJQvxFuxruw4BrL0n0QRpPmtYJ5DULf2TC/nvw  
uIsrddbEBRKurVLIEa2maAPwxlPsNWDvc9H23bfmjJDCz3kx7o0jRFYsfzdFye0  
PC007ot6tqao03qFPnZ6AKL1U+Wa1Dfvs17Zkf0aVgVE79JixbWofPJBK1y78Z6q  
RfLjgUntGvkfoya9Uc2K9A0Mekgyi9vSUa5/66Te1U2TSjJh5sgkm0ap6i0peo5m  
9XV0t77NjUI5QpQcAtXAWwQ7Ju77C6A1PLW0lceWavfg6dQbsy4xrbEACPZlhp1I  
03t/Zt0ryWDTaczglR3nN3V/AYLdhliBr7PwUy3fNVAr4WpRaCAG2ZwpT9VC/Ls+  
9cb90Z8yEFkFv5sYurmvXanPIE8iIvLyD8eFE2woYa/89eYaYQ1uMUg+tFhyUoxd  
VLX3jT079w2mpxw0fQaLiZ3E/jZljy2qJZ48bMPwPwI7H35w3Jm51ZDMwvUKkeh  
fvBwItoHjSLBA47k/MdaVcUYBWqdU9LeH2KqKiZn6lUCYraL0xWCipsTAd6JfwLC  
owm7h5ChTudMLCe8SBDvztES9Y+Vd3g7Gyz9errD6LZF0WFvMNCIxUXH0l5vlug  
oC/V4eyrbug7tcZ/NvYJ+oJyjlkYQq/lSm2NdvP6Z/1HqWZFGwQRO61Jw9dCs7oc  
QfdjOH74vbuq/1LNFxKp5IT/dw2H2D4gqtN3z0pJ7QwBp7kaoe6XCGBoNjMPz9M  
2wgYisEGrk61T0IF/zNBiIG2vJHiQf9prbR6LveuWAXPdizfyWXQrtJHJTB6mZw  
ajQ1zDiQ8EcBsFj1L8KndorPYiQrkfLo583MxfUi98YB1SuDxrNbckc5eoEhi0MH  
cwnKMMp3aVnvrRvrktqFRS4mJEdTPuBB7dtzlQVMlC8DKcPEnf0rzlWDL0jcalmA  
qYsoxS80FhGVGP7D7FEbW036/tdt+xORZ+tQPhZW6NiZtrj9g7HBNWjwzcfL72P9  
rN32S4ny9y91/TH/dw3t64UKyVntYboWcDhYS+RHoMApiqqhPD1r8xCHZBB2B34P  
YfPxTDI4ptFF7dFbZ8YnRACTJp9uaZz424qZYNC43AkrTI8sLz7e1FGJLUpdm0hr  
72EPEoD40buINbr844LKMcbEzLNSCLlap7qc5X+Ve13ubJ8B+iQOC4FnQamTFSb  
LzA0Zie6RLu01rg4WxtSWpJgVYAjh3jF0+Q7TkHTjW1mj4gW22jcAs+3bAkmgzTj  
X/uo2uIWBxL3L44R4As8P+Dxy7gThfLsZ91QQ4lXtyWJc132hCUVN/NfZzFmSYbX  
EDyI/rn27+96sCDHIsBiDDFE5oOnwoQCrBD3xmAnmrw5W9YinzLUvHBCUrPho0ul  
tYTFjpkI4uqOpj7RkSKmp7kWPvRZXduLmtizGz7Rh1KDpZVtxRhEad4vZK4k0e2U  
X3zB1+l1DyC04H/LkY8HRJTI7w2z9WJOnkSZ+G0TtS2hjS0SUoqqLYUCPKdbRDLT  
5cK/TSR56Jp/TZRFAqmd/XJ6XSf/xMUSB06LYLcbnZnfW5o1KC8TcadspEPqY3W  
di8q+y/4wkcKqomJmf3Qn+50P7xariZClgFV3uRfbhSNedTLhtPyggzBpLLns8nae  
ThXHVoRVL+THIGtESuHM4M5WM6JVCMMnsrsUv/CtwRL32L4wvczbjbInvxVt58Lm  
CCFrS26o2lSk6bk0VeELLSNVrbCmnyep1MFPqk3nPL+tEwrPAzdLT9DKbrNiWYn5  
lERx700YKQ+xjJSFjlrQMP4oTAn1QaJtL0W8nmiSHTGJnZfKU0XuGRE+JhYimq4y  
/mdeN3jFB/yshmLQfYI6BD1sudnBFTRo6XpZxadL8qwJab0+LGq+DKCaimMrDPZK  
efCSC7V+HA025JyXTBuF8EmLutkRa23zMHdLr2pAIK5959RoyG2rUNyEPDBkKFfS  
n0leS8efBwd80fDDwvg6WSJogzNk5yXNF9W+Y/0H62TF9JD0r1HZeJeh5DK/oUjA  
vtyhlEraKmvQXR0RWyIezJCMNrWqXL0+mULcsTwtIEuk3TnYp+5AmAffzoLYwrE  
87AS6JgbbpSLTY5NEzPSGSjD93+C9hHRuKVMjwJQkHy+Fum4eFH/P/ow7f+QODRfS  
67vJqzBvPDUWKkntHK9A12zKpIHnoqJz2DlxIPzslAboINeIf51lU+MYkpu/l+1G  
xv14VU5UfOkIW1P+XULjYfHX9joKm9LkrrNcjBfwYqEJM21KUqTQ020syCcs4oc8  
rOmreCkvnI5EHts4IhR86wCyBxt8I5d9V0V+uwT+Ozqb1xtsd7ZdaGb0qFTHSayF  
K4GoaYhEprMenu/lacjEs/FLTf69VCobnZl7fFEqtoLBSi7WSrBPYQ3nYT5QFLIJ  
SqI6RhtdP436XVQkB1o3QMhdF0k5VzqbBYiCUhfn4NVPaD+on7jnPm4Zqg5ZregA  
AmV25HmYHU9JTpC6AsKzN9wXriXwGFZ23687cKbRVYJRVuvDs0ssi0fsFAsZpjR8  
NQCysl3DWLZ8S7u8mRYzPKmr4uLz/bjXQv70Hj1ahebm55h5gmSb/QD3nQcbWQgK  
4si4nnZ/LdvtK0CdFkM2+A0fE5gZWomSq2VkyYuXyDN5iYYEx+zA945le01jW5Ts  
8Gc//uaRafKYCIFZ7D/DG5sZyPg/LigLh1uvx67ZrWmJ0993Y6Lq3fxgPGRc1MI7  
zpYUYJfHdG8lrJ0/f/jvF4v6nNDRJWONidyNylZsRNzJgMxWe+ggYPmJQgxvAj5  
LpE2RWmfSzmDupWVfY4c9MkNUob31gEL21jWGJw4Ri9dhwIeNYORMRyaE+q9BNpS  
2kmit9uTvnguJKzyehIr3hW9qZD1s2OLLYn/DqrgrY4DolsWowML6N+fvvJaZP0  
TtsMLMntNNyx2UvPMv1JgIMVj19aUAKzp7/uDAjsYKi+sTaedVGW9crIWTGXrtE  
ys8BVssy5jsKJxvK4pPG/fTgxzUN5cvUM8PZiaU7Mh1g6rb8PkdBczNQtEt5cMFn

Po/iM3RHZe/81JWwGScjQmHT8MQTg/J+2fLViSwaAQl7pt8p+P15v1JNAanCQ3KL  
LtAxsFJII80PhZ4kghJEEHgunWszUGEvkAEM40Rh/juAOnkU8KAwFcqmAR7zgf5Fw  
STjVkvN00tmg0wclN4s1yhyzUwHGxAZZKsbQ2Ab2aLehsZtd9xX0/78sXtVJApXG  
voHU3rEgK9KTuCySIZjKvdj9RL8YT7/8Zmpb/7BqKrLaG/ZkdT5R04IMq1RKRA2y  
xb0K/HiGjmIQeoXk5IJW5i7E1v1BSLkAIgXVm3RyAU28KakwmdtMUswT8B6WFf3m  
EtRWsoTzX1yPBESQ6TRespi6b0WA04zICWfeBkdqBFfSzKsPZX3u9jK9Yygb6IMY  
16pby9B3RocNb16MkgycJMG+Q+fctRLrnN5b0JvZsr+ebu5jNyBs0JaQr9ves0mT  
30WS8datNLDKdjpdNeLzRw1DWjEuK+7l4Rm0dvRo1q85ynE1JsKjpWJJtqMlaxJt  
sFWCoJF3nPin0qNXo/qxavGHB9j6raw8UUjUQMhtXrwBaaX0texlC1nUH9CPiv2P  
4S47wab3awuxmj0rwxL3PJJHC9BD3vILhfWFAZA9KbkBW3dBh8VqpqxTzhXoBgR  
Lf5F2+FpKYeMipHuUvLflpE9WYTU12XBSZ004IWX8Xr08yhv5a/UfYk9l4wC5Jq  
cpGGvLZqlrV3FCdUaDYC0ySW7DtdQ1CNTG10F7ekg8rxYxpBwYcccOuIxLXd+HKM  
HjBhm1Sv3f/oKiD4LFnHF022GwewpXSMxcaDsPsQvuoThp0FzYnUhf/Z8ZRj+TE3  
xmjUG0WHnLF0x6qyEy3/A0rokYRhaBF9dnWNGDmPQXi7Z56noZ9kvd9d5EfQiafG  
RRlAY/+7B6lZXdlfY3Pv5DAkl6TP1GUtBGL84BLXUU6lcsI+pEzFp0HHQNAZERD  
vB/zkK2+bBDR/oMzWqIpr2dsh4MQRoR4tbsZsWl9sfxP0owmqiWHydlzg0sQkb/d  
e8S0Lo13e8AW0YFchcvLXujhDgkB+6P+WAnjZDEy0Lk6SdFRa/7ieMRcRaq8fWuH  
EcCSaxMoXqvzfpVIEnez6fXu8G97/VkKFvkdPT650qihrJGt0hEnVP1AmQPZLnXO  
CicLek090KwY8FcqyKzE2ygTCBj/AXtxIINm8NJEDXg4+vc7DNcIkIo0qVPGNDzh  
dIse8WnjUm+bVGM88ni+w8vsVTP0qCHLEcTDQmJ8CUvwnMa+eNOYwKLnQJjAjIhf  
FdLwtupbL68mZ4MAXVe6J7eA7ocwnBoWTFHz/8vxLdsXZJxcnh6rgqE32SMLXYZo  
ylTG2DgKd0Kk2bcJ3maqV05Xvz2mP1DGnpaaDscHqHG8SEU0Jug+fMNDp5Nt+Fpr  
Pxgmz0fGxxxDEy4wPSToItg1cJQipK6HhNdqb02ETouw48NI00wozXh6xHrHK72r  
qk1z/dZGjPM9GMNQiBXo3jFzmvctcYD4DzFShJNEAsqHx9qwE1D5EI0bM8V4e39U  
tW+PH8F1XTDx4NYrB4IH1e9tTFDuZVNfAEzWvfpIkrw0guRjs8ahYrYrYUZJ1sjq  
r+SDY3onfQMRm6qUYegJBeao9WsCRF0juGlaFzR6IZq49CAZoGLZnaGwy3C08rA  
lsqFAzYR9Hr4pykjV+57QVlnb72JBFFai+QRg+Hs0aaol08lxIT8BhFr/gJ/737j  
ABU0/7R9hWz0M8dBSLZQu2UvmXX+/DSfXZMJbL0c3bw5/KoLMag4e95bHxP0tzRT  
S4H6r1hpefXaGh7T/BeslaPdQx1Nze8d2Fu9cX4AgUpsSo36fsw5iLCzPM1e2VHx  
YZQjEADlcBqntKuVvYfiv+POS6CDAFmDh55gewL75Ej2/qIWmaMjiaaTy4lSh6D  
yriGZf/OJ/YOXGp8jfdwLfs5mbB9KvflcG8e8YCLatjR4eCKDFAIqbbGuTuAkB+L  
TvkpeWEG6Y4i0x4eV3ai2P0t9XENAE2ITAuqH3lsMf8q531wL4WYBbhC31i8e1Id  
bhGDcPRNYBwXyfl1Yi+EqMwo5/j/20n0trWmg/NwbAXwACBphTEgtBAh688yy9Ff  
ob2h8mqoD01Cp1x3QaflINyu86jTRYwTI7Zj0qg0hVR4RrAJkQ/KPhSSjFaJzDDg  
hkIFFAi8Bmq7IkatN2PRrv5UeMWhMqkPlX2Ln7JNub8j3S6RKYeg0o1hXVyfNRwc  
dLR0VqwWe48DuhnirLlZ9K5inrxIoAerELaZITXCMgv5MBRBao17A3jaB67qbNNp  
YHriPOCDcx0F+T+Xg7zj+d0SdQ7vRKPVR400nftSuyoEP0GqgUh/jRx2mVReYeZ  
8i7gAZfW86ovQN3LAY3i66Tg0ib3EL3wHJBtMqpegsxWfXLMJLppydpaGd5NioEd  
PiFk+KQcnOx7Xz5NF+Iif8i/jM1lXfOxQQHj1PwQ6fmctxt+BhD+yyYKVEhnSDHN  
dnIOYMRMfoECmp2snKLZk7B15PA6Qw7Rp6QD0BvdeZQKlN99Qn5A5cGEUXUINmMS  
J7aWY04x8d1qVnLCFEpfEqXnNIXcPK3f0+k9NHguBAzs6jmuLTJ7EYpzKGjxyA9h  
IwxJv0WXcoVbAVgQvqeZ35/EN+40hLFC+u5/+n7kV+8cJssPiNZKNcduLE1UJW2  
Tc10w8U7HVWuAe9WHgmw2y2dP6+k2kV0VR65Jc3I/pTgQJoGSrUQR0bkpVJI07Y  
6z7eayPZzpUrJNjCDRDKL4/tU5bo30GzH7G40YeRWQAUV7L1ZNSwy0xXm/L8b/6t  
0w5/lx771gGSLhHlmsm+iwBUwYqBfqYnzILpqezpDgaRmYw5x3fcDTY1h7h1n1r  
zsSVDfXyWd+v/+qNopCj5DFQjLuIO5dM1eNnJejo3awX1Q3ZSaP7Bwe9FxpmeXZ5  
zvzPR16cBl0gahk5quYfgdJM1LSpk2+d0fDc67888aKlduIAijgIOPhkTt/EQLpB  
tiD+LZpsWtGHoIZNF9cp12aATw/ALbM08oB/cblyzHyj97yjCMfD71mR0RQq89Lz  
3+zPmU0PdOKZRMCTmn5R8e12S528GkIsNLuqKfk+lRAWzxWQ1b3yr5MY67PI3iBt  
6CXHG6KJezaCvCOC9gZCb1Tq3c8InjnByGx28crta89jqni55ekMYLjRZKRimp4  
RzgUhf0FdAEXexK7uvl9zakmQcrpk60YAw0Gc+jSrRMUneUiCuqFI/ftWFucT7Af  
BqKR+HluzAdBx28nq72b1g9PcESvel/Xfi2t4GoBYvT3EV0/ajBwD34AZ4Ihf3J  
iF90URNKfTngBDyHH+cX7LkXQk0DyVK0+G4YdSAWzhpCe3ZXL/nQiUwLgafQ5xk3

YjL5/bdQo3h2XaUu3MG0gCgdSJJ1LKoLq43oFkwpeIof7ZtFvH/4WyyoG2u5WQWC  
j96+iNauscpTULX2oRRm4UpdOgzg367NMjCeIS39+vU/DiXH3iY3N2VX6I0+5B/u  
Cnno3ulwsEHR3vQULUHfJEZ8Xwoh0Qe7vwXQL9WMS+oR8DQrvwVA9G3SMSG4rD0g  
fgNk3S9k1ncBqC3tkha3bgCCc1rm8boENRpVUaHt92WbuggUk21GQswQ8z6UdG1U  
wdXsnEMqGCHI009MJjTzd7xSSW+RjjtbPLjS0+Sv++LYxGPYyMVMNkywpUPBrhBP  
ELFWuncbCdJ0TH2mZPDQJWeoi24pUJlLqp9s0bTkFREEAH5K28s05kozWkXCdtNS  
houVV/AoKVNhtyXAZpXb4yB7y8eWRKIPKjImQvRbbEbsH7Hw16MjJcsL7X5++6+  
83/i/CfZjaseIE2GHF1vltfjZjGJ1/gAXowHd0S5hCzBIDHLS0obaKi0hIlpXhxD  
TcTomNNcwzINQHdaj+pHqX6080Xi25GwBnaE3ovIOGUJzugZpUY4uyb2n17PIB4P  
5HaW3YkGHUt7anyll801eNASZRrn0CQuL/44aLk8Fyf2pL3IZ0pAdryFEIffI2C0  
ELEYHbS6V5ri1uHj9nuU103PM49MQ3c4x9+e1p8oqP5aNS4x0qJy/UGaL01XgT16  
PSc7LsZ6hp9lmodLagHyIQc+mfeQ50RqLgnIUPnKBoaAtoEsQ4YeJ5ZcHtZ/RZKV  
o1KjoIE5NKJcWa4Uq2h0HrYmzlnYuAWLwiLMnRF0e5dPSMLUDicfGFzwV0wuF1zV  
zxmjT2A2drf4F00HLRkus0auYZWJ5iw8Zd57LZZZkkVXyp1daGNbKtp0Zw0ZnmZA  
sjMFs2twXmPHJ8ARHrCEi2AfJo4YobwcX3t4w8dXxIyZL/lS+uLntc1x4oSfSvaf  
OMKKe8NqDSx4NaKtrrFqyUycDw0Eqodavkw68RvRuLKTPE7u/Mn0Qmm0gAe4WN  
NReAjxaYiqa7z+MmjGs58f1izxo/syBJN3QdJbnQUQrtxTa1YcA2fAhg3AsvcuvZ  
KxJKEbVGH3PEmMPgQqWnAoH4j3sIr05qKMkWMf4Ffc7H2/OS+RqVm9j3JkNw17X1  
SUBCeilZ8eHSLPoq4ND1kL9rT4Tn5Dusb+86B1/ILlhuHZDU4bAGAdH+KIv0fRfg  
8mWSdzWYcqlycLwC0Rz1H9oDhCT/XYVG4rAEkFDwa9c3vZV+PNGTpmgsPGJXL4ta  
5S3IQuk9FtgBqK4REogSDZS8RA1ESU1GrTVajJgjUit97PSf03oo06kKe5sCEBOT  
tYt60tJDuQs4rwQ4SToDCb1AT2EpfSIV1qYzp1ofxZzAzQDibmG8/MvDIPquIyz+  
cr/8FSTJ5b+tGb1xLMhAgrs+BpznDn3CJUuBuyM6ieIL3B2SAwdmSdQM8z2VrsFW  
gsgGjTSi+v+7R30XihVixEwloy6KoSB3EvBS+Pmd/aWYRr6aKu5HX0jka6/Y8oBM  
WuM6Shbu3ZfGM1cNI42VzRLCf0DIBK3skP4A0Zm3BrsQaK+9B+medEP7/QDx5h3D  
AZ0WM7HMOisF6f60DgvGq9stn3ibTjmt6HLHG8a+77mZFJhIrOVqBYixzR9SiUr  
APY+VoecsJWWWWAH81q3bltrb/yq+FyLHjpAjYiCA1KcYunGk9vDLKK7wDz2Zv  
ZGU4cptUhrWnVtNf5+8IWU4tn0qUfrMi8rtkHmx6JOLgdmzG77cZxILJ8SGnRfg  
l5MKT9lltbWmFDYX2sLJcn+DyAHhIXsT2pXkHbLy/oyKZNuaHrOCBaU0rsglXtL5  
yntMg/SSjQhbzl+hQQQKDEj5d3qezCh3MEgoS/VoD0ASYP5d61cUwgi88aK8mDXr  
jEu/g7zBnHYqDLtFWiWNYB7WRLoydCU9c1VCvtwPCQdh6TuAPYM238EL8Urpv08R  
7jXwEZiNF2srQuudJyhPh6qPh7A+hmY8NDvWPxIaY5YGIaAKtUi0YuFGCZChz  
rx0001zd3DYtYQ1M0rZEF7IvL1/zz5pJ903YFCEz+wW6JBbdRPGPkRq/3dW26q9w  
V3FxNI82Pi9Hf5ya9QACfCKIe5SmDUH5kZwLCIfQiGzjJW/t19ma0SY61lMu5pwJ  
aePjilykB5BHD0xYLjweZNSWVeI/cFOSZgE8IGodfsbNxb8BAXG7CD3d0IJupwna  
j4jd7s3EHm7I91jBbvXfenzZwYqlvdF9fc0HsuHQMICCjCyDBmyhzcSSFHVtaXP  
dCXG4zsUIqC1myk5tmSpGdfIV80rQ/JBiRnUVHnLpK/qFoa02DXT7Fdd0PJbvq5o  
l/1y0nhgOQ+n+Uupq8PsQGQcjVMpfCLE0S5VKr6Ysbgr40ebn40YRvCIh0p0BiLh  
6x+UdKQ4DpEqLX0vAABt0v0QgL9eCdrd9AxAhte6HjW8lBYv8RJqWd/SdR6brSe1  
OQ3JcMI49igKaqwm62cSq80KQtD/7hfChzrk5ARQRt99ap47KYqLbniv5EIVzn7Q  
WJ3w+x6Bt/jP4QiRliowH0x9TvB5AYzVIfQPgX/M3Ef2xdwWIusaPj/p7is2pY7K  
Ckr2kD8htacM3Ix8GTHf2FGd7/cftXmtv3lyS21vtwny/z9oX4MnJh7xsfmvpPNi  
Zm2u35Chw0/1oxR/fFpe0Ax75PT90cbbm+N5K/grn1ztX5JvM8NZJLV72RTOHD+O  
OY12Exq++DvWsJo309BT7sw1ocuAd3YMM0m8HE9yv60b5zCx31i0LIVCL5vW6uN2  
bGh3/sAk+6dfBwccS5hsYyFDIi0sXmw2opr+3ppn0I7oP4rQ0zogLKT8uTRV4xTd  
U1hBm44irSbUthTPgQ3wFNzN0u0SdcFdKwGjJuLM0dYKt3lWoF8sh2e+4TvoixC/  
afa9SBXyzQP87Mh1KtPCyEhW5bVGvDUB2542MNUpZoW5/UPNnvYBSBRLUWWC7fd  
+oPV4RL7q0j4CK6ChuzOFEGrIOc0nGcNwiZn0QILnsllzxUNJgPCoRjDjA86+JXH  
R6HAcsg0IMtTEB2tQNGUi2uTX0oY0Ta5cNNQfYpSafHeJW3s/MkbNuDFLXRTMZcz  
herL5vSKkfRlkkqk/dEbZvc4JyZz+XsW2zmoBsh8xTKPT01ec7Zky0+AkRhuMmU7  
Vi3TJXXiBVcoWb8QKP0hHfD4bh48axYoJ7dWQ7JGSZZ7DRipkrzJsb2G0wfmiTPU  
1AkESKkCSU0ftxXZCFtWu46naM4Ev0EjYef/DqxtDfmL0rhgVVxeqJvJw44/TnAK  
g0qwAAHFaJn9e3Cn6mYsobT20Dok7Lnox1Eoc/OgLP7x+zXyam0Nh+3+luLA7V3m

hdr9SRgAJ2b0GeJH2hYGYeJ8M/Oz6isfwWv+Ga5v/6hVQ7GX6JtAYdzW208hwr8p  
10SYFnSfZYzJuMVTRYf4no7nK8myDmyiUsR60AiR20LL0FH5S0V4fLD4LJRLv3L1  
rS0uRhbedlEowI0r0/6YM9gd45SYeLIQy9coh0WJ5rgSHDSZRBuGYS1Pr9Wc1rnv  
MEBFUiy+Y0jKt2KL81onFa6zsaDF0X42bxFHEKmxVPHjx86ANxz9nRevgjLXUxfE  
ygWaYQ4qpnIvRduJPTDRtH5oWZ1WvduMe7IPojR7wU4/x0/8t5ZDgq2lWUoW3Q95  
NyVNB8ea8BKjuMdwAdCKzbjUMr7oRAF7ey9HUaDsk+81Afo1EZG5hzgze4kgsIw  
jIjgCE7xapZQZrBk4PGvSQ60QAmz5TyHZeHiq6IHsYmrLHcJM0nYA8gfS5lG8c6M  
sz+moqL7bw+6nR80TuyE/H1ILkiR27oYqHx4bEVJAvIvyxLSU/LmuFCUSItTh5w5  
hgtC9eM9umsR9B+fOGSkrtv16Zlao/ATsJf4/Y6u4MgqmUWMrIdPvdLnKwKo3pLD  
+5tedmWOHvUS12ckyChQTxJZ8VB64IDuMgEzn8AE8Ey9h1e+SqX4dP6pqrspXsOI  
Dt9jRCb6LACblUvberBs5PUsM/Hec1DiTxnoCFWRS7RABArC8edULGWJW3ydtAF  
yULRCsWxw2EaoeAMlEHcbZ0jGQxMn94GEj f3CyqFnQJqCucY8mA0ry0/+qSgJv3  
jiMWSswcvUg0ZKJqz9A1AKr9nnK94/HQ5oZK4t73KjAm5ufRvAwe5BCQn2pDLM/p  
E87WK3xDUEXcwImfdSLAkLQrPUPD8wsLdA1AV+7cuHGXXLEJRSQQT08s6ss/KRs0  
LxU0oeaHmxL1sSt7tMdOwKN6su56MYIERhnmIiLsNpMJU8+EgpgidHska3VoeUb  
Wa4mNWHJ2uv80Xj+yL2ncqgdWb/qaVTLDaaxOH60Zzrmh6AEH+KqU+bl0EcFZR2  
EjyKByT33s84T9e8vZdLKcLEckAyUSfwoaCyxSQM15sh1SRsuwvzR75DFznjQ0hS  
xKo7bmQMs1TNHHb5Cnedl696HNF/ZgdL+31HM04hvcJgdVn2kByUV4LT58kd0YVw  
VMib0IL7D/l5GBpwwXBauFYRtiulk8V3m9/y6ZZDM8h4LCSt0BtNjMAAPhB/YBxY  
i5ry1GT128desFrUzyt/B5WafmBJ8hgeToGjpYZEQj/veV4xrZXamyW9rh5a9fVU  
MWulc/xaSrocTpt2NnTu8W+taxoEh1jfbHhyN8iTeFNqhB1aBytDqXnDQE2FgXns  
GE5/3Ilyp1aUwQBwo18poui+GZ0QDapDvPgJW2B7VFR7j7Lzc9Dd+Q0u3ln99Ht/  
q0ft7LLaHlW8nE2/Lo+DhfEV/uWyhA/QCePmT0LOC4wRoJdapHfLYVEePe+tbD54  
ALLXcNrY2Rr19XAsQ/4xfzBKik5BGH+Md81Aw7tMG4X6wYswuQq0tPSJ+Jungth0  
9j0TYJYLAJdKRGsVknAwgdJz3pmE3h5NbpVCjxGXuNq506r9mh/dL7n4zyglehc6  
2PnRJW560pF3WYI2X+McSstgbMMmQFMM9JyhsgQ06/qEetplJRR70T1K+zzhzMrE  
QVMg7wSSb7StS0eBED3Zx0ahvF+XQEmWiv0ASakC1FRoEEprv4L/sb9a2nC+Z5M  
XXP3bIK3v8FenE6KJykiiNXs2Wl0Z5YFgb7iJXTcd4mvjuql3RPi552quaDuc/1B  
pAF/0LOc03vVUusqvXqj5pZV0iaMg/QR2BxMQQ0f9U9JztWYgpRhvtm21ezoYtLF  
0XR7jHa3E07Hn/oWjyblYBQ/An5gmiDFIHv4qUGNHVb1bSdKEP5H80ztYpkmBl7+  
DtJY8tDLE6VEHXJK0z+vsocmr8Ydd/8MDTD5gj0kCL3iGVTqHLN85TL5SiF0LQc  
9ZSf0R2YEA8wzd/Vyy+VNNnCKAul7SfJWfz+yS1sNhE760/QmRZBx/IdaTF/lzVl  
clfc6/hHfpyBjkTm9HOYjl+rNct/LfSVkaY4IrpqQZYH/dn6NIS37XVB5CNtJFB+  
f/rYA5T2EX0tmtgS12QJvtJh6IELvOo5i0ZeudbXDIXfgwa5jRW0mci2ytsqX1oo  
nnrg7tBrtifc40zSUU6yfcvJbUtNqSpBUEkP6u2I0sFtUjQXMVNsoN58SbvWdgKR  
LAN3KyK00sz7DiLJCs/P/+xDFKzahLz0DFSTWJ+Ua9m+7y4eb/0IdrZV/2qfX7Mz  
r0S1biGnIsi+04PX9W8qcYZh3Y3Ro0/CyLJ/jl0M3sAv41fiKSDqfdzBbgU7LwLl  
MA5JZVuNcHj7HNeFdURE+/rZo8JQW2W4NbZcGJn6EQJ+OGQCu96RvCVB2FrmKdOC  
oHCZhZ+P7eLp4R9DqySvCLE8+wXJRfPxzrs9L1zj0KP438X/8ZBP6Mzdqkpk42B  
oza1iFR1SLC1k77Xukif4D+5LL+aCdPQY+GDkp3HnyFkQv3C3C0xoL1Ij4C0Q67K  
EiHq1p3KBssPcRTXVPK0wXefm8ygGVRHF6wbl2s5nHnyHay2xW3BopHiSV8kj/2  
tLz1iowZodWSX+q6SrTMl5gLkSsdYogpdXqTdY1iGi0EYrZK2Lx4rk0Y4E5hS1Uz  
8A535DbY0StmMe/XXuEhna+Z2CB0/OmNIdr9t5mhsMfQgqUPZ/7YVlNLoZkPRlne  
4wphvNeQV5P3qBNhy/IxFD9dfvHCTaxZGBlgub/jrcXj85Z3IQmuGK6afcX4NlP9  
AF23iXYU7e0xbR7mGYGNqFEebGw1HhY90ztbHdDM6v9PAeL/TwRctBSTPd2Y9bkJ  
mcB20FIUd2z/o8AddZVDFr9U6DtghSPREqKfyA8R3Uj+d7knUwCIfCwhe7K1KAA  
XVNA08/HfPt4orgPkKw8FCLJSeoEPpkJdkdbKlJWCdHUo6eEd9+B40In5tBoUFJW  
BDbw/8DVPoryMZbeSaZsQEJk34ExRcJ+K0xJFYsepW007YC12iF4S46c6i2JcHY  
xcrnzbhbj5634eHCNNIMwUmIjLTgw2uywxhUi0Ey1l1mv+GKqrmwL0sPDq6K/C7v  
7DyB5C0wJpRqelD7p9VJvtgLOM3T+igFMX8mbR+9RWYIOZ0JlswsW+H2zYxIc+Bm  
XCpMJS+Nq0bZnqFWARmhiFWunbAgED4G8lDC+dn1oH4jEgnUe655FB20Eg7AnTfm  
gbsc310bWrS244J3jnGwDNKsv444rXuCiXtsAVjL+ZlfyEpuduJD5AYDw0rmErab  
3iFIVmii+MHv4MRJm+huBnK45qEs/lZLC7DEmGTBBTH0hVmEBq8SflqqNGJwQM89



nAmqB4m3MwXM5k54vbAt5Mq3EBxTgVaf040nowai0yWEvtw5C0ijRC5kD2NPaA94  
X5WE6SSnIm9NmoXjA2JSSqrRfWLZYRa0BgpPpy8RadZn0touqYACHScZiZAbKRNm  
52dKvcRWsVgM8pkdGZvRFwvRdRE3vIwcrN9FzFq/TGMq/UoWRujwypAYkGFEppsz  
pkMB1GnK5hPGXuzkJ5hzJTUJq/RZ7ldYYeeP0UfZ9u/fbgBv5bb1JPWghvbgZVRj  
wLTsNl/OVJMT8WKIOAzmIDF+rQwAUeEaCneqcHgku4BUfeKq92TnGQBh5Y/mVxmU  
I5bUtwfN5XswGSaNeQoGLLTFTIgxVf2a01R6nvxv0ICpwYhY7XqngBNNuHneLKYN  
F8Jem2C5jGW7pUbYaC+K/n8Mf+21znutxY3A1ri1U7u2RBrWGY7zg1nIm8e05jOg  
H2U4jZ6T5y3LFcbTKaLYXeQ6xo+ZGEfaFZC5MFBsSEyGQ0R2BRopFR0zuJmoN3PS  
yMITuXFa6zkwIE/iAAAFWohRE6zQrYY0Cvd1akpCgALUTIisvc8ixyPdJ017dKNS  
mC1hInLmKt3qNoe/kxkTs+2D2mW4fNqXxpXksfGkLK5yo5r/oCKIzRa0a4gKseo5  
rVJYJmPThS7K248jqN2CbuPyeilwipnqXA710uqsBmbNic/q9nGg0q3fKqn9wkV  
TCs6uHErRLDusJ35J3Mu8FNNxtYf9WwIhkH1X203TYOeWeMa3RUsOpnuqI0+KdFI  
Wcxa99Z3Vx85St8b+Wf3hwETRCztjQeRPZLF5DtFJ0mmIeaW0yYGMKJupGv844M  
Uk93PuRKMznk1CIKXSQUp+kk/PVLMC0mWAYeVA7LZK/9oI5y0di93smZF6b6D/8w  
h/ku4A2/NDDy/AokZdWJ/WXkf88HpTc4xqhb5LUGHDpsFcZi9wDc5IDCWU5n2znX  
IENz7Qn/TaLQCVgfJ8F8rOPcrk3oIRkzm5PUI+UTTyKmN5b2y15ZMCx8PDjNtIG  
SwGYhFlIMX7DIjXcbSf44fnGJIRsdSrQfKyJfVXHMqJATPdowSJyzgkwnsE9h4IY  
oCItjqqiYp0dlWkx5hoR0puz2I4PZdE2aXvVWAwf3DcMulZqm/0/JuebawB80M8w  
n4E7dZ/X9sH/jrp3yokLBERXk77/l10ukbJTScv8VeIEp09hqQX4jQz2eIa0DTXT  
Nv0vEa1G1GccLqclFluX5/y/INLE0CsV/PhrMP8RQReRJTz4Wl0viruUGZbeK7Mq  
0Fq9Em474LxN/YKnSVw+mfl3SuK89VmsG3+0g+Y/V1AcpyUELRT/6iNUneMe0d2F  
51dPvPrei1MX58Vo5ATdmFd60G8zCIomD97FXc9/FitFR0qe78AumY+2XarJkhc/  
HF18w4VfeJKCKh2BMvg30vI6Zhoo+q08EP0hNCuNAispotnZoQXJ//a9BHtmECJB  
FnNRxQZiBg1hKWHSV1XdaSIdbF5qVUIXmfy96LxsJnFB4oFWcu5UZMXQ7DSJgVbA  
nuitWty84XeHfFmRyk401UmDGMxagtsb01DnAJ3G6EuxW19bLT7XGqfn7AjQdEPg  
loC3SZcvcPDC2C2lGgGlcSPxiV/8l6ArmaXFP5vn/gbtRJPG/9LxW2CbZysPpnjk  
w51g7K4osMgGJpr+ks1GqfzRyhXef0+z44uNBUj7fEnUaB/7B6GC1+rbtzzNkHDZ  
ZWAPRU23anfM9Gji80f70xoXe7yaF0uuksaIyp4aswTGUUV+CnsvZbChp61l05u9A  
akBdUyfRYKLBNpPG7JbBa2eTVbSdn/o2btD2dakKyPHuiGwLsoTNAKp1XuQT2Yny  
gwM4d7f4ekf0fsW/6lmw20u5J3/uScoY0grF/TgoXlsDTK4eaDWQ+cqsfczwUBXL  
rWEI50FNX03ulyp06irXD8BTRwSK/+HUX6dVmSzeZB/6BoiwEnLgmi8uKFvBZvJ  
b1A6bo/drpySRyWlmgmrgP3zLAYWRLMOSp8T+8C2z1EjC7ESdio0+8L4MwPzaCpKm  
6V4pBGRB3mZf2ziNe6/ko0ZMbixjddquFoNCVVXs114j/xyZ3DUy9C8HuPp6SNW  
U80qVToV3BeWgtM4yJeDPYH1nHbKcBZoJ1E1YsRUNtdDQcwyDntLnoFlpG9UDEoN  
fHqVCoQX8WN+hgYB7Y3YpbRM4vD8TgMABYgw0Fi/GI4nnvqAzYUYisrJg+9TwJkw  
ptCxGl3xJfibittIn6ZSYnsqHo6SmSksHLtta0YGj05rk+YmbidCLGLP09hHeAj+  
lwiN0eBTLAo8dxSs2wHd/eAetcN6J8IKs1vKP09BbzXysUM6RfwXAmnVYJiGypmd  
ySPz5sC42X67o6FJKQ0SevPL3n3YexETMzTCdMJ0Q6vYHUCK6pvUfCiPH1vMNo72  
q82qQMw7u+EQSLKFZvmsVFz6RSvEBodKkMRSikqXQHDvo+QoddJuupT7zyLfjSSz  
prDPqGs64B4DfSE34PgrR0zasSyxMMWdTNegTpBYhF4rmsRtltMc/ZKAzVAmJkV  
DknQ4QmOxenlWUAxxCsNRCFNWUGPIaJUoLvCxQNqHX+10F6zb9XQ89P7XrR+muhW  
9nFQmoE2EMHe2R+HIq/t7APLJixisfnHDDT/FeAqznCp09X7cR5y0mk1azlRGNTs  
YLshzyf5+aAa0MIcCpyqk0Cnd8K15eP9SHu8/sZiqSyX7EhjenspBBL2xyuox2y+  
L55G0oKoudQqIZQQQOE/OVatjwvoZp4fFJ/v6rqmjP7JBQQYGTQz/eHmeYnzwLCx  
5R+w9CoHtf3/8+9hR2TLp7WYAIVz99j88xalsKEVrqwH9zDpFXt2Lf84NPiUYfxv  
bxnA+7u9Z+Ivjkq/qQFNLLse04UqLUxA8eczSft2OelWkehTxzN8CPwAhLE8huZ  
5T/nAC0qA4nAXEGndat7I5z/l04GIzil3FabIGzGRi8u4DI1rl60Jlop72czRh5  
B0+qtXydkngl8oyPeNZLdiRU/2xP+5szwBfa6xgAezNVCiLi0d0gD2zBBHuC99dw  
0DStTpRE9LoBGuA3B5KN/VPeMEZyc/rRq8Fwn5p4LK5bw0Ci15AonwS5kyiGE22l  
kg//8U9uiVyE15JYTIQzQayVfKcKJ/TqFTLw1hJ/AY5m3RQ49LC/xujRjZ97sqgv  
EWpVb2Uf9FkDWHGREB3DKHKysQRpBGYPABXpGqvQDiCEHmlBm8W3W4yaUETndPBn  
9Bt3TIdWrMs5+Scg/15BKg39YvDwaTYMb2sicYeZnf+2ruI+8dD5eimGGRvOyUa  
1WeATPdRB/mBpHSIqooS4fQTiXFTxdwFneFs/iXrAzakSrKqHDrbfWh4BDT3If4y

QlRx4ikVUnD5nVNakSm5rgH+TAWf5xLBpjh0j924xZed7B5lF3emDP0X6qv2fsgM  
llFXnBjxR/hx8+rsrcpwzK0IRlyk0Lc/vuVCbC5ywfzQH4ucfhMEqkXD3X4azTl  
DqKwMxetB0+PoyHZ248EN5fF9upwRxM/l0P4GQgpy1s5c+rm699cijduaBRGvMVD  
TI1Pj+4GmSizf4fk1hUYIcNdeHAwtc/xMUjWHF6njWmHzljxRwmIAtFMnWi430BQ  
3tm22XXWVrqmtr3zfjF7jY0sWBfxH646xLBtsgRSkcZimiwjLXGkEem6NgwAe08d  
vX1EI6QXd/ptcJnGGGsxk6TYHGmJKyhyR/06IF7yuwEHYuT5a/fsVAuMFuqK3hFN  
zUwIqM2k3A/90Iw5kUxTgk3AAvGu1uboHxI701cMRvktUAS34WPo2gWPXKkrGUm  
pVGFfQhs6t0d2hl4Ey+ZMJwN160yBTMHPIfStUo0LJS3oxsttz52ThwzAdFYsmA7  
13/b/J00TChCvjblDEyQwHSGshnDsICz0ZqXfc2alt3RBv81Z0bgPLi1Z+srfvV  
vC6M6DiRdxqZCtEDx+PgCNj9BJ3XlYnQGXXn4CxcBobuDo+Uv4+0oUIYQYnfAqRY  
Vkaozbf7I37SRML7f1io+QrSnlrAEbZNOQ/4XNpV+dSxEjlSbalrTVv50f3SoQMa  
Zm2UgW5QC93NLnetVD8wa8fYrJr+xE8h/G5N+Pp2mXHz+Bb0xeXfJ44t+hpWXU3U  
RTFZ4GKcRzBRlCgrCqYrReKWgoU+DM3jbbFEAnlL9jq8Mw+lgwkLi i/UR1uo7pTR  
YQJtDXb0g/t0FAf80vnbT84BmDa10IaJRod+kY6RMYUjzZ5FSjxQ8eTouQPnArb4  
EZnaNaVh2Q3J6PWgY9BAVKjFiv47oPOIJ26bvCLwLr0J634Td+9m12D3Y9lksBvy  
KBwWHBL3yflDExQd9U/tYw59a10wPLKD0WK/fcNKREKLnaEOf4EmUUZHHiBLo2FS  
Py3NFQUULqyngGW+5P50hC40/mVBEENYJZZ+svKUpcqyDsY8u74+MvTpzwC2kdHs  
xL7RUOD9lj7/gyk7cIfoo75VtRSZB/m1/IJ28CgJMum11QChek7hEkg0B1/+d9Sm  
MDuh71fXzy+5/EXBdZykKGSvY96e5gQuZ5mqBbG83PknJtceooD+BXz0zyP3UpA5  
LEyxI6gqBzL6r2LFacBY0LIESB1ZGz4MLzV5rPMdNmvw4M60oLU49ES6jczfHww/  
RzuXH1iaxNMP7vSHF4aGcP7I0qGBYAcT9Nf8dKcBD++nlef/Aci8NQuQ30r+Ch+W  
l1soZjVzy7ENV5cvVnpEbE/jmLhxU4pXbkXxbMrLQUCCUv3afcoJmGYfhiFqwonM  
laucpamLRvili7i0M9HH4vh3dIYGbJcquF2wzB2EQFDN9XGLUkgXb7ZfSd2IXd8F3  
yc1nMTDyLICluTV55iwl7WvLQyOGUXPHMDqocbuqTdU42+00uJX99fsE+IwVHD5Y  
T5ZRFjKGCjmlTbeTsqq3yaB6kJ8VLUhDJneh2x0M11/fvFvpUulF8GrpXSE/zsoS  
v1a0AEfgm/e936Ff7o0baUxz0+qbygPxB3jUyJTEpT0vVQEtCqi+Pj7LFQU6Dory  
HK2j3StlQ9htVULU1ujHtbo1miJ1tSGKjpWX2a5zKBG5m/PgeQngTVxUYA9x410u  
EUjvWf4Jgz0aAzqMMONoQLUpi7sSSocMoB/76H9g2AQgN+f4FJQ6wAz02mZbYzLF  
a3IUgoGE18oVhBA0kTYCI1fUI1Ejsqe/4tjRNQRSCn9V59h+aziDbwiqApMDSBEWK  
7MRqGkuUNXm5StklP8UMIAX9D0FLZMD2n4UE06ibYXxQFmwZLjnf0EUwkRavBhxG  
1apW0Wisw5b7l0DdafHp9TH2LJPV4mELnATLYD3mFxeUCpiksc3nbMlR69f30xgK  
Xu0EjTk6dnraq1GVF4FyjpP+A13VJyYm0wTxpsiMab+4M1d5y8hPwd0G8Xx/yTEl  
Kldtzq+Qqlh2DkpiUiHC6s84uXXyV6WPE89P25pE6viZBAWh0sRumGXPr9eKuZnl  
EFtz5ihy/5jIDV7vJn+nUvH6T6Eym5YdEb/vEjgHCysWoQKcCmChxok4m1r+kE87  
BMYSXnSt5hrP4cAom5KR3b0+Y5Tuq51vHbBDnrR5rtVJkEsGRyKA8QgiBchdyRZ+  
MtIsTbAwSngsfl9it5RQWLZKQFKExrn5P25k5E4Jabv7ShVTwR5ss9jEa8SMHyu6  
P/vXGMNclmqlL10eKLV/iyXLCd93w3nKERSw5yUJ6fZJuDybuWRITtZwcDkIHug/g  
EBS9e/XW3iceSchPeUOPSaz1eNXiG5pxJELyDhjJzGfLad2o5JRSHk16dYy31nnS  
535yEV+GjaVHJNMDpa4JzZw3ApgA25CSoVe2G8LzOwdRumGxxp+6PXym0rkri10B  
eiVMGAJ1ZICq3Uef1D6DqUTGL0KCDgJGkAJDmbTy7QWuFrip1wJqxk8jN61wp05o  
HpMfE5Vq/ANlH58f/6RUtT5PhzQ8q6IGC3Ye/hxQlpJ3hKUJF0cqBgYiC4btb1E4  
7nzb+MbwmDbunwf+c6/NO/bUnkkBEMpa6YCb7YIoCyfYANv26DIJiKuhpDjU0xKE  
SsHartCKHZLKJerafi+SgVBRSPAWGqHudBbYPyqWYQ9ZQtKjwflg/rC40mQ6w1oZ  
+JFuh5+Md9g+mh4p6z04GA7X/Ry1eg7tK69qCuWtielppDCRngoBkThSCw3ZiCdL  
OegKsLNhE7/Ee0rYEu4qrmQL0d0WrEc8DGjLV/9n5TuPH2lMXRdW7We0xt1NpBuI  
NCSDQHl7I4c7RzCJb+y28Z+UszZ5mh2U63BPchnpmw5HwIVnnBinqMnN8s5Ft3+j  
ZhGglh0K3+kWcfWbHBLpaW26d4Vn2N5HVjBIop3lo+eFyddzX/t1jcCbfbw+lMPrb  
5tyoc2YnEr+CjlGpV5VKubksAewNt8j+0/jarabHtLLCRccPNut21dru02DeUQPq  
xsdLF1ArrHFw0JW7MnKNESlv3JmDIOldDpoX4mod/jhlxpRobgyvGho2rQs0PaJU  
5BBTCicxnXzfJNmn6H+ouCZk64yuk/etbwadvb51Zx+8qXEPUK/A9Ht7N7x8Jjp  
xBpieufJDUBY63TYdzPKJLI1fpduKSOGQqjC6nplmmQ8ofqkphbCDpTLXYA4PoVJ  
a3+R0YZNBXIn0GqB2d3HyMpe+tmvvXKyfONm+Zyw0ILRjMhmKBXdVhoYmSp9HwUU  
ftUGUPCKZ000Imw/HUF1XcMR0jF5uITukBdYqHH5od1tSa/EEq8PXQfZ/0sWEaAa

ZWeWw5x FqUYWKGXSbrEfU8JxMarmxZPnl/afz/n3za2AmxHmjFt0UTf2FfQmVPh4  
3CNTiB4XLwdh2+AW6gfSP7dyAMPX/TR+n0ugd3zG1+jbEJ0rXC0kIR9xIo3sn3U1  
IfmCm7DSM+kT+i6mDuEZ4RnblE0JAfcIp7TVZigWuKK56Qz+gEn/RX/yaN0lHK5s  
pGdRKUCRJ3vdQXq49sf57NlyarjKT3RIFmLsbC7ExjgylIGfweJwKynl4Y2U/LAp  
BW4vW01vhwAJlDoT6Kmkortc0eqg0DQBsa9PHyExgR5KN3mTI1JHDDYvFjy0ftIN  
6iw7BRkdorP3IWfxzqXJpWgcSHlIn1EmXdCCryVKr9Q3igdVhWhax9LyGTZvAxNo  
AJGurkobDbgSgqG2CmnrTJiKZ7Xw9bRiNMrwtbykV4a1Rc76xuVhTY4G33H5o7  
+Sw/kuWs+2B7cPZB29i01skyrSv5B80giam4DAnM5DU7su9gydKigVMB8hQULI1N  
iqhJzu0SNBbDnFGR5ymcr3uxMX670dcyVPgKdq6VDHi+7u1iX/eT0Wn8MVApCt5o  
IX3S0h34Sf0z4++A3CLrWjmpD5yIMX+gwf00Qp43rgkmL8jVM205tmylGVZCVky8  
mDktCbw3GUCwKndbgv+AwywUhzzhXNLqCa+NwpeZu+ho17mzhBiw2qxKMY/lcERB  
ByNr4tBIadPze6Mgpon21qtdq8XSMJfAJKm9NLRQcE+Kpmgs/Tnv1FDIPzNy1dwO  
ecBefsI2xSR00Cvm9D0JJxM5UZskljU2UgxDXWWHqE5oQNRKEuMBBYGgeulH4/6w  
8RMg3T5Zg1CKEyFLJkTtm05xi4MiSnmGodQLZy4Aq2/vcqKha9VA7+Kc7MFJJqAb  
0aV/Je3Za1vcY7lhysyxs7uNx5B5DXCfrA9ASovtUdblvahHcn9M+hatYFp0cy0jw  
bBGS25E6m8K+0QuDhA5gXfglhfuRdwL75W9+D0kSP0p5L6nHkWTIA0N8rEs0eTAn  
AwWy5LRCZUIFGt/qzRj5CdCy3V4SsbCr4fowR/JAXcU/vo3+37+W4n8SRkof7m9  
m6X6EAVLN051kT6rCtHHhtfMZ7u3GQYDyVEv3wK957iE3ZJasPgWUSAnib1BnayD  
elBvlqqB/r3dLIgt2Im6bixwyd6xWM/5ZpC4Wtpyq0EcRlA+0jnKkH0Z0Ns6F3d  
24NP+ZmPxEOlIqgx+CU/GSnKEfcQ6oi/Ni68ZTSzgPoHceYbc06nXK/ldgrcny2n  
t0xUcaQS120k0TNgxDcamuDjim0ws5u6iBZEQvfH6+Wx9mp9/FBVGPRNC7bfIzNbN  
IYUW5ljDJD7r5u3eT2ZAwjIwiLKcPV87NbShzKI8T00LmCCSyuME+2Us5bGwRfpe  
4C0Aog6YyLgzM0rpCvnlXzvJm2oPdVt7oP/vxHMzCB6KWMzxwMTDAawdxZ6P5VSk  
GqtQecLAWutjuN8YDbnpW89C9IiUaX/cMYUAeuxCKRlGtUNnYI9B6WpCorlRyd7W  
oCr1eFr/nzjQhm+saVWo/G1swPZgFlfE9JLIZ2WJZ/8MP1Y37LPHuH+wE7R7ow9a  
IDs6XGSUqwSelVe0Vx9fEFMLcz6JhWM2fQt2ewureSdjxrzzGMXWVl5zCkr81MYV  
tY3nT40HCOM1yGtgZxForR2fyyqzSmBpZZBpFzU6YInaq0/56ZcIA4B4dQhktvmw  
QneykByDdJ0ufa+WNi4V2aN01g5UM1/zIhwN2/izN8LKqB8AAICSJD7sxLGCcmNT  
anQQLcXxyjThMmHbp5yMa96rf35M+QcqcDPUujwsLHXpJx6wqAJr+rjdVFrwBrRB  
RE3y0wvPD9dmXGS5f6s750f5pF4HeZ01P8mox06cZnZJ/r80YDAckTfaS4HUaqXA  
X18WrqEMLB7dEo0UtM/fkhTjNjz3l0Dp2ssCCZIi8QMLmrD6Y1PjRHGy+QEuW05M  
nS6cEoPzp+xF/nJ6Qjw9YZkhjxbzmGx8hi/o3C/yqxvSEGgfuul2bmN/NI4w0hxb  
UW1sRkdp04TpgLdnBc23cZ2dmpaT/Q09fVp3GKhdpLu331r5+7or3Hrydgu15cPs  
3TDenU4S5B1bw9PsU0+7LaER0erFrM151o1QsXclOnGkaHmbA8ETIoDJkmpPX90+  
Z6GcSK+ZW3a1FNaXxjFijUG1DRo8qd16ng7kQEj445sk4aY0wwXZaQ3ZY1RAiNK9  
5CLWANJyfkMGv5JiKWpUDAYoESXP1sh0Dz/iFPzwnA9Dgx81srMsnPxncCVBAGNv  
tK3aWsYXZVl//2Tagqlr9TA5YnjViCtS0PVkfp26p8a7vUxsLJ5XKdLpBujb0+qn  
sh7A8d007ZAMg99xcNLRAUbeG0ZYktVLR0i0uKG7NXJqZVLiByakig9/t4ZJ2VgA  
Avk71aayVjga6ziMquZzcGNYePByLcmGnbRddc50gqmQcdBt9znd9aop/FkFA4ez  
+KF1I7TCyUhIoRka0z9MUjYjNnIugxj67i5tDjHYUrir6bPgNyR5PsLLVhXspJ5u  
pQ/aHmcR01CjL68JkDixfP9JWHDa16cjVxkILoPv3k+Q5if+GHt01auj046WXu4  
kcoDIKVD1f56aJJja5A+twKLYsX6CBiNx0JV3y/foSSDJGW5veLL8+IIXfvFSlWo  
rth0wM2/YQ68sYMBhr+IQcpgIh5e30DNf3TwjUUFsFOXt6zIQmZn/Rp8G7cZlWfx  
u7FK+7nPUGVe7ImWgFauumzNwCS3j3BhqR0RwheBhoqZrrEezlIxBzzLy/YC6dP9  
VwClcRn4nWVWLbEWY9UgpopKyktQSXu0cXsiH/DaDS7Px8f0OWqxnPrM9vNc19L0  
D8n06Yu/UmGPH0ep7raAWtjgVmR02LH4JRHCyw+mcwWvjAAjMPih3+MaqY32aPz1  
yXsxrM5yWizEJl+bFmk930V0vGESKxtJ2ZozX1f0JEoESHFMKQlturGLMg7hztIr  
Js8Uz+X4oGNIRrFd+3Ty0u4IYyJHegcdK9dcRNCe7WqlMr8Q00tBxr42mi+pYqg  
qNahCQaSD8q9Vqk/3liXZTPL/2Fsi1yBb832DYHwiYz3zwt98RFcKMYb1uwDeNv8  
qoszD0EKEdT20o1I74HZbsp5o4e3vBRrkLpUNzT2FjoBngaFU7RYyeoqcq01J69  
xKlrcjvdC4x832EXwvt7hqYFo9fZveOWZNAPkAP2SHRYJmZ9NW/CcYH6MzS58MLY  
3cJGDLQBtXt00+V3nbXEVbW4XjXnaKz1juFsRVR6fyNs1qn8M9xZDrhxZr830VtX  
SjNLAtDKjdR1qeo0gFjeTogAh6sngmnjnpN4GKMTFX7tU04lWeL6N0ld0mmtP/gu

8rt/ASgJqWtX9j4qyutwCcI92HZwfznq60qv6AnmeCFBCbJpL9m21tu87/HGpFpI  
JY0UcrJwFvkB2XPvGjn0TFdQb08GYUnjswqqye382SqcG5DDn7xvEfR+9J3hQCqB  
sMYSdTK2s3jB7BCceGcW+YsptB91liBy4W5AEqQCa+Mr0jRvknjxcSXf7Pt/i608  
BImedrjGQkw0Q2FdBVp+nuY40cQWSUKoDuRdBUh0G2KVQkgboarwjHlK8GzjKW8R  
go1cAi22fz+sTls1hqHfYqXAcE4uBYRr1K2dp+Sj5GzupDbS5J6t4ZWfHQjo3PA  
1ezLDqwlQwPtNDyeR+2k6iLjLXxrRZmjA7IX439ffn9/heLrcujC47cr7BENZl98  
eYm1LSLzu3+GSctYVme4bAXWCE1aMebk8tJvvklk+o1oMfojVml4Jd0adk7BKdGh  
hPRd0JW6tK9geiayzUgZbn2MoXrLUdGL/bvMv8Tq2uD0o8WGD7NKQbQtDTGpP9My  
auES3T3DfK6Gkodpk/ueBR49e4UUVlMt74Qn6KkCAJzWubYJxos2bIUXjhYr3gBS  
RigNz7346xPLaqZR4at90PgmYnTg8QvH06o0WG/BkLwXfcDxU42W3PwHBPey+vEs  
+75vu3So4+vu8+zHLLq4p/+vvtrTrtSZud/KYkN2k5HM5i8QzneVst60h6W7FKze  
LTfGYyLLOQj/TjLXWIuzxprp3f0p4C0AdKZDS0uK3p0aVy0oJx8tcDBochU9esCD  
ul9rrXJiVwF4xKRHTuAGHbkNZE0oMLZS66/HRnioKUPmcRUDDpZnPvZ1yzzV/UG  
IfZ3iGjbuFhmrVbET5MK9nxf2qdBRifgdWvCRkoNoBz+w08sgSWa5sSGmlUmgTm  
IUBwiHHYfLFRIB5E7ojwiJUGUQNK4lyyD4ooXVxyzI9pkS/+BBJluLZsYb4cdN4Q  
QuuWz6qLzHPJet19jvmYYVA4tK0KGaEvObA189jPYqdYSlotcJgWEeIzftCKXWdH  
RlorERCnV/k3yDZ5BP0qVQUweEJ19zd/NZ3KXPaxrT568QJ4s3zzfSEqQLBHLHeG  
+fmCjvfhv9WgKpM1vZRJKfvg0zUx5aVE/Arg7167hZ0XpiUbAeFSaQ6V9+b8Adp  
gJgu8TTDj3uwULCt0qjh3+pP97aYFFgtgZKn0BzXD7y73K2/p0qZlbyCghelVQEQ  
HSVzHyeWcdj1p3+G2QGFmNFCElihyt4jjTLP7luNeS7nzwz9kpX8DMBci5G7MT0e  
xrHXVs9bEZVGcZ3+FjX9gSPk8TZS9FE8Z2C8KgVYu0jgE2HTk4GaoW4mxcQHj5Ec  
N7JWtXLUZ4G1uV3f2VDosh0wWvF787jpDP3dlIfgkrPlzSQUNwYKXXB8o+teJvN  
GbqM6Q0qlyBHBCiRuZEDhzW4C8zWIQv1oQHsSqGtPwA4P900TjipUFYd+Y/7CF9W  
uUoi32w+c0F9JwP05CBd0cJxPniOGbcgtJqlN0/Rr99br9bSYDJHSQEOMMX5Exfx  
DuLXku/EzvCTGQddqesE0d8uhmWKLlX0QT/RzS88vMgEPiQ/UT76ux+zI3hl8AX+  
+N4QaLRixUjkkM8lvEgdu9tYFU1B0BWK1nN30v8VIFkfGBN+xCDaGiZKtg1Foyax  
crdrRwt2Bt068x60/c61qoZeMW9bi5u+FnNhnaFNzBNHdRi6uT9pQq/XL4pI2FJS  
BXokg+eLSFCJJd9ACN5Y20ZeC0WbmNNSP9XydDgjWx8+vo0TFDKpSp0fXY6E59eh  
fHYJUEI1R69BiBvQt9CvB/uINLbBciZ9zYNc3abjSw90Y/2SmWaoQ1Z6NG6JUCHo  
Xf3ksmu5cX2KxC+WnAqFbRAKzQM5bTiffSNUXeixCS/o4n895xBYt+XkmgBIiTyB  
7SN5XpExfwEwaIjMqEsssOnmDokgQ0r+x370sw7JCKjTZ841i0gaDvw7chFlQ0vP  
0YRWE30jk3Dp87weyTbvtm8+j+5pbBLK2nZpDgSi8ySLNzN4CdA9ppKNpIGH+grs  
K/8nqMWWwD481UII8lj0RozXAAgt+KvcM2+v9CtaArPfw3Zm0tLMzEVl5GJe6+Q  
wh9qhFHqCAmSNRI2LhmGDr1RYFh4qPvEH5s61j20Fvx067U8znVt5osNKYkurza3  
b04hKoRhX5aPst/emN3r8ad0vtQExMZkTdj58MHGygEjWgX2IYTNRy8QDJ/zCP+k  
8Js0q2KZpDZ120DOP4fFR1TUxJg3DV+kANKBdoHW1iKxKkn4Zf0ZRLITeWss0Vp5  
YtjISHkczLSRH33+/ar/CxU6rIuTuwCBy8b+5M6yTkawZgA9iSiCOylt/kPE5soi  
1EzrD8k7MVOrogXwDEMP4ZGLMT56mBYmWouF9HE52Xs9wRcsS+QwZUPdJ6mt4C9  
PhV8cBw1rrV0zJJUPHH2EnalfmwHwCmYw2wjH+74h2IQ+MVZyvmfPsJBhLpbYRhY  
S5GLFrUP3W0G1R3pKECTLPetTrhwTbMnt8Z2CrEXAxsGhIw4Tm39sieLW6eWVak  
H5H9nrtpB88jRi5LLQLBLXtdyd4dCI9THJuVH4VSMYD9Waq2x++DcQQ3NC4+fYnfl  
5SVcsMqsmNu9lfJqWTV8D2eImAHRIAyv3GGG5AMeJdQL69cGLa25tQyPyvPXu5s  
RTi9NkktB49YXF24rEaeyCHPJ8p0m3G3T0ZoYfDCBh7Z7rCbgeR7XgafQZfK1Fhw  
rslbh9W9tDsaku/i2/uPvjhyJETjPHxdH0CoqUT+EU0Y7+1WVzaLJDSMyz6WFq2m  
RDWiCZ7HKrp3jt/9echScy048XGf3VGDLdaciP59dlE3Ur51zyQShvSXqNne6Zms  
1CjPTieD3vPVC23KUT5ZklwP9X0h60tYnxg8SI9lw31mcrbT0QQp/oTk0+qvnom  
LqTPULqpkX1vr7w0A6DF6f1C3UodlmYhIV6QWWX1Igd5awFHMkXAOE4eHPqx3pQB  
IVlBmzaggfK7x4Bk51EwWZxc8bZmDxIMUuynAI+kElzci8p90xvL+B5sBodjwG  
eLUPbEa+YEDN4/2CEYIwZks9zxQvNb20EBqduyeEU9S6nmU+7npRAYnk+avr65wc  
VjnEoNrfrqwn+6fxab2zPXbMfIeCfvcXR/Q0j7gW0x9lXUcvxdPvGbR78fTYdtq  
BITrh7GqVyUuJ2JQ6B3sLzQRCWbPC6qYiltJ6NM1AU0CveZaCE5bcHoQlnsos6+Q  
cfBUExy1T9NJKcPL8L2ieT0wul39e3hHSYGijhw6VANN7qwn/N4xRs5BERQDLmg/  
rd6o7SMMiXpRsqxJukFdQ60Lnss9FGJxGPprE9k8cQtq7MGF2nKnfilrhfx7i9p5



qX8QiQ5+RmW6898C1WaxsFLFP0ZcmzHXJtV+ju4pGiRfNke5HyfEa4hvs9eBWLdt  
OL08ZmgjtErIxlCaNHh+DWgUoYasBpxKFFmnP1XSq5HJN+rq0p2CVQmpB3CsUJ  
hReKaUGQx3Wfdaxq4ua+zg4/TF2Y2bgXrf8i/1QZXG3fiwFswuDASaJDMRQLPwbQ  
klCp07d4Bz/GqveuckEBQzuxmTpHbHTNGGP0Q34ar2b/IG0XXEp387CeAirJboYM  
bxtHb0U7MXeoEJQ00GCsebeuDCZuPB/j2w0g5sGnALC9RFSHPaNPvstB4ptUBm  
iC4hqk8Edejaay6xYsUL/OkdLyS4+Nadl5ewM087GqtG+w/Xph3QyONmhBdqt68l  
/wB2g50uQo0i/BeEHLAbm6fe4cBa8M3RQSZllWJM2QitajuwamvZF/a177beC8a+  
Yzg7cFL7pa909vcw+8EmL05uLiYliWQa1RbuQNDf40yyCqQBMgd7tRrRv4WG1nJX  
MYvebKgdRu3WPMGwbcLmryogqx8I1ytDbRmhzwSxkwh8QjoTSa9lsAQr2h50Aqh  
8mX97y6xxdvYjQbKQLZ4A0ADNrCh6DdZtDILgnAvLSjfkBz6b/kpag/MHI78irW  
9m/86mZiUyPjG9i05PyR5rxEzV3/vqFornmg8r0dMXF+KjgdW0QBZRLZeMp9P8v0  
pQcXi/Zc07nEAzhfTzUjofPCTcNPQotw+sGVuvw1fjW0j+doXKkbLPPueV978gFb  
rr2uuj/qyb8RtFaisebmbIH9lwqN/v3IS4P0s4CSQ64MFOXXVjvNFHXP7H3pdND  
3nq4oxj7t0UfpSGzgYwoGyQHJRNWjGQR3+jymIl3YHKYaDtcfDp9f37oiTk+gyyN  
NXfabo7SnAmj4hhyyM+zW7foYatGR8jK6LZ8tQA/Ap1N9+kQbIUMGM73bpWCyD+c  
OLYfofHYAA/GWxHT4p3pACZ/efpKhlrTKLeY7iDEbIQX4mafWsluv0+xgic57m/s  
y5aIsrNnLxQByQ9WqpwSeCwNdW1DbopQoLBM1oa50idHpDW4RZCLE1WDmxxPA1e  
AFGteJb0/fZ8ihcFXedkV0UaAZypcPdPPqygkSrPjG4mnEIUsHji4es3MZ1gDWe  
rTriutzzzzrYfY9YaxyZT7LRjd1Xz4S5FegghwMoqLYKLFor88LdA5HPFuxfWcLP  
A5zAIoZK5n4WGq2xI2L2LpILsFkS56G7K0zsdgOu2PoRT70+pAWaPFFcVbxmstlz  
oULHGyeSu/fUqt/ksTxjOqbZScKcQxMLC64Yu/BKB10wQZ9P9bLHQEvHbALrSp0Y  
PoMJJWheFeh+c4fTw39r59Pj0MVSiDETYssRyKyjUt3IPJgqxoFm40w7JjVBi9  
VDU/CkpEOeyaVUoTrGkK1dwuPdI8jPt+KmRgumsLrGU90FecJRu2nnRsSH+iMXig  
U3i45Pv6yPVaYlW2IqkQLDAUKZbF4Ktxnt8ITTF6zRslWfPDTs0ir49/zAFci9  
DgRdt7BxBPjwnvauN0w6deQXSSyJz8CzZoQ3jY6qft2/D6Lxcxr/Y7XFCBXWxeuZ  
Ctd0WTnYxzA7K8EGKGy7UcuEEqppNdsBVQSwzKtOCTaIlbA9SX+gIDDBgEZEJc4S  
gX07GNT7h5nbbSqFA5HpkQIEBA1w0Ebhg28R+XecEKUrDPuLebDDNuJYEKVELHa  
3X3LVYP4Dtd0b61dDtankP3SRsbF4aqTAmW1iaR9i3Np/6X6xqyhBQI5iDLJuIVh  
A031zC3YGih10/z8zIfdHav+8COQwp57ZnM5ZLpUPCNETLNsO/dpflTsgGBydWQ2  
t3SLxt11vYg/pyJUM5RuZb48PUHsg0NYws51N0XAoLVpc8pdKAFSSnLSAp2hzic  
uTvXC4FEQqD1nrA9z4IkR6ratIcypqAtZ0nDgbSIWs1FiWjPRdH/aYa9YsZdxUjM  
RCgH6FCT4SPDZbv3J3fA4pdLC5tJks5T8h/esWdr/M88PwkUb5kiBTn0ARbkxBRg  
SBgynXpePkq2f+hoXzcc8cGq4u3MDzvuoAQ6TI9jS6Ybxhz3AcaAitQQFaYM3KWM  
D52RvxT+scOFhx1vopZA/LV1EOYXo6VcaFUxWIEG4BPtIrAPglZcZDVuyZBL78fj  
o8M3MdM9mrQoehBziszpLzvoPG4PqcRwHzUkGQED6KxoCxxpsr5jFPAjHoCIXD  
tp8RRgbB2NGrWwFyVL/hLqy2T6TQ+xA2BJH/Vhey0keXzi44kXVVTrRH20FFTBW  
m6nxcJIONKT9hZ01Ir6sZdbjB3tCuedGfBmBmzPzGK1rnD2SeFpGbvR08S+J/N2f  
anfpaieE118AnXZrqFOxgDMS3rJasTOEIOAHbS1mXI1XxC5oiVJ0ZuE5hESbpOr  
70lMyXhBsCve80dh93hAwVQ10wE91STpbLvvo9H002juU5+hnGQ1dVEMXCIT53aK  
bG3rm+QPTKwg/o22/it7TOPd2gByJVGjTGKJvk0WRh6vjWqJUpxFW4NstTYnSsc7  
8JhVR4PkgZkCDdneIrP3NsBg0PKBoti25yNaxCYFubyJmcAw+izBQKHASKsupk8  
D8obeS1bCce0qc/zgG7kT1MNaMTQBjZ8dj02qx2UuDL/HxEyHoRsw4R08zwrhPnR  
E+8Nk5xNRcsU+iJll32LNYsfzjYrsisLR4Lur8TWSOuE34EHWB3TyE4kqQL4PUHL  
axjX31qyRMnawgAQF7MRXMZDCPUPZwzBnYnmkuWl+kuck0DqkHjVTUA3z3Is6mgU  
M1CA74PLwGLVXtYUGRoeBqV4P1z13K5F12e3ZVJrHbjs08FkXBxKgZ2FFt6PrX  
eHpxIJbLz3rjTsUagpTazmFacIbb6pX01ghHjwLaoBsyP2PNo8RSUNtwjiYzrPN9  
zTPvjehNLfQNM1dk5TptKjfol/QCc7ysrCMkj9Qm4wZtQZXp4p0Q2dFJDtRfHEUH  
t5xjJ8VrYXUh90YFKLJBC9IANCXob/0SJzxPoN0EmsbXzw2b0sA/AzdgH/KAc12g  
Fz0lc2m/VQx7/43EmJajK4bC+nDHKPKW/1Mx/WI4mEiUbT/eQLtkDfuPhF019087  
is2NrOgruBk1HXFAHlszcXyBG/dye5GLRXs4f7yvpI2cGWLvy5lGS8LTcAmSMLSy  
ezJ2zrE1kQF4tesjVX5Y4wLjsHUXA86hNr7Y/LRjMlRXP6KRtyzOX0un0junhD/  
PYLYc+qh4Le3zLMJEHPmaPsh0CKKd9s56EyggMt0jRQIXW90JyNOIuG9nit9IgG3  
wPuBVBo+IkQBwQzxKhIcLw5g0hGqN7csvgjqtIszpyqzPTsipGHm+HmciHdc3yHi

m6zuwA89XkFuacgQ3kYFHRTUmLfkXy/iHlWLInJ3uhyiz8KAQaRpXIdQPy8gugMR  
uk3JMiXkzIRrgOPe73Zc4Q1zxz4ef1vTVu5E8KnvKHnifqSP1nIRlb7KqP8rRvLz  
HxKsCGtTa0815TNlnZsLxtvU8EPKDHMF1tsZio1NcCWZHZVfrsBtxDIukdmZPoZM  
IgHDIpnH1MPS2h9j0JnJNNsgs+jETHAG3im5R2iunW2k/xBL7aiEJaMs+u+m0Bu2  
u71w56jBNLK5HiVknh1ZaIMc1YfGtT1ndDHM7Ft4P9eaGmUDaLSHB/vN4oY/fUn5  
z25FoKwZefDj3ea2Fu0mJHP1HhEwy4S+i/17EjmJTpuiCbNsaveRrmNUXYC8/9b  
pyeiXVXTR1VscKlbCreBBcZ/6jtXod8YslpXu7xdfkWJ47Xe2TiK0P5N4tWE8ZQ9  
m04dTN1KG611KQG00q50qjPiSnA+Rebw054QtbJ5DMIlwT55qFdnDs+ISTxL2Vdc  
UHW0PH5C1aSoG6cmpZerRVxrRscfEHtAzCnJYQ4yKtPeso6sc5VGWK7R1ROMC5p  
2r49Y/DaFt3QaE33GcxZn3eXw3g37yfBDq4U554wFM/Uy9wnv7sdCfnECJiiG20  
S7Zch4B3u5UvaU0oEffdqYq2lHktk6Awis+/VKELEUXr+koW7IvUDvzjAvh/1UQd  
LokZ/LHx904fRBdyVv6bu761x0TevZkMUyjhW4Xfb20Q5p3xoo8BORLUZ4HjrmhM  
bn1DBN87KKMIygelB32f0rUL0zyi0cjJd6vRKCaI8zX2MeXQtC0NEDm+kDYSQDO  
YPPsuYB9E0bo0d4B0tGuMaLWjHBDJe+QfhPEiw+VV0gtUTOMVDuK17aYiJw+aG/A  
mFspB4xDn87WYGEf0Z441RcX0/py9UxKD3Gc8taCEDXjK5nNsRvW2CowGLUvaA  
QI3Yot15hgFudNQSOgsSWcQL9BwW28t/mAt8orp8gE5qwrom9AcJjTPnvM//TFyJ  
DLJ2UicVNLAWdIWIR460etvzkgCgFI2s/jE2B6Z5ImfQ2AC9rLLa946vmKNsegGw  
/xfSfYzTdZeANS3qbg/05R6VUMIyBaQ1v8sX9uWJcAkoefwQNnyzMP/bp9LthTxv  
jRxBFrenYtimcCHNQ78fja0ip0TrgzdkpsQSAwihRkntZxJDTUV66S8bBv/gy0J  
cK2oJ6/7drmlDFyBgu5LrvjRn15fQ3oziM2m8ELJvytZaniYboOywbNw+cMh6V6h  
EGtvezkBWJC+5AFAZEXYUiflBEJfFcMqk3BfuzuCA3atKhejF+aALKTI/v59d0yJ  
fK8WP/NUBI3wfwizmyjY5UGDwRtoCOaz7esm9PAEhvwuHnFzUlc6/ZTxqjY262C2  
v0p0qCPDXbaGC773ncVn9alpZy6L6FBPSQEemx4Nw7LHhuQqjbdHJ1APw4GS6U3S  
bFomp02/30c0syDH5duA2WP9xirWJKAOfTv2sZdVc0LYvRo2YuUzyIYK50Cnb1Gs  
l4c0c1PuYw+6xLRgScDYmbxJCEMB7xMu399YBmmNd9/CfmX+7BuMV37m3GK6tKHg  
GCYpG0tA7KZssGdCqov1NnkQp0sR0pScta2EPc/M3QQEXx/q8Rke5mu/kxlvTWZO  
UNKzYvLGS5Vxg8d9QFLTgmbSFw50FttoMBu0jK5TVULSraZDMmqkk900Utzn0iah  
firENbyCfwkzmcXDfJ0Q0h2EPfpAMXGgKx7oCEHmaoID0Xpp2HjJWhq3h1cA23rB  
5EWoppw1+54B6JaRzAe7T9JvKYr9JoMvH/HEakp596dGAKC0Suls8hfGXFp1F0QU  
WG79pXdoMekT3DlMjvMd590vdNQD3odeiLGosTPFydtUtJBPTu0xZje3We2rV7RC  
IYhWqyJu/OWVcxApOPxq10ziFoTJ0yLwIfJBUIYGVhDaz7Q6fdv12ICxFblTch9T  
0WobGP9BCPYun8d6b0Xun+IBAMxm1LtEefx5Sc25ZBxUmIgy3tNY6qPwJqfXEhKJ  
oR8j07o3imjxqu0frf1HspSm0nZ8SeJqtxGdEvPfl2XBsI/5k9cZ8W5Xr4f/uOf  
JfPZdKAGIFKGFCDs/iOUOqB5JHBKH+S+LE0GKGK+UMQ007kCGy0Y2TCmgND36/9F  
GXdxIYqepUfuru+g7cQk3VwUGSP1fhjdNSh4oXs0QKLvi5dYc6cC7UiiPjZV4ecN  
l7Z81hNvdgLRSAUW/wCQGLM5DlPxQuuwM93E6UMGYrl+oonBSaAMhui1Lbr6k09F  
vl0ZQ+XJ0ciLotLztKTJlWbTC51NQ3UTH0HSIRnuN7iUWEarGF88wLc+0GMXB+87  
7ZegDaITLQ2C4/RzomenhNVWMTMDmnBuZ2+BjJu8UKCxlgLgcLZAx7sUjkQEBZHbC  
u8TqZ9NWCUh0QSu8odZ3AuqB+4xRWxLkgvZ+ei8mGiWttL3yggd8gqUnwxfukD0v  
CEWTXEUIuNlR7rcN+FwMFNUc56vhUgeXLBGS+6iNkOxLLQlmjyqqOyGSZbpUJTyy  
fNF+9ks7lj8XvImypZT0Y4fsMzb2AWN/hYidTzsCpn6HQ257b9FH3e7QYvzsABpr  
M2wrx7dDqh+oNJTG66R2M7IjbxEnf3ih610QKYZwQmiHw0i3HajpQFxCntFal4aq  
lH708pAnY19648R/L4mi84JCG3ISsiuULWbjNy/e9bTDxc0REo2gzwwsfsPPKxZ  
kHq6BanE1xGZpeFcllw0CL5qG3X+T/PQCBNK7gjupzuwf+wU1KGrB5140fcLysE9  
sFCmzJdIO0+Ts0+YZT4rHN3/UyoiPpSrLb2LUWnYNk4DKMh1MXbp0SUI3Dh6Ysp  
dKYb52bgzdMJHqZHyK093YcwiwICeKmR4h9JqC1mjFENBvQGxUzPAco0+wTf4EED  
8r9HdgnkfwiwceTZgJlMR0o8GDdeSbUjiagno3G0Nqd+GxZvblmsagsna7xcyX/l  
40aqflhhBEKJ4W6l0p8SSImAmghd3A5gGKTCLb4ZFaynXqC3BQder0z1TiWq4STw  
OgTFkqriJ7nBuSMY5ChvdV9rFv6kHqfd2nX/2q0p08XRdCTL+Lk94lPSrrqbDQDo  
sV/YzpzntxsHrsjUY7xs15nN8kz/wfV6cX3dvTAmboVxH5o6y4uRaHXv1naBT++k  
z+r2KEJxZKfh46rhLeKUnRKE1ZIPBhkZuvwGjdrGE0JFJTVZ4MeHm7sAqNIkfnlQ  
w4MCAa9+ObBqhIt8tWmrSQM+T8eIGvb5XQG2DhDgsfESZ5nuA2ABJ0wiaTSLHhs1  
zKxjag50d5tU9djecebvAF9zD9RLwNqQY6X+pKjKTIqRmk2+rQvWJN3bAsD19xDY

634p8U8NL0QSVlx0qeHJCvuhmvaKywWQTxmEvORKWkwMA0jCBLT7waQPGQRtXani  
w6U8eg6qoS0oF9krAp9ClgXevp06GchReI57wb66eENFvivicG1cgERyPYnX9XvJk  
rg0cJievBwpCMIuSDECKZrIdoojpU9GrW5lLoG/xR/ua0lWd3LvsqzeMu1omGy+Q  
KW/T/WJFy4XjesVkcT3v1fzmRs5UTDhVjHIVvFT+K7WSRGeXyePC1apx4lVNtPn2  
lPC4000T20FyHaikuXlJIGbFQLNEJI4/r37RQ0TSySmu/23mARmOUS3CtabK/RX3  
AX6wA0zbPH3D++X6EoxgrQFug2aAV3FFv5WHCAtf+4aUwYg5arH8/dSBtTRs9u3Y  
vqgGFYAm9xFEc3Kfqw8etM2Klc05H6PCxgPwMgwKQUW+3v0svRTAKJPLLV7VTGH  
2AUcjB15nD+WshrvCV8zHuXZH0i903Sq3YhcngE7XkH/LuygyDDDBaeB7Nk8DG2p  
sk63Abnktw3wgUmp+E5btpTJeOSZi6y8tkuCeAtTDlQqb6/p1tXcDAIGGWTejBqU  
iCyNjQ461wvCOQLAommyVYqXhTziLXC1waUMrIeE7dFGZ2V7eJE68JyZ5fqklyLi  
4V1S67ck49oEOSBd2Dj/t08OnfFjLgET6Q0E00iyazv07UcHNjMfFoiEnYjrwuz  
b4AolIQ3eg2tpR2Scv7rvefKQbQvEmHyLB+/YXKe4Chcozk9puqpWy0N1b75T/mz  
4wTTuemUUD17k4bstJRHuIdRbNyJVz2JmIzk2d9vkWVXQEGjgSta3BoUv+2FTt  
CjcwP3LYWABP7L0kR1+BneG+DGfnpTyjVtZno4nQ8uMxYj4+IVfpAID5Drxg+H1  
dKn0XM/DzkCaCrQ0LBFTq+nJ9Ujd+bgTh+lA9kR3b+l39UDTiGQLBU94cJ/GbsA  
gK3dIbc0eRuehA8JtEn2tpgE918bkCUYTUtFDWFcEAUBTG+w0mW4jT401yLysgJt  
JUTEuWNg8H+GA2iCRsXhT0o9KRpJ5vQ02cZxDFW50suZ75AxkPvXmcTVpmuBjpGv  
HbtBScw6pFYbDdX0ITYfPKEIakUeQP7gH/wKkhE6U2dBdWs70BwmjBtVB4i5aIa  
/fXgaeJswsV8TA59m7ru4kmGBoLfo2DyjVWBNS1I7yLxuHeeMnPVQvHYe3bSGEVd  
TOstxvTJTDViMvNoG5eR2+imC08XUKBGY3vZ99+aq52k0eP2IKnG8ko4lK04lWhZ  
sA20pLPci+fBLnV3mLKl7YbLj86wu0aZGGB39RniN+s2206V3P0LbmQ93cgVWUK  
QDkm60nlKs612DAHxKCU5DEYep7L1swrr1lUbNqXy7mSZ7gNtr9b8Nh1QpIk9/E9  
OK8Qwnvce5TXJ8m0ETmThktKztG0YPH0RMrKp2Vc0ELOJI/ovrAHfKqN0229gGQm  
Rk/zjeUaWniac2u2zKrAfCSN6mWxdMIqj3wsnkqhN828UpIKarPwixpnFHysiGY  
QQ5xiC7Rai7KAbiiFoFK6LjckMkkgxWBFMRE8sj/PjxfITcpLLRq8QM15B4yHSFU  
WUwYPip72B9MaTue20a1fwolgUmxbtniUdLepeMqGqnc0K8HT0vQfNHw9Nc76bpg  
CiW9B6nzkyLBYYJJfct7DUXvcJ3KjgTFfsadp+fWjSVCn91bPq3ZkMf5Go+/AUK  
K2dvBDKsK4oCtV8qelLDAgVrNE/qd6X8h9Hym8BMcjr690TtcilGf+HCAyIhZYZC  
GEIT0FEq3lV05htWdlSCAa08Yn3JV9u7e/FagxbAVNMBLg0y7ZUQk5ZGEzFjsvCW  
cGzwbhWvSKe6n702F1wp4G5P0p+ydQyXHFwT180aFKQ4rf8+3KTdW46qtlzKemfj  
58H9u/4StUZ1lN0jcPpZVrBdbK2xr8qmsmxdaN/uk9Vp7l1LFCqeiuICBuTIjXn8  
CQdI7C42jU960X/btw2vWaWYVU+zbFzZIoCKr+XsJNiP0tvpCLx45MJ660KhE60d  
1YrF3GDv9Yfd1as3cRvLvw7+3DYcF0UTma8mV6HcyFoDa52/WDWrfxBgZ7nqdZZk  
VMXpUpWnTCrBzwsionwuILimjGaN7P0gncZsWXZy2aEcVWruadve6LKYgg+aYGj  
QDWKuEYe/c2r4B04EtVt6ZNaH46K5qJ9aSRmFcGb7pn4sEjKmpCh4z/u8Wkv8Rbg  
XR1VPCVCSihHtMjklTtXt2PIAyNqyoh40wasz4kHVIFly3Y4k66hpgWH+4xvGBC  
ekI09pAiBhESEHQufqoGcvQ0ca+J5fqauHVwJBzC8PmlApvCB1vy0W/vZFt8C36j  
A7V4DBiWJeoC4XGsiPKotfkP901asAi99+9u4mAcricGNn5l6c8gtLCQNN3isA9C  
2/0tv0fwbtiTJJuopqE6lImAvzMHmSszwafY+BZ+CfsYuaUSy2v8M10r6RAVBF7xJ  
I7/dAI/ypJYPEEHvxhPrI4BqgqGS55g7kl6J4cBr9veDzE2A3iyZ9y3N7XLGqm6T  
mJ1Imxm3CVb3YlrlAUrnt9x0Zy1EfW9YOGgrWnfQdEe6p/j1El5q3q8ziDqSiTI  
g25nfIcT1o9z8Gm8UXRr8N8G+FKXoXX4EQrYhWCaM8oMZj6S5TuwMWGDTfQ7Q6tq  
/AgGZvN0epKzigxL90RGcEAS9eDu0DtNikRR9Lmkzn68uihMfp6Hcw1q08uY0RHU  
sPdX0065kaJQ/vcL0l1L6bkQompJN2bHHjLwooZnVxsTq2gTh9P40iKS04vpndN  
qZq5kxdg2TP/TrN0kA8Cwd5msKx5FM9x1EJNGuC0KzFcCYpcE4XfVcW8JnG4JSgm  
MDwy0B+Ruu/Bjo7QJjStjl1Lpu57GFCrmAX3HVYkLrv6QgifiXhqaISlpmgXdss4gu  
rwHjmsq1723rdASYRjRvne9n9TwkDTu1WpVKPF0PIJYauw55E03faXDuKhVAdQzs  
ZQD/CUPo4RbPluo0/ZeDeHH0u/jYarFig/awXXDga+TjiY6eu8FKrar+vaM28LHA  
sF9DrDph2YHDcE5kD1DeAhcbck0qsCyoQ51HAS0Pmb6W/u5yFjsHaDVtJMogwgEJ  
0HlZhP+NL+5D28j2akrS5nbEfdYFJvk1c043uy80GmqkxB1/R+HfJM8sF6fkQFnw  
QpyuImxP9KUbfcHyjNRd6gESQwQrvxx0j8mr0mThH6JnHtkIJb30bIJo6M5aaJk6  
jUUb7lvJbkvDFxUYRqaM9qg00Su7XD86tgcw/zR/NJ/F04cacIAxEc0w5VHVILwi  
K+iVstEMTSIEMJhGcrTbZaaYkNWnF2IQuVyh/xmxLP/4wdzioix7I3wGpmKORLGI

y47MZZIa7C7WVl9Plf0d9ejMh/8vyEgXGX5KNgenpBmwH1Bzty3KQNPdIP2S0NAL  
j0Q5nLa+ItTEi1pu0M2cv0vhwL96cdeWQgwD5PQj3iW/NZsM+4hrxrZ1vnEcV00q  
tlz2+thGWttNrPp3+8V9gTScNynzxntQ47fveMUogh0zfZ0IoyUBrl3AbcuZUf  
y0bU9Db+0+Ajtn5lZJGYZivsL5NJaPdPh4c/LGeQ5N15gZKG/BvLVfYg5HRzG0Q  
CUqGS3FTnyqBqdmfbpE0w8x++yM1ht2Js65jDDMQ3TEfkMV5AquoRy5EXPRx35WS  
jZke7m4b+fjSpP0/TpJVkyLeIFql17o02xyHpWo2xiLcmZuohPeSns6NLtheRlCl  
nQf9d2phr09UxHL5GzZb8RUKj+9hdk0REPFJR+ibz9UfK48bKqakP94KH6b5wD/  
3fFjq2NLEx8yloy27VGwy6X1sJP1iNwL5kvMCVqsWws/NfvbsY8UQBL9dG1aaQ8  
0Us0GXNAJiF6r9J0BCS+DkRSPQYAuXfY4j5j2xgSgX1Fv6LmVQqsmmClTy2rrD7K  
XNcAfgv5nAzqDk6ESED8SBUislGTC0CIFDSZ2m0X1oHsbHjdlAkzd0Zz/zcefGow  
LpG4/30DYFegg788TD50BFA5ZgPtlK9RTZ6TvhKP0i7Qyd9tiBiAwQqLjK7OmRe9  
QMA+3fh8iQPyCZNZx6UP//bhjBmkZs3nJ4swLhaBa/rZop8UHwvXT4+Y/YP49raK  
NwUgyN06m2VPFo60jm789XP3cnsSMU/0WnR3BruDsqq0EF2G2LWnXucIT96gaeZLo  
AWoSrIiHbtIRGvRa0juqV6Iqw7mqq/EYwVAN4NOBdm7m68QgUhtPGTNL3qqDc1lu  
QCwjR+Wx/RT12P5tlJmWuTD0Jt3iempdtZ3rXeP5I/Knj0Aiyztj0vxj3/PK42d  
N7l/wZLY9M+nEBgd3/TLjhet8p7loaq9MXx7DPl9S5WqN3DNN62QVerzhzmPI0sU  
+09xplJcnYBMSjjB9LFmioT0dZJXMG1Ro/cYGjEg8/58snQzQvQLg8IVMMwa1Kcx  
flt4E0oXncz8iubSb2XvLV9xyfTbelGeT0A7Ih5JE+dv4VEiHhpy2/Zk8UBg4Nb  
2wQD/nnyxiJhUmz3q94N0iTW0/p/F2yj005FHkcCP0B2hLWh7BPGag89g7oNQ/2B  
07cZPotRiFM/SVLL18I9dj9JhKsbXrwxllw9HT93Lsfca1/UBU0yvNMMkwu01RU  
YZCX50dVd5jxy2oC1INAMWqT1UF0a7vny1SPBKZnZTPwYZC2pZOT532bgzVj4iNa  
2WobdMtqV0c80qj8kVJ6etc+zxLSewVLjF9F7qiFhjBkZvQ4cKvpoHMX/PjSR5o4  
hUr098oq7gekuQLSXDE+e2nBCK54mdrrn/GvLpgDevFgVpL1YicmYzbXswzZNA2  
goMeRJ2KRf+19rPUTBaYzu0D8F7hdUXS3tc09Hd0bIashJ5Pr4twL4bzaxsNCI  
pi2NMJ5CUpUDtX1vsgZMQvUEYlAvLE/Ojd+/0Wt7F50Q7xQVINqNzmVgn+i/k/V7  
gD95Nv3I+uJDR6nP/vtJZoCR6Zo0+VabojW0OMD5osUCMV+49rPTzyhqSHI/zfJ5  
6FMZinXi2o3Z7SWP328fG7uHi2uBMV0z1uMonmdZbQwB9zRSPtWaTqXHLAdBu7jp  
HKXhbFIT2GYMo9qtB3w07DBhGu5K8z1RePbz9f0RATsocm1lNXN/TmHjpPKdT3Ym  
o37lbHSvfB4IMWfAkyNeGRGDQqTraLQK7yNXJfL8/Zy7ZCw33bX2dC43d5j50qMk  
b3oBWOP0Hkp4ZpU6uE0spj+CAGb+UFVK8nL7mAZsD8JGHDsKLZec1Xf6aQM1o/4B  
XDT+nThG000DVE+bGhrOhigCcnOG0214xYADbsZ0iwG+eVt1FRat0ar3B/+VsvP  
eoz7t0UhkQjtnsMCuLbVa/USbv8xYxQuwhSS8oUCQqCBroNqoDITgflWHL1V4QGk  
q32TWyNF6VV4bxbUGtNd/1MrFKVK3z/FHlx+E6E+mMrSLbMy0mwIrky6w/xpoZW6o  
mR4mAtphsTJ5ltpeC/yZLvEcQ/ujtFq0g3r4qFM9/W+UNIJEfpT60DvoCE5/E3bm  
ypMW333yRN4U//fgEKCKa1VzDos46EorXNuMinQYIZMo7KZf+dzAExRjME5lk+ly  
kaQRLYLULZivMCuatX3y9mNTTuP+KBbUZEuAm3/Y4lSdsAqPWFJwbXFBtMV8084R1  
LH72qlp3Ibw+MF4MbNfWc2AXKfIENNfSmQZhu5mHR8dSEyJL1ULDay2nECX0Hk  
f4y2D0SE+LKN0fFd6ft6tk4i80S3/AvpyaghYWQ+4sjhJ01gxZGyHSArFmbfrHZ/  
o2RRtLqBvYGHo556kssMpLSYIL1PtPJWWD/WCG8ZZGV73lXyKsr2rUm1XMfCPNgCY  
tRhjHA6G49Xyevod9mCnhsC7m0Edf0mLN5U8WcimXKZpM5N9BdFOjahFzIwUUTF1  
qP2fIIMa8EfjgfEWhxAB3pcR1EOCB+Onv1AsHhH/ggKGXeahP3k9EpZ0WjhXH/BE  
dZ0I4yr2gzp0E39QcbarQ2Zm+/sDB2+I6P+Jq8b+nOFyTb+wevPSiNl6t0Dvj0tm  
2Yny+y3ybTRhzj0u1JkybdicMyPeh8WANXmv0+MxuFCMhp64fP6sNNHcovA1mWGS  
E6sa2JTmLHY5kXDGkl4RTNBn2rSJvbFxxUHqD/kpYalFA1P+iyoMotWkWI6Uy3Sd  
chVZW3vyEZvs+chnKT8CRoSNEwifW9480+LJt7UVhkAWDqAqA2WUGqqoTY/oW48v  
zxmYhETWdaepSNhBI9MZIXCyz/HGrxDVi0nc2wIKrrAd+9Nsv4FNHqYt9j8X8ULI  
bi0LdX/zCL4egbl6bjNxCpES79NLAz6Bh9yXsSuCicebVD/oxB0S0oKqMDLWCW0Y  
jEEf6Ys6/EsZ5+GrT4eZ/9tKwhLqdG1uSwW5Ih373W7M/wYSrlo/0IDfXMQ4bM3q  
KqJoLmdQEDspP/V55RCa1fo00mUD2pSfBcvjS8Js/UXkHUvHHmBayIF6wvwX6Msn  
XIQHcQsrYBwQzpkK/yz3SeeI1mFXbPB08+XnjeoHypfFziCk00RkANLuXPPKctbV  
WJufRy3zuZallwD82zpGYTRUXmK08IsLaHJ+RdG/oxA3CFx7JlGzrCt1k0AA9q9iJ  
bYL1h+j8GyS9zvCNKVB6Nu3zhxaeWs/JJQure7K+0sRAe5Mu3zPVgpoV/ODvHzmu  
uqtZ8zD9Uuof6wsi3oMKhw0iJ/na90WR/HZtiXFH2pkuRRzL413Utdff7SBaM4e4



oBp8jnbpm20e7VLB36ENVweprrXwhiRwJQfRYCGPPx+5j6fzCm4o8aLQwFB20CL  
omPP0mMtOPgececYN1b2ft5L9x34yFSRFeGTr3uWSC46C0aqwocVj6H88ek9Bz2L  
9Jf1EqYryQ34UtCfzcmPIEEVqDvIxR4WvqBTWmqYdlyQxEqQdk8dEtTl8dQNVxaH  
wBKe9WG9FZ6ECM99P54Mtacl4Bty76yKRB0uVAWhlTTibuanTF38S2DB95iQB0e7  
AG/S9qg7Wo9lDD6A2sVdQzL7YDApGUMWaIlePC7ccSCeATC01ILj1DbxhaXQD3ke  
hG3BAGvKLEhmZooWc8I2FaRrStp402upXtdysjizz76aBtXh9yBQJ//TLFv+HDLJ  
gcPDPEnHKg7hieVpD2GwTs2VyQTbxDZW8VYAnEezscRQkehduHY/LI3Sa55vYr05  
XxmN/KFq9J0zfIt1dbPkBAZstA0qFK+/p0+o10eQRo4miNZBntSLU/DWn45q93D  
fupFYWzbf0tdPYeuQ7h61lgyLeofsm0jLRE1DYzsFLMLNLSCoXcEPQY1IPGoJmug  
9XHIDAcI2Q2G3U1knCSJVTa8TTF/P0QqEuJL+k9NC0s6KuS7+xbYAw0gJwerEMiq  
LpZ+myg0HQvoqykduG6RzqznYrNSBzvktDizs3hodOF8VoETH9Xn0xl0qxqbnMY  
UF2i7KKrtKH0f8FYyeV7zcWaJoTRR+/DLj1jZoFSP52nG/Ye9FRchSBQieBrPgSi  
lhIGJKXmKNo+h2tAonEZFU7qBjxKbsbpNtQrA2zN/Y9fU4uq5en+XLZWkxkpB2Ys  
VukPVXFK/sG4b3IggiSy5vmaYX440ZSYkjtnrsioG9EMmhtSnxZtLQw/vaIFreQ  
s3iaNjMMfMHby6ULjRrprsbP1NoQtjaVvGG/vCsGGCCx5N4hZ0ViFnV865DUeGwr  
Qna7PGdnPwBMDEUIIm7Q039BJgYGCUfXEUyrgIFUCAH3acBy0k58C7fwtZhad/UD  
A3hsx5NF7GwimU/D4u0P+tbQM03B6Sg2w2ZJH4oV3p3QDx0vf+Yg06j/PmszH0J3  
vLFioBoB9LDki/zXmcyFfcg2Wf6UMjmbXk+RZ17Tor7A8hJymznJfINCBlizlIDq  
rooWeBRNRUgbzvTI02s8v1Dwvn1CNaJHlP6nBYyrF3ii2R1YJmKcq8E3uwqtW4kN  
D4r7XZ4d0VNAJqRJqpQOPixReJT5Mda/+Gv+35iNy0aG0Byvafh7T0wGCFBbVMp  
+TC4AaLwvKNmm0rceKKGWUeo2JMYc8wBzife7R0jqmogxXj0oFwMzg5DL828BhFW  
R8JLSMDx3vGXmaNUUJSaV64SsaKKPx+ikfQN0rpKQ8EaMxl8gTyM88F7eJfjUxk2  
tC+gte2inSGiFgtEc0lu/6fVBhGz0rof1Xv+JBAiaIBaVcj89GydxC7nEYS4Ltt3  
vd+w1ggrjnFro9WLjt3Rzv8c1M2kYBsceo8DGjTCTphlooB0qI8ROZA2MhVzIQGO  
ZF1P4q0ZwF18x5c1657cgv82YymSgtAWiUj060TBMUJT4BDNFhmHm09k3GFr0PHC  
9upyw2R1s/ez/B3A8nNADAXc9xl/YEAgqfdiC+kyxoZaro2/9nEs6HUSekRBmPh  
xQuRNmGxsJyDbG2zMzYLa7ty7GrObj0aT+QqR7aKQsbm+qo3idvjKmCS50qCXMcb  
U9GDkBB1YvwlGaGCVuqK6xQJ3AlQvFQ+CsuEe1mh2Y71mF/wTa4LDQmwZ7iIHfHm  
E3L4HMqZl1p3SeNis+LjLD3+YaiCSiyHrx8Py24iCCbzVLyMUeoG92f0Z5JJIfrM  
VvZoKePdJ0yl32tMtBN0s+g/GJ610WPD43SzlfU6w32RRjsjFJn/fbjPAk1zgsX  
xL2ifx0l77iqgbS3LSGKM4etr93hjZRSs1b02+owMzc0US+8LoJiZCjlxUL7VP2N  
ESiTLmLRAiMzuA3ztnr0A/D6UREak5sKCM3ovZ7h6SJ71ZT6W/y3wxVfD8LVBKLF  
1QspwvJroCSWroN8yIy9V52w0EFhN9WyHSiEGhGT05B3JA5F8wqPrHBxIpGM/L2a  
LUCF71VAOZb3u3UkL04bgfec5FRELQgm3FS0wBE/g840LDb0710nUVwAM172iX1  
VMshq1w1ZhJXGPEoT7IfIeCHfoZ3/iYkiUpNoshIntvvDdx047XbZBFAjvluUQdR  
hxRm80bz0s+qa4KUWFk4+8DhdSbuMgPi2b1Y8gSK+nRVy9kdjTg7mH5eDtdG+uJ  
u3qkvxWlb53zaC/BE/XoQLnahPQc3MH0yKgSK/P8aLpJR6yUoMSFSk6TjCcb8AuG  
yF9oJ8ZhczXZHyC60kNwdP71FfIljocis4wkl88qV1FtmeVvHpWc4SQNWWRxapAC  
cYJ2j66AKR8pEBMQ7Jzia7U1BpgXqGw1tw9+uZRtymz9qnfUTDyHy18hTlaixmnt  
H/HPQLDAkdM+vUVye2+tn9Prmo9IUmn7w3L/OGih53yneHPoG5G86sf6eQtyVYE/  
FJ0UxxXqFQzEdM6X3t67nqAbLmSmlWLwtsQcfi+ZpLveNHGy1SSQfxo1x+4jnf3m  
Cs+2AVD47ip189gluFjOxA1ZQQ/o0qM7Xmk6aVScDem0IsHaPDu0/MQjnIaeMohG  
1GdorWbstq+kIxZ9DCjqMqn1S3lpzqjwrGvKe9B6w2MMm5DnuFYTSKRix3ilUYxx  
vYI+XXRrbV4fQppFk2LLUGaTU42wCehgLHqlaHuoBWPnB01EUiytZT5g0vHuVp26  
gtrv3M2NaI0zKNtDAjN9HOD6eU+UF2kGzxkEPD4vAvVpA8YGmGoLS4o2IJHW+QU8  
Sg1VnqqEEerdcp0274TZse3J7omlswSCDiCZs5m57w33M/lhyZ9HPICvJvwVa/Oo  
bAJ0n0EnOCMeHRMFIAK30xg7EhtBkIVUmrF983vi3crSoa7WgkB9uFBxFz6z/6IH  
lom56ID0Z26q2ja00IdGwVtkfkHijssXBLCZCiq4W2QM0YI2zG+sNGJKMRunuTG  
2qRCorEi0k10jtldn0ZZpFBGcPDLD9dyF/NUK3JYyRXrmjtCkc30mYhFEKWxf6WS  
+hX9HKAL0GwzqMph6NuNLPx2NETaTwNed7zCWCK95w0JxsxNc4A3nPX2EvnKh2wf  
e5BH1BrPJmERmbcmC8Zbvsg+ULM3NUPD+w6B3GVmx284ew6HLEyG0oBubMZfahS  
6WE/wsEwEJPiym203+utrw9VRjNZ1jNV6v5PLC6l8XXYEpZwxpltuPR/513rLSq2  
ZZu0TdcCNr1k3p2sPml23qHPC1SY9PHAEL3YKb804rKFmCH+LFJxfwMKUZn4Ad7H

Bj4gmLV9LgxA7gg7i58lJCMhMnfcB+vXK0vwK6Za+U/2kcyz3emkFf5q8S/wVQbc  
GztVGywfhe4dCgTkssZhnPVKBezHmPX8RXQ5W58Qqw3cw5mQS+8qPYXGE5WeYEpm  
CwsrkkhYJ4GDZ65TgokVW5iQQIepNU2HFHx5Sn+G1yj9fo0wzXMK9W2/am0kSNxf  
QLKieqovXJNVKHv2IchbD/s+wn66kKFtS/sgdcSQLHZMbgIhl1PTYWd2clPFcwZS  
4LGxawe5Y0UDh5j0Y4ZseYzC7F+vpRP0d0BpE7VQw8s7Am/yx5NUi01d3oEjT+Pc  
yFayClwVwU9M41iwmBIRKq+R+Z3Attpf0GaIegsyqC/NHX5tHsQBeacHPKcjZi  
+lbFTnmE35t5oSJ5iU5mk9sMWY06VRbHTMpGoCrI6NxjR4szI55YifkCSsXFWza9  
7pP/ZWbG1q6pD3oeHaYsyoIUn3W+ma+CyRgLhMn4pV2dZNqUo4V16Vdytz7gNxgr  
Wku6Vf0nmYiNuIfoGljZi6vbjplHNeiQAZzxayxi/jfj7mXHYgRjV24C5Z3eJslo  
b6UUbJgwm7EA1AWfdJnqiUg0Bn6hBOZDutxEIDICi4C88kOgwVEsKsq0jUB2hDDg  
lsrnuJpdw2k3XduWvs9zS37djBaicv7SU+j3EJV0SEURWnPloKLAoG3KQC9bUACP  
13N5EWi/woBtzZnTGLKNZLvF73Chd7Q5U8/pB0sutIEW/nBpx5weLCbty+3kIaWI  
CiSUNi8SYf8QdUAvGNGxZHKr2wcCwCwKb2VMStC7dGY0+ZNfNTltt8WL08IntbKo  
dJ4uDH/NF+rPkdWWttA3mMRj7AAKkG0AdhWKMZjFd5s2GEh1uSaDOumXJBVCmWPg  
MQUQm6EUK9tgUtwet2Ye/N5Fg0tcEdZ7Tfuc8QJUouTQ9K6+7vF3DuXIF0sMuBF4  
1Zti83QCjBx96ZTdbYLMM/us5I5G4vzMj4lnDoV7/9T4lepPCVki2KFui/FWDok8  
jToP6p0m0eQNKb9VN0d6FbMzorom2SnN5Rn1Tu2/n00MfvjzSZ1Rxxj5ySiJmVRi  
nCd0WXEKL7FbiCPTD+3T9gFdZmLagXJlpfuYjSlzmGhdociQfjAcRisHBalxjW  
ZjibyUfLwW/WgQ41cD1AZQSW5MQG5b1J/3Cp9ukr9W+cwaQjB4Ia9fwiyEz4HVMU  
RfSpy3+2cti0Xsp5G86xegvVX2GU7ahyblBquS1nLUBoebPGLHcnL+YdWpQmUrR  
qTE2SDCQ5iAkeBx9TGcbbfSLvbS6diU9zATiv3UtQttypj6ziDAZ3QQdLmBCYQslr  
LTkC5q8VYew2ypibo0gf8aPaG4qvXJYbLbVS1DyGN+o1GbJVSvlOu8qtp62NXSpV  
fHc1/OxPNchQeSSIDPfnBskMcsDQkrMXr4Pjz7mDbBW/Vak1Sqm+MA4LlmaDtrHG  
0Hioz5isRebxti0UBWiJuM0BcjDT8r0Im0alGpJj3gAF3sBmCcNGtgwZJhq+inkti  
Jlz4euhUXIGbrj/rIvLk/L424n1eNoI42cFDdmQ6WqTkod6NYWhEC9NWNQ5NAJpF  
XcpIiQ03LcfwnznHamp0oY+3SAJ4dSonawUn6Ik57rmCyvUz9qYxDrG7rAncvNcS  
68Y88pD8Cd80hJmi87SLf4dF2aq0QsPX3uqf1IBPukMh/59lpkeTzLMkr/FnKBNG  
2p186yuxGRZHPk/YOImu6SLRX5Q0mwBGqExKbw8HGsXY7mNQWHfgXc9XaOnM1mV6  
ow3s7t1XkEq/k0DFKx97QeyQu0vX3LxnXdddp8t8uTdJYwB2mYiFQ7UpsWS79rvE  
TWjndD76fDJvDNZeR0wSuIn846im4QIac3GbnhCSpWDeJxm0oGUdGrMCImiFH96n  
2SopLz8k+jRDFfx/kY3b0pmSXkBT7CZVwGXCx50ivJR5xQXD/LPz40ukF2uxHBCh  
Fj8ZNVANf6V2j+WFH8RZLSoFnMd/jOWLktfGsI7Jq7jm1e4z6ut4x1wlZnn2Fvk  
+out/K/B2Ty2gSuMLUYQQRDtLrKBJFQicgallYE8IOkDbSgV3E4ZWKK387L/k65S  
byysHwFdQvORndRkYWyN4E+LUyf2cteDHcQ+jSMoYsc/OqJVMNh+/bxcpeiM2FLm  
+cPzKTu9q00fRenRgNsK14smV3Q4ZmwEEIZ6cMnoKYwUabfFQUeWrQlrejm6tKBC  
21Xgqrkay/mCiPeotDMSBItxCJzp2EkPN2jXwioVcGRNsNdwTJNT6mMcp9HeijeF  
vQBWJxcrNv1eGe51bhj7QIwcEuSBq9yVD7CkrxKtImAUn/Pq5Zf5JYGrCqj6Z20f  
70+YxL45Ju5KM0qyd5i/8TJQ5vNRhOXLkdV4fJ99j7ERaUR50Mr6XBGiz97HMB1C  
4fKA+D1b1q28n3C+n/ncZp8xRiYWUDcdtybF630pLg6gHdLgW3ogPhF+jQQufKmw  
afGe+0iSC7haeub6z4E4az7VxKD00YWyx/s02zPwPuIZRaEVy+C8mFBUEtCJGgyi  
yOC0iE2HeUgPlarkcoMAF6hNmilM8z4Q/ppXXdzSrrBei9NyaVGdStdToHasR9Q  
JXkU43m58zdDPcqM5gfVxIWe8iDSgA8JUICKQ4EaPHkRg7gHJ5pphz8LHd5Z823v  
KDuvQKgvIaWosbEUvUINWmEvA0NMQw5wkV0NAX8mZC579U+b0mvAkHU88ZzY9HBM  
Mo7iSt7ETTQWM0Ep1Hsf7WF4hi06FLCiMiMCwRG+q/dMntqX8XNSm1jt/8kv790  
XfwjYR5cetXJsmDNlTItKJ8WpBLQ6XU+ttGT7xIMiLE8+CNhk1DiApXsUDTegPowW  
b2ZZc5ijTtLBAmS1hn3Z7RWHukSxxBI7VR4KCP/4n4JJcLPGReB/4YzoWsEYDC9G  
gX1Hvw9w5izk3zjw1Eh+nLq5nYf7ql/SMi3WJTyEWGyoqphMHZ9TCp8LnEpr609l  
3pjsTN0W0cUYUieVySN7DSLz1vvG8llASymyYjUqbdrA5M8KePb5A1M850uhcIL  
xuWQy8i/appFSSRAekTo3ZZrPgg7DEJh3UP5zDTJNkzPMYDE/c9wkypX7SneoIer  
uprbrjckjvfgTfQ0dkudg48cDAEAdVqbRt5ES16gcbUgUpYHZ6rad0jIkGyfIar  
waVIq/OCt2LZjXHCsepJ1WQIpzuLd4TrmWTP5Lfa0ZLS7hXuoSYR1pSwHs+Hn8yq  
TZXTcIh5B7vezohGWam3uyrsZDtK3I7R0o0BrTvi3kgR1LxiaQWRmhV3mctJtJH  
Mc02GLxtLCq3AHxgKvyWxM+SSWMEheb+p1I2zZHsE5MzCPIU6j4JpZVaQ9/26hPO

zSCQX2xdpydHqY6P1WSTgF4T0nL5N4mwGHjkaArM0mxusRqxH97pna0Zdd6MEWT9  
BJQgrnMUVpaX/Bc3e3NJVMRaDrrJNPAAeXQhFebYJ4pvgABQbPTmBguvg/eFRiA7  
yJE1xJDDNG5NVBaerJgMTz4XXPtZLY30stsNaee1e6E8Sk55gcyYacuWL4oWC510  
7aztFDWLpsjTV8/NWzkwq9UhNX0q5+OP4bH1pqijP6qLUahXJQk2usP0WDqbG/ji  
vMo6cBGU+IM5D6P/AopBimyrbjqPaRXc+oeBetfPsE9n+97zGdIScIXd8GfLi yzk  
m0JP8NgAweSNKm05i8tm9aR4Vi qV2k+pQnFnW+lKsapcwpR/MmKzkKhSm+hbH+cB  
1rWvMWPd28JepPvGt7Sj90UqlJFvVNZvKW0E2HxZ256LeXKnsxqptLevnmDnnVFY  
gEXB0lkJ+HDV/FNe0yKLBcmWLCX8LhEjaYWwCqIryocqv1QTJDTFspBzyjvf8Atp  
hh9X9edQaTR00Il7xZYX7VcG4WW6pIF1VwcgbLGzq0VUhj fHigo+6doxEDBUduTw  
40JBwBp5/s6JyR4G5jZRxRaKP1WuzMgj q8bQ+Xk0vN7vNBgU9XkYxOYmTAP3hgWb  
WPCZtKwKfVbraHK7x7efQ0hEtF7tea+4Kd9UgNx0labbkPu8cpLoOrPQNKxknwR/  
wRt65y8r4YJudNuRaUVWyd40/EewCYmqBa03UgFEDECydTki aFupRiZrZT5Van2E  
Yc65UpabLacSyc8Fh8c0w94X3mMFesiYRpYsK8RGJ6W04YRU/90LidhffmCqILN4  
RpG/0NrX4r4zXCt/6i61nvB/VAmZf629xLTLP4kiV/BZfinWhqvqKR/eL/VE/o5z  
LY6yPnKbe0Z2CHmjEZrRmhrFVuPsfRILPynlOQ80hgg2tucdS0H5M56hcXblEDxH  
SDAAS9FQK8WuKxhiLbERZD1b/vc38mPKiOCqMpHn12tY7kmK16TODiF7EAKsATNZ  
Gr4dMJ5Hsiu8jFntgDSWYB0ZhX/ig0ByjlcycqSeKZLXCb1XbXm7xuiyq193Grabc  
Ad7Hz40HER6G6Man83n1lrPoJNzI6G5bWQgktTou1zKS8il70+58VZuZ1QPXJVAY  
bpD/pj6RLap0D8LgN9J89IUJLUFcgv27i1gzVxEqDzc5ktPUQZBIy2BemT0UL2+v  
eLZsnAa4cs613Y8BTu/67Ehg0Sa5NZ7oQAQKQpyZQt8d0cjDbPLI5s031RWeEABS  
R4smWRo/5s/gxRJR4WLOQGP8pgv27IvfIdetH9Jtr6ozhepsznmx67BMbUh48/S9  
hyrPlfulq/cwAddZIUw3wCBh7Wz5zzk35FHjpfrNYGSPqRakALnqakYfSAhwVjW/  
4X6femmMoRZi5L9mQVf23LWpVGF4nDl10dGSm8MTPBIGsqTQpMnDgEgTJ+oMl1Sg  
d0i3+jcIcNlj3QqITL+ZhY5coHSzpcVdCujR/lXVo40f6ymxY7t51mMoXMU5JlJr  
d7MTzhs5yf8wWfZ/ij/OQVarS27SzeIPQEGhvSC/jrHXN4o0RgLuoJk0ES0nMaDp  
ug5DlrRgTQt7IVqxe8IItY390k9njVWoRj/PyarBVCFKAN4080K1ssTC77UjmZX3  
M5exdsnxw3mLIqG6xDxRAnsMG5N9rjY39ELs4D3GHTVHjI8VYKKHwy8zFRh5rBht  
th6M/lQfrZ/PL42mJaVbUfZmaaS8XAiWXX2o5nj2HD4Ri iDGC+vwRGz0nNj6xwVh  
nbpeUm80DRn0lxPBx06zLiSUKfx fBpFCKnz/KV/hdApIDlbKBp5YhaIzoeKQahbh  
aFc7IZR8HIYwz+qfqgr90+r8DqiBwBDNRttYDxXY/dgcsL2qKQNa5qHiCQzH1zJR  
oxXPmQPZqGEvdLPvYFN6SmA139ca2+1N9wmScFqayVDuFHH8U0iEdzYZxgoD5mL  
ND8bZs238o0aImAN0z7PgmbPAYwiwvMiPjzHXCBLhd37oh1LN1HPpj3FLl7FfMe  
gvH0EA9e+r8V7USk2/cbTo/1q+1d7M95FXStKsjnnNUYGINCKYUxgPqRaQcNFR+s  
zaUzPGFP2IfZxK0DbYf0p8L426NpURMwbOUVG9yKF31jPZR4+DwfNwxS7YNmNlv9  
Y1irdKcW/a/e1JoKso/ZsmXWA2LiKt+q83GVFU9Gg0yLWR08zGv5eKv72uv1+xe0D  
fbsfKw08Dad0RymdDhHAcUHT8TPvWxOelQn2vB3BhMw4vgYuQIGIvdXUeAIAIdn8  
KHHukHnqZt5zrvbNTrX56yYym1+AUGI1lmSBxp/mRxZ2xe+FwtDR/jSK6jFdKdyv  
OXpPbemv5aJb8IE0S9QBAFnFskfM907rpP+Cpc/AeH7sgSV0JANcZu60nlCeJ4B+  
bHSU8nYuCBW7ahBd0zv9EGp3qhIDaGbgTRovWAU0uiJVu6pqLV4+gg/BPjK2xu1b  
2NCnKcSg9jX43p+jMcwJj4f+7TGAKcKyBjMVBBIWYU3XIMvjwdo5Ji71lce4L/An  
KXEISelZ6rZ2S2Ej f5fAbz/0GvxxaUQRh7SYJG508vFF6xez7903l9pPZxmxG746  
Q9+ZrFqvtTRf0RzbLHV8i7wp0fS78YDY2qkZt7n9FZAQ6g3xDq3kyfh0S8JrA3K3  
RtMNW0uVwhYlJdWEEauNXSCXI0yof2CmNSrg70vqiRZeMwG0USFi0qWuZIUUVv20d  
/u+QCPRXQaaySXQoPuVtZwt4raMVcd3utNKJYsiD3SeTgELK+5S4w6LExxZJG98v  
DuZWV1dWa7guTB7ORQ1ZClTV+t/ua+LyP9YzxhC/Nt3PBEqLOXrxd8Mz+xOwhurb  
QinzrW1TDl901UFx3PBHs2z414YS0fgwCopdUeTu7vM/q1y8JEdBCFn2+HS8K7PE  
6uYM0mYKT7TZNYh/Qa/UKctSyYahVXUt9dA4niJGDee0uvoyP8zwaRpHCWTdvor7  
6/N+Go+ea13J0GktpE90QixixYpL2Rm0h3RuZ67xURvmoF+8dv16iPy5ZsmjDIY/  
0d+47cxv3s196WJUFBHs0zAyKReDzc4lwB+joJGKcKba3M/IDjSZiXAonCImhc/F  
F06cEmj2rHNi2kwx1DhC41V5ehaMEKifnsfSug3m5tyciSE51Q1mphYH0zGINQYV  
mwDqNuicQc8u7GTVn14ugiNPgKiUEfWxYHvXdj6snifWBJ13FwF/PFGPJ0mF0xer  
SrGZpfffsSZu2GMXFV0ckvHuIUfWkblCtOn0s8QS5ttPBsemX41G7k3f1/1CP+R+  
ErKYca4DD7YXeJXMuuvMJ/fAnhSFcLDkHuBdo4RW0I3ZhVC26H9P246/wCwzWTtx

8Z32UHOP3saWF6z5PBkMTEis2KYFHZnh7WrNtPval/Y/Cf0N+KcEZRhOSU85Vkkd  
2LGEFNQts90zb0YddeR9jzAzvn6j0deyYeI3IudA97t8uhgZldwi4HwvUY3qvFAF  
he4SbqsSMv011+WnSuNwNKUKoHsh94f1CW4A+dvbknaSR9Mpm0jguSSc80gWCoP  
mUvU1IwvILW25axaK6vsWo0SmbNMoQuG8ITSoTtb9Sm4tm/QfZD2bJ+tu93aS24j  
4/vreU/oZR26z0tJh0SiaslRxc9dF1uNKa06GaXbX9wc1LFKZDJgfqo200wP6Hk  
88Krgm8r05Td9+nDSm9TIscHVIVEo96gL+pPkweAhBDJg1v6YHGBvb8r0HMPYsTv  
ej7h++9Qjfr20v6e/f/Gd2Saz/TlWYl+Qlcy5QeDzcMaTXVBHdpwi8uDEytG2PU  
UaApyxZlZr38Q/pDhfUfBrng03+c/FoZzrFHG2Dm1HEqrUelycLTZyyWiTaBkQ+e  
7QbKFV5ZBhvxDwDQxjrsEqzdl2w7I7ftJFo6Zt/CuqGRybrtZLQ52fH0vho69x7F  
w6/LdigPmmsyQYF5x/THMoxj5DjU9KtLSZ47B1ReBnHQKZMoILtIP9EeuZPgS694  
9IhdQZuzh/PbDg50cs0FxpY91WT4zJuSY/xE2JyGpk7KY5wMDAXQxzrWFFbCoNEM  
bFOXQ9aI6GQW6o6CbjipYpXmYaI46hJZc4PUC+FH3rzdIcLat8XMuxCictMKGPY+  
smFAzKA5cVlZXRfChMJ5QpGU/qgl1SP5BNFfHbhJIfiVPPLFoGoNLZ2rE65tCTha  
Z2VPNZImn8a0cTpkXB0ZqDUxgUuq1Kb258gki70V5K/vKakK9DFkmP+Du2XN1QR1  
01YD4rT3Kop+Ovulut8eUQjYb1N1X2/QrtmKxtpuZDn3zfZzW1pOkUS/oEpmKZh5  
sFX1QP3GedXHZUCa6k0RqxXxUwZTtyln+u3A/JvnoQecGjvK87BHHGSApw6hbhJR  
688WTLJqd7imPsWoz2nd4sWTT8fK27QtbQ2+TjBPS6aQyVqiVRsyF9RCaUcIvEFH  
/XasDEeAnuh0ltE29/Z2o7jk4XHAfDKq6ltUKWdlqskuIex14YzAsJ5yw1rtyt4q  
m0JgVA0BxLUvYv80csVIiw7orvjYn3wPrRe3NotsJWK0tfxoKXHLvI240jm0hN9  
AVQgCAnKYvFtmh5hHT2kLePBFL+OH5603DH1AvbR56gZ0/dp37RgSevFN43WT/ko  
hQTgCgeid10Cl+DCCa6lP5YF35sDi8kXU4pZMge2gl5JC7ILmStOhIMwwSi6kizr  
YPBK8NWof2aZ33PPQd/YWKWUlj79Z8tp/x7L67c0o41uEnxfVhdzFLUoeUG9qgAo  
V1k3FB8urZ70by0Ah+Q09oZFoJxi+L4HYKv32qhxLqNUuJYFY5r/av0Upv353pPL  
r01RrF+Kqm5uMwqMX6K7x0WGMbn1wLAm4dDzEv8n4DYg4EBDE8idXJXewxSTzYy  
I2r0Md0pMRKYiaqBZUvXJ1ux0idVamqDlucehcZSt/ehhNpXfmTKKcvYJeRjFvDZ  
lAr+srpjCjSjHtzFK5Xoa080WbrhdQDJvNTLzRXkmk8DonaJExohVqFtprMcrQ5f  
7wtsB0eQss9/XSTqZX9zzTBjC7QcfWu0TYm+UspyrSgE+gqpjCsI/WUGrby3JXQZ  
z10FqsPKYjkguJUmqQTa61dwYGHAlA9VrQaRlwXNCptlgV9xAShMqGc5Qgcnm3TA  
V0hmiAB/bMnqU28PU0T4MaZ1dxHHA7uKxXfmx8U3QBntxiJZ1Wqve6epQDKRMI19  
CguxtbQHy+Yy4XEm+vFfHbUgsLR5JLummc7zqE1p8lnIaLlXlZCILjPLjtnZX1PA  
3I5EckC50kZD/5A7M5Qz6bk3mSZQBahj8tIs00WaJue9/+asI04cg559ES0TJeC5  
4pvgI9wWwa/cYURBiVn61s7Lyanxx+tkohn4UOW41yP7V6xjQc1CJIAqSJcx5Zy2  
XkQtVXaDm2NzF/+y3rbisLS0mAmavoCTwo/CuNHlXlgNw5nDYmf045MuqhUXybac  
V08+019Bdjymh498vZpAfJY/PZKt8CMvYAPnjrrhrf4qsmix02i4fWK71Bcj5bqg  
k8h6tr7P56ZI/d5j4xgOYe5IJV+CgEXcrS295oFAlNcgHjtIAw9LPdcnU+JJ07G0  
2r7xPNAJdVgNaFs84XvN6GNEsgQtJROoGpPOMAZt4mAtZBtpHh9at6zUbVXsIG6v  
XB4+q/nyFsFvJeYwP4iEVccK1IS+Mc5W6Tz43BPF0AvzG+43C/d8YoYXuBoAMEqB  
REQ7lk27SCeo1CD/p900THmAekLgg5IC5VZ7RiGHpjB26nJU5Qh16sC4I8VNH8Ex  
nbfMu9whdC2UA0L2JF01jhcEydhxlgI4CS3FXUBCzZKBiTuIL9FsevwHl7Z5ax5H  
QRRlbyFRKiBgL5dpwZrEdE8/TS08tFcP8BAfqvWXf0hs0HHtdUNTq/10/8qrSQAk  
Tp2zqabb0eNSf9lsc1hGZNYJN33HQFCqj1scHLQwVwhwGPKDUYKKNMTNWl37ML3  
/FPr/6wo30/qn3URs/pPdjEe0zpPaMUIx/c+d/BesA+GIXLU923xChpgUbb2duTB  
glqXXzLUsvQLQaWhGFG3M2VAak2jaoE7ovKaNzjpRQu2dBFppWj5a7Qz/PjAvHMH  
vpsfBRWwStwSxu1AmYvcKQ1Gv4bHvkQU841XgzsB5PCZAQ0seY3oWtb/Npqyv8nT  
5198TYf70X7FoGAJkGjtBhzw0yc1GrB9WuKrXkCk49013BCN9LBB3Lk47qUTfqF7  
oEy2f8jloKyt0Q7EpssU5Cc8F+pmV84/kILQuZkkX7usA71YIwoXvd1fzGUBFzGY  
mN2QQxgkAMNWAXa5vbCaylCVL2yXE/0Na+5afizJrJT5pCHEFT2af/c60GPxnSIL  
NlhH9xftayffo9Xtnu0K+iTVZ6EyIIzwyTqk2knKBRvnEA0VdnP9CBVmuo8KR4/a  
LR5mW44DAfnQWefcLQUPlemQDA365SVhgt0BFlslxS2a1bTUs96/niFYFD+yjWel  
w6u6PGYo9i7pKUSLDxUPC+R1jnmhCRKH70z0M0i+eAHgsJHFJ/Imlr6PB+ZdZKQL  
WvcYz1G0kip0gfe+xD51MBBi0EGWpAreYpFv5Zx9wBhT4ttuIDb0+wh3CC1ohAA  
V8exn4oVmZCAIvSxttgk3/k0ZEbM5TxlTaYMG/I2jsbpuyaQFaA5/XdD1E3k3WC6  
wUF5mh3ljazSgQEtgDp7eVtqheSsEqhyasFT4q7e+bi8J0sApub0AKUfaxit710V



YhXVMfj0yofotYM35Ajq+kEM298tWn6/KERQ9eEYcwJVPsxtk1S7zg62GrvpMaaF  
DKuddQ3gQGKn4u6FR95FhDVPQIT2gQ3Yp+3wKMoRPhzpIHIXAwUGcYPQM6c6gZtg  
EZ+QYP7sL6JM1RkMMJBT//MWKMunq8jEJ91AXBoIB754DWXqH7qWCG932/yRVNm1  
RaFolxU/jXFcNpzohntmV0PRsZK8BteD/Ft5vhhI1xCvANYvGdmNVjeZe/Grqsyp  
C2FnrPdgrxrtVTZBIb0XbY8B6iQbHiYKFe5WxXrGN2UoV5lsS2eHgIm0UDi fX0zke  
RqZz+1p3SUzQoA/Pmmngt7TkvYN3L7mDWHf4rdgp1N8waYQPXJJ0DWFGoEhgnVXh  
F+gvJQLc04wk16ScoUBGieFHBjFhjDAItv2LwtMeKd0PntV0inB842xUAh4g8Mhs  
VkDpA6iKipmh+KqC9MHR9r58jkQcbH3tMfP4YoFLf09XrtIVWYkgiEBZCIOVGL0  
yQKxa4RBKMGAAqppmtoE6aZtkea00y/Z82kp+JpS/7yNL4JtSMUpCyINYkgsV+fjY  
HXv6bHzHjF0+gNoFeMEu0g+3SnaszPZmFWmtDXs3MQf0Ggd7tJCQ0zU07jyI3qJi  
JjjYucAL5YaZHTOr5JiVye7MYbpapUoCDscMHDfa2kEVOM580iLHLYEpjg+zbKv  
yR9hUdvv5K/H43UzHrU5JiW2TkCL80BaSxiSM7dqJmjA9XxapVX2XE6QHjfgv8k8C  
xdV3tWFL34sR9FYT9CEXQbDDL4Kc8m+eMMLw3iv3Z38V7Rgef7IZ7hEZeTWesCy3  
Ul5X+zWHy++uBQy3qyFVq+e/EroIq6csG3e96usyEo062s/5zKTkHbVtUrwfEsPq  
OMfYfYwJjYK6xntDLGQh2IScRGry2htCwtc+etYQaywFXx0TBjxYKVw6D17hcOp  
cdoFMpeQJ+TWViLxtzGypxtJ2YNNf+uQe7AlVe3qDacslLa/r01DGo/h9ZCcMqZm  
V0h2se02T606rZQYREUfX6UX7AqKSe6UQkaug4h71rOZ9e/XCKw9Qoia/t5S3qXZ  
h3RLI+0kU2HAV10G70pcy9DH7xoVY4tEaDLZcqysiePt5QQuk7/MuI88fyfwk3c1  
bl70xhwKA3D7BW4P1wwPZeH09y52i0/9x7Gx44gPDoiUdzPzA9L3Jg5Jp2RTTyPc  
7r0GmgkL52L3qiesl0vxf/+bpEqcDxRPGEARsE4z9cJVJy3JyvYFUYQskASxPzPc  
YRdpXj/eiexXT4dt/yPgWmKGtWn4roJ0KS1kPfZm/mi20yo3/wUq69eZLEpLV6aV  
w+kRFpbv05T9teyxEjVpYeyffMX9rexBVeyeCVbwBzLLJ8xJh5TacCX/wuToLQSO  
k8AXft2+ttpg5UgsYA2ehthTITH68ZG0aceNWOXHQPtgKEBEaTPwLmJ0xMMwSf6t  
yPLCOXR7T5qr7yqTjY7EwM4GLExY5uoJ3SNew9du+6m7lf8StgWj6z0MfKEYbhQE  
tLfY6/y1AxDggIOI0lPalMo4DL9z7yf4T6esfHZ0dSKuXl2HJ7MxH68a0MMwXcE0  
qsHgtES6udP28uHAYfcTh8fjrg9UXu9YWFMBH9dI7dCY95dBleedSV0He+gUhlx8  
kZqxeP9ySWMJDK6I6NJ70RE5RiTQackII2ljRlfq+qKfr6MKTf1JQvPQ4H51oj+T  
KMohQ30E+wBhzrj0c7AQt+ainVlt+jWfiznfyh07L+IOogDL1+4Vz8gA38WxzgXt  
cMe965X0AhIVXn01TPgirGKcg3YecK70429Afs20v6XRvBkQ76RKY3F6MmIchZUP  
eK0aN7BocCXHvdJcXp0kMBXCo2S05BzjYs+JvT5xuhwQJ+LN8USUvVh4a5lof6M9  
xQp3Pd8v6eEPV5SCQRpZ2HbVTgawWmetUptEMQbuWI4ckA6C3kU+0aH9SBSTaP0j  
OKfQtnjqNnPrbErKf704ITGjkwsX9IaWLzdt1PwGXijS1jx90+sHySXHwlpDJCrU  
tmki7Czx9UAFy6SUCla9sMNMEXN7WoNBVSM92s1nBHs0wv6nePw+jT/39qjeFPX7  
VEn4eGKVCdnUZjqrUisNNveXsto+Zq4KbEYfZJ4ja5wwIcrnrw/7sScoVzT8nWxe  
pUPvyPALXqmKK9FWo0FQRuCi0ahn2c53Io+xVsXybbGrPhySoCmt7UFuShggs230  
UqdWABt+z0cAnCokPEprpi+U5P9EaQWbbz7ZrzbZQRsN5PPwSRvRv0fgzpr+Q5tC  
eaY30Ht2SNZJnefQVfRGKQPMostN2XL3+dz9ALmK+2E6I7DH09dsenbmAGYR+iuL  
dM8qHSUbdvWvURzMBaQZCJGsTlMu0SkU8QPzRAhqXeOb8DNInM86ewox8RUgPJII  
AfXNOYTuNnKsfCiNeQbRwd+vQu6ZVXTdx0mXhmbB0vCfWSyTG9Km+1xvRLe+V7yu  
XO+CfylJhV5oiBuDsa0Ej09tY383h1JNVK6ibv7y7Xh9bL7sV6DwFcho3uf9zWb  
Ikg2SxBMUCPyPpmJPP4RWT7DjbMgTntgiQD1pXloj1RZcPWvtFM8K0xq5eocLl87  
TWvyQyr9iShCykB2VhEmyRz9k3JNS58TTzWvWRs9cG3ZjJwp0YjBpeDWz2qR3Ig3  
I8eif7Auc1RCCa1EOAiBV3+4+YJorRa+okHLMXnFPxcJl7ftfg13mfiTJ454TXM  
VTmV0hMMoCSsXWvbcavbsZGgg9xDEOIPcBXfQp7PHmjQVSPs8zctJYQ0Tn2gAwq1  
lT5YpPqjCIPNwr1Gjbit3G9WF3lko0tKVHa9B8nVf3duEmtAVjdZHfzRBUnl+1iE  
6Wvx8P1TPjncp/MZUAxZT2oPousTzB0p0bl/0SRz4fFVRpJ0tdueT8Luk+wzpW8K  
VSswhk9t3wJcpM2My/xBgbx8URSL/zKzCaLbMc0mSnWre3NfcEFpDRy4x2T3ciJC  
wGVE8sQFLZG05eiHovorrX3VtYBzfPESjerP+XSx4Dwji2qN740b65bUxK3WDFGR  
SuGDi8gOUNPaStAkA3W50jWqGisFABKmN94+XruovAJW0YD2AJNzGTn86+3RnGln  
4YGjcLdf8GFfzqBXnzKsR+kjR/ZZLkQI/NL1ZrctsnMXKREjRGQ0ad8ZqnFpTXL  
+qN+Hc4snFm0MqEEFyluB0ecwfNuGP9tgY865RTv6Vh9hoJucLw3a0czzUVh5hzu  
uvxxxVd+KofsQITcRLr9mpbbeFqQIymttC74mCuJcZntfJGdYypTx2UVV52KApve  
YBXi+r7CoSDK7VLiPUz63UNgXt4uozeikkdxcd4MiwOH3BFi3wVml348C/CLAYqp

```
pp9NyaElphbVrwpBWKJU9EshsMJy0Rk20gMr75s6gXSNhdqwxM0ANvGXwx/9iJCw
+R3ld+RfrbQbV2tkon1wonZ5cz9XboyT5wPegvu9zTBjpgg8B932pGXH0u6vVj2b
QP0fqY/gUclS0zvt78xfNLFj8iuKYMf0Sm1fGnk0W//hRtFZtkK/olbdKCs0KGnT
W041Bkj/zfmtv6EkL73HgjfE6d4QH2st83rucAS9iLK0JpmI8awe1grAKnPIR/hZ
rCmZ5SfZoJVLswi03Yf/12Uei ft/27CpwYQY7FKfNux+47L6M94GETTwHQ9tuRJK
cLYP1yqq9Ku9i4wCxdIwTco6Zg4Gj08Zm8F2GjCzRbRBJBvcAFV7l1zjVptCha0
jrAJrtdLvfwzyDpjNMO5iyftA/d077k9pQmuNK2PzKJq+07s4FZs0MtzDYmK112k
MitNDfPyi7eccs1TIkzPmYjeeC9PTg6B+gSTi+gePs42fKdB5c9C0Yuhj8uuzvtp
0o/jEEdYxFrIvvr/gkxspip6dVKeLnHLZIAH8NUap/aL5sCnUuEy9KcUaitERjFA
stzQYwXJAVSgVl4wEhVuPG1gL3JnHPLSYjN9ugthpAyaWNt14gm+gFJfjb5lRQAS
HN42kC3CDeI1u3QcNR2qyc38wnvg7SiBT3Px8I7TG0zsdjn0LUD1DzpR1X26aJVQ
SeaubLn4QPG7NB8oHuCXfVjEL2iQ2s648Nw3lMHBo6qjw02d0SxcasBVyYzan28/
MI3Spayn4UWvJuZrsNIbNlniGkZ1PMcdkfoEeAHA+Wmdh5rn6LXLNzon4QstkVVg
DfsaGuPUJ7m3va+XKpasR6w/nLIZ2hGcCc+4za5fQ6nu0JDLISpkYewWkYhiwkXG
cz+vRSWM3F/aLIWhTUPWnKez2yJQ+uBS55F8l3pFZXW0lleEuB9c3DbYCFagh8Nz
x7t5sc+15PKch7ZGBNx7nUGSu0JvwKvt2oyw4SA=
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the SPHINCS+-SHA256-128f-simple post-quantum algorithm

Use the following public key to test the SPHINCS+-SHA256-128f-simple post-quantum algorithm.

```
-----BEGIN PUBLIC KEY-----
ME0wCAYGK84PBgYKA0EARx6ql5/SCS1BkE/R6nr2q1a4TrsEJfEQdER277IRvZl3
WPPxy7jSJ+z9XbFCVc7pYvL85Dk1f53xYmhB43710g==
-----END PUBLIC KEY-----
```

## Sample private key to test the SPHINCS+-SHA256-128f-simple post-quantum algorithm

Use the following private key to test the SPHINCS+-SHA256-128f-simple post-quantum algorithm.

```
-----BEGIN PRIVATE KEY-----
MIHTAgEAMAGBivODwYGCgSBwwSBwGG8/voXg4JTpUDkfYZepMvbzddevaXjA9LC
yl2/uhp/6a2DYvBAC2ITM54TBS0KTwrPWanRxKSo3j+L12Yg0o5HHqqXn9IJLUGQ
T9HqearVrh0uwQl8RB0RHbvshG9mXdY8/HLuNI n7P1dsUJVzuli+Xzk0TV/nfFi
aEHjfvU6Rx6ql5/SCS1BkE/R6nr2q1a4TrsEJfEQdER277IRvZl3WPPxy7jSJ+z9
XbFCVc7pYvL85Dk1f53xYmhB43710g==
-----END PRIVATE KEY-----
```

## SPHINCS+-SHA2-256s-simple (1.3.9999.6.6.12)

Use the following CSR and keys to test the SPHINCS+-SHA2-256s-simple post-quantum algorithm with the 1.3.9999.6.6.12 object identifier (OID).

- [Sample CSR to test the SPHINCS+-SHA2-256s-simple post-quantum algorithm](#)
- [Sample public key to test the SPHINCS+-SHA2-256s-simple post-quantum algorithm](#)
- [Sample private key to test the SPHINCS+-SHA2-256s-simple post-quantum algorithm](#)

## Sample CSR to test the SPHINCS+-SHA2-256s-simple post-quantum algorithm

Use the following CSR to test the SPHINCS+-SHA2-256s-simple post-quantum algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIJ1GTCBpwIBADBRMRAdGyYDVQQKEwdFbnRydXN0MQ8wDQYDVQQLEwZQS0lIdWIx
LDAqBgNVBAMTI1NQSElOQ1NQbHVzLVNIQTItMjU2cy1zaW1wbGUU2FtcGxIME0w
CAYGK84PBgYMA0EAvUCC2EqHM3A1hYoRDdmLUH0rBpbDoKnlfLnFbpInHjct7cMX
0vRd6hFz0fIC69yciXgk0LaYuyUGww3i4gxu+6AAMAgGBivODwYGDAOCdGEAV7mo
vLSyX5Y/qXGvr4F+5nRd9Pf8dNEPkedqqlhKkuXDfXb30s60Fc97R1pqRDkMLXgE
T+TBhmIHbVToe17lkQsTBTETQJQ4w+fpFcBnG41D6oagVU0RQoCJkDW2Yy14RGRb
LQLqwu42U6a0Z3cQJe3h0u06fsZwxB3hsFwyIaSri2WFX/DqJ+J+XCGzWGLdBneK
578M63deFCpFtdRQkMxgvW6IR46IgAlxc2xV1byQ0mKMqsaGe0j4m+7I4KXGWQlw
WrIGpeL5T0FzJaii3m8e1knKxpZGLkgL/QnRhVC/e7Dd7H403oE6dLxE/UE0o1mo
YVITQj0BetCDWJh7/lQ9sqJ/4uS6izmCYM8a/3CharPGDJPlbTncWx21qF5Wt/2W
HDdbeJMCRC2jXSMYtLRrc8xsuyBbc0WjJLw0vJMQmn/XU8dx0hFSBU08ZMJDYyxz
UqK5Q3tqGr+7BEIzgnVbeIXZkbflkpYMrXf8jyJntSGAe2nWw4SwXi5jke9KzLiY
kdR7o6ELI+c1mexwf41nY//WtKsY6005jDwETyBtNaVQb4R9dx1+0ateHcI/SkS8
5uk90J2ISBEtktU6Ve6vm0dLIpPZ56aixbFJD692LFJ0B2ZNTmv1JcfjNSNu8nT
epTxtT+k7puc7YiYt+sMIcHLRC+ScUdfhcYby25mi7xJopw71UWPu6WjkqFxrma6
AhnIvA7fBwD+rS7lwt45+QKkDBAFyeiNigc3sty1+epwaBUls5fECAf04urdYxI1
jt/yiZgRhFF1aLUtTUY81H0J4H3AiEvGfYIr0Wjd3ddDTb00M00jqLF5iH8+9mzF
HdqNbWU0JKZU09urfwFP9ewGNyYDE16+ix5YfCqFttLWBn8jkjwqBBCaqi/Lz1IX
LqtCUjaGz+/aJDssm3SiQdQQfVNVqidThdPHJ08p2e8XYjGqV8zjjU8rH6fHEY+q
SMC0qmbb3YapYGaPewwvVZGGk6bhAdBYGem1DRpNkR9wFN+i/IuLi4L+kyJRdCS0
60+Q3XqQEIOxT6wBdn/0GJpDi2SfOLA1hpwnuIVr8l/eM+ftCHCEq0aMFayfGjp0
7XAHk9TKhI5dJnwbk0Hv10Iy5E2fAHVL+IXjrdWuS9tQLK9FNf7SpsPXQFfJYsv
lgQbJF0zUy9jvFi7TtuZ3TKJoJhJQ/M1zfIQ6vjSMjJqQKAb++c2pZ3H3DEY8mc2l
sMxu4QmPnmPGs1p0RaDcYNw+gHvYyeiqzKw7RJDQkmzanJ53/vxZW60TsZbbk7Uk
XTsv+IZoNaUhw7KX+OTIzp0CCtrU2K+osacYt0EcGxsm8Zvx1/hxE1uhTL0IGxE/
269tQZULA5t068ieNkuP7nk2vQ/T1YN9bX4aCLgJam35aWCVd5NsT9Ko7lFZNovz
fGCGoACZUW7QpMJsB/Mi9zXwGcb0qTY70fAJ2PR8y9gftJZq1GGSEyPTimm3SiF/
dYTrs/sJSj46Ge8zEvLqMbc7796dcvbHNuehCLEWKpBRd4K4a3JH/GE1lX0JuJKD
f4csgSvLzniSvv+poBkUg8o0QI+s16+0ViZmflAVLHKnaraY53UnKt0uqIsp1Yf5
L/35kkIwCPKZLd8TsJy4qjv1oSKazNsjiA9Y4XKd58qTlmdllOp3bGpt2MshMOXr
Nvg3yqkX4dw+LIffrww4v16kKiGakkeLy/5HoYZTPCHY9iTApykD6wWo185ebmkF
+DZm0KzM9E8Fzb08k8FczQUS6FE0+/+auPW9h+hKKw4HNy00nYCNtwyzUs+BDt+T
64MQfAc90MTHgZHuukU5a/KwQ5ArI28FUM+1jiwo4p0jWml1Xp0zjkALVCzsExZc
CK8uiIsLndoBqKQAQ42hSssqaQVNCQKcSDJgPd9sFSk02MesAHSHKU7RhIuU5u+x
piiy90F5vZWDvr/NX3v20edJWJwudJNQ06Y7E78pZ6ipxukyafUTynYhASghFoMt
fh8gyhnlk046faeJanPrIegkZsUAuI3YBpFz2nVyoPBvYhNo7NE/yvpirtxu7R7A3
P11e3wk/x291ICQKbsvGUUB535xCjN/zBaEE5RVGLx/SRKjwRx6rNqVofr4QFwdX
ThH2GSYLTYUXkbLM+nN+Apjll0Swr4CyGqkPMRVlyZ/7JHPtpNEdpCrVhBzpp0ib
tvGZsh7nseJVw2595k0Mif95Ne0AS/DcjhCDwRb5l9cM3/2rBTI0RkPgApQfibEs
9WPHJs5q2j196IgHU9HwKLA4AZkRDsFvp3aii6BWTi9mXXgG3sJ6tkRAXOFI44CJ
DrXf8dwr4WyMy1qVtf9+0/CzG8/Y5jG/RCBmCic1DA93sut7j/bjnxzz3NXaRWG
9pF61g/boEjSIPRSg9C16hwK4GR8KaBTUDB6mb0RC8jT2do+wKXBNp1XQNEIeN6S
HG2oZ0Kww1UP/SNqS5NzWZA6IKHuHhe7Ke2vwziB2HZA33/qkbg15jfyRh37DG+V
lwAXaj0gFWXQmWwgYOWLmUx25jc/WN+4I4ZVEMy0b0F7Sxqzmz8UQtu5hpMjMhe3a
eA517+WWHkWEobX2y0C6A17HoZSiHx199qPjgwI0AGmumExeVGDvMYCzqAVxGUua
Y80Xm/QoRM1XzKM6z2cN0Ts7CVpY9k5Lz7R1LUsr35XaCCsAuS31xGZ9EYSruWQ
6kGpqqTn46XAQh0qPlsThIQiBX/HxuS1/p4w0V1NXQSNajSDRUjPR7US0Rm3V71L
```

6tNfVjQJRy46UBbFqXaOdbSaCuFrhipq9EgffiP5PAAs3JDu4NoLRkzCcIjTTEnh  
zRcxfc+Yd/Fbenxgqo5Y3tfgXGybRdh+CNTUvroTAjltRGRy+lOKDvh/REHQHZyA  
c9XYTf0orX1C9d5Me17yb3RxoLO/dTUWEdkhPbNvsZ7HeFbOLqnX0qpTvzaEH078  
khLcJe36MiCTKUJWS3EVCZXFQo671fFrJ/02M84aRjT/7lQlofyM/BDJqxm3wH3  
eHgSBY0TSyXtcbcFccScyQovM/hy3FqKesEBcdLR353nyt5+I6leSyE8ppFtMa3k  
3jFbKijEZPLzCXH8WPocKjh12vXphueg9S8swkotvIlp44/tTXq+Tfy3nDysR4G8  
HHnH2GamjpsGHcFg4PXELrVqtiGPxPNYVergxyQLK150nAx8yMkd+any2iT/WT86  
E52PLerunckE4X1LS/4DhAeWBqs+zxc32xa0GjEHqijEngDMLdtAif7/iwwqLz4Y  
oL8S6PHxnT04kSD9kj/BLfbyZoWQdhLPmUTvYKjWqChX+GLnMqRdwm14XsBa8yg1  
qErFF0Q6xRVORqShsn6iKk2H4pAA6K/zoGUAf0d80Kah4qHrBndJHkcBE4qHc+TQ  
9oTKFucrkx6u2vnT5ICKyb0aSBQl6/squq3Tsmuou+Xz810zLptatbpeq2rmcgbBB  
xoJGJTgwcs6IhU1pX4jtyUvI3vqF/KIq+zF3CWMfH/izf/V0keiw7UmUGTYvZUql  
XghiAp1AtmHJVUBMeWLDAY7bNp6wvhUgBB1vxBzaiu45xplHJ6LGzeqC10AWfrkx  
fhdGcSD9iKB6CnYVnabi0i0G3nGfz1FfbvVWoN8D0QZw00AjerDUI3A/sz7q30U7  
Z6xRkLqTfZGLh/veZY94EdY769khUSe0IRq3Uxfr2hyY6GXj0r5/m72YPyfl7jhw  
MKsbmTPiu2AuAYZ1UhWjXKbBmqum0BcSK9sSmdqczr8r7yblpL3gzN3m7qQFoN+NG  
hR24qpZySPcNMTt4QvEhQb5RYF/JUPYv2qFCbyh+oxbwLZ5lcv8fpvz3SIyiP8Me  
HFyZ9jIf4pkKEGqzROGMaG+fg+9mQRvvgeXXD2qprne2wJQGwzBnTdkYbaDsfgUK  
ESVsslzuPb1MZOS/HvOLRSgGLHuyvcbjfCLNe6Qz6lcX9HbrwuKL1SyD68Va7qZ5  
G32phyoZCEV5dEEgNjtx4IILM13Ey8Kzc34BTZbMxya0fouhKfWD1C0eY6liwwtc  
zZ0KiRwW9bGYMFBARo+L3BK/cfcob8GtQG3Xe+jl/W+KdZ+09zBTtep66TCsNGgM  
v1d5tCySfaSY13eVYBN2CCugjNgLA5tdmkNyC7sS3v3Ti0BYyBRTMsgm7eG2rEmF  
kUWgVqZFzXCo33+xeL+YvLQefVt+fZKpJ1V3LCJgM7UcaIPpX6sG1WPLJPZP806U  
f68rfLaYi16ls+jzJ6uJAHhb3y3bh9EbIqHUOrWDo5rrh0sTLL5c/FMyVIL8pP45  
++iseahk7QNr1QGKRIGjo88JIKRyIJTM7LkoMgvn7G3+edKseGNM2JSGQIWLmZff  
vtvTsUzgl1XjEq3LVten9BGMb6s6BAeM48sc972LJwNuPIQb3xArvqGTegaeT6BO  
YpuWtksGP7yhKleSJ1CsGNG8cdikkpmK2rFqtpefOKQAIzIginAnE8VWi3M/4jjk  
h3BKuSWORTag+K3h0xakApB06ZY+/8Ynce/7nWH0hgJfLAH7ogHHAtfukHJcYcnq  
lZH5fDe3jdtfo4+srE2xIMXT4W7cVMV0MERZXbLCHfhTTKwTBMczyowP1bjCM+ZB  
ZFG1tawQisrkv6aqUCuQmnV8ehfkYYhQ8+aJlAgCPeYuT9SMKUiirj/90F94XjIyO  
Tj8SPERUSdnfvI2C1g09jS/ltk20FWox0rxEdSEZSQTVniNKfIs3o5DxzW3gs08G  
LM8PIDcZd7L/NeeF8W9fK8bgK+qq47gkMfX7CI0e6p1r1+u8PcRkxDGjL0JvF233  
aCWM0BFU5RHuPhybVfMscS+sdffOu0aGmHHqcMgc3ZpHqDFCegVca00zSVX8DwsD  
000cLma7eIyLeMggtLSy71A5hqSB1BAZJM0tyo9XG/ZvRs2ncd92FkZ4nej0yPB  
xXKfndPf0/gRlaInvbpyTLCIVhou0/deaRdijz6rI4LnN945BnViZGbSGNhX/OK6  
GqIPs+UjIxUukBgD54XQ3JCiJYfrbInxr0NYcxK33nnyZ/K0U3KPBqmd4IGg9Q6L  
jeVlytNoxPwXAZxpe+49vTy7UA2YMGmU8ZnSK3pIGyx4VaLXnHZNb0K4rjt2AeZf  
ii4pIgKQbgI4hqpt55IyJJ2Z453ru0I0iwY9zprY1saHp3+JY28uiAufbu3UfeLQ  
MQPdDES3BXanB47rz+PhOhoLhz4Hn6FPqNijAUjPXwCir3zHZUdb3YOW220E8E6  
P6Zr5SCfn33jDlcxWzm0N+Rl0dpDMfWCPxu0oS/uGuS6HK0nU4FIhic0pEcrNsld  
EJS6Lwg5fH8mk2LJU+ltovNXtMPpqrEpJ+PHov/jXUioV0FK5i0YNpZztTmONQea  
ZJCipcsAghPrm1rHPFYWp/S05qJRaIpaY8y6dGHVtaddN5RwGxllIuZUsvkv/h8  
iehQm1LVJ8puGPGrcdujUn2t03yRRkyl8F2fQXzoLo89J1CCuToqzmyJr7LS8RsU  
1Rm3xZvZLiUJwwJVzxFDKMDL/q0guj504vRA60vHYEsuXBa4m6+XsvuxUn7JBm  
60VdtjrH7JEQUphIR2A4oLRpTYZLI6EVcl7IEQRUIC77CYyjWLFH8mtFAlNjRdm8  
8JYHglydIIGR9MrXYezAM+zCvp+Gj3H4g5VZwmpZh0LxH6dx3c2fmw/esuhr9mZ  
4LSE3bU0hyHtkKnGZvqLQsHr+nbVUe2uUN+rnm60YJbv20YnbevFqqTghEpyeSW  
HuYGHYqnZ9X30Xiyd248lijelQz5djQKzZhvyOwb5LZsODilD5E9sHz0AIXxqIjb  
c3TuG4NyDy38TiHaciOXKEW3PDTE3JnZCNaWhXh7muG8+RCUb3uik/4AcfyijW9f  
d0Igl1st8K96Pu4MuWHELDpyUiafp2Qga5f+uLkvPeLiwhFJtKqsJcYUbnNtTBJ1z  
e6prolF9+sruDkRKsXm/qR80bViGRZ1EPjXARFyCGN4tCePL3CkISfa8uZt033pw  
hqDZ+/0MnBZtr0r+h3HeiUHzMZeCNC/6UTn1oDBPvB/2TZLxPBdt+swb0FFfjXS8  
IXuXAccwHXc0GyEds+gaHNSpkjYx+Zvo3zU1fZJBt9ojnK4LQE+KRifeN1vUl3Nl



mfa3FJJrKUz7+aBY7fCs+f9UTP3kB5U/4SARbKAa0sh/6JpKi9iR6zPFSWy/vY6O  
24MaHgHom9CiRH46vRhZ6dfDqpIvPsbRx0qPvXzq0D9rDVH4kitPa8sP2Jt7rFFL  
81BIPNE+cFXgm2MAyyaa/ar+aKqU/fOLrTxVuruYMcKwvQLzdWAXaXS6rg5sE6r6  
QEYScNTVkoqGoq9/BEhnflpdYiDH/OrR1gyNhMHah0LJ9ujw2huTy+BGJ2DAM89A  
SL07opbdwgE6u0RvSQ4CsVvKdAiKhPot044IQ/sLagIiY2+vBjsSPj7kvDm3/wtO  
e+GbiYEzEGCK65w44pM1UG+LUV7e2cGAMi3IdObVkJ4gzK4yolkKqZ4/lnxBTp5AC  
tdoBcTnaTbJqmb20JFXwFdkPc+fTLNeCu1DrY/eQUoeBz80CRDSF5ptRgBM7Dw5N  
EgCEfMANYe77nhsa7bN/3hKq5ktwqa0EecqfLSic+SKDLfaXFo76910i86s6NdN1  
FyN0fS+GhrGXIOA+W06Cq+uEuxghu6iR58ydw0jGAq3xYnt26k9Zcvo+X455cHU  
amTaYqmJj2rywG7a1HM1J6K/j8xBdtI7MA7RbLWWbDYHXPSPRGMFV4EBp2DF0FT  
l4n6Ehew5Mr0+0oP3jB7E7/TWvWv46CD87uFMT+yvObTYXULwHnby5mQrg7osaib  
HUEzjYsLkZH21WankY72KMLxBKPPr1Mvpzdi7JHmosMHdtiBQxP0GrSTXBGJR6EL  
lQDL3k+daP0S9SBhurJ7y98y2w5Z0uGAVI2YU+9z/6YkwwllyHCzaLmrb8BE+8gq  
2QX9Ws/MzLDSVxKwq3Ur403n5pW7bk/35yMBujmx8wvVbyKGxMGUnCEoa8s818nI  
zki01IHYT/vWqukhjItk4iu3+il7ohCcr8Gbl199v96qFheCnaHyRV0dyQkSqFzf  
MtgDjyJ3gtvfY0/ZDb6MtpVCKB7NhLu8Pg9AC6CMcQI+RpYHNoh3khZDWcUJfjRa  
ZSdFGWQNRXhr27HB2vt+coE/nTsSk/neuKl3WyXcbejbx7QGkpNpMcjU8dA2rZhk  
TDUddNeZGqodM2Wy5U0BqeGcDDjZX4Q5ueKjwZY0f7xV8jLaziIiJuX0BCegQVmc  
XckzRnhmNbyaG5374iGTpugAJtY8bABD60fsTsl2Kn3DKhfLG3eC8WHKRGY7JqbZ  
kAkhx431cDLgWVTL5FXAFVDS1EQoYLZEBgrsfYAHZDQZI0v2K6LSa5Tb/wHn8/G  
81lvPm7HqF8/dxNxoNmKp9tjIp212YTonC2oLh/4RVFL6Nig2IqIOfzYD/p0GGBg  
M8eJaztwl7NCyBirGxKnozh8gi5JvqGmjQ5SGDlxtgu7ZsbhtIk+AlrDAco8LvV  
wGfFT7TnB0uGTfW3aQzTEaMAumj9mpWgCd66wsAvA2Cc7eCncP6UPymfyVAnCGDC  
wkVXH+Dji0/alK6tTgaJEAnaanaDk26YersmzwuZC9AwKhBTLn5Mat0F5a8EXf5A  
bKceHo0NBefl1eqgaZExcqfLawh6m/tjycQkGLPT45CWyxwBRWohvLCDeXqS4Zhv  
72N0wlKv/EI0LLK00n22Iwb6yI2lfZR5MeVPrk4t4fhdB7wLPmG0zfJXTYgfYBma  
fTbWqxRZqdmFI3VmR/CgVQ0kuIwxWtv1Q/ssba+UaBtH0t38hcEKuR8Jdk3zEqo0  
tP4lmaRNAkBit5hda5Fpfso+Fv67yHKqM9VCKbW4uVPHcUbaQP09aok0TVfxMII  
sC0TXkGovnb+YfHp7tT8XCzuK0IBt1mzNMGxCkTnRLI4/ZBm6mtFquM0qm82Hdaa  
9f3qvPo/fRMgYGCie219Q9ZX3I3UgH3e1zFHjrFJn/icPpUufz01MY0+R7yqiPrX  
VwCsosjLR20PP8rCKRBVx22LCUzED2I+GDhAuZXICzw3ZoqH7l7d0vUdPXTTC+vJ  
EpTHCLZsfA56YoZ9/FAaEIkmaV5acxe40zmm/Ikaymbs9YgowThUAK0MYN6Zoch4  
6bIcetgeKXxC4kqp1BxUjCpPbGrQLtqmGcyiGRlQP/tWoH6ThZuSuyC6i6fRYKny  
NowSOQu833jHhgdlfYwGHLf6oLkcJqnJTL3b4Bz+dvH8rmwCtR4aE8W55Kqdhc4  
N0Adw3rgFEWSY8ynRoQgMuHxWU1f/cEWge0tJAxeZ/XQaF/9J+ozVU7Aes8f2WWh  
yAWk/E2XnKvr2spBk4rz+sBwsBD0wp9o7Nvf5gM06PCODcfAMRM5IahGgeHGLRDK  
YGWk1kuLbL1yNacdRgxLmtekUclrf6WRLjEXfJI7bJmfTyTtik0FdesSgWZTLmCW  
/Haq4LlLQpzTo8kTzmlGVCuGPgJdG2iJyPMg+YhGwnPWYkC0ZCuhx7uUadXRYEL2  
m0brmswhvSVf7eVtPOQZyL2LnIiKYmj0cLS08IZvmLHwAM8dRbso5pJIFBrApLsL  
UT7t0nKBCEwyVy7kA0+k0Y8Tj9D5wdUiRaAR11iIr4hEobckq3JxBejDoLTQHRog  
pR+kdwpn2vLK2ha6hV9+zNTYlVrLFLohwf15swKN0DOW5aM1efa3/Xi/mi5+JG8V  
nYVtmvQMvhnibQLhmX3liNbn5ZP0/qsZjByqmnv0IwcIr6fXF2zgD+Vg+b3gub6  
JjI7aIw7Y6NnoJ5XFWYKNlJfTnr/zojvYwHJ8mhsUc+aEJoTDvTN+D2NeHM5P9ux  
4FWvedD9W4yTiIl5uYzZuRhEY4zoblla7oewWdJ00ZeW9nn78ZzGBzvwFB86+RdQ  
2RrnXxmFKVytioAt+p0c5+yHD/G/lPfdes4Zogn8qv0mitDyd3X3zwQvU6zA/q3m  
l7krmV0PCGrYOP0CHMFEPzTsFBWcfJXNYxLiM5YXLWFzdCdlegWZctJ8IUR8yyZ8  
noSobJMozWyKelCvKqnm18CFMkigJeTFAR5atJ0Ld6H23UagpWzfIgxLuVDv0245  
tuFkiYG2c+S6hGixq5JHHWcdLpSLt2rIUSr0h0m23CZwxBbefj3n7f3GuZ2y8NL  
R1yWsA5fAfyRHajm9qbOFUpLDi4oFS3bP8MgZf8kkYON4PBDKt7gnqG2VZ3GnfFo  
yvl3gnG9H8XV8f42c3MNfv0uZErow0Tat6F1TMN2ELzrZehS3kDLuiPBjx2v9BzV  
F0CuwGhpV2CdiQaumF2uARpR/SVfW3DqahTuVPq5UaXkpkvLGebI1SNrMvBlFKRN  
gPahwno0ybGInx78QZ8+/dYxsnrbeNcgWAm3bbR+ngRorB/62IzPrTVUfwoukUBj  
Ts0f86QYonJUSZNtDxBYD73Vbqz/YJ9Dg6sFc7Ur0AsFJGr4pFzw5KmXgM49aELw

508t6FpJcNcr63/G+ZHjhEPk+Yk9sRIVbwQgz6eMqjJ+BPewGLE109e0hHZ6JB0  
WqAbn8s6tC1pGKBqI6CCRKsQUQjaCY3wM0IFLQ27LoTg+KFXg+H5i0Q+JPlvbN+x  
MXMIZcf94wGcqKZjvZl1b8LqCoPc+un4cYZLq4022nM9LNifbu4xfggR2BqxpL/k  
lyp/aFD6fvnIQWsGzYqRnYdN3PTXvkdQZSJhciodtOL00ibF4xPdC3ZdBzCmNzWI  
TM26tL/i0gMYZKKqlaqooN4/SR82wUtEeHmhTZ6MLXL61+B9AdVP00hHDBLT4Xk  
bJ2M3ljHAcnfQFJ4LzJGUcrkG6Co2jo6VJf91nv4xzjV63op0tg0jwz5r7H5R4z  
PVOI16B2TFu0R46VE3Iw9EhrJiW8keSrwmsDFJQ0xLTcq39mnia4MJJGhK8GMANR  
0QdcsHG88Nks5D7aVcjPwE4beL/qbbp4B6MNkdK+AjYZwx1IBuK7uHDZ70+wd4Fk  
Ix78zZs+saFiGoWovziFqhcnPQdhJ6B/vrafsTQ0m6ZnS+pyZBEiNwTqP6CU6SB  
6jV74yPnSLFzqfpaA8sOHMYzyYyBsTwI+MC0GAU9qTfGDeudFrCm8oaH4fz4oxUM  
1Z4fZqguOoBlsRdfbMasu2tJ40MkPn8grJQLLCuS85jCVQxLGx79MShtHZc31Ht  
ctoS2iIPEmNp/nit3ra86yF8MtaIqaLhu0w7vEG6Eh0Zrw0yJfdVHb+P+G+1UJm9  
MfkG7LcGU0SvkpuxXIzBfuggA68LJuRqbZmaCSKzUzVe5NH/n1t3cYXJXf0WhZcx  
4DzLcygXt/wDf25mbXwkbcdFL/D2iFuUkDSuwi+HD1YG/Q0plHBchql8XrX0y4V0  
/ztnaaImva1JaD1b2e3w6ulDV1rXI0hBOY0BrAKM7AYML13RuUC6EoLibkyaX2  
iDQRIXIyAfHzgi7roLzXZSnZ0rGgUKCR1tH9YM0RY1GqhW29+FhBC4o+Aq5xcW3v  
YY6Zua1E0LzayfN0mUjnLxvUy/Teo2nK9gvU3FyxtNBgWCrVN7T5JcCDKynNIT3r  
L4tI+ZTPq7tN3WcICBcMTHz1Fiz4Xz2b0S0uaGcjE5Pp6PnStdFqQisS8KMjcQYo  
VF74cR+o0A1un5ko000T5SAUqxkcqNTfYKiul72n4aVnAd7syPxL45AofIMqo3xR  
p2zYjNy4leMvQMwulaU/gCfAJHGBIgS+jVwy64i6Ne+VqK9hOGi4npwXsAshyvX  
y/Rf0hafXMk2mrUUIINw4sCc6/DsL0lYnlTvtXTnaNrcXBjKY+nNWgeNxY6XMXgYqk  
kLyUxuE+ONGQRATtESW5gM6l0UU4aUn1uV7Xu0DXvDikiR/jFUeoZVrtiRBN2koD  
M8vVfELunx8FXKMMEz5b5e3pV/YQyrctpuUAMN07ZnreM0957McRKcdw9n2NmCcs  
qXw2eHnmE1m/rUtKHwaYEEHwaCpkZLAeL7gf31r2PkrdL9MxYrKqEJM16m0Z4Pvr  
NtdlbKzy/WKIHUot+g5cv26jC8Fd6lnrCgNlF8RgNNQVJTfjYHuLlBdI4e10BbEc  
s89fTjPfwBngN0mSmKA9E2pEmH0GCBw54RJjDOHge0Rb3UaB9Fdw95at7DQDRlFu  
9Ew3U9fn07cdo0eR9C8I2yM9aBdZDpybFQo86MJjb2ZaA3yyB3rv10rL5dp9Actf  
WFMiJSSy5zdjcEw3tFbS1bv/r06yzq7XJfikBd2Ysin01omp0gSJgGRBIF/vHEtC  
c1ls/8k3hvmrNhfh4pJwJs+4YwAJBhL5/NLTXvK3YYxv0DHEC/2ouVFMteRI3UBL  
D/kLQpx/aImIPHAbetjeQL6ijgrhfIvXj+6FLYpJAKalNf/t7j//a4uRW9aG60Y  
Y4GntW0wQg5joFoQpPKlag+7QuqbIazY5jc/8HKH2gwZltxJxuzit+14/NrL7sn  
X05dhz2f2e0KUEV0SHimkacmjPZMsZIr2xeMpdHstsGGQLWNWskTP04qgBTIgH1G  
u6/G+5sSnKhdJ6Xg7cVE6wYE2FF0lahvYtLJRn0Aabqpk5YAx/SwzCP8+EQCZucd  
7ZUbKS7Y1ES1wfC4bXeUfvuqLJXwjvn4lIGbcNNpIFnmCCPpFdLfysLm76Y6lTWz  
9zjJmo+kQetyaIa8QJrq0D7hfZlEEUtKTO+LNd0XLXwjTdfzb37v+qWYyGPxgrJA  
30ML23m1B2sLG93bbM5eXUuzWCY/iKqd/9y0XRu6mRkNT0/DJn9JJFYlD9NzuBID  
TLZCkHjppTTAMAHFGNAWYuHoidJSk/9SyNnSam+PpNUBezzJNVgpnv7RByTY6cNx  
lgtDPLNYr/t3PN44js6IQHMCmjIqad8J000hmJM6fleMNndAbitJJ8Vi3zvedf+W  
5gyUfwoEDGRnfP2sBsVXxHZMgvZYdU+0Ijfwc17x42QUB0YJCKnVwa0s7r3hInZ  
ywmP99wEEr3eKvEAfwrIt6rY0Vsauj3YUc+7nN3R3UOHdNvtJ4GML29F+rW0ZFJW  
ZlJ/XM5y9/yKaKRESigF35xxw5IV634/s/TXrgydJ02ncw3AvBPhBeSRf29lAic+  
MlzF3Ww3TjQB+KlF31qAc18fswC6KnX0jfuW8L0NYT4B7q5MrdtPd3kc4zeJY5cX  
Bz7KjvEF/CFqc1wQUyXCSg5cwiKqUqSiauudW3RsVeB9ci40GQFQqz/bJtAPHzG8  
c00caaapRs+LwXJlIg1ZO1CXbM3/7NMr/10HMSBWBxkoZ424EU7J09KI2GIKs+oPN  
bj/P7Vh4kBSIAoSZxfaaIQhxJBsdVatDcYg1brbl0XrUYE6KVvii/a43vgU3Lv  
5L05vYnKeAb3kar6gpUon1GNeE65pNmGQFiN135wZHUUviEvrL0BYcHTzmY0yyJa  
8FGbeg5eP8ELX6J3ZCMgTl1b8a7CMC7d4aLD0D7Ne01RImEuOWHLSAiRX2G4SV/P  
JU0Ft0nkrSvVaTgkYPmgY885Ed9breQW0N148T/uld0CtMZ0fVqTmedj1jH8CB5b  
IPOCAfPHuA0WL41ir3o8JJYLX1yaAkoLDx9VRJD5WIZIRSPYJ8zAAixqE/G4p+iS  
MskPfjz3KZ/PEHDnslvZpc4Y16mUJSJ8REul4fnl02vduYioVrQvgjnnHsjvmLmP  
WbLwN3044sukYNmRcqSnujMuk47IESgA5fZrf2+2XNugACR8uguskc659niTpqUi  
mK1HJcfaya0tix3AfhMwGTHB/axG6uuhvV4bFM9fyE73Rh2H3ZmRm80ZJw/vcK  
x7QP6A1RWldLlBGAN8dWBt0kqs0R56j02xi+XGzTnW8YBdFQAKy7HmRITWZA3PU9

Fmm0h0pDXxK+3/XinNF0nz8XTiBho83hfS0HR/J+BrRoKuhGFTpnMJqfrnGU4EKn  
XhywG5Vboaosjjf89lddRFaxi5tAHAt8fdQWXVxWyfhKDVY7Wwly7BgjPx6/VW72  
R2ibaBeGrm/A5+o4/wlQ0l0rbhpEK1LQm+3N+ylSnUReqx/2eRHR8hdxKB2HZOUP  
CxFsLghmaWxmzZeMuV1YqC2aLuk/eSrTqsWQUNCByNtsArHcqtPFYg+bDg1F9h1u  
VX2idY21rgEm0Sk176ENVyxbldfvoiHQjG3pFTCe12GA/JsmmIpn360sr2Fv1r6v  
Kvhkjjv8T2oes7/SjpBwRAet31sHKEDjt3RgBPKRiRVhQLGGIwKBFFw+aJvwJP01  
B94wqKuQlPnq6+Qe/GEawf18XK0LDU1o0Zd0IKgty5vahZggEAzBIw5r1fxPGXYK  
YHGgXk8LT9IwWWhvPRPPKDR1bVTOHUmhIgiJf4ggh6q2eUN+bILmHCIQkBV5TIpA  
gu0jbSzoIvqA0CcgvDAF2reBm76PcQr3mpK78m+s0h3oFXX/xGvednKpDilt/qgP  
QANxjxjAzSvzo0batP20aal/DWtKpXuMcRMivVZxa2qLYJv4o1r00H+97oEdkrG8  
AF7r+y9yh14p24IKw0toTwlWhhgCLnQBf2VQMGM38296RaFIjoDzspW0pyXETloi  
8Uy2s9AHLRBVixv9hadUr440FPFWNG03zEQ2RcmL9D9M5j7C0t7qnqBQ0107g52m  
+rRcewukbNnlXYPgKZXiDx/0uL6CuabZvi9LIL0zx8uSRqBloUSR50xziuoY2rnK  
1J21jp2h2JzTnKP/HvW0u3CUhG/r1/vB7xr7t0vkfUEgreId7Xk25J0hmpV+5Wg  
HFz0nVaqWbN/e1AK3lCSWPonBvtEpVt4ty11hsQCM/Uen1UZxpAfh8FpEsNsIhPS  
Atqwkjb00BCQMjILeRPkyk4KcTvssqPmVKLEvPYR9iEI7IYdT5N+0WjQdX+Vv8Nb  
vBh5bzimMOP3RiJWd283BH7frewMzWQBEQ4er2cidNcMwq6jgo1AT+PCNpzXu7Gt  
yMAWoSzFwpQCngegz74V2fBAzXK+KfAizCghBwqLaUQCYKB9xFeAwf+r7iuB9+kv  
qExMV8ywduwC9ty4mfl+ZUpZA2oPnrIRvz3Cid5JYAfLRZxLZjkZZCG4HEKyz1  
rNZS+a3YVvj0sLZMFJ1GLD9TwoNxHnVZ1BSJfb7NNUbY48xNzf0E6jUsxRZwFAGP  
Fv+0U/1E9a2o1HA7WgRsx6v0lcIuHnw5kc0pcCuEDD0BrGYHa/4nyhjt+7isoyoZ  
RujkygVEoH9vRk9SrvCDPk1GPzn6Q60Z04Ls1GyXNqnWt0BpQ3zm6FitLFI NGH9  
9kPZebdrwKTNs6HbtbVK00Q6kQLTvwdTCOSUhi3AeL+52tkkCd3fYbAVNBL6v5Nm  
g5srI8hbC+xF220JXxp5D0jc9RLcT4LTEM7hZqxG8H0opUWBSuqLcJeASY7IEZQy  
qfrjVICNdECwH0bFFXChijydrGJpytDTCvoIH7a5f9uvLa06I4qyCV1kvKryanoU  
rU30yhsrbdS+EkDLYejeRcmj7w8GwghlSc+uQzLny9WKMWDDecheTBaJfGKL7m0c  
b8N7pcvnrMxUBqYpILZnQDfN7qZ5x0D4gRd3D69UQCphzWu7KVikY6nK8yxYAqIc  
DIy8T7Wspy+fEcVeZdWpMgV4YDGEhZftzoDdjMjwRwddu3rq8AewQsEyblOTbo0u  
6N31mXAQxrXbjGJJL4k8eJMyBJQgUBfRMQLsbHxKhCc09DLV4SULNrmtmG0eUs4Wp  
eecZGJysSm2QZwa11SEgpAMrZ8rLi9dz/08NbdVQpmYkWhud4NQEEG17D30ntTu  
2/fhMdnz68nWGLxg2ZIE57AaMZC6nDxECGgJCBi9OoWRu0Sya2bORD65G1oKsBx  
onGjCsSkbj1CsFRRliZ0wGJJnTyZ+qccdmoe7sEYBkdqPpiGc29yAtpbgjKCEQLL  
6tRX3fWLPgAioRTxngGNZiCpklq9Aa/bagPCuV7oT6PG2rbkvUQAtKzd+XqKXQAJ  
Ovtj5ebIRI48BX9n3NuCTCaE3MmtRGmXb+7wLACT7/gsdYA+Bt5wFJ+2B+jozEpY  
WN5TFAG5Pp6P7vWc506IS3LA0HLQsm5Kk0FV+9xgeeaxSBWN77Q3PHsgHP5VzcNN  
Fij0N/JGVaGNO4MgizVdaQt1C+T74Dt8p3TJWUtqb8ThDVeA0K/Jzx4JEHDC4kjP  
W94WqWyA2JCwPomdigay9+4Br8YnqcwLj0Mu5F5AGlnPCWku8xp3R/Citm1LSJLr  
kw3aCW9eLEn7Jxtt5FEL/oIoBHswp7V3+vbrAbP4uA8wWuDD0YyGSb+zn/dxisBC  
WQP/BFhU3ZuknXDoH9LoH5sjiFyQz38QCYBy2T29nW6adPz3e1zGuqPoA0TXcQAN  
EY+GV0lCvZxafH1IaGbiQki36ki/ZbUb09Y3yz6Sw+U7A9YMrA220vb9CSBa2qgD  
hDGqq4Pbz7EnQZZokh25dbloH0WYVNCpnLy7QFBNa36CtBF37NAzgE6oqVtxrRXy  
b0VgvoikCGHHnrav7RMfgvlgoRqTeUkfyi/fEo8iLKJhZaPKv4voGIUCYC9kdZl/  
p90KaLpFrWx728nuQ300H3KaY5ZJ8Lxa3BW9c3s+PACRr4GL/hwxORTmKjxL8GJV  
vGWEqqh0IJ4qp6cdRBQG0Q91qWCiU2iKk126KK5rm3p6LDTbDMUCoZA+rM3yA25D  
0Jg9xTw4F+gCgD9PCdZBQsXrJcID77clGz7+GxsudLMKbZnFt2bC80yTlpGMv9sa  
8nxA0vrvU6VJysLh6obTCS8TKRM37JA3+00qL5XJuMuS1awruzW3ThPq0KUbeZ/b  
WyNLCBoWdbiN9TOb082dZ56jceZN48V3j8j2tG2eTWfkn/eTiXMygmgljb9K6xD  
L9uzrjs04HrG4WhpHAX7AZna6JRTUPDeFEh0JDR7efut6/8YZTLdgG45PezhZk+B  
aCdBjJrR/yWftH4x7SP3Sw+R5+BShley73aEz8EpP0LERGV0vKunKIhS/PWVlmn  
XYiLUPrdgufmKHGfYniYmIF8DKAvrYgCsTCrLHKC3dt959a9Pn0FUMg5Nr40myRB  
3TTdt3oLwKycGYMCMZil0I/myRE9bVK8BaRI/wVhesjS4tdGxvvR9LkT+1TVk98J  
zsA3sZzc5uHCpBMLJD3TLBC+EFcukeJjWwjA0xrZnUgSasKiijLR/rZ/YngKazEE  
CmF6m9wSApkehcbJuNpLS/1vrv15NT0AMCLRV42FTdiWywQm05c0GD0VXpsjwjJP

oHwj+9XVsu7dNUOU4a3MdFar9j319vUf3mieJFNCB0qPG9BU/latQv7f7r5uxC3e  
XVZyRvZIpdauY9nBRIT9yXwKHB8ugdCayepHMa1p5i0dvxE2x7AF9qQ+wc/+x1u  
SLD4qT6P/DvTZUTj2Y5wY3LPJIIkeywO20qXeSHFWKVL4nnWDMjia/38pTmomBw6  
1NK9EyRbbrLlKaucCX/WmOFmKgRwnAA0KtN3BX+csbHTQhaoJ2j1nVdwPgOUWle7  
PnTWsdIAX3ZIn4Prqb2fhm9mUhRerEjIclR0shOR6iszFCynLbetqSLdejILI74m  
k1jLoiNLXNvhK9z7DEzPSYTsHeQK7QRTQ9ktvU/iNi/xUvoJ16ygYsoUaP1wcgoC  
tqjPob2qmbE5QgmAha01PZn5F+Ocl0/RowX7grUk+1RigUkbYmB215W6KYGeWx2l  
91z/eJHA241jMfOoVtiSRBCbsjMfnVT73W033XOVpO2EIUKLSHOvRKTceeyLf4uD  
QsydtI/GJPnuZycRavnfxv07x5X5pGRwr3webMRZ2rY+eLaSdETOFF4nJFr3+Lkm  
LJIF/mik/bplbGFFv+3PDd164JfdnHqQJ581exM3c46gYuVg5XJlQpPfr8LWewGe  
RKoCEBy6/l2P65qIWRqRccBpiR12IKFWcMw+a0p/JR87QxCbld8fivTPDj5lehmO  
q6P1HyhbtYd21B2GDF9hdVc9h18C74eYKnfpzYgusBfdm1t4T+FoT1CmEU0XD+QZ  
ze6QGqgXs6lzyrmVcsae6JXMuHjBhBx7qQgQ5/Zi5F1RtqUhojsS1VcY/TRXWTRJ  
JI7xUWUXpZMRDx12wIeHhZgx3jgU1pI901dwNsQLvDPgWQ8dYULSJy0s6RnBjT71  
jwbODKKlvMPTDJH0PxpQWqTRITYP+mSt/F09LgdXS50M2u/LE0KypGBuSa0BuvV  
R73ndwYzpMFT26Kygl+VGDSv9uexum74iE0bRf5RijLIQ93POdn90pREUtSglyT3  
ccMfycDxyzc8XVJFWC3CrhDV1CPijmuMtScGLTOFTFYUQznKI9fLWCI/ctrDzhgI  
REtuUB65eb6QMctEOU/UcGPaSruhu6M6Yaj6GBj6f6hkMREB7m6rSgASzPsNBKfD6p  
Ih5BeXPQ7DBIEenwtzLgiMidB0n4VCGS8IERMKBP/AR10/iG4PprfcLkTaZMTHFIP  
01zez+w7A/7z/j6Gb1xbH2/1G1iS7+sgiSraRuqdsH7eXMHiiwiGlyJSPbGUxp01  
90pZRK2SFDI6yq45CLpSnYccJnvEGQn0+2ApzYkMmdjoFmYYsrbRR6f/wXnZTVyE  
VePGCCz88q5/MrqugaPRPR0+3frvWTXG5JTqKEICaAIH14U4rNjQ6Pmjdl2BG0QO  
e80P0wVyh9t5LNDiKxq9A+wdLmM5Q7m5gl63pWxA1Ger7vkZN33JktP00xj+h/wK  
vQ7MDXIKBhBx5EpxAWyfyLCyveBBYsblU20BMsMeJxQtYDmLXLz0KRjXLB3q2yk/  
NJUNtnwVSjKcVY4i95h2byr5HcalnxHZ9vdFMfpDG9e3a5y68l8JJxwa4XNEk2Rl  
ICjKnOkAFERMy7w8cfJI0WU91tn04tTKjmVIZZxUb9Iap1RcaPj2N15G39lBvEeZ  
+7o4IQ0vEeDozIzfnt2AYnBt5Crs+izLMG1fCQVzdAGP69CF1wQFpAiC5HDuFIJ  
rdgvXYg5V1LX3pP6ms7QIk+1Wj7/rM9Tn+W2Z9z4FGuTChTWYac17Rb+jF0lgmYB  
S04AFdjM9oxH0//yxlBb9cMyDsRDVl3307BMBt0NuS84hgd5W+ymyu60seXP/5EX  
YRpafLhB87wZ4nkiIjKqGINNSnaaPUS/dHmVEaanVXKVG2KL52xxqG1RtZM0Jk8E  
a0RCvxdpeTJDxzTPI3M0cmHphAnRwv7p42NiMpYEmALHiq1Vx0fbIBzKuEunkXaw  
UGcIEK23eaKcU4Yy73nYI9W+54/bUrcJKGS2RQ0mk4STSEfuj4R0Tl40H4Iy0zXh  
z90ARxFTfiXU0fuPJ50S2rfs4A4oH8qnD+LD0D1pOnhADjMjy8VT1n/fiWv+wnlv  
DrwyQ9oTOHfBeB7+0PN8UWMTjT1CLi12qMKstDU7g80X0K8j8XoddNfm0hgcYkOg  
5pd63SBSHxYsjeB4lC4s5hE79RvaxN4k/+1KEfmeebhoG0u4n/NOqsc93ShWrtK  
5ENBh6vcrCDrsntQCaKW0J5q3bCNDuhpfNVhNxPiaBaZ0LcuVjHrLzzSoFaNGtCy  
RPrjBxmZCyvDDCjFhzVavp0WgAT/lIQPLBr+ILzCq2nvPidI3jzSpLRuPGbDK6Hp  
9RNn8vvo8LHUu4bCTtenYLN56LXgVh8TRYgAw8pxoN0YjvLIbLlfi/ILhox+Z1i  
7vqUeNn3vfXBN0vxaUZpsmU0fDNwekt2cTuvifY1gDs1PFc0x2A9fx12wtCKWqB  
dRsuELXhtpAK6VC76Yti8tzxWouinDxGQdlyS4Wi1+Bi94xDsGiLqCpFxnbsb1c1  
ItNejXg2Qp953kTC9Y8LSfz+0LPaaMQYx8cKULrXLCZluswEnjUOuLIHM7gyH/Qy  
LDM5L44Qi/ay26Idbkn4NrQ0W5xBEFNlPV+oBscfg+87A/XogXCqNUC7X2UBKXov  
GGTh+S8RqgNTW6xMQh0IgMew4Jr6ahptz11HJ9IYhxyJyR1U9pPiWys8KGRoo85o  
gxWNK6LirQ71JsFkM3XSrKwi7aDnLsSSc0MuXAZFnoe2trcnRrp5ayM25ILdUGEv  
bRDniqLayTsJb6+0HU0eLMPtaXwcj07iTYCI4MpReslc0xnplTtdI5tqoYD7n8Qt  
E0tyYDUlMJKG09hcJAygOv+YZgLSagtd7J6q9dB8PUlloau++FxNchSwrI0Y7o06  
z+lsHKrHgn2JBr/pGb64Weh055xr6FeMU/TIPkZfYNS+JjNjR8QY3xTDIU+wMHw  
Fv3g80nzXxgxupjEPnqvwb2yt4gRcS9HVqnWsEvuMyf0BBK20NaHG+1vmeMPHJ2  
Ay51/spTqCGB2MMtz7sMFqnv+F3n3sTxIbDZLJJpEXUx9j42RMJ6KKCQzKq01qGR  
S+CZKjZKQh2gIepcHcVnu7Y42uwLFHyCb1JoYz1NoLVlBIZFSxDgKCRf0xxu9qd7  
uU25QKUJcT1kSKBEj7atgCJLhYVTs50m8o3StJh2qL/zVM/guNb7ak3awz//V5GK  
L8jShi4Wn3VgEOVQHZeG8VcA9wjBf75SuStz/bVFfa25n+2n+GzFupmux6UFx11lH  
steLoLIho7XGK6a1LjLFyr+yWimRGJTSTzFp5HEMoh533k+7pIuQ5ZHQgqHtBtF



BlaMzI75xQD5o1qs2ONGMeZ6R0RF9mdjIUVGW3+jsuodpEbJ0jW1LUcFlrNzz58J  
0cjVevM/ZH6fqK/7t39ZQTDgNr8bVfnSL+fvZm9Yk+gumn2vi4JLEj/9UD6re9lj  
U7ykZEGDgs66wrT824QZi8N8+AXa03Su82D1AcnjN0jAYMODf8DYBHfZhJ02/qre  
6ggSjcdT3AueLUhTd6MgAyNN3S026t/cR8MN7UQmxHGZvFB4JGu+G8j1yh5tQmBl  
wXoWTPyR/IpFwhknW3rK5fli2aI08F1aChqkUL9rFPEheQpDqVSce9YVUMLZzhQE  
7a0V1KZ/1K+7n35U3tjut47VEXVpM8Zdm2M8dUzNLAXNBuni3uLJqtP+8/m0yhTk  
TVPXqIRAFuV/MXzrkQf+dRos92g0o4JVNBCC8u+YQ5y8g1yzJ1o1y4YzeGtgX/YV  
2DjnJx5nk6t6BgddE8fKsdKt5GeIudI5+HFDzTs7/VeBzpZCdU0CFfZgFv1UQw/d  
8UZEcspyz7s22v/nVdwRNYy/qMJI2RwEJB/nPic++TOX9pCCGFu+gVbIXhoGVUkl  
VQKYre/XdbpgVgyT00Wu42cyITGaJIEe/Vz0v5W4LBF0ZueiKai3UBKk0b/3hOD  
z3lGV+iJm2DfrGA/srR6zu/zpqGHA121r7T8U7sMRn5optLKyijY8rLi68p9BHSs  
stl70md7zgwnqAlIKwB200LVG02Pehi10dplrJCcgBe4xJJHgwBGM8/kQp6GhTVJ  
kFV29t9U3g/+fj9scQzb76ZKuF+9Ava0D3MN1iR7SKD+GabRbcwLCaBEAhtive2  
iRfNrSae8qGtWzFsvXvprkK29yCJEyIIHeVpyB9LCr0cl3wceZLkQr9x1BKVtxZ  
7x1kGlmXE7+0LJEiEe/GXFK0DGgKkvdQneABIPETvU6eALqA0ufV9e4I2k/uXkwG  
a9hB+Bn/XL41nQt96fmNmXxp+OQ07+siTP+ETRC7LOSXFKwV3/OWajd1G8qouN9  
AY48IXqoPgQfXk2gI4mwhhNpJgo3yFj1FfQxU/AXI2sYZZVK7QYqQvflUcNRspcs  
FuTYgH2HxUubpr4lZeQtxim/it9tCXCAUtu8C4a0IN6pk6CReY9hT4ERetHKOn/W  
LtaH961dckaJF4qsmuYtvLcXasWU5sJ45cS97tBp65zc3nQdsdIgl7XnWDjddYF1  
gFvRpidblg/ScEKDtVrnroYHNk3bFyEAUZFsqOMFFoSf4Rkxgi6tGNhvj0a05/V  
kVcEnljMST5ekKez0mXUTL6Gg71eVDZqbFLq3uIcB7QbWJjpl7BKzp5Lt+EmBS5  
ZGs6f0hVHFkdWmWRGoxgygwQ8X012wNHcGYdVrQx2nwUuoN3hEx66JfuBq2lsFks  
abLxD8eXVVgiikHw2Gpd3cgH3H+ncVX45S0IH6AFRvCd0zdKXig3K7l1ivvoF0E  
+JYVuBV090xomjriW+octL+545FZa9bF5XBCpR02B4NzuPurW6imHUH9E7LwVb62  
x08gr01daGTOMt+cMwqqOWeG3NuL7d8t149yW8D9gmh/6B5tI/845mEMvH3a758H  
yXS/6WjltB3Blo3H1q01E8DLIzNFBgLKPrbhg0YPbHshSwxTwnTX1txyexJL1L30  
9ivoS0xKJFuef0bctDR103Kq4eigP7x52WTPbUtqzmNrcFOS+m2Pc80urhHn+cWe  
VCdKbMKG0qRt8fhVis+rX5MmYf5zBC2hMSVts5P07X7FVwH2IFpLH3KKkqxd4S  
MTxM95CTN6V4aHmr7aJvY3qGP7SRWOUc0q0C8w/g7lf7G4BE6tEVnY792guHzrO  
/DpInPAHYLSxBo2HP5L1b8+HXRGdZ45HWSjSr38mkbghIr7jh0QHUB5/ln55E/wT  
l0msA43d/oIhm5lpTGBN9GNzR2rsqpsdlXsr7z1MF0ko7lvbBc/B22dHLPiklGc4  
JdYER9vJKsNr42SwkU7BGh6V0c0zPH6cPy7XKncLi70hsGeqs+KurS01bD0Kmu1G  
rFlLRUiHdcSflxU/izwGUEyvrQVaM5W5+tpSfm7g6UKMiajPQij+APlnQh70csqb  
Djsnvj5Rg7S8IgPdmglmZTKy8mZE3DLZWFC90aZH2FKAaa4yPflWo/+0cqwHqA+1  
lHe1DoYcz/6TEy1+sY9BWP6yVNoJqHaL4xPzKk+TN5iH72D+wyJ04pfXEh7t0bR  
T0totQ4Poxux2NXZSe3SpQkpUvNBU61zWp/RRJL08NLAGwvZ1fu2rZY4vvh8TTDO  
PIvoSWnuWXJshWl2ekXuLLuLP69Fy5n+QB91IiBlFYozVwtWl31W3+8U+tpSkgAq  
zofrdG0BRAN4qJ28Xo4WmY5q6AbrQ/hxNi91NP4dJ8t5AvrQmduqazlvwFh09MN  
n4zdXF/shgppCouM7w96nqtgMPnlznGP675vw+PFXShVV05aN7vPuXQCgve4fxA2  
DXf+LFgE28gosgIwdRSYjx95/FKE0rs7QgFxmYiSpH+psPl0NFDHv5bqiFA/RCoc  
vJhrvSZaW0zBr9dgJMOezrjy/MsgLwLbn/gTVU8sBcw9N8cTCCPokouEgdL7E6Gy  
36jGoQ1RSFBb0zxooq3rX60e0ibuWAH+5kL52SnCld8jQv0VWVZ1NRRhx1eJDlft  
D+BQjwYgcHB0E0vfd07qlkPE2SxfwhREa9VANTnNlc2ners9Bpdzv31E2GJYZ12/  
9hcMhLxPCvPZ2bbMg0200gbf1qYQyS2Dwfgu2JRn4K+If21TXPYvQNLZTKXirNgL  
yu9JiuwJxUc9kPz26/1kRAprXIZHeiyqcG3uNNhPYotYDfhLMuYI0SCZq1lVeZ4D  
PTHq8RmcVNtUkmqShfis/uL1bxkwpOpjpJPfTmcNr3JSbZP0ibQDL+LvEAXNHKSu  
zeeZFoa9tE7wjyFPr29h/25iogwaak1GIa6dl1wzFziGsN/X6qhEJ3MQ0siPNKc4  
we2sfG4jV0k2Vf9HhQGjchW96zqKcZbbnzdpSjtl5n23+LDBFRW0z10aYb2Q0n5e  
82LI7Xf0MHYhMYnzQpIs/H6QmKDL1Rg5W/+fYCavoZVDWYtUwNpzuSqt70cj5Ey  
WhuCdCrbL1Ccr2Ylyid3rdulyVqkBfc8ZxweMW7ZucJTt2PVEALutMncd545tgYe  
00nRoHieZfXrRn9BbJIRRoeZDkEg5DKfFwkG3J4t3/I0z4CSrZfM2kUZUvHaI5zS  
qz9S4S6ku7wle41SQ9f27QVayhL5dSeCtgS1ViuJJbqUSXI+c7Jp13TpvJbCIttN  
I3Qk6RpU7VyRZYqYUNU0xw3CPzEt3Wiqh8TBo9DixW57CRxtt55HgZ6IVWCH80/

ffES99JsnsH1BtE2EUPbf+SFjbdjagyHj9qQbSq2F4KZGoLhY0Bc0fKJ1FbHTyA2  
cxualILCE5Vr2a39mSaubGcpNf008T3SA+f5/cCRceOxKN3dVN07BwfaM9fmx+Rm  
dBkyhAjf56WxY59dBxLuNu7iRpLslk/yrZFz0tMVWHj5F4gAqG3a1hCdrfk2uacf  
vmZ3ce0TosNK+1At9EyBvJfGbAR3A+qf+UErbCOFiCQMhb9BTPrIa5giB+2qD0T2  
9WCwW59KSfPRqTN8RLAZotS1AeT05SYVac0bxxRilrhze3nL8TjjMNF+VkB0HP10  
eIkbQGT6ViJySDEmhi9zoSGgMiqcEd/tLuTkjNK3UXM95dME3ZokSTTwnG3JL/f  
hUtPhT2X1Hxd09Ib22t0lq3chxP39uWg1MsAUDTjevEQQRNTJAn+r87Xb0EjXGdi  
lf2VvLQkICHKf8/VAK26fw6+P0Fa9pPMWQZGhDs3XDt5aJdbbxb6Z55Sjo9ICGw  
w0kTEbT9/pycW1R6DLDLZSneYWvFAxUJX+XlbIzrbVOW2vGxfEgcEEDzt6cQFE/  
wvF6EbSaGYRF0dXt5UEdZQE1sfZ5qTJbvZR4gXRBhBgVtgW+DDz/lNp9NKHfayCl  
P10df9wujQTClawGeAWDLLbE5dANDBVUSETbWvpuNEuEZ5yFIwAZzEkfk/Ej0y+d  
cWU/OZdj0irnU08xiAIMnTZ+toshJqykpmgcljN3bhV3t9LJm1JwouGyKrogY89  
ssf0wFCNFBBfZvkpwgMvau0h6gzxPH7uHqrh4b5TQa5toQHrcH4rhTyQ5/cEQFM  
WbvKfY09VqyIw+VJGLI5S2Zml5S0xDKVxX9prEK/lTM2Z1ULOXeNfis3JzRW2EQ9  
+MGJqBa0L3kJ2WGL1FXymK2q4atn5PLosKQcthiZoX8+M9eoG9UE+VMnAgczNPH4  
mu8m2j+GLy6v5Q5zYZVliSk8vt34G2o2BQybVjB/4F7ciMsoAEIoicZrp7DFDZ0L  
sMb6UXznWma3VEE8nwlP3AdpeNWx3h0EDznWmpb3kPvoYm9bjCXMIwIF/I+kMvX9  
RSCzL+tRNDhhH/rfU/vLQXILit0YsB1fQIDG5z7ENCDFvYS6WheQ2x94gmhoB+Di  
GIpsb6WmcRZA7Git78tPCr4stos+Q+yqCPuo0XZzU/VQ0yKG3JhmmgEHKxysRUSI  
SB07QIQaydPphTCGzveRWIAArBQS9/ZvseI16YdQBvANGt1EG5xKczN5E+zC2atI  
cSSx4REIwwSm2jZxGQ/YSHZ16TDBU03Kj0bo0cGyQFTTVY26muMZAktTcKrm+whU  
BEnCEIyz1spayws9Se4ZAKye80N56eni/GyUxirP6aFYBxS9f0e4gHliJ1n1VQv8  
jXfi0W7Mq+9EzKfoE/Pmj4d54t308FACJ52/lvtukatPvo+tCvzYqKBP21xxHJ/  
9i8ZrYEPG7NQFF5LNM0keJGv3Ke9baCI f02/M9CrXNuLNMji4JxpxSNoP9lj+Ox  
SCULLWQjaY6DAqGM0eBzb1009AWqMr8qr4/zJTA19SthBdahGT9y9a1zvDEC/2Tb  
LC2Zg0ZmfcdU+8Rb1eX98927WA7a6gHCLrNP/v0JEokKL4sNfu4n1l/f+yJPVy88  
a26eIJyI8iYto01WnuhsIQKbXfzblNM2+bPkKI f0Zm32DkWH6qI13KCLj8Us0GJL  
f6e3ZCyUTkI6rpcpT42B0L2hio0kW4Pepx0WpoGJaSwcVWkU40MKpVWUdw3qNf7N  
y5w0Rs/oxw/ydrIBjB3EuehdYquRdZ0IPbe0Y/qjFYHJzuRLSDJzjZR/iuQTm2hf  
sa0H06SUWxnJGwwDPFFFuRRtzyFuHDeIoG+VAXD4HovYpeo4cKIppU1Y20eoYk6YE  
Ue0VzaQKtFqNr83RYJtF/EjFYybtT35kW04mMx7do64FYkFdweHdsAJ7rHpVPSPo  
zhJVL2UGemNoKSgWKWSi5dyAMtq2HjdiiTvrCbYfYWF/tpzNI408xhQ0/eXpfwmR  
SBqDRVmNM+Hng7kStovPAre9ri6xY1RH2y2qk67bvv8LhamDQtYhw/5iGTjurZh2/  
8ZHxUgW0Adjgbkbz7Wly0dbpEx1xRgFWSEEFt3nH/XgmX0dGjA2EcDB6zzNRR000  
bMx3i8Pf+gkB5uI7/YGX+cc+cu+qPQ7+offIrLjepKuRncmMwx7GGb5R7btBmgf6  
eQM0HWP6L40068fEDEuhEcMo0dD3dTI0jo4KIyb/Zlytthd872NEQI53Rlx5BMYb  
DpBYHKO+Hf5c/SwPXE1jb47x9v+a/Eo5YHL3oquxHLI+Y01VziScwta3MhR6JR3L  
Wjlw+7sLVLB/0dcll/xbkJXbDM0xeE3bgBksMDEZkpzfyojAGZR11krXY5f8btxz  
0Lem4tZ1XWrI8zImyTFEC1LUXprSSoERvAm2i/Yf+BdRaGT8DCvwbzAt067VqlV7  
4/1q+vh22rmSX3Dut0eHaIFBP5e0nd8WJmCGAi78fI1iJcr6yojJIAB8zGfYqPqU  
UjjBBZwiLmbqXLdy6DIUHLmG/a+wiLWh1oE3ALxNXXN/tYhwjGnjENQRUCZxKqJ  
L0zLzpbKbXfVIHsbsvMapWS6rjkRUcU9d4Qin+jsjYnZxHzkKfbYODWLqk10URuf  
u/gasm910akum9du48LcrV/RqrjmHS78PihpYJdar3SN9JCJdhK+L0CLsVKGPPrw3  
k5wk0iv05wkAK/7h2EARxQzafJI5yL72Apwa5s09uhtUu6fsiZ3yTeltdtVQBncDr  
e4S/FWUs8TqWhbQEXS/J50uQqKGPvnnW0ihs3IhvFsqsK/GiUN7ldA1TNu/Y4gh0  
WTi79cuSqHvWGZW/UwvDuVOWl0xXlj1m6rnkQ2VjpcKtCJRm50N+6YkRzzVLLYM1  
h7kqKHXdkqozh0XhH0JmF0AN8Dp2tDlmYekW4G5geHyQxCi fQTZdMxnk6ft6uw1+  
y8466Croj2LTaJLK3s2dUR8CXRGkJ8egXX0Q8hLHgBGQn3JG5FJ4KK0gcJLh0UgO  
iMkaUSnVSk50wilQeiv/bNU02i0ES+R64CIritLftQg0VJD7LOTM0dx8+Jcw29Ub  
zATkPpwXcbp28j0piVEtE2iH4tTKamBef70MKHPSzTKKzCse30cnigz2vsIaAy7y  
iy0ezyEaHUGW/uqW40NaMave9MDIuEwgwc9lE46QhblbLKGMdgrTbpldkpLNK+2c  
XThojULRM7aDNB4qKP7jE3mfFdTmxuos8Z0G0eIDY11jS6FmR2/wzC0y4PJ1jXLX  
cN03V26FnKVHffnCN3stv0w0vRUQENMQgSXDE1qI08ze4f6IGtj/os0QJyUl f0R3

wQJGNUX/CDmW3vkKqsMzF3SoTfgxc1PPx8MXH/GVnKdZuJE1oLpjQj8XPDexme3/  
ebWL1Rs7a8GfCQvLqzA0NdItBm3GsMHqhL6+GycgQGojRpHbNggkMfjVvw6TvFE  
Us/+Re0BYuEkXCsQG50affFmnTEXv2UHZf9s3DJjZiaWBQCbnf4ywl9q4ZSx0sf+  
hSAjB+X0YxNDp0HhuYDYBSUHe/NPTTo/2l3eo6TFLNX02tylXUvDAMGzBW30z5o8  
4bYuVewhb18IRb0h2+j0w8F2Ztw0co8ryQgmdRuLyzZLA6dBd0DcgeZPv1oz3BTU  
eP1S+oFnJLmdxMht8oBy96JNWWHiofe0HoAWc3mG3BFeLuoKP4v8WjDVX+5Sa59H  
tD/ysMEdZiWIPqc3uxMxSfT9xnr9dXdoL+o6Hkgtf43LWJ+AZ5zXPvI6gSEvuwXs  
1L8p2wQqSuVvKkAiMdTgcFegm6kaxXu5e9RACkkr0/X7VMMCzj9CWx7GiWKNfPlbK  
/xFu0NEwFCux/FyijIB0NFJDDtPf9/l3vqX72BWVsumgIf3q8x7+X1GwpTPRxU87  
nWjJ3a3dL0t+r51luiaFHA23Vo7MdnBv5yFks8Ax979xi21mmA1igfw5KNhAZS  
uVtmM0nqQ00+USYmSZNp7/KzRIIsFhyV47G8Bwnq1UVOMPmI200B83Kwr30vLzd  
YmRdpLKZTGE0hCC0BuaBf/vFbpCBAmSwMVUV0cp446llQew7d1pezsQwKCv9zgP  
IWhTQqkMvEyD+G8PEH+MrM0enghAyRx0/e/vB3x053rGN2mSkcFUVA1/yqYxwWrL  
T7J3ZdPhP4Aveiept4dHoRyPHqvvSwFaeqZysyZWg27LPE9vyJzlcEB89mZu90U8  
3NYe2wRAoGKybe9mKzz4pxlkkAJ571CIwMCYwX+iUjC8IvVm7Dtqre+Gq6MQ11pj  
/J+luq+P6vlqAGx26za0fe0+atk2NRjpl5wQF9ExKVZK0JsMDn0IcuWsrnz8+Ewn  
vtgPYOWze54wS3A9owc8bP9A3oNjhJjOD1WESUfmwZp1vE6TRiIGNIKGGUG/EML  
brzcys/b+g02v88wJLlMTr8XpwBwa6E49lp4r7KKx72k2Bt1viQNY05E/KsFQd8c  
XgFedC2jZ9P+yv7Y3UfWryxbMzv3uENVd3irD8auOmD2Xw4B70zYHuTkiX1U8jY  
AAxRbGoh5nUDNsdxIXAaw4pKd8YhCso/0kmUqCSVKglu32f1ipjEQpVLSpFz894m  
hODNvHgicsbmbyAXqrEe9+HzCjqTUVMIIOqj1qlAgQTn2H/SzELS+JrsGj6JuW  
EnfR9xlp/BcekWTiuXhZe93pEC4AMYXSoaLcJd9qPex36/ul0ZbyE/j4105rkpx7  
bJZtHzP1bTPFIVd8G0gdqVarhYIOfBKOU8N3Z5bfehIuqT3I9VRQMHE87o/B9sYS  
9CdFX/9o17C5YYk3bTAoQYlSkacopo4t7+5Bak1+1kl1Nshc1dmQJrkeUMCAfJy  
AXSwlsYoZcZzWi7iqKJQ08zHrjvEjs/9zxT7Qk7dz+3wiQl7peiWNvZHCqzWhr16  
fj1Z8NmYr1WxQdnZTINJYBcAc+oeELztYWP0/7ZQp5Lc0aCowD8c6C72p/GK1j3  
pxQMnqStt1vBpayNnF3DLj2nQ+U2kKLMZp/m9uf6UUGVippk9A0hz7poFikXCcU  
Qkk2mpKTWGHthzoFongyo14egz5hVZ2QZ7+cWHZBrR6r6T++v4pthhVgIun1eq8  
sBhSr fm/IqA1/2kJRRXR3qDu07Y3DtoduT7mFkNsunWpV8HmzGXEWYsX4qVLV5s  
olb0f6QWbnj6UQUWUdjfwAo+umj/y9rF3MGI4s1NnctCrdtE6E3Ca6FW7MBUQotoF  
Bm0vI/UmntU6hmeFsnbGe2KukZM2Nd9I8aAal2RSDKzX0yxD2qx6ndsAVspfk5hy  
AwcLSLsTc81LFT1lsgExT8UxQBwPzzKg4VGIOt4CAYI4PQrrC4hm3EXZXkIZi0Q4  
4XS4I1ZSkVGUVRN10mcsM2VJl1zFhRkfV7uTUjjEEjyuA3M/54315cEB1cGDaPan  
koASqojtAaJPRs31sMMmAm4d6pn8K0oKj5T5D67EJR144bmP+ZGEM9pGSqIpep6E  
aZ2HbKkqv0z+bLVwEfBDjjEDmNQD3CQZwJyYxWxn/K+z9M04uyXQgZbX+Zh0+36  
Np62TygoEIA6KB1m0okvxS3rIsI3jMCjdc6tg/NjsKgxskl7JrhQnbHCcjZ0IAL  
6VVr9D8vchXx6QbGgI0RRxDRXGA+hEIKcymvCUpaPr5bxfQ5dXpDtQ5pBoe14SOH  
F6q9sIL60wBc5cM2GH1yRqaro1lx0j3GHWAGddaTTiFDuxML1GzRrBU10376YAwN  
+5h+wDwntuFwdQ01V7MKxwh3chVX7jUDHhyf45rJ3yGEd/KasWPAmi/rF9VwUSJA  
vtWkgue4k3G305inNSrkvx1BbI38X3WPbd031DrIfYwlcgJemEFpUtGTq+dCMmt  
1GVxUo6gOLX2mvIgganVQR+AqMH2cavsTUoToulh1ITBAW4KRzts1p7rzBxc8CfN  
awaoVqguPbH3GzgvrCUaZywg6e6SULAHnx38v453A0/aL3NPLAuw3FBfZ1TC6cm  
w8Kmx2aT55+buIys6iRch+hip1IfnIk1mp078URn4b9uCeWZRH2k2gzPNoilR/6  
kxnmVL7EgmnCNX5b3FU5hBYkoqfhPa8oeziwxtk6/GJED7JFfsUaLhL7ja6zcZHI  
ebCfbWf5SROAw07Nf0id51Qz9NU+1lqmRLZriGeK70FznFt48UaUJ611sRP0axg  
556PCPM5uIBJYqyHP0z2o+vXkDChfr9xuWwZ7jMZIA24IzirFp4pR7FjPpPni9d/  
u0g2AbYfIwgrU7Zvk20yKboe2riEtLBfgYIiygvBmYNfqHGKsGrYqyQiFpUrTHHY  
XMuoJzLbSyL2RLxgAhgfrIjMjtCZd+zvqUqcFjsNQJ+0107X+snoKpPwBfGrrh3  
YhpccTTeJMy1A357DqRIVkVJh6whpEDN3UU6EBpmt1ZuTWXDP8qGqXKEt1QZxr14  
Y4I/qP4YzVaw53MX93dybg4PTPCLMSv4pqao9g6nfb6+z2Ulk1hWXJY2eGuBW9Fg  
Go2XsWxSQIB0DM/NwS9fB0eytppI7ia4/6v6VP71xpPPL+TaX/gHzIJF8dyausaJ  
PJ5dj9BfTudZ4eVtgjphWaDeP3Q8VqkHGIyc06Q19nJTKcn72D0uZ0ltBEzLBbTX  
Tm5RALH3NPtop9lXIFsG5lrFCQoY9yGRki+7nVcT4KKDdTqzGawbqqM2JieXQ3XM

5AbbJdxZzE8ZTl1B6hKEHc+ftPf34TDB4Jzmawa9ZrHXNRvUIfdFd8RDrLuAkF3A  
uMJSVNQn67ak/Hy/QmKnBRTcYsePGY4V6B6UfyL+dOZpkISa1L1jY4KrgJNlg8h  
0TTmap6SeDPIwzzDg0o/42wD+Zl0zJ4xJj4hhJivg8Dd+igUch5zeHLZIDlpSZIC  
fN1fqmbt5dGIk98Ubk4zFa4by0rHW48pS8jhHNA91ln7uq/ICRgpFonp/AIFL7g4  
718j+Klib0DCfDL88t1n0D/NhnwuDpothqEjvTV0ct/3g0QyHdy839f16a0qaAAB  
A6FvjPDclubhpA1Gfw+LegIU8lPsuT3TGgzdtmRnLCaW0iVQnaUdwd70nc6GGo06  
ovj0BPmX/xab0SdBZ5ZeGX80aCpXemfk0jJ/mslNxtYLDsj0yYqMUXJWIpZt9SjX  
wK6d80zrDFD7GlgZx/d6BvJf6ZPCbafPoLps9+ruyS+B/MXG/VDYdQhTohw1YkWB  
p5lUWafxE0kZqQstYthJAUeMj9Fg+DoYiLHCXLe1yRt4ujpioWpPRx6d+8nhtGtd  
Jxo2rfcxjhj0Vd8z3M+LBtBjhdUC74sYG5ZTLq8LKYp182/JwqP+hrTFto9N8Blj  
/WWjOnTua//2eR9s016qL8uVgiXRSaEhlKBSnUsie/cxPNHxUnbYVDRfQYxsNTD  
8aIJEYeKfQGYtn6XHFHxFLDrYcSL04e9eBc7js2RvYH57Sj6IcwB0mSx69b2pCpM  
+1MB8tlkUaQr0tEKmVil9w3uZ7R/2M5VNYCA7fpS0nUoXTUsIJLPosLKHf96ti1i  
MyAw0ZptIby5Ryi/v8wnsuVlAyESSvdFufB7F/NgVyUmauIfSfLLCRDDPy1izj4C  
XweebQz8HmRpwZUIlAiR13FqgQ1vv40Q284BkV9ojqDR1ZCtCImR4Yyo9MJPRx0e  
bsNwrMthREpNkCvBzmxFFcogzJMU6FfglcXt/U49CoyC1TWZcZVpRpLXdLGT20EQ  
oT5xtJQn73ujUSGpsxiUrvl4mUso6AaU3hgznSM267BPYJIR1wQz4HyZ3Q3k65SR  
hHg7LyniCWizVJZCjR9EPBI0hCX+rzX0Loc2XUXmxK4qZUGa0j4z7KRnevMah8DR  
f54y3LV/LQgq3jOMZpKQSBkg2BEt7Gy6KPITKpncZjma0jipAZpA1gqlx+QZb4Gy  
nBl+PCWAJNh/8CdBuIpDZeamp/QKLHJOKhP/Z5YzwVkw8wPCyBK3q7ih/fU9icLp  
o/yELL1xYBj0n1SZT2uQf9Xile81BYStW+nJ+IQA00vP5LyhffLau/Kff+rWG+n  
nWmDuxC3ku0yKPhCJVGCtCLJaMdWQ87n29XUAKcjaPw9mf1mWWhMYIZhuADU518  
WTbJ15bbhMP0pL7ixYwKEHkJ+ZIJjqqTM0o0hy0C8X8dWG9mN5PAmRr+3KVy+kkQ  
2TvF97qNuMSE/jhIKvLPgbb57veMK0EaGGWeh0tqiUNmTTYhv0j1axdxnjmE6tM0  
FGTulBGN6rWI8VBf/T8G4nMhjvpapPSzJPEIF3b7iQaEfR10+7rnHnFDUug1Mud+  
hlbI8r7qIDxQd1ceZh4LVj+ugx2xylcmtTDzMXicPGChPbRwm9fCfHsudP5ljfBG  
KQBs0veSLZxq+hM5Q3FRVezFLMonbFAME0CpfU5wbVsBqCQqJRbj9amGw9du4ePP  
pzLoPa7bjbqlop07qQCoQYrmRnBKid8TinDxMMYLXUuWZQA3tEX4g6A3uygt4Bdd  
369Wjee8/fmedKfooS56Pk2hcXZjxPt6vYi78HdDfti+VnHsSKLfeWA3aN28neq  
UuISfDAkqb4p7FtAy6l1bF4vyJWm9fFJNVr2h4XTHwS5/dDnoadpr/cVwr7JiRgR  
qVI9FBE9VWwLeNXCT/JKdTsKdUx2ym9YXTGKs+I10N4/P7V1J8RjvxYnSuwjHwjK  
LmDvuc9R77TroHZ1XEDJp1AqKLu7T0nvVbcg8hqgaxZIiN7fiqZeF7K/TJ5SXTW7v  
yaa7YlSFGG+viQgBrx4Uwv8ciybyMOR3sLClt7c9eqwwiZ79vre12JUzg96Da2la  
c9BUTJpymCpWBU5CG3UnMhXbui0OUQYnMwzUjEH1viH5EmaRosdo7HndD2goa+kL  
DPxRJUsW4yXI+JgxEBLwLEiukCeVHXQ6h+P11KiTu03Aj+coXgfnbcZAaogeebn4  
cpfDFey3iyhVCWFdFgQEKAasyf0sOR6ViaeZH2/oMZKIZ224AlmSd3XHHGWk21FK  
VxXFAaqTHH0A1G8q/EBtW0a/cam3JRMw/JMQ+2NVwDo+3e6wWdf3fCmef+BqNp/t  
ei7rVZ5Ksp54mgbxlapnk9Ch4IILVpy8SLf+MemtscEtEzEUd2GfY1Mp/2pVjnu1  
wA0u9nHVMF5iuXpjTnemYjneKPCD/jgLZ4v0l50s4XwT0qCNjnXVltME9E5Rt0An  
3Ui8y0LP7uy/m4KgureuJZW+1pFmDZP3FxpKXPPHhitouvenGZacB10ZKqDuYdY4  
upKsvotD561yL30cjtZLb/LpHu9aZ1MBsMBC+6T/XEmmsQLkha4755gj4SZBoTa3  
+7RNJOIzm+pFnt6KyfZfDRu5phrinVLoS8r2TCmEZIRaT8xSQ3j09KTjDFpoIALE  
QZNmbuUxw+UTPZe/HfbXoeP8phRWVrNvsNDYh6gxm3zaA7uK0LCznaxxoXpokMIF  
b4TIcsguyk0wmkyPh/Tbg1Fb0rmtgxhD/ttgaWmtLVaMLNwdlhkA4u0Y1P7xj23j  
wrGLkZpAbIXrRK+mF821fZBQd87Z8BtFqRTvWwiTWDAo0MuS7b4RPLN65fGdzU/k  
2seet69g5xebWu+CzIquu3CEEL44wSugp1nmjork2Rdr2moXBtxbKnGpuKNrGSUP  
et6k8+zUqn7/vchMTKqOyhsDCPMQ2XsrW3l26TcQgHvYQhcbTmSzKPzS+qV3cze2  
MrFEbx/qfez6iyGU1tkfHG1sD2JifNH0Ag6Dyc8bn2fKv01s2Jwaq9iNlFv5XD6X  
SDCDXwl7GnIM3NtOXkyAGPYE2Dlm1sRfL4VfgMe6Zs9WchpwhuFGdRsK4EI82ZKd  
e6REeqVYN8d0/3jCiIbGajIZjKn6/icrn67BluzZHEd16p0JM2mMqM3ikk0TKS+h  
7P4JX9aGADfx6PG/l0XtksgVTciDV41fduv3LbPIoFZQ3Wi7ElcO/Ui9Vf5NIJGm  
9y2jAvYQ0pLk5JhcjZNRZhb7G7IQZCCLU0Vyxe083H3MwWRMS+lwxF+E6ld2uF8r  
XvWVGmNdEkc8huPtoews/bSFEhLwwuz2IcmNZylNRRcV4kmjYpLq8bJpHaQ0xNdy



IX8eX91zHekjqBgC2ThrFWFJTtOQ2428IU+duFHKbZzqXAgTLC+df0D0VS6exPQf  
TmcPqZ1I8DwAqwhd6Au1lv1eWho0puuk0bozpL8fukAgs33YZox+Dbu9BKIdVdJ1  
jcH1+RUo3W77NEtkJGB9w2r7E22i7VuFrFyQ344PewjgJ88Y92eSfIBtHtDkuup8  
FYB5FJGroy5ugCjuyhrU0/D6yez+IMaD9N9Q8f4PBpJ/RLFLCFHaL/XiosGLWZn8  
IbgTvBPKMjFQJTud7bfwda0zzoDV3HMDbJeIbEap4p5n0YQiaMoPlmxXEdFBRIs  
nCBfIpWefP4c3sUYCikolLqLgEL1HZwWn0uRrAnvNV2hGeCZGNX/CbCYF4fcq1t7I  
97p5j0i+urYikrTKaZBBhKTYNX9MNzoaCFfMpRpxe8WM3a5t2nf5bv5peCS1IOh  
97svLh4fC17IXo2ci6LLFwzgydNSkK5/DsmQhsNxc8pAVPkwe67A+ovVQiFd9cl  
fApoQ2v/Tk+ePbriVpEpPA5bwX+OMhSME50/vcD2rzavRe5DWvf0kBb7m45DVXY5  
H8yXj2fssgwLad2EVh9C0qfmUnII09xeMWpFeSLfxmyGckZgo1A9wdMj1LcmQm  
bfkKLeq4xBDkzsdI9D7X1bCabJPKz0GaGyrxjnEKHAUIJUPOdtvQKbaot7FbZs  
8I3eWwkm4JF3c20lzUVU7BptQ25asdhIP26XVfVoHPDx2ibP4KsrZqEEM0T7QHDT  
hujKIaLzrY5m1NglsmqmWwhHfGIqhWA6TziJ2RhkmvC9EaSdd5x2QpwzXqYg7Sb  
Ju+jKJ7fNk1ioi1HVTCTZnJnHWyLjy1zFsXOS7pdITPVD8NXQTdV7fQmdx/KRWIy  
ocKJqi0wjW18osKXM2s6rxw8tpeUThsWB1qw1ncfdwNa03p1xL08n0IdG9mnJ  
iG0DS0qEDcen1AWLxPLOVCrWXRKuD8yPiSRbQUD90Pg9hpIWn0U8F7LT4b8TqBDF  
bbui+8R2jzBSBWaRG92HySYKFbyKnXIzgDKDEy8Md5357UajvzLi+Ua50HYfUHp7  
v+E30lkxK4iqSkhlFTcZj05xNqvEcobPHrNfzcurhNnCL7Ak5+rp7P/LEFzFJLDd  
fBnMBtkANQ105ETuX59G2Jw1TWa8c/ove+HDDHKfujca0eSc28AdkdLfYBYrVKpq  
cj05o7TwgXDkwSsz2eXmwdNFKMhJijbSvh/Bq5c+whgXur68N6B0+bA57a/s60x  
bpA4VVwXaE2/9tnky3IVPmyhUIJa6DB442BCVUymYy8ATgu0g2S8WCrNvenUmrLP  
UKb0a6Nfat03eFcaH+a0eAEZkd/St9Cop0eurGhiQGUsZ0zb4YYn/ppgfeY+wud  
WJXkRAmTQI60SVg83WLJqXI8unBHZObRt2701UcL3+oH6wiR36zZwUzI9gnqxQTQ  
avzEyFYfVRPpmZ++kfNwWzBq8tqoZfWM+CILvQYKTu2QgF072hhAVBSe7f6Bcoq/  
vkNsnZNKkpMXa3RWe0TFJ9hxd6FEyK53ZkooXYY2+cC4lugkcN8YY5eUrIyGNlFB  
DCOHwodED/en+hZPm19G6nrEhHIPcW0sERigpW1r0K8WnbD8eqpsf0JT46FfhWXQ  
mckWIm3nu9IZyR6ITpC3VoI3LTTJ06wnVax0emYfi8FCQzb/CnqdxT0pH88/hQoQ  
dlhMKhv9RoerQk6MMU8dn34tDWzG9CT50NZrPH1VoIiz77U0n09Twi2kzUJaaM70  
TbsHNnIS6XJtaGjLRqWIh0/VNLI+gcip5ovLbHupWvWtN0w0zkBX7M5vLLyhK7tG  
KFLLE0+CSNZeEAK5TxUIovYdwfeny+IwPvfuBdhabvFwHxpmeqU+3zZseY7/f/PB  
PhymXd8QLsHMBm2qt6/HuVnrSsYhkUatD069hCc4R/YSpqypm0QZS+Hh9xJJ6We0  
ih5+y2hi+h10NHNLo2qtPnitXlMTecYBeXbJypprNnk0mtembXe7m0BjvfCsnw3/  
4mV+xqXmaizZaPdQkx5DfmB8STQ6Ej0Fgq8t/5cS20ChrEJO8hK+NM0wlj8/y+dh  
+DioI6/936uVVG448NZt+lN0hZgQuAinobLDV/qjZAaiUtN40F5NmmsLezZsOnY  
P3CK9IZ8fOVIYf44BB0z6dgt7iqjDH1aCB0+Zgxpla/zZ+gl0rwPZQk0B6aleAme  
WmS0EJ4Mq7LnqLYZ0zfwVHAx4GLiQ2G+KvYJwLHHTCNWwGVIIIM5be63XFIIUula3  
PdiEs2cUSNk9x7rl2aaCpRmJVWCmUBpTTwtVRSvC50aKcFP6+1bp75003XeFj+Yk  
msDfbdD8nApAGU0pHD66bBqha+MY5G162yGcBNpVwJ2AbFUaBaXmxZzWvH96W6FX  
mr92oa2n+qy0eUaxDxivzXyN6NPKPu5LA/HMg9rZPLi929Fb9DlV5+QBXKw5jf82  
58RXGz3TD+Ze9NvJ0LARSQ1k5nU4tAXY9Gglf040D0TENpnzdz3u2uuru0h1SXYt  
PkrK4wgCmZG0lxqcZJKtsa8iruurrqQ5YJmzS90TwYp0+vkF8nWjCGZj1X1A8pmg  
uDW8Q++/miIXFU+okTAYmr2h1s26fpevYYL27MGVUjAheChXU+Rcg7z/bwwtjcfD  
lmfvOX2frGB5VrA6gnP+WXX56Dvxxwtq28FUoMceCewbAHUrVN5ErIGHAuLWHQsA  
E4gmESgcdjyBa09EYH+DcVepLd/bf9to9sSF0gG1Fk18AdSRftR6R0FS8JYVnpVE  
CN6o3RF4T9GJyo/AEofKHSWBl4F+OygLAG5s9n9yfvSB4ip1K/q4EQ6ebw62AE7J  
wQowF+6/cdFYiQL+7vzUCTcI0ixcVWNTOPiD6bgeTJPTQDordtGarlvXi3UmoLuU  
d0BumrY0vMFap0u5xKk7vuNMkzr5TdHpwQsx7z86bkemoeW1nJ8FFE20PR4I97yA  
HaJmXMzMfVNG0cElTgb60oG9bHfaciAmgTKgLvKml4mCNv6ptezVufEuAxLTJUyT  
lJdbh4rZq7ieu4PgncHnGz0kTrtFDNJ5Rg+Gt8TUWn5SURhZol9xsBHd2/3nAuMJ  
HI51BhQ2l7Ag06dqDQwh/7gd6v+q4Eij7ApXW3ytEAniG6Tqvwz5Sba5kJT/Y2a7  
FW09zcbWbNr1a+7npDii9znnCsVierWieVGhkPsJH3fe01Vd0s0FHoFY5vB9dKuFM  
lF3fyDih00a27gp0MEBQbIOu2yIL+azbTJ++Zc//+hBzUe27V4WVyRyLtxD1HZ/F  
oxJgBLnKi4VGF6YKLQ8ba/V0T80+4LTllZqE/EYYyqUaDXVtkPlEWce3UccyJiWk

POFPt32aKNGX4WBSzcz2Zv0xmeMZPfM6FYLH+wSmMZDNUgYgB8988H4yECy55CT0x  
LYnzoI6ZSGh/dXWdmZq5yBvNsgy5a03SJfhLtsC+dGkD6Gw4ad5dokZPrzHte6a4  
ThT+UN4cyJikBeJkLannjCuZC7evyCVHgfP9ukE0cHiLKJvbu5KPxbWLP1m5Yfe  
sMwIg2r5/YUo/syM7xIQ5E98AdEhKSXbrjKqHCwflzws9gfUKo3RE2Yn9Fa4lU9T  
MQ8YE0Frh0dG1xeLwbphtpAIYTTcQ02Tkm1WwbWkwc1RPWec4Gtd//VzMnN1JODm  
qV0gyu+EKXsgzEbbAzRaxTe63cLEXS9o+FommRqHVN4bZHRzEzF/gE8r9ujMOM8z  
2uRACLBWRUb5iGR28cQpkMt+McH1PCKVmiNV40/subgwSt0n+aHwxRMCzcIWDMP  
zHMvMPb17qHzcdiqrB+dbfsC0fa4jCqWJGB0ikVb1nzqRXYJiVsu11FtnVsMp8dV  
MQvQTBcPDybNtLVixWF5NhEApS0TLrypP8yR+7kYqvXvZ4xD2DRKZmHBZW6ePNCs  
kl+xULrLUiDFQaYcxq43gGJWzzCyYVfx5GXoR0ZaUbJnzsw1YBTgJDCHHy05kpDx  
q+FK/7FVce8ZmDhc1i3vdBQ1DPN60qSLtkABfdJkF1pPSgBpobNU29uIUeqd02zN  
rjDbgu/V7NpISuzYF0ombEz3m0rnCZLYDmPic8YnQweq9YncKRaC01qDt1gJgOK9  
Flc9sPRi184Eik9EMSkstvPZ4RcgwC0k1AVS3eqiCd0VNoe8fg9+fHhNHIGSPjb  
5F2rth9S6aItpkAJIrgirnHEmBDPAhAVzbZFK31LxLwqiQZPVnE3Pjuskv4CQhiK  
54MYyslsh0zF5hmnHA/BxbK4FdvH7w9fUQS1tktaycoiQvizes50Gi2901aQkzmo  
YgkIK/8wF2b9PFvbLQbfPFA/nF03LBEmFCpNK4uF0tIDqVIPerp0mYgcHX0QFSXH  
rNmudjOgsxP8JsOpQbiZRsChc0F0fhK9MIInzMTS63Z/j0wkEWuYBvbtwwAAsZeA  
mlkcyk/iQrMp/rflZQk68qMRJgEe+SMpoaI5Ssxqe/W1C5UDp8FgQoRHEXXwab4w  
GKsYXax8rxxUHI1YJ085bLvWevz6P/J+mBSYEmsA58ipI0RBrKIIoB0jnX0XM0pd  
DIuyM3SQd4zxMGALNngINAYX3ZA4zqiPy+NgVbgY3tdYT3cBvk7pyC2zvFvqAbjU  
nR8lkL6H5A5i2IbW0xg2eLUxjm5uKSY1thrpaiBqA93Tzgh4AQ0A6zsm6inh3Fwd  
iZ5sArZtMg10t1l13w11x420028qGtF3DfjwTfRvSySovp0cjtLE0MedJIS/rv+cy  
/5QvRDcV2eEKHA2Czcl7sYLLaM7JDTuPtIEZFFDK+4rxjiJTCsSNHyuzFBLJPMC  
PyNrH1Fic+MeMJqtZd0LTtX205LklFizXpaqL/KQfCiIb041mXy6/e4w+etXxs  
v09LY8u2yxaCUFKaoYilKUF15qCnJFWZIGdxZxlyjHtruMUZ9P9dGIQYcj6n/G0  
BLYqgLQjFQtwqcX3/tQSJUDgFAFc+EVL47qTEIwTtMIF9w03JNrW/+GhILDf7hUj  
4STEMb7mgheq8C5qVkeaXmxt493oZ/qGPNebHX+oXxuHiXrcL/BF7Kq1miZWz4q4  
TsyaKRREXo29AtSx9jc7k7DzZaq7hJKCp2mueRFV0LLODV+jhpnNC5fYnDj/KFV5  
1CGYiGzPQ72l0kRNBG/uAkvbvwFPmTuUgcSQZzW6rKtsoPVt7qxOG1EHniLfYVzn  
Q4Z5uj0rk10zMjsY3XDfEkB8wRYHJbLJFoqUsliMH4TxcX6qF16Qs/X0qHTC3Jvo  
zyaWvs9IAPfcjz9loH1Ty2P1oT1VGmYpl9zj+So2Dm05Rjo+nuh0FWyiK3ZDZmig  
/3Txg2LSb+WDfyZzvkgarO/FRQNmjGYHGI00VdPRBR/4KwXGXhxtNN+DnQ/SIUt  
hYCy4n5ncfmflF7Vvk3npMrcFqi5/GljzcPH2zkWMyyF8rZ/hoWQk89h40NW+LxL  
FJKuDRoSZJ3a4P3tkUrhmvZwFja+4GuLCkNKVDu/3wpaXw7luhyerW9pg6IIqLYk  
W/LcPrfT+eMYsSvdXedI+K1CSMsDfqiJAdGwaQ9JUgBylnbyeLuImQ+XTaRBKpXK  
BStA9s6fWPG57fUcJbIC+l0k86hqI1MYa4o34WydKWHyGorzOPzWr/0HoXEOpRoJ  
tFR1Qs30FhFV/LKLCQoVTLJyVfi0f2utPinMz5MmdWBSrphum3hQtF/fqiLQLxiG  
SDiBdkagfjlbDVu+ghS21geQnH0M+JnFpw+xCYauYTxQP/m/ZZYfZ77H4pNInc7  
nT96atjaMr6yLWeWhPTPTHTYNGNOGR5a5jqQifjn40yuhoCZcerQ/b0zQjhCXPj1  
RYUckVeOFxfELOqmdFMPKDuGE6z6um+dxTLIXvZrQo9gL59hvPxDR+zM8C35zmg5  
UJUHOuLziAJzyeWGL9D/p/e/sTFZ0cqXtk/lxKcMvFwizyFJu/euu2UYg0UToF3  
sC3Wh9yszYvJEIWy6UtIcqDwIFkMJFp/kSU72URoZYYw5TPb/e/YBLNSXgtJqXz  
Z2hdXwIb1kkAqKl1C0oS0Cwja0+6w93Fqco0yc/ejwiZcsJy3xc592gwqMpQQ0R6f  
KxYxKZfjcxJVF9U3MLZ6Gc+0ZYfsbfCqBA/Zhe0munBrNLZ5U0gRfT5Ub2Zf04x1  
g4aW5k08MpjIS/AuarmzsuiehkkyFAZhmeH/6i8CGId19FpY2SUUHp9/le+c3TAC  
pFoXFHE1xB1R/LXz1mcUhlDXMH7D2BLGuiast1dWu2JRuiXeIGCRSig27fa7mLyn  
aAc5tYUVjB1J5LUUW/n4SzD0M7n3rcMirEAlzl3nSxpReyd+aoixRYMBru5k2FHT  
KE1+b+l0zg8c/W0nQljP3fNevIJ+gZr924Ta8tU=  
-----END CERTIFICATE REQUEST-----

## Sample public key to test the SPHINCS+-SHA2-256s-simple post-quantum algorithm

Use the following public key to test the SPHINCS+-SHA2-256s-simple post-quantum algorithm.

```
-----BEGIN PUBLIC KEY-----
ME0wCAYGK84PBgYMA0EAUVCC2EqHM3A1hYoRDdmLUH0rBpbDoKnlfLnFbpInHjct
7cMX0vRd6hFz0fIC69yciXgk0LaYuyUGww3i4gxu+w==
-----END PUBLIC KEY-----
```

## Sample private key to test the SPHINCS+-SHA2-256s-simple post-quantum algorithm

Use the following private key to test the SPHINCS+-SHA2-256s-simple post-quantum algorithm.

```
-----BEGIN PRIVATE KEY-----
MIHTAgEAMAgGBiVODwYGDASBwwSBwHXLajRuLYX40pNjA56PVWVrq3iR17koJWSc
jibx0U3q0a82jFnjEGKQwZLcwbnyFC7N+Y0ENN2+AgPJT+wB8S9QILYSoczCDWF
ihEN2YtQfSsGls0gqeV8ucVukiceNy3twxfS9F3qEXM58gLr3JyJeCQ4tpi7JQbD
DeLiDG77vUCC2EqHM3A1hYoRDdmLUH0rBpbDoKnlfLnFbpInHjct7cMX0vRd6hFz
OfIC69yciXgk0LaYuyUGww3i4gxu+w==
-----END PRIVATE KEY-----
```

## Falcon-512 (1.3.9999.3.6)

Use the following CSR and keys to test the Falcon-512 post-quantum algorithm with the 1.3.9999.3.6 object identifier (OID).

- [Sample CSR to test the Falcon-512 post-quantum algorithm](#)
- [Sample public key to test the Falcon-512 post-quantum algorithm](#)
- [Sample private key to test the Falcon-512 post-quantum algorithm](#)

## Sample CSR to test the Falcon-512 post-quantum algorithm

Use the following CSR to test the Falcon-512 post-quantum algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIGfTCCA9kCAQAwPzEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECxmGUEtJSHVi
MR0wGAYDVQQDExFGYXxjb24tNTEyIFNhbXBsZTCCA48wBwYFK84PAwYDggOCAAmn
FJ0lb5xjjzVQ0bUEY0bozaLCCMuFAj5SPBn4QfCsu+XU5UL5DphvG/qNHdMpHwIM
vsrfmWPVAgZ4su0BUGiQpLI1Hsk6gw2cUMCa2KzZjVWzidhlHqs3IYAwt5u0C9Gf
bYxNDKXV1Ls7QbS7+NMdEbablkfzpsZIG+LFFohoeKCPZdCIVvw0SV62UiaaKfSdA
KahNmCSGnpOKfdBN0bsGkk2J+RljLM4g0sY0OFFqK+hRSzKW6T3eh1YZ7QKbYZUn
tJxOTTxja3kgZlzJ0oE8WLQm5Bz5FuNOX0y4mxfjUAniXvn9AUS1kgTyT9vyrmYj
I6yiq1o0wpiX4TsMGYKhNFRFFBwCopMNIrJE/OXjJNVoeu5j2kpKmg3p2AP3Hfx
XUBcErpmelZCDx0/UWUgFXHKFujdIKSNW1IC0EwbWEmXRjbxGyvqnHwMaKgqDCmi
GiLbNu72dYANIjUSyI/0pCwPXUsvIZABxIZ0jkl6aYXK9XISyIMaHZVbMvTAyo8Z
az1exehdJZ52g5WDyMc0HvDxDy85jvS1N8+PCVfk6Sai2E5FDT8ZDlCtXzQTpwZD
+k0mqMTNg8Qdfuv6/y6rnoq4S3YAuE3pgfQRL0siMmT5MqyBg5ook4bfXXs9SdB
hkhCsJVyNC7NliARVi0popFZtTPZnJUYRLv7GNJwMmxzIWqOLyqt2hrRk+RGfPk1
GkC1BtEfGbvTzawdEEMDDGC4dsCFBSDgbvC4qqoDZHWiDFNQzU1SMBt6M03dJ2U+
```

```
RS/dmmLupJpxrKU9hR6LrNBhTGGVcPCbdpKSVhFqKsIpQTY7tiIjd6ZLi1qXehB2
NbjTkcRGAgJGwx3fvS2oqS3RME01iRW0G0GZkvUg5c1XvwY2FoFYaiIMhLW9hjpJ
XnZ3hFjThmC2x5QX6x1abMGUa6krzke0jl4ksFFmpu7vmZqeKpe7bBdUUNU2n66g
P+pl2uPlEFXRPnkMDWFFptqyiwb/WOEb0fnZXJg9+5qDbna6LcLQsayHJw4vNRPO
s0q9W6GTD6VVref7QBQGI/6gMtYbVl3Yy2ktTNIKEZiTtK+srQi0Z1bVqQEtDqiC
T/RKDRTx8uYLXtY9dbDBsLtIplIY0mMJvEdy0Ivvum4pZwQQGTv5BcvjAFE4mS8K
01AsPsJPs2yjSxCaLgT1bJuN1ufmtac6jtrug6Hpf6AAMAcGBSvODwMGA4ICkWA5
BpW+Llwzampqt27/3rtgB0/HXLPe1YBuzZX7B0pqsmfT4duKoZnicppj23zLETU2
LBI1EkFZv8JCsmVPDPptIRteQUY6riojJyGrEZlErbCtXm5j8yLU923DsCWdW0w
XpvCwLX637rPybRh8zLfvFLSvGwF09hxJQ4rSkMRFJ1hbmP7kkJB3VNqzBiGro9B
wy270iexi0jUVn0TVVQ20120vvkeQliaTsLST9EnC2NLs+LWfFspT1/lySoGxanpU
iqze5KtLrL6K9nk5dGTM23KL7uboES5vUv1enyUCjeTaVE3cw70apCj465qi+
wyfoHas0S1LZNdHRIBNL4MbB8QSh7ZckKHmagroJatpKEjwZAJRRGi5PMVbDxcw9
SJElpJFrix6MxcuWlpeqh8GMN+PvqkUHUc38EzqNG6CZ02s7gwiNZBhX9sK450
mNG/eI1xr0cxyFOImFayHR2CLQuUG60zX4EtBKpp3cRxWTPs6bCN8ViKXGSp0Xau
Vb9y12M5jXVQL3skQDdZBu1R+JIHhFFkZWDLzTFigoakMZizNy2zq9immkGSi64Q
dcoPbtthedkJn+fWoSRs9I9VmZGvG8p3jfwU8nJNUq1nZJcU66AyOTckg7jxqQnr
93k5f1WmQ2Jn0Ny09xaQenckiL5v3DFaU+L0nHnP0R9qYxc6hMWrwLMxQ7SZ2cFQ
L3fuggXRiVOCUqhp6dJDbvNGYzzicJ/5sgx9rsSJIpBNugA6C1INrEBj+LSj5sVv
Cr4/OTLb4WqowVJEU5I5EnG3CEyHK6ibXLV75NiEdT8ypkFfhDr17KRiN0L/qjT8
fejJP8hGgcSR/r1ubg8hzWjgYpjdkKbZcZ0kK7ND10pA
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the Falcon-512 post-quantum algorithm

Use the following public key to test the Falcon-512 post-quantum algorithm.

```
-----BEGIN PUBLIC KEY-----
MIIDjzAHBgUrZg8DBgOCA4IACacUk6VvnG0PNVA5tQTLRujNosIIy4UCPLI8GfHb
8Ky75dTlSXk0mG8b+o0d0ykfAgy+yt+ZY9UCBniy44FQaJCKsjUdKTqDDZxQwJrY
rNmNVb0J2GUEqzchgDBm3m4L0Z9tjE0MpdXUuztBtLv40x0RtpuWR+mxkgb4sUWi
Gh4oI9l0Ihw/DRJXRZSJpop9J0ApqE2ZxIaek4p90E3RuwaSTYn5GWMszia6xjQ4
UWor6FFLMpbpPd6HVhntApthlSe0nE5NPGNreSBmXmk6gTxYtCbKHPKw405c7Lib
F+NQCeJe+f0BRLWSBPJP2/KuZiMjrKKrWjTCmJfhOwwZgqE0VEUUAHAKikw2ICskT
85eMk1Wh67mPaSkqaDenYA/cd/FdQFwRGmZ4vMIPE79RZSAVccoVSN0gpI1bUgLQ
TBtYSZdGNvEbK+qcFAxoqCoMKaIaIts27vZ1gA2ILRLIj/SkJaldSy8hkAHEhk60
SXpphcr1chLIgxodlvSy9MDKjxlrPV7F6F0lnnaDLYPIxzQe8PEPLzm09LU3z48J
UWTpJqLYTkUNPxx0UK1fNB0nBkP6TSaoxM2DxB1+6/r/LqueirhLdgC4TemB9BEv
SyIyZPkyrIGDmiitHt9dez1Jt0GGSEKwLXI0Ls2WIBFWLSmikVm1M9mclRhEu/sY
0nAybHMHao4vKq3aGtGT5EZ+mTuaQLUG0R8Ztw1lrB0QQwMMYLh2wIUFI0Bu8LiQ
qgNkdaIMU1DNTVIwG3ozTd0nZT5FL92aaW6kmnGspT2FHous0GFMYZVw8Jt2kpJW
EwoqyKlBNju2IiN3pkuLWpd6EHY1uNORxEYCAkZbHd+9LaipLdEwTTWJFbQbQZmS
9SDlzVe/BjYwGvhqIgyEtb2G0kledneEWN0GYLbHLBfrHVpswZRrqSv0R7SOXiSw
UWam7u+Zmp4ql7tsF1RQ1TafrqA/6mXa4+UQVdE+eQwNZYwM2rKLBv9Y4RvR+dLc
mD37moNudrotwtCxrIcnDi81E86zSr1boZMPpVwt5/tAFCAj/qAy1htWXdjLaS1M
0goRmJ00r6ytCLRnVtWpAS00qIJP9EoNFPHy5gte1j11sMGyW0imUhjSYwm8R3LQ
i++6bilNBBAZO/kFy+MAUTiZLwo7UCw+wk+zbKNLEJouBPVsm43W5+a1pzq02u6D
oel/
-----END PUBLIC KEY-----
```



Sample private key to test the Falcon-512 post-quantum algorithm

Use the following private key to test the Falcon-512 post-quantum algorithm.

-----BEGIN PRIVATE KEY-----

```
MIIIlgIBADAHBgUrzg8DBgSCCIYEggiCWSSAvfCAhfWfghf//O/gfw/gABBxfO/
QQQPvHAXf+w/PxfQx+wFA/v/exSCAAPBevwffgPAgfwxAghwP+QCguQgABQfQhAQ
uABfRvQwvPhOQAvGwwRe/gg//QA/QhxwQ/AAuBPfvAwu/fBAf+gPQgQRhQhRBQAg
wgxPgQ/AffQfxQ+OPSAASf0u+vAegu/wwPhgO/hywPx+/A/x//wAQSQRAPgvvh/w
wheyNxPQAxAQABgefwwfwvWuhOwAgBOW+Ru0AA0fgAhQQ/QeQ/utvxQew/QQgggx
gAt//vQfQgyAf/Q+uSP/PewgQvPPAgwvRQwAB//wu/ffwgAPQxACHewvP/wAfexP
ggvOuhPNPfgw//wfg///fHA/SfPgPSfgOuyOwgvABe+Ru/+gQPvAyAe9gARQBfR
ewAw/vgevfvvWuPffQvwe/AxPwBfxOgQAfgAgAPxAPu/AAvOuOvARAXA+PAAPARg
PA/xhQQBe+/hPRg/xfQufw/fgBOAxQPgQ+wPPvQwvww/QgP+vCvgPwQgA/ffgPwg
QPwAvAff/PwffQQAQhwRgxfBgBxvvvgOwBQQ/wOIQPgRPFgARBPvvhgfe/OAQgR
/ghiBQOxRvwQPvQ+fwguzPghghfxv/uvhgRxRiPufggvy/ggwuRRCaewRg+QO/we
/gAfAxBOyPAPgfQe/tgvAAAiPxAawvABA+u//BPwffRvhAAAReQftvtu+hPQgP
vxvvvQuugBPffwAO/Av/vPQ+/vBwfvPwvvgPwfiOv+gPxxAgfRPFp/RfRvAfOv/Q
hPeRBAQDPQfPwOwRff+fwwAwRfvP/weQA+egAgAAA0/ggfgAPffguxPwPQvOgP9
/eh+QwCfAQvvhvfewQwgwgOwPQePgfn+uwwvewygAfHfvOAPyvgQd/BuwQvwQf//
/Av///BgQQu/uuQewPOw/RABvwwwSQxfwwfwxePgfhwgvvewv/wgfSSQ0PAQA0Q+
fxA/wBA/tBRfvABRwQhwQwAgBQvQPgQAASDs580DGBv66xDt9/YBfw4exinx90Pz
CyP8DucnDgHeAdLvCP3y9dsH6AEpCQAT+/oF+NkjjwDjDQIS1wr/8g4ECxHhByAH
EhDs5u7/+z9HBUR2h7XCNAx+wbz8iLs8+8H7gkCDAUA7s5srU7w4dCSbj7yX0
1AgRC97gAeDs+fgdAAKHI+To9TMJ0gXXH0wU+08KGGL88erqHdzl2CCz8uTrCg7v
NyMS/yPYDeL06xYgKhbQ6AAAdAiTq6QHcEtwSBNbd/hTRwv8ZFwke1e7pATAHGvz4
HfYIUxXsK84K70TP58XuIQEayBD79AroG/8N5RUMAQRnAP3a6hg9HA7d/gDzAv27
9vsTCPjw69QTCEYIGRCi7hYJ8f4IIxvxGPkeHhQN4ujwBtLl1urw5ioAA+7s6u/4
A/XRBMzcGgcL3fwB8xLq+fb/8yIR8v3VJ+MQAQk+MyYUAYcY+h/2xBADBuwgF+ry
GBHLE8kiDuHn9/sJLA8A9Qg/KfL/MvUHERL+Abz43AD8FvcV6zEg2grh1dTn1f4D
GDEpFuU6Cv/w0hM0BhjzD0k5BSX5P9z42tIa/dgHFvr630Ed/Po0BzsK6BAw6eEB
8AfPw/b/3xYqDSPY+MoK6fr98h20LhUGFQgA8vsV2gMJBhHU+Ck3EOz3ChAVDvIb
Fuvo+fj//ugHCacUk6VvnG0PNVA5tQTLRuJNosIIy4UCPLI8GfHb8Ky75dTLsXk0
mG8b+o0d0ykfAgy+yt+ZY9UCBniy44FQaJCksjUdKTqDDZxQwJrYrNmNVb0J2Gue
qzchgDBm3m4L0Z9tjE0MpdXUuztBtLv40x0RtpuWR+mxkgb4sUWiGh4oI9l0IhW/
DRJXrZSJp09J0ApqE2ZxIaek4p90E3RuwaSTYn5GWMszia6xjQ4UWor6FFLMpbp
Pd6HVhntApthlSe0nE5NPGNreSBmXmk6gTxYtCbKHPKw405c7LibF+NQCeJe+f0B
RLWSBPJP2/KuZiMjrKkrWjTCmJfhOwwZgqE0VEUUAHAKikw2ICskT85eMk1Wh67mP
aSkqaDenYA/cd/FdQFwRgmZ4vMIPE79RZSAVccoVSN0gpI1bUgLTBTYSZdGNvEb
K+qcfAxoqCoMKAiaIts27vZ1gA2ILRLIj/SkJaldSy8hkaHEhk60SXpphcr1chLI
gxodlVsy9MDKjxlrPV7F6F0lnnaDLYPIxzQe8PEPLzm09LU3z48JUWtpJqLYTkUN
Pxk0UK1fNB0nBkP6TSaoxM2DxB1+6/r/LqueirhLdgC4TemB9BEvSyIyZPkyrIGD
miitTh9dez1Jt0GGSEKwLXI0Ls2WIBFWLSmikVm1M9mclRhEu/sY0nAybHMHao4v
Kq3aGtGT5EZ+mTUaQLUGOR8ZtW1lrB0QwMMYLh2wIUFIOBu8LiqqgNkdaIMU1DN
TVIwG3ozTd0nZT5FL92aaW6kmnGspT2FHous0GFMYZVw8Jt2kpJWEwoqyKlBNju2
IiN3pkuLWpd6EHY1uNORxEYCAkZbHd+9LaipLdEwTTWJfBqBQZms9SDlzVe/BjYW
gVhqIgyEtb2G0kledneEWN0GYLbHLBfrHVpswZRRqSvOR7SOXiSwUWam7u+Zmp4q
l7tsF1RQ1TafrqA/6mXa4+UQVdE+eQwNZYwM2rKLBv9Y4RvR+dLcmD37moNudrot
wtCxrIcnD181E86zSr1boZMPpVwt5/tAFCAj/qAy1htWXdjLaS1M0goRmJ00r6yt
CLRnVtWpAS00qIJP9EonFPHY5gte1j11sMGyW0imUhjSYwm8R3LQi++6bilnBBAZ
O/kFy+MAUTiZLwo7UCw+wk+zbKNLEJouBPVsm43W5+a1pzq02u6DoeL/
```

-----END PRIVATE KEY-----

## Falcon-1024 (1.3.9999.3.9)

Use the following CSR and keys to test the Falcon-1024 post-quantum algorithm with the 1.3.9999.3.9 object identifier (OID).

- [Sample CSR to test the Falcon-1024 post-quantum algorithm](#)
- [Sample public key to test the Falcon-1024 post-quantum algorithm](#)
- [Sample private key to test the Falcon-1024 post-quantum algorithm](#)

## Sample CSR to test the Falcon-1024 post-quantum algorithm

Use the following CSR to test the Falcon-1024 post-quantum algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIMZDCCB1oCAQAwQDEQMA4GA1UEChMHRSW50cnVzdDEPMA0GA1UECXMGUETJSHVi
MRswGQYDVQQDExJGYWxjb24tMTAyNCBTYW1wbGUwggcPMACGBSvODwMJA4IHAgAK
fok/+3VjiJn0ONk0bjw5WVYh0Gn+pnEi5YnTab3cMxtPTIxnHTV1ru/aJNBs+jhC
eHWi30YxFFKxEc1qQBxWLKnZsECFyLISE/Pm1IkwaE7G4erUs3YvAzdhAmEEYbTj
mVmW/m8x6aLFvWtXpA1DAPUmwKrBrQiEZvRyyp6kdqQXI0St0ad9YQmDYgwN7HFI
omTTn/7LcKTqa2NVLZRCJ2MWGpAJDJKXvhnICVnPSbm4G4i03TNDvFgZ1Iybgfhm
Ik5q3H+0/WWTJkA7bC+bQM9Aaqg0yxFjwhFCnPhKLo1/rYdQqm5xpejB244sT62c
R2To7r9EJBsBLidkA/oKlK1Ya7MxotdfnaVhebJRfVI4M5pP8poCyBegeUALmCkD
DnBQduXdviQnLL3dR6LarQajR4SI+n3z9k4KILARR3cTNRPNZDUJAz6DQdMYdJ8t
iDlC0rkXVjrt50TW4SNtoKF6d9REspY3FMRAXRo1z6FZUKyKClwkzkZvXWrnkHQZ
Q7BZLKAXLh5XhqMU0d8WCcj7IQdVg2KG5wo0XAFETASwVsMRiCcB/4nYJLYLXfl
3hqbdNtKBWvPMXR2EHm5WeN30rAiJpxei4nbEzHH+nIZalJUSdC4NgGog62FkTa
E1paVSA19s1PTUGxYCsTrDVPzQ0KiUeHo+Y6IiyQS1XZe0mjWD01eIALVahZN25M
Ca0QQ1w1gIR80SyjFLliwvLjdklVweRvzFZpaZcyRo/2kv66CUQpb3jUNDhol2C
t5CxTvyFgUJD2Q3TM1G4ggallg0k03Jvn8qGIUvQPMd9b0gEIUMRHD9aH7sJRS1z
Ed0kPKuvMbiqA/2giWBWkuRGzVmIkZwIF2Boh+VTcnghdEYk/JNUo3adkKwBGWey
Yp1C61verS5SjerP0+dBceGTD+J5nELyYfaoXJCxjEJva1RkQvzqgcpKIG6j0q+b
eWctfWjpA0wxrYNqy0Qzmlv+LiQ64LkxAi/GDq3ER6LJ2RiUqIf5gq0cq8YmvQ/
jlcKieKRw6CRRi6ADGEMc5sF0zvnle9n/QQjXFwOknIeppGadq49QnqLKepS0Cf3
IQ4PerZmWfYi8mHix+TpJN+afKhEpih+DxxeQBmgupREbbC1j81mrs2bAlrHLRBV
ObfgsZsu8hnJ4H66lm9K6dcUvHbEU26WeTnawxeWGSaiRREFq6xFILxH8wOGsHiZ
WfDIKcsLedX5beS3Y3oeLrHsE5Q09tH0LpVWH0f4jBTMMH3wE0QG8yKdaYfqzix
sJPaLm+CqFYBAF9DbT4pnuqZUTmZqFS6y6PbP1nzCfoPSb90cbnQXtyKJpxbWRNS
IZVYGZvJe1D9IHUp7RWnj4+6kIpqEHBo0l0y6crZBSzd8farmArgmvuKQAWbPt
I0Qa/HGwznYhcsCD6U2oEyle1MZA5ABtMXofFr9nFQDTVQfKbcn6ZTzWTGaoHyX7
b5yaVKMXOkubijV5RxFZ/jmcfiIsWPtWHIHpbIATRL0hShkPuUhaIvBHQNGUze2X
F0CxNySJV3NhPU1F1MU3G9UB10T7c1xrNYzT5ozBxT6GFejxpu6r0TijhZZnATzq
+x/R6z1p4xM0jTnh+r3KEV3UWxoAKyWs9JZiWte5UwBTdJuI2cNHHemoE5KK4Tts
SbKHTtyLdjzk4a4pctYQpdMsyonSIhouQIUkFKoKydiBGBWhkzNKdH0t5PLZwziv
2mTjxhiYF/F0h5tiLF/1vPed5T2hyPB0DQ9CPW2Sim9kpb8JFjFULF5wPRsQwLXD
VXHLqz4lExfhaAD0VTQI5q3YM48Dd7rREIFXQGdxR6pRxNmUxadIcd81T8IYgKBB
xrTQHoahDFamaa+a2kGgQ40SCy3pG0yE18MWnxaanqsKkKxximRNY00PkmAKbxj/
rz6DuX6WiaB2Jt0hSCfFq2HyT4VoR0mU6hLX5CvktbYC4WIrrCMXkYmJmAXuGTx
e97WFrU1U2GU2rF8UuJJTte4UFWLgSiCbH7mF7ZL43LIVkkZS3NW1UT3Eq4hBLzh
gDspCzwqBHj8gEpKDB7EIMhrN6HGJLvdpt9VomH1VP0p8e86CY+eCyFhs86VtHnV
HsJvk0eYDVCUuABpr/bNti1rmmnBeYKII24JUUnLRWFLmcUzjAwLHLIsCImSN0P6t
IAb2VBbEBh6kAsalNna2qKewJ6JQtLB3qh0TQPI7drXLP53yK2rRB2NIEBik5ikr
dBtUypxbmy1mDcSTK/AVBURXSCwNjxJPKhvtC2puEZCGLMVL3jEr4hKuXQBTg58t
```

```
E4Hl fKAATqkYaqUJkE6ltIIBBDMK0b3peParosuGac1ZEmwinknzJCQGrom25vGA
4vR5cny1941iLqTb8B0q6aAAMacGBSvODwMJA4IE+QA6kWIJRndOzcZwBN0ZPR/Z
Cx304j1uYxwVLdCcbnXxJmXyAdnbXI8s7vtBDhQQzs fon7K1t039EnQQYYia+TZF
Hxgk2GuS0qbWMBDjoNetxa0PhdxhmKoLxNg/Wlpusk6sTJgl40q4/Gk30vPztov7
p9mPgnXkfV3P04f+yBVNMxaVTWs9cZdH1q/u+SI1qQU3VNriHq+hfoTP/UNyYuCN
YzFwvEcjvSMJKYulFxr6XVxkW0E5yTXOGKyq57T0T6V228Ks20mbDg8Kw5jHtuaF
y8G6nw0s807N55IOP1r9s4nTkanEboiXrvvINwib63mC000RBH6C5Ku0Icj2cL9p
Wd+lE0S/OzmHLfk6FVYySqhl1enYnSGInrQIgJyT7wK0RWARyJyCI5WL8q+gs/KaM
1npkEiK0+PIG3TqcM0/eHN0nyZPuwTn1vnIu3PypfhKGUMUqQeFb9dvFVSFKdgh0
9yc22PI6ePXfaRDEorb9jSLreyFFA3akTqPW9bqLvdWjtFZn2lHsbQYE0GV6Gnbq
ARnZtntbbUzDzEIRR3Ur900Sie4iByyRvRwuJwKX6cIyUe8Wfkzz76TSF0JqxkZc
REVHdVinkIbZa86glIaKReuxyJcf/fIpmWvz+u+eRazNvL60FQ7tJC8TYZee06Po
i6w8CWjsKWwYNGPRX/sOUf+xrX57/wiZx/s32KaVyqMLXl4jkGwy+YRxgpHqaTGI
JEB/RkVY5RfypVo0Pohn4qZEf+tkafRcdBvDkc1E1iHqYBQmjp7Nu8VG9K1w9DvZ
NBDGmE48WytXjWxP90EDPNayAErvVeqEkudey2eK7QmJmGhxEiYJyoLr43Erpy7m
wM5xSJt2wc8ZcyBRU2g2jV2X0F7Y09s6sDjtCgRMU7NDwh0mygW0sCKMWEjIttWb
GfTBS0iiPojKcybk3W+xVeLQSZF1zk7R43sbbdSbUs5s6bJViyEQgxbSHdj+R2xx
GecpC2l06TclK/dXCxhvkQ7ZIKWhrsKlXMXiyyHWiFi1Ss208MBZSAox5KkqG4WH
QYhDNyXEmTzf0nL2xtQxZbI0r0r3nAnKlNduUHIlyCLdegQVdZ1h0UICIttf31km
HkahJ8XvX48MIffJ15TIsMb+rq7nPxwL3724sC5NPuqVgUMd23oawW0dre69mkyb2
yS5Zdr+LswTgGQjTzIt45Ckrx4NyN0y1ajpEnb5bMV5sfcM8CTnBRrBKJhJZ07tg
m7fSYHh0it2ygo+7yjYHqESVnasp0ZEcJJDbn42jhb1i5XschDsJySG3c6XXY5P6
QT0r/V0ow7TLeH2SAxbM2CJ0GkMHijF5kfNLauwJKeNmvJ3M/rsVwEhw7cIZt9t2
6Se83M/mjpyC44nP9pbNviPsbh5PLnE+m67KVomlkrfqS42TsJDb+RPonTB0/IDf
st2c0pxnkFXp1E6XGysHTU+dCpKInUGpXWYFZi1zMI4SiUa38FbkYEGojCMLlec6
2VLw1+IMrZ4Y+JxYyrVIJC8mecPMJrnOrSynxi9aUeHgjt5/XLp6W16X5xmgzXvs
T3YKlaLU/blcI9TTwp6cANllN5q7p2XBw2mJFgiX0Ifauxh0Md0ySyRpVqjZr71m
NjUktW1l7nz5K08GaLQRq2NK5pxR93bVpNNfDkXEJU7GuC/5PuQdbUcydrC2iQuB
SrLmmRZx8YA=
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the Falcon-1024 post-quantum algorithm

Use the following public key to test the Falcon-1024 post-quantum algorithm.

```
-----BEGIN PUBLIC KEY-----
MIIDHZAHBgUrzg8DCQOCBwIACn6JP/t1Y4iZzjjZNG480VLWIdBp/qZxIuWJ02m9
3DF7T0yMZx01da7v2iTQbPo4Qnh1ot9GMRRSsRHNakAV8Cyp2bBAhcyEhPz5tSJ
MGnuxuHq1LN2LwM3YQJhBG045LZlv5vMempRb1k16QNQwKVJsCqwa0IhGb0csqe
pHakFyNErTmnfWEJg2IMDexsSKJk05/+y3Ck6mtjVS2UQidjFhqQCQyZF74ZyAlZ
z0m5quBotN0zQ7xyGdSMm4H4ZiJOatx/tP1lkyZA02wvm0DPQGqoNMsRY8IRQpz4
Si6Nf62HUKpucaXowduOLE+tnEdk606/RCQbAS4nZAP6CpStWGuzMaLXX52lYXmy
UX1S0D0aT/KaAsgXoHlAC5gpAw5wUHb13VYkJ5S93Uei2q0Go0eEiPp98/ZOCiJQ
EUd3EzUT2TQ1CQM+g0HTGHSfLYg5QtK5F1Y67edE1uEjbaChenFURLKWNxTEQF0a
Nc+hWVCsigpcJM5Gb11q55IUGU0wWZSgFy4eV4ajFDnffgnI+yEHVYNihucKNFwB
Xk0wEsFbDEYgnAf+J2CZWC135d4am3TbSgQcLzzF0dhB5uVnjd9KwIiacXouJ2xM
xx/pyGwPSVEnQuDYBqIOthZE2hNaWlUgNfbNT01BSwArE6w1aWatColHh6Pm0iIs
kEtV2XtJo1g9NXiAC1WoWtdUTAmjKENCNYCEfNEsoxS5YsKby43ZJVcHkb8xWaWm
XMkaP9pL+ugLED2941DQ4aJdgreQsU78hYFCQ9kN0zNRuIIGpZYDpDtyb5/KhiFL
0DzA/WzoBCFDERw/Wh+7CUUtcxHdJDyrrzG4qgP9oIlgVirKRs1ZiJGcCBdgaIfL
U3J4IXRGJPyTVKN2nZCsARlnsmKdQutb3q0uUo3qz9PnQXHHkw/ieZxC8mH2qFyQ
```

```
sYxCb2tUZEL86oHKSibuo9Kvm3lnLX1o6QNMma2DastEM5sC7/i4kOuC5MQIvxg6
txEepSdkYlKiH+YKjnKvGjr0P45XConikcOgkUYugHRhDH0bBdM755XvZ/0EI1xc
DpJyHqaRmnaupUJ6iynqUtAn9yEOD3q2ZlhWivJh4sfk6STfmnyoRKYofg8cXkAZ
oLqURG2wtY/NZq7NmWJax5UQVTm34LgbLvIZyeB+upZvSunXFLx2xFNuInk52sMX
lhkmokURBausRSC8R/MDhrB4mVhXScnLC3nV+W3kt2N6Hpax7BOUEPbR9C6VVhzn
+IwUzDB98BNEBvMinWmH6qs4l7CT2i5vgqhWAQBfQ20+KZ7qmVE5mahUusuj2z9Z
8wn6D0m/TnG50F7c i i acWlktUIGVWBmbyXtQ/SB1Ke0Vp44p+PupCKahBwaNjdMu
nK2QUs3fH2q5gK4Jr7ikAFmz7SNEGvxxls52IXLAg+lNqBmPxTtGWuQAbTF6Hxa/
ZxUA01UHym3J+mU81kxmQB8l+2+cmLSjFzpLm4o1eUcRwf45nH4iLFj7VhyB6W4g
E0S9IUoZD7lJQCL2x0DRlM3tLxdAsTckiVdzYT1NRdTFNxvVAdTk+3NcazWM0+aM
wcU+hhXo8abuq9E4o4WWZwE86vsf0es9aeMTNI0zYfq9yhFd1Fl6ACslrPSWYlrX
uVMAUwybiNnDR4RJqBOSiuE7bEmyh07ci3Y850GuKXLWEKXTLMqDUiIaLkCFJBsq
CsnYgRgVoZMzSnRzreTy2Vs4r9pk48YYmBfxdIebYixf9bz3neU9ocjwdA0Pqj1t
kopvZKW/CRYxVJRecD0bEMJVW1Vx5as+JRMX4WgAzLU0COat2DOPA3e60RCH10Bn
cUeqUcT2lMwNshhFNU/CGICgQca00B6GoQxWpmmvmtpBoEONEgst6RtMhNfDFp8W
mp6rCpCscYpkTWDtD5JgCm8Y/68+g7l+lomgdibDIUgnxath8k+FaEdJl0oS1+Qr
5L7W2AuFiK6wjf5GJiZgF7hk8Xve1ha1NVNhlNqxfLiSU7XuFBVi4Eogmx+5he2
ZeNyyFZJGUtzVtVE9xKuIQS84YA0qQs8Kgr4/IBKSGwexCDIazehxiZb3aU/VaJh
9VT9KfHvOgmPngshYbP0lBR51R7Cb5NHmA1QlLgAaa/2zbYta5ppwXmCiCNuCVJy
0VhS5nFM4wMCx5SLApZkjD+rSAG9lQWxAYepALGpTZwNqinsCeilULSwd6odE0Dy
03a15T+d8itq0QdlSHgYp0YpK3QU7mKcW5stZg3EkyvwFW1EV0gsDY8Styob03Nq
bhGQhizFS94xK+ISrl0AU40fLROB5XygAE6pGGqlCZB0pbSCAQZCjm96Xj2q6LL
hmnNWRJsIp5J8yQkBq6JtubxgOL0eXJ8oveNYi6k2/ATquk=
-----END PUBLIC KEY-----
```

## Sample private key to test the Falcon-1024 post-quantum algorithm

Use the following private key to test the Falcon-1024 post-quantum algorithm.

```
-----BEGIN PRIVATE KEY-----
MIIEQgIBADAHBgUrZg8DCQSCeAYEghACWjECEPQBKQfxE935/eB3HwB98xQgARBA
C54WviB8P/9+EBAbHsAQj54QBcCLpQfGMiuhQfpQh6L/AdGQH6L7mxgBkPwB0EI
gdJ0A9H37/Q++TwC97wHRE+MBvj943h9F8A/hJzXe/94I/AEH4BFADW/D6H4Q+AA
JQ/KD40f+HnOg30fRiMAIwDID3fi8QIPjDwZaj7wfgAH/4wi/8HAKFwQACDvoABD
8ACeCAoQBdwnvd6TgCf8TnehF/4xk8H3wBALwbbCH5QGED40gEH/f7+DXv/F4YRd
18nyAPwfPeD3ZOAx73xDJ7XS8F7oSB8AIfk973QBAYACe103x++ARQgCMmei9sBf
AAEOxEB4off+EYR/38YPj38IBcxwYRDADwQBB4Qh9CFQSh9/4AAGPgAkATxBcIL4
uiB8XRk8YAP+CAo/AMP3geGQXAAB/YPg9wQR46FHx/+AvRAEUHw8CEATf6QfvCF0
Qu6CLwhD7/pQ+H/n++//qDd+D/g9J3+Bg5wAAgF04ie6MIP/uEHwk8bwgd8IIveF
72+h6Xvy++cX/CGAIgk+ABSCCAneb6IAPgCT/AA9sgw874HgA974f/D74/dB0nvg
D4Qu+8DYRf+EHeCCIGOE2Xwfb/74AE+IAfbAPvQfuUAcj+HvgB+YAwD+Iv/BGPvw
75sZQgJsJgAGIAg8EYIQeP/1/eCLvR+F/vwiMT4PA/8fQj/8H/BT4ABgGAACa6MA
g5934ge/0Pu9F7vg/4PpA+D7vfhB8gCZBsfvA2EHdC+LQxj9/nxg8AQx96DgBBB8
Gx/4P/hfEboAgAEXiDB8mwc93vuiAL4wi9wPgAKIOhA2Pw/jEEBBiGEPHgADQuAB
znjm2AH/E6XvP/CEfwa8MIwC3/w/iCEHyc/4Pxc6UHuikPQBBAAXABGU4fbB4fh/
9/hdiAH/vi18HvjJ4Q0+8Qgfc8L/yB8X5heEYPwgIMAwBB8fACAQIQ+8PvBC6DRu
A/4v/B38Qdi5/wOjAIfvhB4mgeGHg//AYHuAAMIQk9/XQcDwIukD7mgAAAYhCCTg
h+8IYABFv/u977wA++ABRAF/wQ977pAe+FAFF/gowe/8GggD7vFAHsOQ9F8AvfOI
PjAEX/g/AQ3ygIIAQBIQAQAD8IhhB/4fwICE4v76PoF9EQIf978XPg4HwAg34gfCH
0vfdAEXyfcPwyfAUfQeEEY//AH4B/GDpBEH0Av+7wACeGPxDAOEnge/sXdjIHpO9
J8pf6+Lg+EB4AP+EEX/lB/vQd/z40fFwPwh6IoPiF4BBd8HhSAF4Pgdl7wP8H/4h
```



+3wHQj980wcGIIRhCYIQcEMPzcKD/ve98AN8IMQia18nP+5/AQdB7wDC6AYh+KEX  
wcGQQgEH4P9fH4AAAGH3PD6D5CD6IA084IPxiP8nyBGAggcB3oAi77hPe6EHxgEE  
QB/8UngiDwGwED/ZPe8AQ/+Jr3+BHnhd8Dz4eZCEHxdDwfxA8AA/BN4HvhGHgCf2  
T4gj+MAAdg/vQSC7w0fdAL/9j8YJue6IIBh8ICBcEEAvjB4gR7+UGvCIIgTbIP4u/  
+IodFMDYSFADoS/94IBeF/ovfKP4Ag6MoyeJ8Hg5F7/gg+AXSG+L4hjEbfgiGYIA  
+F7wegEMnxd6EYei8IHwj6DwBCBvvv96HwddAAXx9GMAA76ERgf5/X/+CIYyBNwP  
PcAMHe72DWR+7QDkJwj4Fj/QIvs6+fX1GCjvHw7740/nBe//AA8XFP30Auln9/8U  
Dfw3Cff05hflIwr56vU0Bu0C90byBS4ZKu3tDyXtBiGoIPALJPLb+P8gC/EK5/3q  
2tr2NQ7T7/+bv4+IQHtUTACH9M/wqB/fjCRHYFecC4gQW5fkP/gv0BxvtHE4PG8kh  
AgYUC8AGAE7t8+se6xoB9Pc5+/Mo+/ck78UN80IZ3QNAEe/ZEwoH/wsUCefzFDgR  
9/8HIuYU6QYC/SP7EvM5LAXLMCAAEdb7DOPX09j+GgUN/9rqLej9+z0JDuv91iMC  
NBgS70kc/OLVTRQc8x8g7gDMBxUA2h/0AwEn7/Ik7+kHA+UE4vYHG/zgDvz9Mebw  
KvbyDNXs6xPCFvkH7RX+600XKAAFE/EgEuYJ3/r7BQjR1RASCAP2DggJEtgE+vkq  
FxAfAPruH+EXCu0cFAf+7CRAP7hAS6Pub7PMZiVx6+eEiGx27+h492ecC+wo6sx4t  
50j7KRb1E/7lwu301SrbEBfi7hQK/xQ0C/b5MvoSax7k+fsNI f0B2SMM/Nvk9kcX  
7irg8uQr+wT4/AfvB+P+CPPoIQn39v4L9jMYFOMT6RD13Rc1/QDo2eIS5eoSDhkP  
Fw0S6P4h+PgEGBEL/iInF53r4fba6AHbC/ETEPvgGFHnISPwAQYZA+0e/Q4QM+Db  
Cv4b0gzmFwoe6/vwAtPh7gMM7+XzGvXd9AMUEM4SHCLj9gLoBP4i70cuEPS4yAUD  
IwAU5PURERbeAwARI+PnLSXTfgnQ700T0xQD8P0XAO/+DgoALRYB9sQL4wT1Bh38  
2xYYLQoS6ff7CAkIIWj3FP4NG/jY/hYiG/H5+wEWAHdPEtMhBx3q8C8M3P8L6Rga  
7Czq0g0UBecAvisw9PM4JiAGHgOQ2Qr4GDb15gAH/OoR6ej44PDtMw0H8vQX8/D2  
Fw4a9hXU70GUaiTEyXt/twrGs7HFvUw2/DqAB/+It7mAtU0DwnOPAsexfLjDyI5  
6xzQCB4cFfr89yQeAd7m+xPv9sD4IfQV6wsL0d8zBuFzJQQC7/0I8wfcCeODEBTJ  
HeIrNQgH90cg3/nN/hQRKu3vF+IhHv39HeUI8SES+fj90hC05xrOARwQ8Af9Itzn  
3to9EHMK+A4B4CrR/Qf6GtwF1e4myeYB0DXfBv/+ByHR2kcH0BPY8Av37PMpAf76  
DSrv1fzrEeD+Cvgc++c0JvYU8RPSA9wKJw4UNBAH/u7jHCjb2f3wDx8H3PT+D+zj  
BPiAABXm5vMuERbtBDEu9Qz0+u8ZAdX91fEOM+veDwUS3eYHBxQJGv0U0iojJsb3  
B9z21/ULEC0V8gQBG+H6B/sQ6wUhh0fpJgp+iT/7dW0Imc442TRuPD1ZViHQaf6m  
cSLlidNpvdwxex09MjGcdNXWu79ok0Gz60EJ4daL fRjEUUrERzWpAFfAsqdmwQIXI  
shIT8+bUiTBp7sbh6tSzd18DN2ECYQRht00ZWZb+bzHpqUW9ZNekDUMCLsBaqsGt  
CIRm9HLKnr2pBcjRK05p31hCYNiDA3scUiZN0f/stwp0prY1UtLEInYxYakAKM  
mRe+GcgJwc9JargaLTdM008WBnUjJuB+GYiTrmrcf7T9ZZMmQDtsL5tAz0BqqDTL  
EWPCEUKc+EoujX+th1CqbnGL6MHbjixPrZxHZ0juv0QkGwEuJ2QD+gqUrVhrsZGi  
11+dpWF5sLF9Ujgzmk/ymgLiF6B5QAuYKQM0cFB25d1WJCeUvd1HotqtBqNHHIj6  
ffP2TgoiUBFHdxM1E9k0NQKDPONB0xh0ny2IOULSuRdW0u3nRNbhi22goXp31ESy  
ljcUxEBdgjXpOVlQrIoKXCTORm9daueSFBldSfMuoBcuHleGoxQ53xYJyPshB1WD  
YobnCjRcAV5NMBLBWwxGIJwH/idgmVgtD+XeGpt020oEHC88xdHYQebLZ43fSsCI  
mnF6LidsTMcf6chlqULRj0Lg2AaiDrYWRNoTWlpVIDX2zU9NQbFgKx0sNWlmrQqJ  
R4ej5joiLJBLVdl7SaNYPTV4gAtVqFk3bkWJo5BDXDWAHHzRLKMuuWLCm8uN2SVX  
B5G/MVmlPlzJGj/aS/roJRA9veNQ0GiXYK3kLFO/IWBQkPZDdMzUbiCBqWWA6Q7  
cm+fyoYhS9A8wP1s6AQhQxEcP1ofuwlFLXMR3SQ8q68xuKoD/aCJYFYq5EbNWYiR  
nAgXYGiH5VNyeCF0RiT8k1Sjdp2QrAEZZ7JinULrW96tLlKN6s/T50Fx4ZMP4nmc  
QvJh9qhckLGMQm9rVGRC/QqBykogbqPSr5t5Zy19aOkDtdGtg2rLRDObAu/4uJDr  
guTECL8YOrCRHqUnZGJSoh/mCo5yrxia9D+OVwqJ4pHDoJFGLoB0YQxzmwXT0+eV  
72f9BCNcXA6Sch6mkZp2rj1Ceosp6LLQJ/chDg96tmZYViLyYeLH50kk35p8qESm  
KH4PHF5AGaC6lERtsLWpZWauZsCWseVEFU5t+Cxmy7yGcngfrqWb0rp1xS8dsRT  
bpZ50drDF5YZJqJFEQWrEUGvEfzA4aweJLYV0gpywt51fl5Ldjeh6WsewTLBD2  
0fQuLVYc5/iMFMwffATRAbzIp1ph+qr0Jewk9oub4KoVgEAX0NtPime6plR0Zmo  
VLrLo9s/WfMJ+g9Jv05xudBe3IomnFtZE1IhLVgZm8l7UP0gdSntFae0Kfj7qQim  
oQcGjSXTLpytkFLN3x9quYCuCa+4pABZs+0jRBr8cZb0diFywIPpTagTKV7Uxlrk  
AG0xeh8Wv2cVANNVB8ptyfplPNZMZqgfJftvnJpUoxc6S5uKNXLHEVn+0Zx+IixY  
+1YcgeLuIBNEvSFKGQ+5SEAi9sdA0ZTN7ZcXQLE3JILXc2E9TUXUxTcb1QHU5Ptz  
XGs1jNPmjMHFPoYV6PGm7qvR0KOFmcBP0r7H9HrPWnjEzSNM2H6vcoRXdRZegAr

```
Jaz0lmJa17lTAFMMm4jZw0eESagTkorh02xJsod03It2P0Thri1y1hCl0yzKg1Ii
Gi5AhSQUqgrJ2IEYFaGTM0p0c63k8tlb0K/aZOPGGJgX8XSHm2IsX/W8953lPaHI
8HQND0I9bZKKb2SlvwkWMVSUXnA9GxDCVcNVceWrPiUTF+FoAM5VNAjmrDgzjwN3
utEQh9dAZ3FHqLHE2ZTFp0hx3zVPwhiAoEHGtNAehqEMVqZpr5raQaBDjRILLeKb
TITXwafFpqeqwQrHGKZE1g7Q+SYApvGP+vPo05fpaJoHYm3SFIJ8WrYfJPhWhH
SZTqEtFtk+S+1tgLhYiusIxeRiYmYBe4ZPF73tYwTVTYZTasXxS4kl017hQVYU
KIJsFuYXtmXjcshWSRLLc1bVRPcSriEEvOGANKkLPCoEePyASkoMHsQgyGs3ocYm
W92lP1WiYfVU/Snx7zoJj54LIWgzpW0edUewm+TR5gNUJS4AGmv9s22LWuaacF5
gogjbgLsctFYUuZxTOMDaseUiwKWZI3Q/q0gBvZUFsQGHqQCxqU2cDaop7AnoLC0
sHeqHRNA8jt2teU/nfIratEHY0h4GKtmKst0F05inFubLWYNxJMr8BVtRFdILA2P
Ek8qG9Nzam4RkIYsxUveMSviEq5dAFODny0TgeV8oABOqRhqpQmQTqW0ggEEMwo5
vel49quiy4ZpzVkSbCKeSfMkJAauibbm8YDi9HlyfKL3jWIupNvwE6rp
-----END PRIVATE KEY-----
```

## ML-DSA-44 (2.16.840.1.101.3.4.3.17)

Use the following CSR and keys to test the ML-DSA-44 post-quantum algorithm with the 2.16.840.1.101.3.4.3.17 object identifier (OID).

- [Sample CSR to test the ML-DSA-44 post-quantum algorithm](#)
- [Sample public key to test the ML-DSA-44 post-quantum algorithm](#)
- [Sample private key to test the ML-DSA-44 post-quantum algorithm](#)

### Sample CSR to test the ML-DSA-44 post-quantum algorithm

Use the following CSR to test the ML-DSA-44 post-quantum algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIPBTCCBXsCAQAwPjEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECXMGUETJSHVi
MRkwFwYDVQQDExBNTC1EU0EtNDQGU2FtcGxLMIIIFmJALBglgghkgBZQMEAxEDggUh
AGJP3qXtI3xxFkcc6RczjTgaa1oZg4rhDSzUA3c++EzhTdJ+Om9TFTFnRg7+HELf
GKcsE7S7Rc15HbC6D0Ny5GoEiNBm1glcKLR0Ayzwzch4BLBmyLL9y/qIwwFPYFIInM
rdyy+B7/LIZdaJYpxNk7W02fVpEFJ6ygwaiFpeRh5FcA8RVRccKCESwX6Eg1Yyk
/CoVgUbhh2l1jmfSe5L5vJ1brRHibTCEd0jUX7ekaIM7hHHApBgKlg1ERI79CcJ
CsUHPswV32aueHQtlzISBV0mtdnLwRMP0wK1klhWVuquR/TBJQaBgLq+iWTILCpC
gGoGrRrjqjgubnouot9mYfmtYLBcnhxqcfe2JqA4mewIDt4t3LWmggkYN1AJ5BV
qDFNbeU/w9b2K5CX0WVY9+vqrnwMt30VVgXxkw5Z2arnakCSYdNVq6W1+hDca+kX
a/XUImAligTycKDCsv1cN4802NunnKYG0cS9wZjfJz/f0t1ALtsjoUPCS7CagRGQ
E6i6KTXR6i6wafIwCR0PHW0pwZ0dyLKITgXA7ys8HB1mPN/rIWJHIAxv815d+fu
idtS9/B6niwME9+FmjSKYV/yi7Qeoi6n9yUk++LplnYJD+Yy/MawIP9w5YydtTrl
uFTQMVCuHHEdBgvZDYDCN666JIVp4gVaooGeJbgDocbXltGalmxLYXYh7rJ7B6m
xINiv9eb6GGZF1arnrxYML3MIU553K5+nju2cBtv7scj8ABZTWz7oYviLVUVVNns
RVFPw83c78U9eIwn09Vj7luJj8ilpyeham1hf+W0rq8RaB4639FGKuJqNbXMXxoe
dwYByVYPqj4tptiz/rAVb1KHdfYpKjKJ2UgD6UaDujXxH3FXBCL3M3ewTiLT1GBJ
Gqp25yUNYeJNMHNic9P0y3yduEW/BVJH0QnRhBTCdsbnqZvVL9hoeWd2L2uGeXxu
4k0C5FELXNtWVpCty44iXP20pz+CfYvg6WzohxB4QQzioLJmGuU1MHJiug0ZbFJ9
crpTV/8zxbpEa2MHs4Rim00LsvqfB9wD2jSYSNGZYgzo0wbi8NhRyZuRtheQ9FuG
FyJFqrbknFBX6FWly/j1GJGNZ+3Sh0LfqsP6PIhGTLva+cTf2/LEhSK5LjxMEDx0
ARhP+LymZaUiGDyrQs1Mb41mUFSsibnhLE3rwyT8hMmtr01Wm+ww+OhDdYmS+RJA
c/k8+Sph37PoUgbs3jUyVIfz53x09bkX2JWd8Mkl39Uv+xqHghBcOWY4nkA0WbX8
29QxIWnR0jaTednIFH2FW8I6Mw++zt30V7/tsHTM8g/FVkcHqowwZ130vnY/yUL1
```

5UqbKuruBR3qiv/DwJAKGICzqVVRs5u3jG9KxFm7dAa+d18jbl7NVh32h8Lw7WLG  
6nwR2CQUG1/J4EuM8LrbXzsWRgkbyryYP0us9cjDX/Du5UUPltQQg9jkHUUnkwfx  
3kMFLJkF7gT7wIOW5/hRi/tC22BMiopvLZC42ruSy9CgG8ieC4BCDEV3k0LcVZ6X  
7zG8zqewnJdLQW04t696nWyZeB2/G/zK70lGsAbkvobVg6zP4InXxzIwFNIIIFbS2  
ieElzhLiUs/5sb0rzU0xSSol7mwUBX8fLa0zSCvF/gTWPNGLO2q0r5TffLJlvUNi  
T+RaoFvCLAFd2qumpXs8dc0/HuyjaL//cSc4iK5ABqLH2ZT4974kQtQcRhwhI5w+  
vKICbWCCE4qehgd/5ohE3iKgADALBg1ghkgBZQMEAxEDggl1AJ1cBgSZme6AiRvS  
dI3FryRHHfEuF90qhbXmJkYoF/1ZqLmzwb7tVC0PxWgdSMS3GvzX2BN4S0BhRPPqj  
8aWHuvBoy8XN3iyrIqL9xK0iHl4sBJH/zeut8EgkGNvaRhLoqG6o3ixZFT0CdZRE  
JRw4iTe08z0gbN9NA7fAMnGFioB/ebknGwK8jRE5VVPncLoWJY+RbDj7qig/uKv  
7G7UgwMwa5v0v22kjqL5LSDqMCIm7p19eMtX4zUMNldKp32xfok6k/k0giPDbcnB  
Krzdlz6bE1KKWR9MBrmZ8YIXFrOehIyseU0jcfq96+v3KYiI4kQq3855NAa6UxGQ  
sGz/wV5AtjmHYeut4TRiGk+JPR+8BH2dUTZ0XtUgawGfrhdeJJtiI/pkprquqEN  
Td83BTaHxONDpuexYyZWEb5eh4AtAbWqJI6dhdbF6PQH8KqfGurfuV6ttBkoxaTg  
BGkqTjQ5E0om8Wjo+hGvL3Yq4sHL40WHjv3+pE95TQhoXgBZd+qca8NAjpuw6L7H  
ZilFtDSsEW90XnKkSVcWCzB0rhBuvliLFv5aouVC5t/WA/GPgFP4V1mnz4kphiH/  
t1Zo2oXNwVovy7LIZLmaozLzngynv5dgmYDG39zhGXEY5L+5uaIVLhBe9Mg6tfXH  
G6DL07QvyONBli7EHurmXiDYaxwtcsgGbrATTmPr64FcijNNX2FBYdtutBdqZKrj  
Nl95fUd/uHsLkJIY71Mq2T2M78nUpIP66aeT4d80L8MvDkmkW34g0PWvA08zik5qc  
UZpaAb50LEu8VTEE8zrwzorISUHWiYNDgA54db/1mDG8BkUVC4+oZd0JbeJx1qrv  
K3TCqxaF8rEj8Yf/YDmqP15HT2macuLTAPqIzWPymLFC6Beu+aL5103UKwj604q  
VeXBtsvbm13DEqUcHf41tLqVLg1DhjtdK7hu0Ntq6YDq5aZu+EaR89W3szeR0//N  
x4/H17RXgb2EbL7nU0NzIWRL7UZ//rjGr2vf2VE2g0kP8UrzzEw+oUAR9nen1RLS  
wXAU8z6c//1DKjeAYlRQkeo2t3kXn9i5EsDl9Qm5Y/zqbLxcBLBn4wyenJZlnWWg  
TPHDJJIXu+X1bbHb6xxldtWuR64YYQA8A38Gy865ch9+9CQNEf5Z1d/eZrgIxxJ  
iHDHGyb6ibDiskaj4WzE56kvEZgwp9j1trhpXT0glychMKJmsFuKbwUGmKYJIF8Z  
p+j8vsnyFMREcaz8t4sua3nF+F4KS5fcSjr7yaHwnGzRaD1ptL+H/WIawVhr4Q5y  
zroN+PazUuRgeuIz6xlv0vNQQLZ+9ZHFTMLBNliiaQ21Lg6xuKX1/b7VUoDRVz75j  
0m0FnnqAMLg9GU/pmyPjTJnL3f+NRd8KRPMQJ4ohy9uNXdh5iCe+yTqS9oEGnF0M  
v5G/3L+6MzrrCUJBQKwopT+wCt70V50g/i24NsTaxe6z3RGIQJyYrcas7o6kEz2V  
bz7YdIhjJkIh0Io2TSid5AALBo5LGn8j9kA61Dpzop9JKmaAqHSGeFueZBAfJpcB  
btsskrd+PUP3ah5z56h10SaV26JH6kpMwW0y7+yI61SMbPbdUMBgahfNR2QcHvc1  
WgagNMhBi3/FzUymAlYLaEEWPzmkk8T5u26Fu+dSxc9E6QYRMhfyZfaglh0qXXK  
ta/+4KFJzSIF8nAu8w7Vc2m76LAYPxrtoHljp/fQEtmmWKTtXaiKktgDs0WZWhNvg  
j2z04+n+0kksgWyUoFuvEy87qyv0yyPmUvHcwqoSpeM24qqhkjVpQvL4aynBeUC  
jYJ6bEMUoF4uCsCM2BqHRcbB28IYXmms93qzXK022Vu0cx92UpJ98+bdTBocZYPi  
Sarq5x0bjh3S0zX0rp2WEHS1QkBNbvpVwMjkBEBDMLT8u9z1Y+EVS7JDHU/26EsA  
r2MX1Sr/80jbpKnrPb1wyAzGP0z8+aY2JCJN+4DEc9KAi9r9LfeQdc+Dq0k28bNI  
x6Rjd+UlkN3JZTrfNKqe6v42TTvf6nLBzpsHf+f41qjBW5wEgJF4ADzJAT9Vojo  
h0/snmUU02JSSrIkB4s51LUvI9CkNoyp2Phz05lAdxRAHf7KG8B2S1yGj9uWN1d  
lFs9wsEZq8MLWF0Pl9bSy50lK07Gcxg18XwxG4pdyE3ubwL09fZAGM+50TQSAg4G  
A5yDzHNT3xD1+UlutQ4V/fsw3KiCuun+W9q4u+Jn7JjZWdB7azd7GpwemuVAUqvL  
6aSMxfZ4paJoxc9zc3AMfMGf6NsKB9lozSRgm3debL0LNlq12R9FKLwvF2vWI9N  
u3gmE6M14GVVDE6Ebia4/9PTkLL8kHrK6i2dP+dLeihmm37iKyG1LFMaLMVi3GNP  
U3gISHxgNl4IqKULckMoWQySI85TKmQkoImKqa1R8xcAbDD3MwAFsyn09si0LnJN  
OFdIKsHCauTJYkBKVMY9Y3IZXl0SE9WTSPPW+vkETC+0aTYnb8l4ruBwuW3S+k2  
AZ2NuU9cGHK18kSko7UGadyfiEx8iKMobd8ssmP00Twz1MgzPiS3eUxqTlpFFAjv  
bu/DYyq5E76Bg+2qno5XjsB8h9jVNwdtLGzzq0fivXcZti5uFMPfHB4GW2dS69la  
rWddFSUytAmEQyFwNmBfz3WwqvZJ/ik41Qf93n/7EiLcapHwoiP8YPedQR46YMWb  
HOLyIZeQdmVKxxoYG1kHemAb0rAdxEXnZYAjRb2ajWf/0AIAfEtjEofGu4RpdPI  
nn0iJ2jZFI06cw9nfZnr1mNLVzsFS30HfidfiC4UTJsJEpqVjrgqVXuMZPEaftBx  
gmR8SzMw1ZXwz/Mn7L+3R2Ak4/i90LHJDGyvBxyTYkartkD5A0E91BWEVlPhK005  
0AATuThY11EZzSqyUHTBnrV0p7xeLcMPHj4PxCEJF+gR0YHZnq07h7/vBRnk68DE



```
r/XLQS0A8MKnUWe4gnBmnOnvB6w0+wIwCNhhFh2e2nbSCI+xc01/wqJeNduNnt5Q
nwq9LcXUixzP+z5ltzuj3/8Yz05DFztFXEt6oLaSflutykTMuuJYaeuGaDipIe7u
MgNiKia3igfTCq1Gh1Y0fFEsSrr5Bxoid3ugzPD6/AYMGigpLC4wSElxjp0rsLK/
xMjJ1+Dr7/ENIyg1TVLS0+4HDhITKy4wN10Trf4AAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAKIyw4
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the ML-DSA-44 post-quantum algorithm

Use the following public key to test the ML-DSA-44 post-quantum algorithm.

```
-----BEGIN PUBLIC KEY-----
MIIFMjALBglgHkgBZQMEAxEDggUhAGJP3qXtI3xxFkcc6RczjTgaa1oZg4rhDSzU
A3c++EzhTdj+Om9TFTFnRg7+HElFGKcsE7S7Rc15HbC6D0Ny5GoEiNBm1glcKLR0
Aywzch4BLBmyLL9y/qIwwFPYFIInMrddy+B7/LIZdaJYpxNkJ7w02fVpEFJ6ygwai
FpeRh5FcA8RVRccKCESwX6Eg1Yyk/CoVgUbhh2l1jmfSe5L5vJ1brRHibTCEdOj
UX7ekAiM7hHHApBgKlg1ERI79CcJCsUHPswV32aueHQtlzISBV0mtdnLwRMP0wK1
klhWVuquR/TBJQaBGLq+iWTILCpCgGoGrRrjqgubnouot9mYfmtYLBcnhxqcfe
2JqA4mewIDt4t3lWmggkYN1AJ5BVqDFNbeU/w9b2K5CX0WVY9+vqrnwMt30VVGXx
kw5Z2arnakCSyDNVq6W1+hDca+kXa/XUImALigTycKDCsv1cN4802NunnKYG0cS9
wZjfJz/f0t1ALtsjoUPCS7CagRGQE6i6KTXR6i6wafIwCRoPHW0pwZ0dyLKITgXA
7ys8HBlnPN/rIWJHIAxv815d+fuidtS9/B6NiWME9+FmjSKYV/yi7Qeoie6n9yUk+
+LplnYJD+Yy/MawIP9w5YydtTrlufTQMVCUHEdBgvZDYDCN666JIVp4gVaoG
eJbgDocbXltGalmlXYyh7rJ7B6mxINiv9eb6GGZFlarnrxYML3MIU553K5+nju2
cBtv7scj8ABZTWz7oYviLVUVVNnsRVFpW83c78U9eIwn09Vj7luJj8ilpyehamlh
f+W0rq8RaB4639FGKuJqNbXMXxoedwYByVYPqj4tptiz/rAVb1KHdfYpKjKJ2UgD
6UaDujXxH3FXBCL3M3ewTiLT1GBJGqp25yUNYeJNMHNic9P0y3yduEW/BVJH0QnR
hBTCdsbnqzVVL9hoeWd2L2uGeXxu4kOC5FELXNtWVpCty44iXP20pz+CfYvg6Wzo
hxB4QQZioLJmGuU1MHJiug0ZbFJ9crpTV/8zxbpEa2MHs4Rim00LsvqfB9wD2jSY
SNGZYgzo0wbi8NhRyZurtheQ9FuGFyJFqrbknFBX6FWly/j1GJGNZ+3Sh0LfQSP6
PIhGTLva+cTf2/LEhSK5LjxMEDx0ARhP+LymZaUiGDyrQs1Mb41mUFSSibnhLE3r
wyt8hMmtrO1Wm+ww+OhDdYmS+RJAc/k8+Sph37PoUgbs3jUyvIfz53x09bkX2JWd
8Mkl39Uv+qxHghBcOWY4nkA0WbX829QxIwnR0jaTednIFH2FW8IMw++zt30V7/t
sHTM8g/FVkcHqowvZ130vnY/yUL15UqbKuruBR3qiv/DwJAKGICzqVVRs5u3jG9K
xFm7dAa+d18jbl7NVh32h8Lw7WlG6nwR2CQUG1/J4EuM8LrbXzswRgkbyryYP0us
9cjDX/Du5UUPltQQg9jkHUUnkwfx3kMFLJkF7gT7wIOW5/hRi/tC22BMiopvLZC4
2ruSy9CgG8ieC4BCDEV3k0LcVZ6X7zG8zqewnJdLQW04t696nWyZeB2/G/zK70LG
sAbkvobVg6zP4InXxzIwFNIIIFbS2ieElzhLiUs/5sbOrzU0xSSol7mwUBX8fLa0z
SCvF/gTWPNGLO2q0r5TffLJlvUNiT+RaoFvClAFd2qumpXs8dc0/HuyjaL//cSc4
iK5ABqlH2ZT4974kQtQcRhwhI5w+vKICbWCCE4qehgd/5ohE3iI=
-----END PUBLIC KEY-----
```

## Sample private key to test the ML-DSA-44 post-quantum algorithm

Use the following private key to test the ML-DSA-44 post-quantum algorithm.

```
-----BEGIN PRIVATE KEY-----
MIIKGAIBADALBglgHkgBZQMEAxEEggoEBIIKAGJP3qXtI3xxFkcc6RczjTgaa1oZ
g4rhDSzUA3c++EzhFi4fAFgoySp4hWktCHcF2DCWS4AFpdpD0Rp2ZpI8zGHaaQxw
```

```
gmsGLY80X8gZRI+C47M+LNzWd1EyUUL/JeMQTUA2sE0wLhFj4APgUzyDjNUriRMP
FHMdUS9JUHHckrxXIjIqo8RskoJpmiCSZAiMHEIqIyEiESnt2MgNA8WRA5htojQI
CDIMZDg004JAGYkAGEkulBgi4iBkwcKRKJiEzJYhhLCIE4IAIgJRIKko5CgKQDQN
IjIxgEJlQaghAjWJmEBsYEhw07CRGqYkGoGRiUIIIqSBIZAswRiJJAmFG0lyYRKS
WJKFYABqiEYBQLQhExdugQAhyAARGJhRoIQACbZBXCgmApZBAQMLYkJS5DJhJBk
2xQcm7AQ4YCIC6IxDAJlgkQg4wZR05aRjJgJmzRB5CJx0YJs0IINQbIt04ARUigg
CwVuGcJgzABxi7aIESSN3AaAGsgMUjJuwBQAYLiIWAiqSiRmlBaATBhRFISR0Ea
XKRRISgphDdw0AIp0KAGCjBqjKYOG8MBkTQE2aIQgEQwXARh2iZF2qALGAKKJIFJ
FIAFQzSCVCBKUzhxiSCRhLYwI8QoEzIw3CgqGjKNGoZQEkaS2RhkABgJCscJ0DJq
AgAm0bIBk4Ih44RISIiBWBhxCwdgUzZqGoNhgaZI4SBA2DiA8lhWQYlkcgtGiYI
wihoFIMMzIAkgUSNGMCREQYsLIYBEZhxA6aQCYGICxYQoghMgxJwGTORZKCJorBI
08YNACRIm4ZJE8Nw48BpyRIIt0QRhkIBQXCAQKhkIMNRSSJGEiIJGsQt2hYoBLFs
IrBIwJhECANIQcgsGREGkhIMEoRI0KQp0UZFgchsCBJqIgcM0JgRg8Rwx5QkEcEx
GCRMYMSN2whyYRprobRsIEhLYCSKQRhJ1CQwBJckCqNwIrcxHcaMLDYyAMEBGBNL
mjQBxCJx4hAFgBYq0jJlQARNcXSJmCIIIEgmsYlSYFQBjJwARiQAZsYhYBmqZJ
HEQppLYt4YgAHLsBLCCIFMUAECOnW0KMGrJQEoIJIYkRgaKA0TRwoTJKSZZljCaN
3BJkkCQROaITGBRFiZaRmcgsAYFxIJJNwUQJFLYwWySKmRaQ3CSMGiYMkyJx0BQh
CgElogYI2ohpGrIkNtRmug6qLJc3a8m37dIFsEpHs8tm9QBLDzZBuFih6kphMK3r
ynN8Z2wtP1V0yd1ZjWY0tdCabRRHP7iDlIaqTQDUn4Kime5w38s5R8Q4dDeGY+0
wIhisQUp5eRGwJiePqcLaBiM0Ga3QNvWORIa3UI616Hq8f7Qh1mNC7H0Y7Y4/a
IYskzSB1f8L5pir0TUF0deBCpUGHyq7EolN0mFs9s52DjZ7hqk9WPWEZK1JIf3bb
e7D4WC0jARbWdroRijPtQMaveEtIRPZ9LSZdv1Fhrf+aXjG4l6UNP+biBtoAAg89
InPRICVsgYwTRq1yFLKeyZQ/1cIicGFTARSHxClYgNRA95d/f8LbSVJvPlsU2Yen
33fuAjKA84L5LHG44vFI3+Fd226Y00hIhWh1gXlUVY2Cwp7R0f3iM3/UsaRilgw
zCqvFR8qPpe5ez3ydV08eYcf+0bt7zBF/yxtZb9cwaQD7kczZ8d7my/W07Ui2FSg
9lgDPvVcynr0lvqxdg9fMRfIESbxVJEWMBxfw+BrAHxLwL4TmlqvzxH5TogmBFi
hkVTTBQJFa+Qg7wAgGkRnU+nLzpxqACliZCPvSLRZiPun1bA1ECHQc3Wa6cofoCO
4xm1EkjgmNNTA6dyqHWApecXbgD7rxRyp0FMqrmD7YGRVeY11Ntky9cQaS4DcueSi
t1h0ekklKHXsd+DP48Lc2hUyhT3JSU8SMj1oUsjSQ5jPYRcsIEht7UpCZxrCqm0
GJTFd1qSRFEYteLNwGCPkjzPmCgJ2IDW/NmEqGaXM8orVDMxQfctwpIkJS6Pg5il
J6A9T/YUHEJwXF+sC2mPKNntuBFwK0ckITN7EXw6pijgqw/BLRCTsTuR0A/v0877
GzHJFX7wGoASe1KuGfDTiQWHNmI5NZqv9wvxa0IdxyBv7+EPjIfmCVxGH7/HM4BD
a3LF82vCCbVdmslKWNLS7K6biytrK0r4Sc50CLJguQoXYPHgdQm5MuNtZfDg/LP
J4QFtrPk1jQFuAS9Ap+s2XG01cu6u770VtaJSn4ZxRP7KUPfvHFsidy0VRHpTi5A
hw39STrE5omwztThE0XsJePN9eMKu+CI1Q9EVADwKldTdieanTShTqrAdLdhuI6G
gUfENV/0o66aoTqCm96j3v+c2yJqonOjMK2G9IS2BY8zxWzo0/0tHNvMoPlolvWI
2Edi8JBQKJR0Jv+dHih1bP5MJDYT7mVQpoVHZmx06PIvHW7sYdC/jawint0F8aly
xfweRBH119UQq0yIa2dSZPQz6MQ9w6aQLJkl98SfjQY1X7i9+/K3dN9opjv0GMDC
vn50kWs5XDT9BULpvNynUjP9VuNALP5Vkp2zjLXMqWg4yoMopTS03W+lGoT0mw
lSNqTvmVIEODuzL6firXwFd0MW+4ynH3YxyuxjipeMlputpDiFFltqMEN0Vc+hn9
cMv7dnEuI7BPE9x96cBZ7YVWyNH6BezGryjXTbkztWL90n36TSCSSCG8zvJExPY/
g07etz5H1iqoHN6fbiG06hdM53WyJLv4Z6ahq/c1aJdjWesC/NripPm5MvaIge2Z
DvDGMGvE3K1PmuC2AMmskt8S1821M1s5YvSrUmFqdH6GfR1U75DGqYvzzIJPqkQX
Unl67xx57R23d0Xx93PejVbqcAId+vqc/HxnNpiCGeIsUIELN/h4nI2oWvs4SfDH
OhL6BV5WMmdoFqTTdcnci0Du31PVhxtImIFecM0zK88EVJgCfZNe/JVCIiLMggvC
M1PLf4FEdoKKEfBtQvXkYWhR2rRPVLGWAUQT31wmmxDIbBSZESysHkOXMT+obl1L
JomWgJmx6s1tc/JCNU0svC4ii0eV+6FuZ4UW0fAOpW6xYyHm6b/VJDkq/V4KPCYG
rrBTm5YjyFKke6n+gKqZgyU/AtRoGJgRv/W3EUFkTZxqM7Li4qlsqkLFGQKRmX8
/blCZWAYZCL99MunsLXjRUoxcdHloavm50dVYQtgs6HkgL9cAgdgXn0I06pugSi
AfoiyD+sq4GSq0LJCxEz+u7GIHaXICsqRlnYzh0PKN+c7wZ7n9vpBMAJAQVpca/o
HLtQsahL1LDtsST6Ba/aNyN7PcKRxRxb0Qq0VULSeH2chIhdt5u8NfTwGYKNtyWw
vIq6v1Zsw6IizmB/9ZaOG+uthCY6pkG8NAYhWYrTJWG8D04FSI41qacalTY=
-----END PRIVATE KEY-----
```

## ML-DSA-65 (2.16.840.1.101.3.4.3.18)

Use the following CSR and keys to test the ML-DSA-65 post-quantum algorithm with the 2.16.840.1.101.3.4.3.18 object identifier (OID).

- [Sample CSR to test the ML-DSA-65 post-quantum algorithm](#)
- [Sample public key to test the ML-DSA-65 post-quantum algorithm](#)
- [Sample private key to test the ML-DSA-65 post-quantum algorithm](#)

### Sample CSR to test the ML-DSA-65 post-quantum algorithm

Use the following CSR to test the ML-DSA-65 post-quantum algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIU/jCCB/sCAQAwPjEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECXMGUETJSHVj
MRkwFwYDQgDExBNTC1EU0EtNjUgU2FtcGxIMIIHsjALBgIghkgBZQMEAxIDggeh
AK50y64HopziLOFmLN1hR0rZnUg710P/wRLpPbfICznK2vhXtpCXzR0hv0AWVEw
ic5Pa2AzKQAJ/rJ1bMJ3iUo27P2Yx22grTuQajTQIvKGkAiYVUB0jKRVvCndh1U1
JVSo28UUwf2Z0lqQfJ38/OIbeC4sYguJbEyX5YPZNjzuDHCvp0kPdLj4QzvQyy3d
EeryN/oxvO4YwWqsWIYVovvGxCaZuWtY7gM/6PtznX3YFHMmsChLpP3qqLcOFL0F
xwxEJMXBjF0RwaehCwDM01zEuSfW19bmKVN/yXpFtKvepY5Y0Sfc9gHzD2NvHn6v
F5x1AF7wd6MZLn4dq8a23dqLNVMQgrCjhMPg0ZfkhHqq+LteKbKrMKxpf/gGgRv9
iSzsTUnj5Pk80ylYM6rKALxT6rr4mh3LJjv1CpPCHlz6aDiSPTp+gEYX9DkXyko0
twWnyDAJuApBm51xF4gssAfHxKswIJc2hm+cYemzx78ZTqQ3nddVR5EDEYYijhwv
/t3gykEQCg2e622Sv7usZ+u8TwEwmwD6qQjAr6X+6YXpr3hckNLFwbFMD9lPY/lX
tSTNVoaI4haPvMu6aHXYem6fCFZ5cB9EDUPMq4eygud2ZWgGgZaj7I5VVJfjIYE
Gf4pgVgH6o90eHhroHYpZphm391437wPImFKVNaQDePoXgxas93mbk3Jq4Ycm+bl
CuHWUdWrGpMu0zZIC0A08RzhxRYTb6qtCoArBL0Gnn/Xyf7WxKVUM4o8hryA5LcV
eXJFPbYZvy70PbqSwtkf4w5NLf8fWQAxegftBMxCCH0OnZC8BNFXu5N136h3DIOl
VBqs07y0g9NNVRS4St5FdZzKxSdszWlyGiKImLhrS+Znnw30eQBA4nc6/ZhdhcTa
xe3LYHZ3Ql609nPf8TmXdb98sCQKkxIszfKAQ3o2Ag+D9wAj3mxMwLB0G5ZEs40n
gwcg6Y8p8uHYr8RaC3karUl06AD/2uee+sw0JUV/xQBKHNTgBUMfFmHg/NrCNfY
w/cGHKvaaAsa242FmolnW2VUpE62VW0js+zE4uLm/fB1pWguNGJZg0fnNh23PirO
qd2q6c5b46Ze1cDAPMNwZLn+CQmBCgWbjma22ty81K/s0eYNaIhvsStdgbRU7XkQ
ufAbs23fqDhy1pVZf24PejQStuKuqvD0gSaY+GSs7bxMp1Xf2Uk8aIKGfwLIWUcc
gXhzhshSvsVwgA87cyJoj2gV4QhvmDMYFnMSDNp/9EM4zJkNrpUZGZNJbtSDvdKS
zAxudHpaCLt4UnvOYtyAJ2id1TSKb3VLaPTLxnG60LijpgzHxQMyfX3btpW3okqy
M7JteW5091rJj15u43i8cxd04rzYfPIhy7xK8vHA6aVDZdWW1UEU/GKNqKu6p5Dv
0eoTsKkPsl008RQ7BGBzmJbQ4vC51huGXFD41zoqmvSf2oYBoXDFDfsPhTyfTqw
goazzvKciYxbd4aj6usP+5iYEDx4ktnLDe9Bsft0M5PGCelX1BA523bcPhPJ/qfu
6l2WreTNGQX8Fb+gUVSX5vb2722qhycTDFivMM1FABqesr7ZzLaTCdeC39NV/oHo
F6F1Pj0JveS5DybWo0pEdvPPLiQVJcol0mGmoITVXnNAh2+sE2Joa86tPs8ShCDQ
Im4F9sM36kBonY5VB/gaLTERdnkf1xJQifp9Pxb+bjlxYJ/zo56viZBpzYpzdjG
L/zi9wCRrcSCLHIgw1FWRopFwlTos5m1sA6R1eUyCtTWisnUwxo1ipXjgFXelFvD
M1hnSSxzYov3Ntf0YxDckHqIrgG5/NwV6XEUSgLR4jQYpUvdLp8lU71UYTWDDmCy
C6BdUE4yoVivYdpY9aveSkMToUavTj+fn2ENDEhVPP9MjVLU85AKeJhXap45HlQH
BTgdE1Jl0Z88rlss4zxSmRgBRR+4Hx7r+XrVwMpuKgyT/52RPuHBAWAVBtZUWSQP
BbHiQUX6SBq0nQJAUKNwrPHwiVu+N2BTu5mzZq7Ky41FKMlhegw764vkPvLrj8iR
vo0kb/UkpEhGq4n7nt4KFxfA/OWKVqS1ho/tbxiiCjrm3US8zmkmMZUW0mPagtc
KVQtSoBmENTRF1oPKZzes1KHckBY1YzjyAna0Gyps5CedP3LLWUAgsvm7wWgWfmc
5artdPBFX8r1zCJVSLQBDjsxc3Av+jbLFw0Zjq8Ft7dpBGbqq02rPxuFdrulntdc
Rs/dnZNVqPvY0lMyGndTUYWQED8z4TlhoeghAt2X68JHKDLAmyEZg/9PdF23iC8S
```

l6CTi4k4k0KudDxh9tiXo0L9ysRk0Xki6ZR+4a+v1J2gMWSC08wWEjiQ08+9qI6QD  
0+ICAKGPpsiHnw1iH0p6+z1eqSzqwgG6xbEHL5gyMIX3I9uB0+9+udXzqven7viL  
bI+L6a08HvMkZmWl30NhdLYyykVUtLGSS00P23Tm0gtgNdrGJEqMFPyaXpw4i5+  
0R0cRBVVxnKL7bAKhgsZ6S1ut3gxGyYxhufBZCdnPhLY0q62UAsxdYKf75+BqAc1  
ktgkSPhmuK6dvS1YzBRFA18DzzVBE5VvVUf7VBicLbHYoAAwCwYJYIZIAWUDBAMS  
A4IM7gDnTixv9jv4J/IJqW3NnBmMI4NIoRpzqjwNpxVYmGMPLkdNFURdfHdc5TKz  
s1n0V/wX1xsJn56BwKl/RTrx8otrQX5Jfzpsk/bpgBfjKxb1ctnatkNXAP4pAv7P  
MttAfySNM+ACWVlneA9CBHhYm0vB8p/8TozIHS37yunC9gXd+wNDiYCLUh4ydiUq  
j7tQznRr/fivKej4s9bBHRyAD5lrjcZWwQjHq1BoQ6p++CimBKSA15znNCvQTKit  
ymV541ty1wCbVVPVvnsS2zHkP63KXa00S2gwpMH0u8GMFjyrWjALb343538pOYX  
p82xiH08feheFNT3uDiBHXyGBE9WD/CRYW3GDZkuwHwOLEMCA0g2FWlRfLWK3BVT  
yX1Mrag/6F8G0vyrCA2/pnAnf//j05LX73kFTrvuiIcvXNaNpQOHMTXlZ4uUM+61  
urns3/euLE6DBgqVngg/TVWwJ3czRMzWKVZdC20YA3+hxxdTpST7VYJgjMqjTpj  
eek4+nZ9fXZ3UQ9B/Td/5iMwS78vvvxxS0TaF10LQ9fDxx1RgcFSQ4ubcSKkh7DP  
JuE6oRPERRnen7MFArzFPb2zesE6bbY70YTyBRV96TAk8goebDe+oEaq/VxMppG8  
h0Llwj8kh147U5HQlXbECFBDIsfnt9X/9zPf97UNLMKJnrNLB5JayeZl5JOFYgE  
AifDt028wGkdNESJR2iVA6A3yh7X2k5/S8PgsmahITVUu7uj/u8hN2LPRMXR4RB1  
uzXWr9eacvJm95sWSY2tDnJDfzGbd02qLa88L520MNDysigmfv7Z6myYob/Hc01q  
4YX0odEHHi3daEn5Y+v8FtK9JcNhWmAA+D9/8FjB6iEwdQoruN4XFHU/1Xt0b91n  
Au8K2xQUQyVWy0qkiB++4Vbmg9K9Te+sQCuj+C8S6nrhR0Tq+98H9dQTpRHa00RB  
iqk1Z3L1bJhmdGJ/F20+AG0Q37sVigxdzoGnequnhbH6jsFNEiXFD1kfwSYknIB  
wnZGIfyJ4JGNEd/q8Xj26508P1300E4MJVhxP07DA5LrXlgowxxWR80DtFXxNDDP  
dvQA/Mw02sSegI0WzoisSqk2/rYhD2AJDWrLZj2t3zMLzqMkKj1VgVgs0l/vMrRcw  
niHatAMfZfLJtS1LnPCwenat5MgTM1lQlCFP1p6eRoqA6PNLB8mLQ3RX3MK62ER6  
faM2KOLNLJmG0mN9xU7BD6TrYnjAonEnIIMnaZtKdrf9qfBIGUTf+okGnwtpKVVg  
SoICnxAJieclh+ZihC17cxhTL2Fw03Y7LE/YV0vMUu+0aWfScDbVh7dTUPMd5Rb3  
c09JZnpE4hhV3qbHE2JUUVQ50QGrnKlov1hrsEWFqFuSnS2QupkcGTmg6Zi9BJEuM  
XNjv2KDqkBe36LKb/d2EzYudhKhgMy6LNovEGC0vWd/qahs4mI7HLSHFRLryUQB+  
SiU2LW1g976CkrF3EhgI067+2RjY3BS1Kk/Xk1q1zmZ7fu28ywrngJQVMTaz6BmX  
NpiXdv1SaKpoMBWynmLQB4wcqc8xWt9tF7VyENBaf1axdrf2mLEzTbYosZ2RQID  
fdA/s3DzgkKNADTtXtRqPpSLes9Ud5RC8SW42a7pMh5HfAXFk3WL91QcBky18tfbp  
M05Gjjk+krjIG6hs/mTvv69r1ZNgbPbphgl8ALLexg/5vyNw/9336zpz7COPOTIC  
MSRnQLkBA4LzjqvJThqZw9LRPzXkggvdHeyabPuz7l65ckSfe7IiY7iKN63eayC+  
ow0S6N+RWCjby1qxwP3F35gQWJ+rIfmJ2YMPjDn/WdApPMJ6X6fXukrPchsHW31I  
vEQL2P/mP+z1M1VKVRiBQFpGniavIln4UJbxTeEaomRfKbLAJzC1AALFg5HZ4QZ  
KbF+ac0d9by0diRu18LwFrurzC77f6fX57STpWwBrLJQJon4yv3wQ5TKTSAHf2G  
EvoVTuLSiMbTmAmig9nrV8m1k8Zgc/VEhaKPygBNU27C6Wd5N8WnBAGp5yV4vsjC  
Hr7yEkGieSgkDYqmMs20akyUiEb7q38qL8Q08a0S0SbnPL7AGzncr4n9No8rehbt  
7Gx2mNoTgDStvIBIsIlgak2Z82UYAqa1M5PxJMFUObWaljpJFp7YrPen6j8klmtE  
Ta0axX3koAzSQVL1qL9zdFIivmZ9SQ7nDooEVoPoX16MuAvj90SNaPvZD9dYQAgS  
S+aWPHA7j3ZAw/4TNVLdH5WS20ViteXZfCkG9M5iNJBcuVuuqBDOKiKSSblPwAPG1  
5CmrklAce/Ud+gjdMEOpScwEHbmhhBn90lmOG7AVmhgVSogZTyPuNuhRYJS+P/mi  
5H58JzHmfUbuyMt46gejRXA7350qTrStqTyu4UD20fq6glaHe8gSJRIUPdPpjKCZ  
niyHr1C+i6aYqworQx5RSQTt8NUFB34zfTewK6gH1IuFS0RHOP6PUTF0EEYoqed  
vcVcNypLZwxVH2McS/Wp7cY8H7SbRVwPx7k70PPTN50HIZSLEMxqAsG6YIy0zBl/  
FiliWmWo5aHWPS/lAs+pNZCTdH12PuFAsac3EtmDG7E4YFuNc68xmaWTwt1dzhd/  
ndhPUowKVfIiNiWwraM63fVzI6YxC5fNXno6JRBYikK6fmoKqo7MdDCpnBr/v33  
d2ie9840EOPYO/SNKenn1dSwvlKXcQuMoZhBibKnrdBaxM1v86Vot2+AW32CXBfH  
GEQLCIWwHuC5J+Eh+0/bZNE329m+7xLBx8dKzqNQoMWRiOnC27iQg0PRrjxJE0ZN  
DJKGCxhRFkwv5hMX/yHU3dIhNkCbj0dCHTCVBH2C8hy9AivG8DUdGLz+obdxkiRO  
D3F1juTrTK9pgXECU11HDzd3hzL8dNuR/EMjAT00Y62l7yFD/sP2nt++NMxXBHLJ  
/qkNNYy2P6Kh0bUuo/VVVjNN113gmxxACUIzzy1MiKBeKeE715F1Wrr7eZD8rlhy  
5uEBTOL8QKt0jR/Sk2FKQ+ZJ+Cl9TRTHLAQ290YI7+LxWGLNroe/4X3xxcjT6PYn



```
ch8og5DhidLYqogTvfH52FgyaCgNzVCA9yqhJe3yW3orTRkYa8FecqETq+ln13tS
IG6SQ5RV2KECH4gJP+I7EX08SUM7riqKEfYwdbqWMvvzh91e31wf8gDsYjkm55Mg
LfwJg13VwReyzHiP4MtSUKUf4bUf6E47QajZJVtIoHQL04r3jVStbIQAEWgIFNT
JL90K/6zQB/PspTw5sM17dvi9v1xkabz77qk2ygECI4TSaWnZH48insSU5Svx0V
AvaB29Dh0x/GiKJwIvEm653zKxjj0c5bYjBWpH2MWN6Za40xJTpEYwV/ptzy60oL
VHYnSDSiOyt28WZIONA56ZqtY4mRd7IXMPttVP2I2GeB0NzQvvzuOewRdjbwzgj5
Iqt08mgm1vp2/qPt8BMKKqZ02ANxzBW65DMtmHM1w9HRunuJwAlEFLHz3e5GPJ5k
K/1MACoDHR007pL9AtFt0ijvdqNeEr30xFsXtHuFVGy3viKIKPLepL+IXeSfWAe7
3HF84BSabYRDhF3HwU1/nAJhlpSFKrEUlpRaVidLAVn90eUhQrBtQie02rcjXp/v
B1EgFwe/9wgavbKK5eaEk3Zzqi4LUNiV8DerOvhx7zfVv2o/Wlz1C3u5DPYSZQN7
QAp8YpoeizSD+4LBuHi4W25W2udUVZfNa7zjbLCjnUknVTyuirIaUMA/4xSwsBT
vj7DJxddU79+lcodMlsqTfQyDzygucrYvIcX3gyy1a1Rr0xb14F3ly9B2ZnwG+5o
whols0oQ/bp+pZRLAUZNTLu2FVLvd0/I2Ktc+p5wkbwcqV6wEkRgjfybtzo7Z0li
/yT8P5uykTYniBg5k4FfFq6g0RVMddAcyFG3507GnVg4yCRkT+brRaTENmZK+JDc
LpulYnbkaRujg6dRvfocZr4yTWHF7PBj1VB38+F2ziWrFcT0+33IhSMkM9Cf/UzZ
CLx5PfQ6Lv5x/2jNvRWh5Yj8XAXHFkxE3bpFuxigfP1hXT1YNvL/nRvnB6ZJaeQJ
qST8KZKrsON+exuS1+9C9Mla8EcIWruFTXnB6Z3FTdj3Utdx4Wvj4AEQg1AhgQ2Q
L0QJx3Tk1HFBQPOeeG1cFBSdnFkxpspqHBCm4lo18f7Y8jQMjt5hVoKRC1o8+aet
6gz0QXD17qSj+zmQnmytx99Yz8aYCK3hGdLJExWQhWvR72FDcCTDLFY653fr9A63
oziuZPl2MpQNwbEM5nqdv2ZQvgg4MtB3a6Ec9zJQdhK9jF2vsEFbtMfRB3WpvdCJ
Ez5jZWIEboCIprG440HrITQ6YnZ7gbjBMWG+2wAAAAAAAAAAAAAAAAAAAAAFcG8a
Iyc=
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the ML-DSA-65 post-quantum algorithm

Use the following public key to test the ML-DSA-65 post-quantum algorithm.

```
-----BEGIN PUBLIC KEY-----
MIHh3jAlBg1ghkgBZQMEAxIDggehAK50y64Hopzi0Fm1N1hR0rZnUg710P/wRLp
PbficZknN2vhXtpCXzROhv0AWVEwic5Pa2AzKQAJ/rJ1bMJ3iUo27P2Yx22grTuQ
ajTQIVkGKAiyVUB0jKRVvCndh1ULJVS028UUWf2Z0lqQfJ38/0IbeC4sYguJbEyX
5YPZNjzduHCVp0kPdlJ4QzvQyy3dEeryN/oxv04YwQswIYVovvGxCaZuWtY7gM/
6PtznX3YFHMmsChLpP3qqLcOFL0FwxwEJMXBjF0RwaehCwDM01zEuSFw19bmKVN/
yXpFtKvepY5Y0Sfc9gHzD2NvHn6vF5x1AF7wd6MZLn4dq8a23dqLNVMQgrCjhMPg
0ZfkhHqq+LteKbKrMKxpF/gGgRv9iSzsTUnj5Pk80yLYM6rKALxT6rr4mh3LJjv1
CpPCHlz6aDiSPTp+gEYX9DkXyko0twWnyDAJuApBm51xF4gssAfHxKswIJc2hm+c
Yemzx78ZTqQ3nddVR5EDEYYijhvw/t3gykEQCg2e622Sv7usZ+u8TwEwmwD6qQJA
r6X+6YXpr3hckNLFwbFMD9lPY/lXtSTNV0UaI4haPvMu6aHXyem6fCFZ5cB9EDUP
Mq4eygud2ZWgGgzaj7I5VVJfjIYEGf4pgVgH6o90eHhroHYPZphm391437wPImFK
VNaQDePoXgXas93mbk3Jq4Ycm+bLCuHWUdWrGpMuOzZIC0A08RzhxRYTb6qtCoAR
bL0Gnn/Xyf7WxKVUM4o8hryA5LcVeXJFPbYZvy70PbqSwtkf4w5NLf8fWQAxegft
BMxCH00nZC8BNfxU5N136h3DI0lVBqs07y0g9NNVRS4St5FdZzKxSdszWlyGiKI
mLhrS+Znnw30eQBA4nc6/ZhdhTaxe3LYHZ3QL609nPf8TmXdb98sCQKkxIszfKA
Q3o2Ag+D9wAj3mxMwLBOG5ZEs40ngwcg6Y8p8uHYr8RaC3karUl06AD/2uee+sw0
JUV/xQBKHNFtgBUMfFmHg/NrCNfYw/cGHKvaaAsa242FmolnW2VUpE62VW0js+zE
4uLm/fB1pWguNGJZg0fnNh23PirOqd2q6c5b46Ze1cDAPMNWzLn+CQmBCgWbjma2
2ty81K/s0eYNaIhvsStdgbRU7XkQufAbs23fqDhy1pVZf24PejQStuKuqvD0gSaY
+GSs7bxMp1Xf2Uk8aIKGfwLIWUccgXhzhSvsvwgA87cyJoj2gV4QhVmdMYFnMS
DNp/9EM4zJkNrpUZGZNJbtSDvdKSzAxudHpaCLt4Unv0YtyAJ2id1TSKb3VLaPTL
xnG60LijpgzHxQMyfX3btpW3okqyM7JteW5091rJj15u43i8cxd04rzYfPIhy7xK
```

```
8vHA6aVDZdWw1UEU/GKNqKu6p5Dv0eoTsKkPsll008RQ7BGbZmJbQ4vC51huGXF
D41zoqmvsF2oYBoXDFDfsPhTyfTqwoazzvKciYxbd4aj6usP+5iYEDx4ktnLDe9B
sft0M5PGCeLX1BA523bcPhPJ/qfu6l2WreTNGQX8Fb+gUVSX5vb2722qhycTDFiv
MM1FABqesr7ZzLaTCdeC39NV/oHoF6F1Pj0JveS5DybWo0pEdvPPLIqVJcolOmGm
oITVXnNAh2+sE2Joa86tPs8S8CDQIm4F9sM36kBonY5VB/galTErDNkf1xJQiFp9
Pxb+bjlxYJ/zo56viZBpzYpzdjGL/zi9wCRrcSCLHIgw1FWropFwLTos5m1sA6R
1eUyCtTWisnUwxo1ipXjgFXeLFvDM1hnSSxzYov3Ntf0YxDcKHqIrgG5/NwV6XE
USgLf4jQYpUvdLp8lU71UYTWDDmCyC6BdUE4yoVIvYdpY9aveSkMTouavTj+fn2EN
DEhVPp9mJVLU85AKeJhXap45HLQHBTgdE1Jl0Z88rLss4zxSmRgBRR+4Hx7r+XrV
wMpuKgyT/52RPuHBAWAVBTZUWSQPBbhiQUX6SBq0nQJAUKNWRPhwiVu+N2BTu5mz
Zq7Ky41FKMlhegw764vkPvLrj8iRvo0kb/UkpEhGq4n7gNT4KFxfA/OWKVqS1ho/
tbxiCjrm3US8zmkmMZUW0mPAgtcKVQtSoBmENTRF1oPKZzes1KHckBY1YzjyAna
0Gyps5CedP3llWUAgsvm7wWgWfmc5artdPBFX8r1zCJVsLQBDjsxc3Av+jbLFw0Z
jq8Ft7dpBgbqq02rPxuFdrulntdcRs/dnZNvqPvY0lMyGndTUYWQED8z4Tlhoegh
At2X68JHKDLAmyEZg/9PdF23iC8S16CTi4kk0KudDxh9tiXo0L9ysRk0Xki6ZR+4
a+v1J2gMWSC08wWEjiQ08+9qI6QD0+ICAKGPpsihNw1iH0p6+z1eqSzqwgG6xbEH
L5gyMIX3I9uB0+9+udXzqven7viLbI+L6a08HzvMkZmWl30NhdLYykvUtLGSs00
P23Tm0gtgNdrGJEqMFPyaXpw4i5+OR0cRBVVxnKL7bAKhgsZ6S1ut3gxGyYxhufB
ZCdnPhLYOq62UAsxdYKf75+BqAc1ktgkSPhmuK6dvS1YzBRFA18DzzVBE5VvVuf7
VBicLbHY
-----END PUBLIC KEY-----
```

## Sample private key to test the ML-DSA-65 post-quantum algorithm

Use the following private key to test the ML-DSA-65 post-quantum algorithm.

```
-----BEGIN PRIVATE KEY-----
MIIP2AIBADALBgIghkgBZQMEAxIEgg/EBIIPwK50y64Hopzi10Fm1N1hR0rZnUg7
1OP/wRLpPbficznkxasA0/wAg9Jzg9rBsafPJ+rM65xE35hGkYBmnJaA+k5iZv1C
6rSgqu0iIN1+x/9XyKm50hvmu3QmS0Kf84WZ9Mgfqiiggky+sQW50M0cmdGQ2yyWr
nJi6vKb13F8E7HP0J2ZwYgADZ4UygrBTJRA4NjByhHJMz0eHdHcxFmMXCCF3BAQy
ZTAWEIjXWBQng1YWGIaBF0IEEmh3aDBQcIVkRBcTVYEShzJFMFNFOIikDhAWBN4
BmhRQyI4MThRgWJGZYUyReIQ4dyhGE0AzFVUCdXBxYFE1MSdmEQYoJhM0BmWBQG
AAACeHJWEwhzYxEXRSGBU4MwhjMhOAcnMCcnFXUYgigyMlBGJCQ1A1Y0ZTRMAFl
cEWDhgELNHQeAEJ2cwRzhnIxghgggDUHZTQTbzhCFxaFCEhGI4VGQGUo0EIS0Ihw
dgVTRSgkJTV0VFIBUUVkI3RjhHhEMmhLJxNjMjdhcXETZDczAYYHmjieQmWGRURS
AIKHJXU4EmGHjiQ3Nwf3BiBANWAjBiVECDdUN4QYgzg4hzNRKCNhQFhBZnQCUTJV
QwdkQRNAYFNEUxaChxhYdiWAAoGAODAVEREiv1NXgQYxdngzB3RxISWGNCCehgFE
FEFohRIUUTOFC3Y0YoYWhIdAACESQEIBiHB1BUYHUAc3FDA4NUUKCFIug1NIOBUU
hRYwVCMicQVCymNDJ2glgDc1MWNkgxAxcThTcXByQwd1ZSQEYnQTKDumGFJoBIQk
UxQzcygxgWBwUDIAIgySMVUiEzR3EFADJzcUeIJwQkcTcmhwdyBBCBBgBwFFgREH
eDOCOCBUD0UGY3VjYXCDMHBoE1InQxcgNCRIJyRIaBJIGAYnFHdnNVYYRBM0I3Q2
BHJndxiEUzM1cSiFghZGEVwHidEBQmgIgFVoaFdYhQN4dyQIFycVEwBmE0c0QHcj
F4GHQxQTNDSEIiJgYIAjhVNggQNnQoMyNwAYBQIhByNBQAQzcQRRYRhxhmMCgWhI
MldmILNYNEBDRWE1coRDB3NHIWBgBmeBQ4glBxYycBcjMHOCVBgBYTJHA3YhFThA
BEhyhQRLehcZBERxOGdIMxECAkiDRxFYNxBoJ3JgEggFI2FkRmFAGHMVIQJzNCJU
NBAHNUIjhDEVAkaIckhwM0FldHcDQmaEZLKHD0QwBxgHGAgQYFNWZRJFEFJjEjRQ
GIhiRIWFARMYVQAIJ2EAGBNkiZdWZ3KBBzcFaDYyHFRYVAFwi2MCOEULGDhxMBVH
NAJ3NGhgCCJxcDgXeAFxGHQjARJCRTcdiGiAI1JhhkB0RRQyaGJhNVI3gXITakeF
JYGEQWdGERBFiDh0KIj4RgQhGiG0YVNEMQcUVAQmcUMoUGcEhVJFYkg1QnMjZViE
Z0cXRIEzSEISEjQjZnIjAzUEcUQ0JUFThnJFUoIiJmCGBTUWRggghnEQYYREJVA1
```

ZYI3ZhQlZBZnZjVwcWgyE2iIIXMiRHRxUzh1dEgnI0dUCEVGYWNUYQ3MYhFc3IA  
FLNSEUcGAmBwMkMCglELRVewghc4RARkJgeAhIADYoQRNTiAAHcFdFZRKEFwN4Mj  
AQBNBRZCCGNYgQiCKCBLIhh1ModURQVEGDMYA2JxMwJgQIF3AIJVJGgSRVQxATM3  
F1aFGCAnFAWFQRc1eCGEG0BEN2FjBVhTIYhwUoYjILUDcUVCJLE3gRIEZ2cWeBhT  
JIdQYhBDhkJAJ2MoUFB4FwdlhQKFIXEQQ4iDA2SDYod3JFRheBcDZWQYIAIBZFZ2  
MYVDNCQHuzQkY4h1dnYYYXgySGGAaIgiURGaGhXAxRnEiQ0RzFoNFihBzhXZBCG  
c2Mmc2UGR0N2YzUGRwJCCBNwOFWBRRhkZiAghgiAWGIhoYyd4VRRIRXZYAEU3QX  
hlQoA1KFE2QghYakFYZWSFAFDWQ3hnhidHBAFUNiZHSAdoFzBmEFRVA3FDUQAGFE  
FYVQJUFzeAUXRwEGSGI1RTKGWC0FM2FWYnhzWNdbGkmjgF2DDtTdyEgFN6ES3nDz  
pYC5eyit4aH68I/JsGceAdAMu5Nl0l0JkcU5GyWx0dSklpQW3I7ba7jpKhmCiYDYV  
Y+1NSz2nIHCXV7+tF2XyicCP9U0fS0sg4pR2qArefbV+6C1fnvPhGvw0Bn3Gs/n  
2UUUxQMwW8UnfmjbWqL5rNv4cBTN4gN1G17Rdlekhh5fR3ePnrBHVgeisewmxFk  
w9aTyknTFpAhe9nmPbXqQ/ELZqcoV1b0d/UNb6Z+lr67UU4EJPIImOcVJfu0sxop  
3vuQF/azIAvnw0krVRJ6CG8t9VK0qB3wITU8qXFoH++7q4HZ1S0xT7uX8FBi1smi  
wGQDzyUw5ZeUzFzqf8vwJmZYsyPUlfnxyzYyKeDa+AeTZBiPnl65eXr70FAIyaF  
ai9xpQXydQwKUG8dQC0bWlecFM6LFAYbQkf36P2e+G7hCBVTuaTE3QXkrMPFvhcC  
C+eDmZyVjLZCmnUvzt3Ydk74eLDzYnXAdh1GN0hESR3fCKj0oWkw0ErdeBUN00EH  
lT66USWcw8F1+yrKEI8mZs8vZNCJiWC84UebHGRsgHPuHjXspHM6ax5bxairkGQ  
Db7xwXxxiKx4A1w5XGwuXojHWNiLZ0qa6ViuSj0A9visMVT81odo2GgDNKJqs8wK  
ZEaEI3G9ACUID5iBHBMMkAwilP1baQtFMgTzOyM5r09NWtyzDvnp4lwMcrs+ZEKM  
neilPvjw4gdQLk99dG/ljf7Mwsw7uIGkuhiDfcxPHWQVYYs5/uhJLHccHcA2SZgp  
iX+CUduNci9Hff/lYg/KpMRjNBxJBhJNmFBWx20hkAxZrvxzLTMACPvHFTjaMTQB  
hGdeUjgZ6ocB8aJc6c/Sx4mi2wXSRX9zPaFburp08RJAdQjypCdJQeej4DoQXTV  
0lgJvSG325WPY6o6urJyIkrAv3Z5n3fcytLYsLTDvhLtWuJDhweZRQ36oFTJqa8m  
QQZRUtUzWVWzJMZNdmSkZw6ZpxQJOMff1vAPxMKrvGjVG6wYz0I/nCNKeq7NP2jI  
emlrZNs8Jho6+esnuX2x5KxJ/SeGtyiD+dIP63VLnbzq8VQTtKqV+b1kFQ/EIK  
tqt+QhFJxlye6m8KUL5e9PiGDp5q08TPjL2pNOSqo4SRpkiZ3/cwsEAJgoCsRjxx  
z6YIrPjMV07yCLaxOZZ21scI87aftu1RupJQxBS25F27IHq4hQ3WI6yl/JkSLjUm  
dnDIigKE1VJwzeX+rvxon3SKLldQ1/V5/0K5l6ogGcU0qQsXq+PRurn788qGrdK/  
5dCwx6Kp9HKfIERo/ExlTZ/6cyp51I6hCyn3u1ir/iNyn8gBXl9PID1ZpG8J7QEz  
a1wMTtk4ReuAnhSxgb6Vxpww+s/TzoKEntBZW1m25yYR7GqtIEb3dWxmFNeRavLQ  
4y5NFGqaSBGyhlRJWM1yPySkXADYbJ0Ga2DtPAMVawLX5GNd0Sy9E4XfiONIMTA  
wSiY5yvGVuzDKj3uTT0/XLcSEPCy50tJnlV+oAv4eKznkFLixyvaJh+vEyAVgqnH  
kbV3l26ju/UuFRkS3+SF8/5PSpgI+5bLwSGfyIFewb7AnAlIf0eRa2vS+XuBaqn+  
T1tHr1P8PtMF/yHyK5zmA0oLCo1nSZILlcoUjFnsxBQdzuKTza5E1qpJ00hoN6Lm  
g2EXcOwcW1QCxMe2arUFkETRq5y2EZskZMop+I+vFvH6q1cPs6+P1//k+UAIqaRL  
NP7hbNSV1sPR/92csBLSF3VfyeiZ0pd0TpolBwNzRxhnPTaQStvUbtGrYdWzTiSA  
6GSFIGJ7EH+ag6fYjWP7YVpTAgLoXVf4+N0yGX0uuFvr0yZ2aa77sGX/Q8RmcuvC  
TqpTorOkkf0yBxnpNTMG5djRxWff5H5eN0B5JlzoWyq1JBd0aCkxXWdXAYDoiRe  
d2sN5rL3lF6yI/hDhJ7eTMP09C4D+bHTR9b8Tn+07jpJKwzGBGUEc748ujBSHCE5  
BjyS7lItALfUDUcuVLD0gnMmSlVrBlsdeeyIntI06PX8h/BoU1kMvdue6Y/04ZQ  
NLuv0tForWBzrFDA00hkf8348E1go0BNFj0cmYarsAwAkG1CR0l5H2CmZ2cL6ifv  
V88oDNvor+bnadGqLTgOxMeQGgzCP6qS61Duc6MUAa/zJhHPyJ2dDXd3u519gLCx  
V0yGYerBLXvSwNt1DU2I183lDxJo7ojyDg8h1Ep61JQ1lS3pXawpyJuh4qAdcZb/  
Bk0uWiMzFH9k/vZall+jOzgfFa27cWrPU7re15j/zG0KU67v0T8x3S1ZAxRLJ9yl  
9WuUewg90k2MvVGKc1n1dz7HQBMEFhpJBnXLHNxpcUW2eRB+4Kf+XAHBwD7nsMxz  
sG2cagGLcLkcsDojQb7dTeN6hPMjvoIwGRUodKUbfEW4P+cvmvI2ZPZRMuuzSjGY  
kOV5PuvBoh2ChpNTwtMJCb9kCsT0tB2L06z+m3tTcJ712NAdYpEzMSseHSEe9G9P  
mbS5PP/b231ykP3cK02Jk2Lct7pa6wkLRJI/x2w4sq0H1V5tTW010/815600EeHb  
fRJL0q0rQLHQXhxpNdAhjZQ84vqKBzf9n9LKd4QCWBCKck+9FjNsEXPoJhgCzxy  
hIersoTIA0NXchojeIHBFgCz7uSEDitxQ5kRqwdUwPIuMkhNnhkF0f42+gQ/6L2R  
MJuFCbnd5i8sl0b+dFcpP6EDr6utSmVmtgHm1mnTEmeL5TxyMsHlioFaZmQblyTK  
/IGAH/Ez18dHNmiATUkwM2cXpos/lB04xTlc67d5W67j/AquDju4Qd13SFdbDUKA

```
NSC+ksBMTRALMcmX9GoY8uQD7ao5ipagUmCjQj1RypFtHjWGLURcYMnbCuIZPhYi
TFDtz020rUR1M6fyffuehfqrueuAl84ZJ8h8D97mVfeyDQnMFHHtoTA1Ey5IdGf5
TxnLheS6BXZQu0vaHp2vjCKJNyr7+YqBpC7hKuSOF4T0qmb72KJRsxW7gDcNWWgC
DdGHe7wY4BoabfLC0xi fax8Wqwfo3ti2iy80tQM3tPp/YaF8eAsLp3jppqGYl3KUO
2h/rWDHkN4m7GorYq/ZoCYn1ugLu1seImj+HDrZTVRhpuAZXyV6cBdIeSXwAoCAo
CnEh/k0vuzVeqYH4K6Y106FuLAuzOp11AjRAN3rnpJULtDxxI9TMvGKq30m1cA6y
Dj7EnwSsF7BoYFn7jZHwtFXczjjTyFvFnByftemJDvFywwB/BLj3dsBHEJHrp+S9
V+hhSDsAeVr0Db2rLx5+VNERaYtYwLWj5wuC8w==
-----END PRIVATE KEY-----
```

## ML-DSA-87 (2.16.840.1.101.3.4.3.19)

Use the following CSR and keys to test the ML-DSA-87 post-quantum algorithm with the 2.16.840.1.101.3.4.3.19 object identifier (OID).

- [Sample CSR to test the ML-DSA-87 post-quantum algorithm](#)
- [Sample public key to test the ML-DSA-87 post-quantum algorithm](#)
- [Sample private key to test the ML-DSA-87 post-quantum algorithm](#)

### Sample CSR to test the ML-DSA-87 post-quantum algorithm

Use the following CSR to test the ML-DSA-87 post-quantum algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICpDCCcnsCAQAwPjEQA4GA1UEChMHRW50cnVzdDEPMA0GA1UECxmGUETJSHVvi
MRkwFwYDVQQDExBNTC1EU0EtODcgU2FtcGxlMIIKMjALBglgghkgBZQMEAxMDggoh
AM5xelVwAnBZd6BpAyyzJjPQjb/UBhQ8CzT9GYNDRT3zJ4icdMwqpGupWIIIBZD2S
+msRQ0bmqw4jRcE09ZrO8IV6UHXrAP+CsF3H/w3M1m9SB7D0gbqLBHTdWZuP0JL5K
VkGi5y08z8ndT50Y9ieUqLRHFwsntDJgd+3cV4yS3sKvY0V7bzMegMmvPDgqEaVc
Bj9DBKnH1j8F9iNAXA8TJJes/D1I0kGMrVZTyuDP4EtfeghJweTz+hVJF77t3vln
ea7ynNN884BUPbRw+QhKkChR2Kjz2WsKwKuo2GIp99M4KkAM02qECzbpNCEAOIfv
Q3FpvUWX9X6Z4UxykCH+sM+d12cfvGYSmNB1+jqCM280c29BAzr7a2/yC2G/fdSW
3+0pmL+CcmahIUq3NSZLFi56wiGQaE0MyDTrlBf4s+Qxk+58Lity6njS/KG38oM
xgIR/QZBkvPEGLXACCM15snADsNi+Lebw4seIJU0G6+bVqwouu9bDzViKX0r8qXe
GDoka3VTSBqE0dwDymbdcfB+9sjWWJ7Kzwa3Ek8tePPv0Grz34QBfxYn/mGmKdQL
DdGD/YoU78kps29VRzAjWgdtkgXuLtMv7FrhVzbQH+HayAaH7BIQtj/yzqDZY1
dzUgdMXgAZqv0jKWCPETAXHFH7N0s+WxtDu5BKmxyn8w0dncoALiAUMB0Hsz6oMy
P0fXnaos/sWroU2wcyqa5MGeCcw+4DEjvPeRRMyeSkPAjQwrQpOWs+0M00ItoDLt
6hzQ2L6hrkv3/dB7Ggz4hYXHGOw0bjVcy9x5tZTiJ8X3Hc8cApUtIc9jv2yXPGdQ
BCN/mnx7co7FwUfMiXSqoMkprpw0/VdS7Ug/cQI6YyLJgQVVjaLnk6z09NbrjQL/
ujg6onhz06i10BSBxa3K+R2QAH3sHCJnhl9r9Rle+boK09DZSjKV9sr3tGTr7UsF
sRhmaXdbR4tPZQs7wGZW0HfZpJ2ayqG+l9EBqcjWU+RVc7m7u1QtUAd6lT86gb
3CzFLTtimjqeJVS/D4sPiHRgjA2dEd002rADBwIOxbqERuK54jCmED10uyNPitAy
0TTY/yATBLWVCKGJWwuaFXS4n3oWYfFY6HV+mRm4qSwbDh0FlrBP674TkclIngFk
0X/+Uq08c72EC+SVA0xC9sk7ULwW77gngjTFkEdDSrMo+XoR1Nbiv8DRhQh9vLBM
svmIJwPK2htIrQLH1YbnXRcD+/Mos2occ72WdkT0+wWwyvHARzflpsvi8syZLYG4
rEz47ayWJ5pXhjCHR6u4NDHeb2dPLbQsr+T2kw06CyDZ2U0pp5+6qztL8LjMhsFv
16T7ebbd3nwSZgaX45ouJ0149TxlKTuH/XdU2ymY6N8UqdHcwnB9weQLXyDsJMT
cwebRi4CN07Mxm1/H71dPTG5jPI215HLIetdNNRTaPWORI+fcFHct0pb1QRgDFIB
BWodW3ubjXiJvLU5wbFIJ8jqo99+Ln5FdIiWSFzUFYoZvIVfy2uEDR63VK89WrV
7TfLmASIPWeswA+91GkrSp0VyF8cnstyz+n1sYTNJChjjHB/rRoeStVrgIQVNjhT
```



M6UxrT/glGVNgcLEJZPTc42dzbTZXFsnFQwWjn83hTBGt1aezGJy0sLaf0EZFTUL  
iVZh9sh1HsMeKY3b2coyTKu5gPe7zsmVTakUhDa8gvZwruRczA+q1peqjLmp7zo  
hdDI4F0bydFnE3S8jedEfeHIoks1whU3FDrS2Gi0xHvJGwZmBc8w6coXJLZnPZRi  
2MeTWh2ez7nfakhPdxG88ReiE0SWF2Yac+gYtA+Ej+uVrhP15+QRdNn6D/mmNjZk  
+rJcl2JSjLYidwyagY+uo/sVhe/spEomd/1w0r+T/UioLgmL1Aef/V23viFpTV8S  
LKfVCWKwa598n8pUpfjdolp8rTzSC619iomTbrgX2ixslaESk0kHTJXid103e2BC  
SgwzzJwlveWcwVeAad8nVqFP+mG5Sd430H93CvDuGmeTRlu4Z1By0AzDGeZoT2mB  
c4qddqDwSDjSwfpt0MZF3LtyANFif22Ds8wPynE/LNjR6q0GURGuJFRc+evcYybwi  
Eg9qiKE0SLMCiISrPEMZ8aDdrHtiIn0I0u4BfoJsJKNeoDPRne346hJnS2YC5003  
1J0dmVe0EV+HGAldznz7YnqdHQ07iF3q3zNGq1mFrLTKKDRVvd7C631nuvGLBye  
IjKoJZVEuonUXPYL7/tWkvxolsbZKJerxjBJch/igjKCCe4zW5DNRpWw0vlzkerl  
SblvQps4nYQENSsd44yH2U4VN33ycaQms85KhxnQc2+AViqEx2gIa/BMKM7Alise  
U/NH5xg5bsTIamYeL2FXFW/Mf0ty3wAsUZtUzRtfrY/DihfGX3KL1bf8i0ehq07D  
AuWlmDGVTDrBPLfT1hArK/0Xa7TveqhwYZDbXW5qLcLo0tzW/SKcw+CAErh69Up4  
ipu1QE3WzW6kpf4B3YJVGiWeiyVhOTfnN/EIIGU6F7D5gUht0kvZj0ns9h1o8NRO  
gPgJdsqSDJ3n1+MT/03s4qMTBbnHACLQmu6VIRvliQplafBbIiHPI5t0r5Loc7qZ  
bkk3m4y1dIytoIxWFJJvUsUx3u0kygI/FGJwX3IME300ZxRPCey20ZLCWwA5tkxf  
rorhVp/pnihMnDJA8m3ZNIrVlNACwWYk957a7LohSaKo5uPc/txccAI+44M1vkOQ  
uUWiDNTLFZzyLxi9vgcxJD4vjnd7lF4uD2eKynAtf0ITmzVpVVsoLay8C93HW9gD  
5n8ovAP9nH5/vmoT0VqsshjM5oBA/vnixh63pWoKnS5gu/5ecy/SdHV0ksK0S8X/  
OflnUlr4TgC0r2b1dZ0R3JG010NPr2uJJW0itBapJT5qQ41FaY7yRdAXigHut2hk  
D6ntUG6ETw7vZf9Ecaw+Mmmz70d0Sfv7WcqDfGhw64+5+OGHRm64fPtYnKbncmLo  
+oMuMjWPfbnrC1uPTRUdw8F+R3isxvJn7iydHp7cQgWaoRqswopLRUjnv75R5R0d  
SM4Mwi+gpxJ35JzPU9Pk5q0lv309SaCu7XiXwiJcgLJpMlEwS4T9eQI6T2HMeCl1  
CdQxw//uAMkDtgBbmua+RJFG6XoEfIUmm7xPlwsSsuUJXaZ205a730T5oJLSd9PX  
5W1fCTdrCrQVJ0unt57zjKxQgm5ll/O6m/yTMkqDjXri97jtejZt8Uy1MTDNwd86  
lQtbeJueYJZ8D/N+cyyr1Nv0CEpRmFTtmXY1E1PJvzFk9ETjAoIys8e0Yc8YUTp5  
IE0dZpDE7YteeJ4zXB8gy1pPIPaahNL4J0aXlUSQtyjINd9oZnHMSjjsTc5jeIdp  
7vywjsrUNY5TafkKHdvY9UxgDxG1bsiC5EVB+syfuJdRcJFxI6hYZT2136//ZNM  
H6AAMASGCWCGSAFLAwQDEw0CEhQAmIhbyanPa5XS5Sq5PQYtB1MmV+ZvbRxo7gQ7  
SW+t02Ynvcf3EEsg/mLgz/nf9ELqoZSbbqFnhXoQC1oBGXhxd8S30quIxbebjg6T  
0aI99RLlBd9fJGyNB22gR0voXJCeaWJvhG4z0Ue3M9c0ted9cePW0PgpFaufGHQm  
TN7eAQ+ufzbBLbjfYgAmhuX2I20zkmemFmD0L9z8wt7fAr/apBvr75Bee5cCIr3i  
zNta8B6Eqq3uJKy7cc6N+FJhqpDjGGr0Gtzn/HA7m1WuoxYDq7qeerZqufIRYKJb  
hUhokcJeE4ZcWaU9aTEBbtv1TDo06ikk20xzIPNQoBy405DDusHkSHbHdsko9Op  
QYyXC7H3pzVgqNAtC4zK1GWPJEQQJ8u4QDKx/WeoWipSABzgzPgDpfIQ6t+MMEat  
wux1T83RNTVGyb4gc/DS9HNuEsDM6inBrRSS70QdXDuccef+mul6uwsgD030AXYf  
WbrdMZdp8PSigm2azI8FQxiHy+jWRJPx5Cw7FzbKj0VrUjUW1ASx52asJLS9JUIs  
E02H+2/4gvkxRdUiuEnSiDrSXjFo7W3EVnhmX3V0r3Q3a3Ewb3mZM1Ubcrt3t2nc  
NRzgZx4vt6NyN9N70j2TMvgAKLgUQmDJr7buZDk9zt18+vyiFUKTQk/LjyXDI74C  
+TKF9AC0iq8iWfL3b4xwV6f04yCX4W85AE1yVwxYGIzCyT8/kanwdMx3QX/u5fCT  
gTrDa099fpFe+AXei5h6mo/1PXyr3vwn6EF8HJzfcIASraJ1DtkHbN1pWgJfkhmJ  
f5uF8yByojOMXxF29YzgHdcZ3iPUQmMmXZLQqDQ2009cFB12GAgxpPrC6rkwy9cm  
ZNC7eLAist4pgvuu/GYZ086ddBGWolwf7EJ7vHuW6yLEl95/xiDvVo9CXHoWcYKF  
SBxXoQ1j8Stlp0qu8KluTVH+mASterdRDioU0U2aPzzDCaH2PTZiPuGMcWtV3SIO  
fTVnEvhY2xgqPL026rnBgwwPnen8c13bUbRHomI6Tvbed7cp0uHf1YfhD99aE83x  
YIxriU78f//Vw1nNi0+9oyk19qXq5UZONJ0pWvNQIWeY4Q+ahg+Bvn601CDMBYx  
rgApN12AwzIS3D3MrmF97RKRvZg3kz0udG2s0W08Y4t1b75V/JgX79RvybE0jo0A  
XQUQjsi+EvWEUz1RRGmqxVLSSEFWMKck7PwIggPu6kJ+qsFvBrQYLMEDpXfXCo2  
uArAkI+p2Sf8oTf9WxFXJwmqoYCrTJaA0wloH3zQWa71g4g2gdcewKxMCxyzIOF8  
FWo6LZ9poyK3TNDa01HT08P7lu6ECvuiFAv++DZSiCFDuP7C9+W/nX+QzkzrUB  
N0HUrPEn8le12umbWFFxEd0MmnF2Jiv6Dwp8u+h5n1/mE4a5gxFwkeY24ef018b2  
mnqTngOM++6GA08W+ScpeRE1qpn2jSSicw3tZbOPT8MQAbomxNQI3HcF1V007/BU

/TXQJbZX0gnpcZ4R1sw3lFZOX9h3s0nw4oPDUT5EmE3nU1yeykJmX0kL751s+Fsx  
n9wXMxICLGe0ledWe8u4X5T89Vib7A3LcSONzsiRGiUgWnvNFDG9fnhWb/eevw7N  
pZ6ofsFPD+v7Id49DbTjdn06SBa9WJLPXsNL/BvVoWfZpP5XZvmTrDbb32y3idUi  
ytSXvkrdlI2sUsHQtdTdp+JDtYX0sMPVkvVoLkvhtDZe6XpqL5kC/eZxLVFXpmTp6  
J0eyKvkt7efG/SMlr3BldX6Dwn3YaTLwfoB4lbU0uw9xjZ9DoPSYnmgv1aoLkyc  
BWxJARfRSLecRbeFRnuFtw3NCRCt9hu6+p9Rpt8u+Y7gfsFC8cu1tSxr2lxsN5u  
FkJIX0dcLGF9ChqcCE9RNTHPqNiK3+MrYlErhuqvaAzzsvRUPTiz36WCS0ixuCS  
0TPure9YjzxsGQyi00UiNXLan0YwDrN3iNtDAuvd09tJ66HajXJ7Z/xhFcF/LYeq  
Fqk3GRA1fbxxNrzdDqo4TX8840VBr0s4WbThpCU6FMFB/5wldveEvsZV25mDIREU  
4o/pFNd2vyMxyQSI1XXn/S61jaQ7iXrbzbzn+n0yyDxoFNSZ+S97fh2pwZHTeC1  
fjxH0ZOCjI9VK22/M55V/hQmyrkM2VoypMoiISrk94uMMuyk906Qs/P72UNaj01  
op7/4xN0LNNKROwMIRIZ2J+D+cedwnayiXJxe888VCJKFESnhjjZMH+AgSJTj4X+g  
HAsfxwRdg7nwAaJTA1wy/St03YD7TyUyhEaLDDqsRQCX/ku59XVxfILGMC9SZPQA  
S60lzBXpKt7z62yqYy40nrvPCUIeQX5vQ+puMJfEnK8NJ4S5qDG5DNxu9cW4YUs3  
JzUYGsPfAJhReuAzzdBRRaA+K1govnEw+ruRtbFtL0KzEI/mT26nEbesseZ/TwVS  
l0XI0kQu6e98m8f20sUFRdM/tazRsrC3RMNZf3NafwAphvpvbsWCiE/XNcrNK1fM  
R6670aDzd/qjFiRGD0oDDFZpyZx0aBuialrxvZWnVdnw9zBVfh/rM7ocmrVEPGra  
b0RFRxNRF+LX1u/DTaXq21ZVz/WBE3mGU4zir+AjoKRh2DKq0qCUjI8J4jpDcXOD  
01MPV/ZdNxd8/yaVATwoQVmrdf7SxaQixI4vxr+tUsmQwi0eXCbElSk/Sj2BosA  
kszw0ZlLsBoBVg8bQDs5Q8hdZ+yhBQtfVaISVYTMd7Y8GimVTK85ZJfXkEftsn7P  
GSyd3DDAGhUqwnizi0kRLXzc2098omcQ+BFqB7Khh1gdZd3Ch/op5JbwvZFrwbZ  
4QdHxRGR3s0jecQL9cGwOB16ZBmkcimFgUwx00Q+ofiwQW53TEkmp7bY0FE8eavP  
v81LvJ0JzrS+S6gJEBrZwPUhMMJbuCQ7TL3UvxsHvZke8GZuQ+VUJ3TsDj0motuQ  
YfD8tmCPryv6/2642E3Ef2e9AwfbyxYf4l5DVcUzEH13BI8Ifwhlqmxu83ZDihYc  
SJF343+Mtvgt41IyN7Est3f04lcJ1CY4ZETAP6kbBq17iHzcK8IlkbAjAU+h8m5c  
DMiUj0SpsG4d9e7bwX6nxE5Un3Sw8tUDN1jidCBaitLhxRnaWg2I/36WCG7eSFeR  
dK1FU6yAsCnSKaiS/25GLS3sKj7w4/q2s16JS/QHscF2bYUUAUjuGLKWxj3x0aEDk  
yLIH9SmkW8H7y0KqAxINKLXYjg0Kfe6c0w4+RoCd4NAK3peufSZUoKwB8DkQJrE0  
aFcFR4JcyAXr1nLyr10Yohlsx9FzplnFW4xfw7aeBLTkprRzxUZc/uPmoMw75BCDH  
npi1cLAUFxD0GtYWUSwqsexLmqpwaxdG83QTUuIyc3aZU4pJZH8iDbNLfRZPJFpl  
+pLlaZcvpwa2C1nNrGF726HfS0kuXn2HnYSVhf3yOgKVjDhgTgDEJKzvkcIa2o  
+o0DQpCHbt1vFjhDu/4rQVqJGqgcLGcFbq/hcnRcHdp4p5rva6W84TjogkwQxiI9  
227aevf7mFP7MoGjHgCIPuTF8WmznA1ZVR08cF2RkoxXD+iqnB75RqT8ncx1+rx7  
wwM/DEPxQUXW0mJ4MD0Axxms3ZQr/DrTPF1iIpYIDIpqE9YBgpjGoPUiTGMUPeNz  
2uCfAaM19AG3csIEKBYi+WBjDSu7aKEtQh0SqwroLEPQTJQVg9sevMWM50Nhrfs  
vg/p4qjuQreMoFGf5tfAgKLIH8MllVsJf5IdFI3gsZtQNNqPjBGRZzo+lTquPG7X  
+jRthmMA2T3PPYwnhrwBj2aloud9kULQSCtIleTK0sfyMivddNdCzrOPXFDYg8qP  
Jr3QpRYx5iF/IF8UJEq9Km3qd4Gx0LK12Ng43LKSHfr4LMQuyh4qTSUMDTfnt4br  
4D7HQ4pJq3LkoQ9U288rhp+FAyTpVJEf37i8FVVhU8hm1gtabxcqhrf8Zl5xvoOP  
WWAkVtK4MN9YMU/EI1MsQ4c7HuvDm9+/6Z1KuyY8LuaT3X6A9Q8t0yIt6eip4Hlc  
pmGu5sc3EzdXajMn8tFZat3yZv/ZVD9R1xQb928pcsBjSz7AuanZ70i7BXsy10Cs  
sHeLa40qlwMfqTQGgBg+XMoyN+ULPjQsksFsfxK3dIYjP6mBl/DUCVSIZ6FibhNW  
fLKy+/jyeir5knc03mwlsi3Cqv3eG/rFuQN51cMoHcM/NJwbD9AGDVgqUjo8z3kN  
vS4K3VoaDLvPaUFU4qZhpr2n6ReG0z31XAJDCLkJ7Zx5spHVpBTI90SdAgeGR5tz  
cHuxWoYAxL6tz9+/Io7qXTAIQ20aQ37BgJ54D/hyX7Q+1ij0ctF87WnySBbyU6n  
qU8Z6/02HKqn75rTsFhzETd2B7gZewtd01hfA6QG1tK/Fu521ndaLCbqx9+iF0ZV  
5Ad7L6hY2gnjwfbDqawvEYozt4dNJ2gkR5dbJPc0BMAb0yHSITksj8fyzkXVNd/C  
zmwA400vtib2lnoyi1kvmy5h0kAnjIWE7G0Elv5Aet94r6lN0txBBlpDbDTrI1N7  
HZSWJ9Gnmv72L0KoPQjKrXvf45kYSlcOm/ThL0ebWgGxWI3JER5KN80/IfSFT3CO  
JSyB7c7tcaPPEmEND0N3J7i/92TL86qRLxNJZczMw0txrkpnVokl+90cpsTkfnCb  
Z7llMt7h0wE6DFyQwnMGVxNaYc08qdBZNWmV9iGvJxnJlQizPwJqdLTYvbQfy4YR  
4Cr591oPULwyikf8anHpI91sZokBEXPhUC4JsQGnt+lzSZTESvepaxx7K8KDaXHm  
36q5E5ozc9wSfmZdDlncvuAu74c3Dqww7x99T7Qq3Zbe1MWfU915gQKo3gW6FA1i

```
Bt7P3DUNyA7b7tEWEZSSD/I6KkvkBpKwEMS4WLncdP5CxxZWBQZdDVQF5KBIazjF
iS7KW5r0sln0mZUBlg/vCglTz0mvYZpjzI5V2MAVyaBa2G7COPARrrgm5SM1wLV1
Igre1n5idaMi/XHB+r7Ra4nRtUtYNNnqVHQN91PuBrLVhLtAvOcD8ERF7xjILM1
Chubr0Q0aLS4A9n/TQZhC4n+P0t1LD1ASlmHJ5goinq/DPK4a0Ic1YG28XhcIra4
RshRmhYYYqxaxzl6PijyEFnd0/c08Bv+fumM2SXlvdn4BEyiMCDynMct0nB0Pf1X
RnjUEByxv3/h+enp75BLEZ/jFRLFAW0f33eHbeI/xY2qbV3WNI7khoM4T5kmp119
lFtRfs0ZTgVkJXAD2CxxuIi7Y0+03uidmf6DjZECjBf7a4cmwPwGzzVa4wrjMmZ7
9awIcla0xv7TrVnc8LYY5bamaWjaQ1bNSrYff78fDQAz4U8YbTlSCg2lJhH7bWiC
FrSy196rGTwwfJB9AF+5X64gPycq3MdcE84TXYSqLZny+GynkTFedXQYEIXZJm7
4+6R90xf3XIiEwyjMtTZJkImWUgux6BRakjZkqWGEp2TQ+Jp8gnAFmfu6X4+L3k+
b4murPLZWpDi23rHvgC6kmoUu6Uqq3BPKSJrOR6JkL12VluV00zXCOE4NYPew01J
LfrLdDaMyKWuUkt6gVkhP8YyHutoeNVFKmt4EiVpLMD+3WMYG02HZZKo4fD8l+bN
nvBciJ163+V3AZcZk3Ej+pS0EZRsuGo9ECIH0zHtJLC9U7V0Eib0zHdQbqJkxvG
JQXndY36xbwGHhUpHzmIprHY5qi+IPt7Gq0v4ukjoEghqoE8seqKcEmczRc10QLC
/9RTNnzibZCCHSwe/vg0Ync+sK9GjcImNdPEXE1wzK3atFW3jRblEnnxlJdA0mp8
kvSj/nfVU7tlqR1mVMY2adXUw9xsnlgqzeZ0EAI7y4cQ0k90MHJJ/4CXjP4AAxUI
nkHLG/PB6sFakW58+8zr8ICKiYVXRtzh+iYqKQdGjmt+b87IC41CLUrFym95XBj4
q5GX1rzUArBFESwdSggfTjaRBbW5l/wF/FmzYJ9BKVQn0aNLjiJQdpkg380uT4p
w1ZDwggLD1lucY6fpa2usvENb99Pb4GgqK2ustPpHxLYovc7/gpTLJldXyN8g8t
U3ez3uX4UFtws7xAAIOMDdajZaexAAAAAAAAAAAAAMDxxkKTE3QQ==
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the ML-DSA-87 post-quantum algorithm

Use the following public key to test the ML-DSA-87 post-quantum algorithm.

```
-----BEGIN PUBLIC KEY-----
MIiKmjAlBgLghkgBZQMEAxMDggoHAM5xelVwAnBZd6BpAyyzJjPQjb/UBhQ8CzT9
GYNDRT3zJ4icdMwqpGupWIIBZD2S+msR0Qbmw4jRcE09Zr08IV6UHXrAP+Csf3H/
w3M1m9SB7D0gbqLBHTdWZuP0JL5KVkGi5y08z8ndT50Y9ieUqLRHFwsntDJgd+3c
V4yS3sKvYOV7bzMegMmvPDgqEaVcBj9DBKnH1j8F9iNAXA8TJJES/D1I0kGMrVZT
yuDP4EtfehgJweTz+hVJF77t3vLNea7ynNN884BUPbRw+QhKkChR2Kjz2WsKwKuo
2GIp99M4KKAM02qECzbPNCEAOIfvQ3FpvUWX9X6Z4UxykCH+sM+d12cfvGYSmNB1
+jqCM280c29BAzr7a2/yC2G/fdSW3+0pml+CcmahIUq3NSZLFi56wiGQaE0MyDT
r1Bf4s+Qxk+58Lity6njS/KG38oMxgIR/QZBkvPEGLXACCM15snADsNi+Lebw4se
IJU0G6+bVqwouu9bDzViKX0r8qXeGDoka3VTSBqEOdwDymbdcfB+9sjWWJ7Kzwa3
Ek8tePPv0Grz34QBfxYn/mGmKdQLDdGD/YoU78kps29VRzAjWGdtikgXulTtMv7F
rhVzbQH+HayAaH7BIQtj/yzqDZY1dzUgdMXgAZqv0jKwCpETAXHfH7N0s+WxtDu5
BKmxyn8w0dncoALiAUMB0Hsz6oMyP0fXnaos/sWroU2wcyqa5MGeCcw+4DEjvPeR
RMyeSkPAjQwrQp0Ws+0M0ItoDLt6hzQ2L6hrkv3/dB7Ggz4hYXHGOw0bjVcy9x5
tZTiJ8X3Hc8cApUtIc9jv2yXPGdQBCN/mnx7co7FwUfMiXSqoMkprpw0/VdS7Ug/
cQI6YyLJgQVVjaLNk6z09NbrjQL/ujg6onhz06i10BSBxa3K+R2QAH3sHCJnhl9r
9Rle+boK09DZSjKV9sr3tGTr7UsFsRhmaXdbR4tPZQs7wGZW0HfZpJ2ayqG+l9EB
qcjWU+RVc7m7u1QutUlAd6LT86gb3CzFLTtimjqeJVS/D4sPiHRgjA2dEd002rAD
BwIOxbqERuK54jCmED10uyNPitAy0Tty/yATBLVCKGJWwuaFXS4n3owYFFy6HV+
mRm4qSwbDh0FlrBP674TkclIngFk0X/+Uq08c72EC+SVA0xC9sk7ULwW77gngjTF
kEdDSrMo+XoR1Nbiv8DRhQh9vLBMSvmIJwPK2htIrQLH1YbNxRcd+/Mos2occ72W
dkT0+wWwvyHARzflpsvi8syZLYG4rEz47ayWJ5pXhjCHR6u4NDHeb2dPLbQsr+T2
kw06CyDZ2U0pp5+6qzt18LjMhsFv16T7ebbdD3nwSZgaX45ouJ0149TxlKTuH/Xd
U2ymY6N8UqdHcwnB9weQLXyDsJMTcwebRi4CN07Mxm1/H71dPTG5jPI215HlIEtd
NNRTaPWORI+fcFHCt0pb1QRgDFIBWodW3ubjXIjVLU5wbFIJ8jqjo99+Ln5FdIi
```

```
WSFzUFY0ZvIVfy2uEDR63VK89WrV7TfLmASIPWesWA+91GkrSp0VyF8cnstyz+n1
sYTNJChjjHB/rRoeStVrgIQVNjhTM6UxrT/gLGVNgcLEJZPTc42dzbTZXFsnfQww
jn83hTBGt1aezGJy0sLaf0EZFTULiVZh9sh1HsMeKYy3b2coyTKu5gPe7zsmVTak
UhDa8gvZwruRcZA+q1peqjLmp7zohdDI4F0bydFnE3S8jedEfeHIoks1whU3FDrS
2Gi0xHvJGwZmBc8w6coXJLZnPZRi2MeTWh2ez7nfakhPdxG88ReiE0SWF2Yac+gY
tA+Ej+uVrhP15+QRDnN6D/mmmNjZk+rJcl2JSjlyidwyagY+uo/sVhe/spEomd/1w
0r+T/UiOLgmL1Aef/V23viFpTV8SLKFVCWKwa598n8pUpfjdo1p8rTzSC619iomT
brgX2ixslaESk0kHTJXid103e2BCSgwzzJwlveWcwVeAad8nVqFP+mG5Sd430H93
CvDuGmeTRlu4Z1By0AZDGeZoT2mBc4qdqDwSDjSwfpt0mZF3LtyANfiF22Ds8wPy
nE/LNJr6q0GURGuJFRc+evcYybwiEg9qiKE0SLMCiISrPEMZ8aDdrHtiIn0IOu4B
foJsJKNeoDPRne346hJnS2YC50031J0dmVeV0EV+HGA1Zdnz7YnqdHQ07iF3q3zN
Gq1mFr1TKKDRVvd7C631nuvGLByeIjKoJZVEuonUXPYL7/tWKvxolsbZKJerxjBJ
ch/igjKCCe4zW5DNRPwW0v1zkerlSblvQps4nYQENSsd44yH2U4VN33ycaQms85K
hxnQc2+AViqEx2gIa/BMKM7AliseU/NH5xg5bsTIamYeL2FXFW/Mf0ty3wAsUZtU
zRtfrY/DihfGX3Kl1bf8i0ehq07DAuWlmdGVTDDrBPLfT1hArK/0Xa7TveqhwYZDb
XW5qLc10tZW/SKcw+CAERh69Up4ipu1QE3WzW6kpF4B3YJVgIWeiyVh0TfnN/EI
IGU6F7D5gUht0kVzj0ns9h1o8NR0gPgJdsqSDJ3n1+MT/03s4qMTBbnHACLQmu6V
IrVliQplafBbIiHPI5t0r5Loc7qZbkk3m4y1dIytoIxFJjvUsUx3u0kygI/FGJw
X3IME300ZxRPCey20ZlCWwA5tkxfrothVp/pnihMnDJA8m3ZNiRvLNACWwYk957a
7LohSaKo5uPc/txcAI+44M1vk0QuUWiDNTLFzZyLxi9vgcxJD4vjnd7lF4uD2eK
ynAtf0ITmzVpVVs0lay8C93HW9gD5n8ovAP9nH5/vm0T0VqsshjM5oBA/vnixh63
pwoKnS5gu/5ecy/SdHV0ksK0S8X/OfInUlr4TgC0r2b1dZ0RJ3G010NPr2uJJW0i
tBapJT5qQ41FaY7yRdAXigHut2hkD6ntUG6ETw7vZF9Ecaw+Mmmz70d0Sfv7WcqD
fGhw64+5+OGHRm64fPtYnkbnclmLo+oMuMjWPfbnrCluPTRUdw8F+R3isxvJn7iyd
Hp7cQgWaoRqswopLRUjnv75R5R0dSM4Mwi+gpxJ35JzPU9Pk5q0lv309SaCU7XiX
wiJcgLJpMLewS4T9eQI6T2HMeCl1CdQxw//uAMkDtgBbmua+RJFG6XoEfIUmm7xP
lwsSsuUJXaZ205a730T5oJLSd9PX5W1fCTdrCrQVJ0unT57zjKxQgm5ll/06m/yT
MkqJXri97jtejZt8Uy1MTDNWd86lQtbEJueYJZ8D/N+cyyr1NvOCEpRmFTtmXY1
E1PjvzFk9ETjAoIys8eOYc8YUTp5IE0dZpDE7YteeJ4zXB8gv1pPIpaaHNL4JOaX
lUSQtyjInD9oZnHMSjjsTc5jeIdp7vywjsrUNy5TafkKHdvY9UxgDrxG1bsiC5EV
B+syfujdRcJFxI6hYZT2136//ZNMHw==
-----END PUBLIC KEY-----
```

## Sample private key to test the ML-DSA-87 post-quantum algorithm

Use the following private key to test the ML-DSA-87 post-quantum algorithm.

```
-----BEGIN PRIVATE KEY-----
MIITOAIBADALBg1ghkgBZQMEAxMEghMkBIITIM5xelVwAnBZd6BpAyyzJjPQjb/U
BhQ8CzT9GYNDRT3zkKZQL2gtwFz2Bz+sc/vtd+9G6KAFV07h2V6+7SpGK290stj
U00Tvm7FP3XSdWLDyKUQRtVoFLB+na9AItP8Tf7P/N0W30sW0BTzU+Ufb64zgqFJ
Rv2bEI00BoNuJZ3RwzJGyCKEAURmXJKQQRCCwDaSUpggWsKNWBRw2gYgWoIMgxIs
IZhJIC0AEyhuIBkkAwJEGRaCSxYxGjQuAUGxQLQtioiFpEBxQ5KFUKYFChMBSprB
opiNzJSNEgcKCwKKC0UJiWjw20QACjBgEkVM4TJRwKASVCKKhAJqDLklU0AIEQUu
2YCIgcGEg6Bo4LCFYxKMkkRE4qJlIgcTgABMCCiG0oBNJikFoCAqAceAwiiJGgRC
RCYQpDRxTLIFIAJmCBOQCbsNCaghsQKKDBlhVEYLcQkyEycNiUIhCiMGiJNyGcUs
JLMtxEBSDEKngghyIBhSjKSNIaUtwBiSwygx0AIyKaIF4ECKGidyE5EAakhJRDBl
WjgwgJl1SSYmykXjUwJxQ0a0mcABUoYwYCho4ThywTZsnEK0IMIpUkYMM6JEw0KQ
WlQEYCRIGcVhC6VIpEqxFIZoJCQFGQJi00aQICSFC8dpmLCJWhBlQcIFXCZBGskl
AsELyEQEISkMDbCEEYcsE5SMHDGKGhZiYBgGisJtQYAI2YYhIyQQWbaICEmEWkJR
JCCIJEhA2cZNA8kFQSKNVMrkQbQxQIYk3KQoEbAheZcJI5SQcQqGAYEF06AsiUKE
```



pMJkCBQFfigIpQkBg2bYk0qYB5BYAGqREGjZRJEcMBCRoCagsC6mFiLhgGRZuEjhi  
GbYhDBEyki iKTAIGE0YB0ZAI0DZmyiBKE7Rs2hBlCZgskoBoITIBw5AwAJhFJAiy  
2jYCGjl0gRQm2oREgMghEAYQCJLJRBYBECKJGqiN2IRN0TAWIAYsGkNGABkhiggs  
wCJhi8JR0BJ0mgSAMCCQDJLRxMBJ4BYtFDgNLAa0AhS0gjiKJJZMHKNEyDBu2wKB  
26hRk7ZFhCBuQmSoAYhyzgygCBjBhRUQiAAZCIUDhAIRMS2gBtE0AlAgKGCBg  
obglSQu4CZQBCciSxBBW6SMzKaIQUYCIzNgGEksiRYmmCgJkxAxiphAYkSQmUBy  
GzQphBRqyqYo2sZNCBQM7YoER0CnDhCEgPACeEgTgAEzRRSDBNEpVEI4RhUwJM  
AwSnxMJxkgJRiBRS1KRFQqAoQyYACQgxAjKCC7SIAqWJoMhki8KNW8QskyYyyggm  
FDOQUzBKwKABgcRFkYRhQUJtAjMgmoAJUBIsWpZJGyZG0xgSCxhFIqcoCEglJBNU  
iIiWELdpTDIGJLKISyBEIEMGGSSF20aB2UKE2YCE4SCRW0YSACgFWSRNFJEppDZy  
AJQEpAJIiDiImTYQsBFZIAA4MAFIsiA4ACRA0ZGYEGGpFxBKYBg7BgEqkNSkSJ  
yBAOWUKI2jYtgTJS1DAS0kRxobhtHIhgwYZxksAgkpQpIpMkSsCR04IgGIUNWyu  
oLiToiMQYKndhOFCBBSUhmWJaRIbMMEDgJQygfEoBJGoQxLJYNIQCJHIUtyEiC  
mLhI0qZw2jhWgAMGgKB25gFIUUiQSRWmZxwcIwirIoUriFicmQSZaIygQpEsQp  
BMBhWyYgIyAGGhcg4xSE0Uho2pYaoAhiUaIMBLQHwZQwmoAo0UJJ3BhMisJsAago  
i0glkESFCQBIGDExkKRg5KKJmcJQFDBQErIJAhhMIINKvBJyIQCM4SIOQgZKmgZK  
Q4gIGZloABgiwbaE4IQa0BBQJMOJUEBF1BIPighsGxdilCRK1MIAkahoC6QMybJN  
gtiKwysN3BQnyKRSETVEIpDFCQJiQaKNEEHAAkUp1MJgEols2ABSQKZtYwhpmgYL  
YrZoSSII0Shym0REGZGMU4gJXKYxCocwopSAmhACi5RIIicyERWSI7MM1CaFA6gN  
wkAhSLQECSCE2QEW6hRy6RBkwgygQJwFDcMw4JoDAkuJEJIHMZFWBCGoBZECDQR  
iqhN5DCJCjCRFB0R6oepimvp8nHPr8KTY06t29s5kKEL0eo0d0KmUkuwscobjbu9  
nVpaTAP0C0Q437jwkhRMBvaceUUGmJ/tDGL3VdcS//l3ht4z06nVWqnfXjop40BW  
U51Srr52DHHaByGkndfr2QxksEPdgtXtmyluI4eh0h+uh2lvycGdUCU0Qv0LVTS  
CXeKxCS3SsSbg02zhGIY066mbfLEvDIbUPvzu5/AMJhXs0yxFBwkUPjACjn/zoZN  
zDULk8DrLVDotP/62+WyyLrZKK6N0Ej2A3iYXMwQkpHcPac+qvRGvEujtpSyF9SL  
K01mHEU1K0tmko238KLwZ4QIv20FMkbOWneUPJGfWCS6k776Uw1ZSR8WYc48UktD  
DA4AxJXGUa0zBYK9aagi8dmqF/ELk27dc3WVvSrts43REinQ7oKAuA8tVNowI/jU  
FRpHJRbuIXachbx8Qc1jKfjFmPhYmGaikJm0Lsv97NISoYSjCwepkARtriem7lj0  
785ZsmsSx5+8k94HHDfHP4kNlnRJNGYX7leiRMnEprwZEU9+6gg7KMoe8Es8CD  
D47TGe8xbY0rZhZS1297CjDk2VN756/wxLDzPN+zctZkx0g2NHYd5hhVzAdvBer7  
WN7b/mu/ZjPYvADHg/1vgT668Y2FX5wI3eKbMv06yqnt+dWRu3SCYVvK090INjo7  
S6AmX8SDl1CMtpUu4Tl6ItMe3i680ekHdEoivc4rqjBFAzY0LSXqFEbj/Ie/b7L  
XJFm+PT9+M7zhGHvEN5GbTJICPyKjRdW8agP3Fdhf+lMnxwJMrkS2LDRMGKzzm+C  
ij0Gw/q71NcNZAUkzTExX54hgyTtcBnfmYSnc1djFPTI8AaL5L+iruvIJve4PkZU  
NVLGfFWBvxRXi+R8v++zSPEjVLbIYNORZ/6o0/UVAj/jgs6P0ZtuR0tyXGrAnF+X  
rzJnTkd384iVVvSvBnQosioMLnYd/QccBSb5Y935Nh4c6WM4UhroEfR0qtL8T5i5  
xS96dKhckwnqAQ0JdSJC8iu9s0F3TAPfoXnwheBdLRZdrSVRsv2QPcNzbXzR+Kut  
jOMJMmgI88Noxr/uABqdBre3nh0yqxSc/ln7NNQUk5EKFIAX6nW7h5Sp43c6dyXp  
OmM3Hn/E2Avt1rXpZQRivCSC2LZD/cbo7EmLtUSjVWsgIN2NaZVBpiGEZ1xpnEk9  
+aPatT+WR42cFuJPML2RNWHXQKdaqf70IHkE6Sr3qljnfN5SkLojLXXbtssXB2WL  
8qTL9nHN2Hphk4NRZ5u2+39MjeVgxPr3qVo4ydpX0y5QY7MuRVZbbW0lcmgUWi7a  
GxjbpOmKJCeg3Y0va0dfi/tr2eoylJ/k7bxDaImpVcdXZsvxcfUkka/5S03pGyDj  
5oeLgVVKXNV0n7P0q5HCbfJxBDQxenYIWKQzTGrYtm0ru8q22nkiGBtiWc5ZxG7V  
salHCGwuDEJfllAUzc94sodl6qYVpTwyZqg8Q9pLPa2s6HgTeZ9QknJKzfktZ2lz  
3j6dxXhlZrzKk7tH9Xs4Q/1NpjMdp+4NYhpMavo1N0sQ6B6t3TEd6FcaK0y+GeD  
pQBYZz0ZvIgnU1mSnsUJixm19wjIwo3yZd4yzXlBCoMwrRauMco0EKxASaSBmGcI  
j8yvt2VLLWB8keZzsHDjqu0JhT0KxkOVAc07ziz+WhuAj56fE1hBDvvRT9LA+40w  
fEoQLdnFCHyCizLvH4hbfRA6xGzMoZat75LQ+7bE0TRNbPV57mXdGxac4zVWKch3  
vP2sShMTtidmKURvFEQ3giNmP66xBa0UzRMwCrcQXTTdMMgl5SPR9K+It0csQez  
wTc7ubzAtPGfC6jeLUjP0lu45FZyt0w2j9nIUKcbc84m05CLVecQ65jQ1W38bLXC  
ZGfjdszn5DMszxL4H3htx5YStLz6YioSrLr8Sfdh+3Jdq6104bIU5ljTo4/9dn5a  
culMQZljFZp5KHRp67ZgmioXu2o5Y6NEp0Kf9BFHb2KJzpEKV0Az0EACdfN+ixeI  
Ux3BaBIqSDxvW7m2YYIVZnzwujWzgiZAJM0SgoD7ax00TCVjyKATA/uRwrnU2fmK

```
APGGQTWJDFv97Ieptav/HNhlWeUifaX5uDkPz9TgzIuikF7szmlXLCMQhwZQb0LG
RH832bt5RBKv5gBSiqYunRNvzrC3CjDXqXb3aAQFovayj1l2ZP9kLzCccU0XJCM3
S4S09VzpuD7mpFhZYXBdbZV0XwAntpih+GUYjRW6m4NCLMyrgE3onh/myIb2lB//
LgxkIR94TZrJnR4Y0pVZUcdtqV5d0dJNFvblWNY0DDHs2tN7aYYxKKaBq7Rs8HBj
XwoGuwwVr1labJWiPi605vwjbYL5xR8S2IxLqgzOD63Nruhj31uCsBHXYNVWU715
44ebgPYC54Wt2tFRbmbKZtLM6HV64s6vFtrqpLM7wyAtHQ2oeyfWHJPNKMEBb4XL
ibeXn3ePziRD1yH3/uIDnBvMOGmSBKEYRfpYTIvFYzMavyUs2e8N5dWBCdmjLkRr
wPPFzaufA0ZBTM9H5R/MspXBsOvCrAJD6+p4knPCrYqcALKgP/YKG61EvnR8bpWw
eQwBc/log9Iw0YrjVLcarbNm7Ka4X0R/4eHex81CNGu6+UKkcDMWmd5c+Xg0+QOg
d079i7id2wKZfjcmGkqbcV37udJrLT7P/JoKM7bkLsd/jNs8TcPyZvek2TPxLjze
Z/KxxTS6INkfhSpckyEuad4hYHz1+0igz6VheEMHdbKUj2kskJfI72N9yK4mRYKR
f14HRg/Vf3qrBegREVGOjckz3+hNkhpahx1767qhM4U0UbFE90nAgKm4ChBFbaBP
9q/nSbjrK9THHXjGkiqR1mMF0hfVwdXTLLCr/8xw5ajRVEfoco60Kh2sHbPb7kBE
faHJfzKVkw2WCnHkq1gbLT7I3RL50zpKeKiHNoZbnTs9R7m8rHAzSleHfgQ7WXRZ
yZ5u7jA008ct/RCUruXB7uRN+RN8xswzaCTKs2QlpL3Xm5BXPQtxbNHWoVUpIhz8
Xsog3/bruVEXfjaUy8KwbLm4gaqsluQscZZwrd3SshXI1yWhmtOpE8E50eanHLeg
oiJNR/CrAQUfLVs1JOQ6CPLuH/j6iBxgVmyvd9BVNZviFFttweWR6wicHsEf0j75
V/WBcb2ri3yFgR4VnM8371DG06gcPgAmzQILTyKh+wY64+AutnFQbny0BVyP9gkR
GyL6svEt1RNF8X8iVZ/7HunFMC8hAQFfnZjI4HI9hlcAd038U1fItocMwYQfeNw2s
b2cs3RcmiHYFB0RT3Lo4AL5ZZG2IyjNgkvnR/Ify75727KfEZin8512cWfmXwGQR
2r83ALMq7aFLjq7XVvbmGH340qvFv5Y3QSnCs4YepHz2Z56fnM7CNfjg7AISw0si
jFPrGULPUB8Yvrn7W31LSX9c2Ex3gky9qNtq1HLV+9fWu4xYWXFL10DQeYIgrnKFE
bLkov20qe7cm5P50hv/rxhXGXySJ2F3NA9vZ0Lh3YhPr4Rp6LN+Bvt9+ejw+OgCk
3BS9SVyltZMQxT7GyXhMxqYNBF9ac5SP7NMiD2XcuyaLBsWuXJ+d3kZfgJ7+R2/u
YvN4Un+w6uMsn5rlBwf6C1xY8M8SSy6IRmdN7s198XDu1BckMDJbdHj8C4PY9taM
1xsqXpiwlgFU2imL+59SGgAIUGe9epFFDauVrMIRRwsg4B70rTcto3jzR0nX27Bv
k2PzIzkduVYK3yh+drdabu0PwR5wKWuRUCdyUH8kS9UzbD6QaTub1BEBSLTG+wui
Y5QXtY1v3NHFMa0jjLhEL6/F7H1r096EFhP/+2bo0lhrpHSmF7w3WtmBqEFRS8XH
aPaU7plqmX2HETQ07JXLiY0Ay/yrIGrjRe9GGR6GDcOxm4/Fj3Ab0xY1nq8lSyfS
/pvY452JwMfe0wPt5ADiIdmc8EIEclIhcS/i1nUa2BaxhjRBUDG2Biv+lgHXm0vA
agzD+QyJmy6T5/VtRiYnqmM11dKZDJ/zCskbQG6w3+UKelmzMYCtQqh3a0sUedaQU
pwAwk4akkE3j/SFXLYDiXsWRpWdLu2eI7MWxr501geagYj88gY93tCtPUzXg3ilg
dRieQIjd6Lcih1hy5ULmm/ABXdW9RCho3RRJx4aDkzrfKljKJg+7a8Q6c50ZmAaE
JM6qJ2VTNEh1Veza3KeS9Ch7XujitNfnJqengOR3DU/xSZxi8mrS5lcGRvi5HEXL
0ad7CcyBQx4h/qJAYZkOSDrTi8ABSGnerR1srZ5nEX4XICLdInnl6H7oRV4sjIbn
VFeuN+wMD73knIe3dHgbZy3QQvha5pDlLar7AQD8lnXG06JXdAwcKMNSSKONVFhf
SMfrxk72CcoihP3vhgBeT5abiFsdZG/+mEG3nw==
-----END PRIVATE KEY-----
```

## Explicit composite algorithms

See below sample requests for the supported explicit composite algorithms.

- [MLDSA44-ECDSA-P256 \(2.16.840.1.114027.80.8.1.24\)](#)
- [MLDSA44-RSA2048-PKCS15 \(2.16.840.1.114027.80.8.1.22\)](#)
- [MLDSA65-ECDSA-P384 \(2.16.840.1.114027.80.8.1.28\)](#)
- [MLDSA65-RSA3072-PKCS15 \(2.16.840.1.114027.80.8.1.27\)](#)
- [MLDSA65-RSA4096-PKCS15 \(2.16.840.1.114027.80.8.1.35\)](#)
- [MLDSA87-ECDSA-P384 \(2.16.840.1.114027.80.8.1.31\)](#)

## MLDSA44-ECDSA-P256 (2.16.840.1.114027.80.8.1.24)

Use the following CSR and keys to test the MLDSA44-ECDSA-P256 explicit composite algorithm with the 2.16.840.1.114027.80.8.1.24 object identifier (OID).

- [Sample CSR to test the MLDSA44-ECDSA-P256 explicit composite algorithm](#)
- [Sample public key to test the MLDSA44-ECDSA-P256 explicit composite algorithm](#)
- [Sample private key to test the MLDSA44-ECDSA-P256 explicit composite algorithm](#)

### Sample CSR to test the MLDSA44-ECDSA-P256 explicit composite algorithm

Use the following CSR to test the MLDSA44-ECDSA-P256 explicit composite algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIPsTCCBdMCAQAwRzEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECxmGUETJSHVi
MSIwIAYDVQQDExlNTERTQTQ0LUVDRFNBLVAyNTYgU2FtcGx1MIIFgTANBgkqhkiB
hvprUAgBGAOCCBWA4AMIIFaQOCBSEAJrtZIG9uxx9FNUIHqscfZKM2PFI fmp8mnFb0
oCQUDoS+891HsrMFALd93pynT3s0yRtFa6eCcg/+Ff5xJJNNlvRLAEUDo9NGtn1
r5DaAjOuLIHQIAJmVtS6liyrDldWcp9CA2hiuxBehU6fjUma9t4muP55GGWCzRr
zKUW8BJ7+8sfnP5JrdnQdfyt/hwfTG004uszdgnJoPM+4NkiTkcz9ukJecV7rw0q
88RJU7kNwCBjC09nc365sX83nqiVCEb/uQtcfrKT+wdp8GTLtwF6omx3wQsdGV0k
o1TH0vY2wPhyMrtdVwvZn4KZLTmVe870Z0HaqimUdm9LcP2sqV9pT1ZvDTHWHD
aakLXIwUAMdoiAFnPVaDx7Hh6ptFvw5GAAL0GJzPU/5TgvQN21HzxK0SgCz6+BX5
6/wjs3Zn2o7i6wwG5TAUG0PbG4otv74Rs/ZhiMpWSzRW+QQSTQgICgAtNCcfzhZ
oEP+Khn7f07N3sxC8+iQWIKr9E0+3CKTJkyLkKMx9lh0cssUSR/bSdKpotyy8st5
BLUu4G96gMreaecmRMAoDe491ED3yHmKwn0k3wQHSxMVU1dTFxor2vIhTUqT4auT
82WN9qzPb0uJil1foTokvC9RGGXqChJ100Gh40h6IEdMEB7Cq8XR1oJ7LoR4BFMa
c/qXd40p+AS8FKKf7bZ7AK7vSdmOdFapQ0UVEWMHEEYdV8ksP7UWYBnPy9CXr2u
pMUh6kuu6nt7mni23KRBZYqEiKe3f0D+tRC7BQBDG2gJgtR9y3H04A3roaOpYn4c
vLwHsaexYF+i0Sy0/9I0lKRukAjj3vfaFwkT9Qw70/CuPqjWJH/oAwHo9jc4I/oU
rTc3DPVxSxGsU6ZwI26vx+UQeISVRJLjld4qVvem0KMc23Tg0jc+H1zd+riJixn8
HP8NJI/a/4vz7KwQc/qeiw7yZOCgfKQHNfyoTcwu0XF/K5sdiS0kmNCGMS+fxVw
ZjelSryVrY080SV+Hr0T8bN9CQxPMwAJnMDIIBvqZMUUwUYSdsQAGMB1u7+cPry
gwWazUdULNq+ZaaozgcF9xe90JG2Fbwfw9fhG7b7QdByFT1QxyewWKUTF615NhV
kBGUii0zQ7LIRxPvfSnMDugmlt4cka1tEunquWLFpq4cDIHDG0EblsmWG3W8U50
VTzb0STckJsakI52yEwLNVbBakTFZoZeGxHh941WNK5A30lwffVZmOcYWrCB61JN
ITN0MKH6ZhG6XmEomwFYasIVsRujViTiyZzPH+1MbMkoo1+syru/P6PeD9axpi3i
OKiUb/FTLytpKy2SbVPYZOMPJCZJo27R3IX3MADXkfy2yv8phqPRB1z38wSB1FtKK
Xwim+51v5o+lv6ybnYs6AZ0VPfWe20+9ANW0HjMTV8ztNHtVeSnfcizVS6k1u2UT
GJGef5VRuLkELJQj0qx+qGohTYLvm9TfE4iaxLJZ95mf+fWPCLCLhHiFdGmpz2cf
m8Z0YhZaoYm96Rf5WI+D+QqDpQMx9BNV1a5R4g/cI3YzHlqlNvHC61ajxBPLS8
DbGhES/aVYWUL3NuEgrnc+Di4BKkPhKU9qZRJAV9RLnVjQTocjgkNswMvp3Kuu/
gHSqaWyFex+Uuts3Nlu3r+7yUC5ElDzwTq+Jn+U7ILRqs2wohnFnjg3cABxXV7ii
7F4q0PoTZhtWP+4KyKfqcggTPoV5clqJTri8A0xv4qsIQHrzgNCAARxy6iZUXq+
x1siqMQcgllK2MnQ74X8Cj4KyJsEez2cGSevPzFDjPOhTmNlBn90o6iV77mDENhP
2340oF5bb0W+oAAwDQYLYIZIAYb6a1AIArGdggnHADCCCCIDggl1AKvPDX74lkdL
Rsb6enWuUrxmTor2Z0iaTem4kK+zMg3esL5iuoDxug+/rTBI/IMzXVpDm2Y9i+cH
riIDr3t3KKh/YCv/tGLK+ieqEzaun8IYXe17bHbEbTztBVZat2Tzr932Jy5+pWZ
6yW7lhFUTQ0N+cXwLH1bm2N+qP0jvZYXpnYGDIAnlFfm9BU0cWAKKcr9WULIWE7
HLEX0j1jmPhu+inx/qgPvVyer1tq/kBz5q1ereKmB74gx0nsqkdwKAYaktpTJJng
1bUz6/HfDARXIQpiGkq1Jp/aKabU4wQhavAsevlbqaspl/QymwZkv0PYk2rWZ/TC
wzIwAMPeP80nk90RE0BvmXPj4wCK7tkOX4SXh6l2wm1Pw8bquDQVLkud11rqeGyQ
```

```
vaxJfKZ6ULAITKHXYmiFTmicFLh2ryEb93dT197nzq90KFLINjkrznlbDomSKh+1
e6rs1XnBvt20FsTeE/dsptExPu859goDpVtbd18h1gaRvkLH78S3PxMdNgdN1Uje
YyFJosdDoPtAJIiq521PQLu0jWrQvAqPUZbFkX3I0ftg0gTKVKosIF2+QChsHC68
S0tFgzvNQDT8f9+yi0ubrSLZ34WzZxZ502Vwralp+GR1FzAjw5dTYynUtJdzvGX7
zTr8nDlsloYjv+ts2kuVoc70SQifeT6d0I2cQMgbqMVtbCqhFI/ZxaTw04WHu3NU
uIfctKewUT4R00mHwvfL0LsKikDnwGb+CEJTPttRw2Le4bEpfnWY6U1vuS25kiuk
cfINpx2u8g4jEV5W3eH6EWE0TWp/w7D4Iz/ihmGPfEOhLkSStBCR8UHHzoL5ziAD
LGJAAT/FG3NNRP5arPhaklXYeg4JQL4Cc8AgsgLHslrj3AlZrLM97rNPYi984IjS
dUKy6x7UFuLX/nQtpeabw9o/n65/WL4n0h2SKGgiogt7zu2dJoV65hGI2KvCszf
9aF4ovyJf02mAomErcuFSPghhG/JDeUtP0jr3UUhbk8L3Wp8PqhuDBaUFQJvm4R1
7uf/QzvGTrfjZ3/+iZ4S3I43g0zIxziWpk9jPttSEWLxcDTvLxUJOAQFrLws8L/q
VtHLEuT952HxgAy2oyWAVpryS9/hWwQ/jrvNLyAtpyaxi/xdqx0lBaTgQhdA1B06
YFZyoPdthzoGALomzbA4AAbx6j8q2Ms1tBYrCSb0+o5jDui4b4uUsPBQ8zKQ1Q5F
FPxFzqnUhm+cunQnu0j6bmq6XoJza5JpCAidraybqfQKvdkq/Xmakspxs3r1WsG
Qr0LskBuEaKjxBTTQ2Q7Ku/an6xq7A43Vjx5qSLvAoZeoTLOP0qhTa+hSUxQ/a
Jl7DqUrGILgAKDUI0mWQkEkBVI48/ivB4a/C900smAX5FeayvJTD03oGIfpFh29K
6+19kBwdZ6vu6CHJV0LfInrdd+LBAAcCn9aLGT+0W5yLLOMNGyMXWFOA1UwxCPRM
ZBTG5KMCDIbqY4/5VmIeiTuAKDzD5ck1Zs2/wykoLFLH59skKRAP6Ubm0acWBIO
f0xn+hzhgUdCCAYMvjKPNXAx/vB702QFdp/Iwfgo6mHpTiVT/oxLtsStiBiWHWC3
e57kSDaMgTtpWAOmEkAu5PNsBqgV/3GfrQgBXAvoJv/Cn09kQ5G+oY6bCKsQr9ox
qsjjHLminrStVkbxdx0WTrPQKFVQHL1Y980Sfoi6g2z306sAMtIw/IH/dgVI36nbW
u7vE5vHiaAcSNGrmedlq0jq3QA92mWudMYFVL7DptSpUPqkfw0+gH3IHq23ZAcvQ
xdil/niu3vqlzEM2Pd0mjX0EM4Qhx+bhKLFn6vEy4LXBaQ3jEI5+qMVZ1+ZBY+xy
gGXoKwB6WU5jX+tcLwn+p8R0FhyQhHSSYR9EYPnJKLCaWL0Kt8jTBe90a0kx02hk
DUhM0obuDv6EUqSiGIhXXFnxm0l0QwjPJzn+LW01bBNN+7JuA0AKd0lFDl58wNGf
uES8hFc9zmFhD38cmQLt4C0J3lFu+YNYAeTvYTv5nmzhqxF3hnMT/gULfSc6Su5K
o1FHGiqlfjktU+5iA32D6RB4W+sAF9vccCHKVra2TPiZUeGvlyVBNT4wtAdVbvcrrr
U0Kp/f0H4sIu9YBgeb2MceRBiP8LRgccMRsmVcPFyGuiEEPqs4m0ceD3vD6sRvdb
zYCwUD0jhEgVGGYI7UaDYsZr1l0zQsXhDfAUiNePFkbEDz8sdgzSSLpwS97GTE5C
0cI093IYjvYIqW9krfuKAiS/V7jP+J/bjpVncubzJbJynLhWCdq1z5yv53EEz/bgA
lKe5dEuZxuXfVLl0I+zZB7/m+m7ociSzkovPddFibx3upaPC4g/Ty0TBkaqRex7
pGazoTW8UTPjB04/qfE+/AZPhYTSr1l0NNdgcxb4okQBQv3lRADgGumn3ewThaZ9
GfLvF32Stf/5qNQStUKCbUGwZIOU9CU+tnToQuiDlepW5dK8fXk/Pc5T8hWGA+10
zWFOjd1vDsw5AdR/Ux/Ryw1SWUvCEeeqeXLAUnv//t68nYK0dld9mPnK5TuEBaWH
BZxohIbH3P51p7E8tIjZH2Z2NWUQTWY3Sd/D5GIgTZAuau0/5QoE5w8Kqx6l/xQV4
XswStgJCeFopFfqcLDGx7La2VcWAT+XN9UreJ8lR2cExqoN8z5MhLM4gPyVkJZTu0
FpVVNtd3rwKhvhWQm24/qZlZu16K/zfaSvH2WunZ3CHyayVQEN6mG+Vnhn9p4TA7
0lW1JVTVCCEcSJBf0zKwrsFRWes0+gPrIn0Dpr1mXhNPSLSHMth6Uzzv5FY/g6H
+etb/h3SwMvWsdvV4LHX4BIUNduWwZAl80JXcAzVg89e78LFp2hTr6EIDg002d
endVCy3nZpM1nloNI4yzXK/NFRdzJpaZlSskb3h5lRpGXVSPH054AgT6rtSkRj3nj
+dckRP7NHM6zGR/+94VHKD8XjeHsN9DxT2c3fFg1ctfrpBuFBlsrU3Kr6j1XJZlt
Bfa3h0WiJTXuUz2Abynmj9sT+lzzkdF1Dr7zfI2eitTL410gPL1EQ2ceIqoPoWIY
eecr+FKcKqoIf6Lo9JD9g7chtnesnKjJBCwyYGmAs7S3uMPW4eL1/B01b3d7giP
nMXP3wgNF01gcIeWqcnc/gNJWF1sjKfFztUAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAQHCGyA0cAMEQCIF23GLOP8gk76vJtzMxvJ9k+C7doUSPS1/Hnk5Aa
ovXuAiBNkMABIOXNrpH9vc8v3bvzmBAqKvTCaysIl6sYggqkdA==
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the MLDSA44-ECDSA-P256 explicit composite algorithm

Use the following public key to test the MLDSA44-ECDSA-P256 explicit composite algorithm.



-----BEGIN PUBLIC KEY-----

```
MIIFgTANBgtghkgBhvprUAGBGAOCBw4AMIIFaQOCBSEAJrtZiG9uxx9FNUIHqscf
ZKM2PFImp8mnFb0oCQUDoUS+891HsrMFALd93pynT3s0yRtFa6eCcg/+Ff5xJJN
NlvRLAEUD09NGtn1r5DaAj0uLIHQIAnJMvTS6liyrDldWcp9CA2hiuxBehU6fjUm
a9t4muP55GGWCzRrzKUW8BJ7+8sfnp5JrdnQdfyt/hwFTG004uszdgnJoPM+4Nki
Tkcz9ukJecV7rw0q88RJU7kNwCBjC09nc365sX83nqiVCEb/uQtcfRKT+wdp8GTL
twF6omx3wQsdGV0ko1TH0vY2wPhyMrtdWvwzQn4KZLtMVe870Z0HaqimUdm9LcP2
sqV9pT1ZvDTHWHDAaakLXIwUAMdoiAFnPVaDx7Hh6ptFvw5GAAL0GJzPU/5TgvQN
21HzxK0SgCz6+BX56/wjs3Zn2o7i6wwG5TAUg0PbG4otv74Rs/ZhiMpWSzRW+QQS
TQgICgAtNCcfeszZ0EP+Khn7f07N3sx8+iQWIKr9E0+3CkTJkyLkKMx9lh0cssU
SR/bSdKpotyy8st5BLUu4G96gMreaecmRMAoDe491ED3yHmKwnOk3wQHSxMVU1dT
fxor2vIhTUqT4auT82WN9qzPb0uJil1foTokvC9RGGXqChJ100Gh40h6IeDMEB7C
q8XR1oJ7LoR4BFMac/qXd40p+AS8FKKf7bZh7AK7vSdmOdfapQOUVEWMHEEYdV8k
sP7UWYBnPy9CXR2upMUh6kuu6nt7mni23KRBZYqEiKe3f0D+tRC7BQBDG2gJgtR9
y3H04A3roaOpYn4cvlWsaexYF+i0Sy0/9IOlKRukAjj3vfaFwkT9Qw70/CuPqjW
JH/oAwHo9jc4I/oUrTc3DPVxSxGsU6ZwI26vx+UQeISVRjLjld4qVvem0KMc23Tg
Ojc+H1zd+riJixn8HP8NJI/a/4vz7KwQc/qeiw7yZOCgfkQHNfyoTcwu0XF/K5s
diS0kmNCGMS+fxVwZjelSryVrY080SV+Hr0T8bN9CQxPMwAJnMDIibvqZMUUwUYS
dsQAGMB1u7+c+PrygwWazUdULNq+ZaaozgcFP9xe90JG2FbwfW9fhG7b7QdByFT1
QxyewWKUTF615NHvKBGuIIo3zQ7LIRxPvfSnMDugmlt4cka1tEunquWlFpq4cDIH
DG0EblsmWG3W8U50VTzb0STcKjsakI52yEwLNvVBakTFZoZeGxHh941WNK5A30lw
fFVZm0cYwRCB61JNITN0MKH6ZhG6XmEomwFYAsIVsRujVItIyZzPH+1MbMkoo1+s
yru/P6PeD9axpi3i0KiUb/FTLytpKy2SbVPYZ0MPCZJo27R3IX3MADXkfy2yv8ph
qPRB1z38wSB1FtKKXwim+51v5o+lv6ybnYs6AZ0VPfWe20+9ANW0HjMTV8ztNhtV
eSnfcizVS6k1u2UTGJGef5VRuLkELJQj0qx+qGohTYLvm9TFE4iaxLJZ95mf+fWP
CLCLhHiFdGmpz2cfm8ZOYhZaoYm96Rf5WI+D+QqqDpQMcX9BNV1a5R4g/cI3YzHL
qLnVHC61ajxBPLS8DbGhES/aVYWUL3NuEgrnc+Di4BKkPhKU9qZRJAV9RLnVjQTo
cjgakNswMvp3Kuu/gHSqaWyFex+Uuts3Nlu3r+7yUC5EldzwTq+Jn+U7ILRqs2wo
hnFnjg3cABxXV7ii7F4q0PoTZhtWP+4KyKfqcggTPoV5clKqJTri8A0xv4qsIQHr
zgNCAARxy6iZUXq+x1siQMqcgllK2MnQ74X8Cj4KyJsEez2cGSevPzFDjP0hTmNL
Bn90o6iV77mDENhP2340oF5bb0W+
```

-----END PUBLIC KEY-----

## Sample private key to test the MLDSA44-ECDSA-P256 explicit composite algorithm

Use the following private key to test the MLDSA44-ECDSA-P256 explicit composite algorithm.

-----BEGIN PRIVATE KEY-----

```
MIIKnQIBADANBgtghkgBhvprUAGBGASCCocwggqDBIIKBASCCgAmu1kiD27HH0U1
Qgeqxx9kozY8Uh+anyacVvSgJBQ0hQtygH0yva05rHa5fPZoxjx1e6w/2fVfo4+E
3uqJBXk+cRPHhqKNGv/26ezD7LS3F+b1A/P4iNjk0C3DHUUMFw2/WeBqIn1xIQ35
lm91h8VIMh68BhIEX4HbL1RC8M7A5gywSBIIKYiQCeMSKczEBKIUUZg2hQmHScpE
UKPIZOMyRISYAAuAKWGULULGYcmgQFK4ANsSURFBUhsykII2IpDCgdAEjRFFKcvG
bBGVRdsijLICRQGTbAQJCbgYIhqVEVKEhNJEhkAScAopCAq5jYEGUgqxbSGmBBiU
KWQETpsgMEqYQSIDLVswSgqjhF02jCMIZsIYkeTAKNMABYrCTAg0KBoQLZAogS03
YNu4aVxEJgu5kYEOjsuWDRAJaEMGEARGgRAHZZw0JmK0jEJASSGnZZ0mSEM4EhyZ
kQs0CoC4ReSyaFiCSUA4BdEEMGDEhSHDjROGiNyCEAm3Qdq0SSJGiMoSJU0ELIAI
ARhATdwQDcgoachCEQqYgOCycSCwhJKUKgCVKBtIBeAEQIAyiqCwbOCmhJE4bmMw
aaI2gMgQBgzBDcJAZYNcCgEpCLNECoEEYEhCARCXcUQwEuCYjBqgbYImAVmwmQA
gtikIVDGgIikDJCAgBJBSZIAUEkmUCElgtlGbpE0USM2jVgUKdMCIErCkYwCbhyS
```

```
kVAYYJgUzMQWdHA1IJMWAdw0gUnEbQlIjMwiYaK2bUpIZiMWDMS2KWAWSMARBHG
IckShFyIjRqiQAElThmLJcO4JkG4bJuYtUHCDBuCIBIjKhAjCduGCQQSMUHEiFEy
SFGicBSDBJFGQCfJRokmIqKEYCHHaCQCjBgUTeKiLAW1iICkDSQyINiyQeGGJBIG
EaNITIAyUBQRRhupaaMCjkgohYkoaRIVahslgSCjYcA2JhG4CNQAIVyyKYQoUBI5
gFQ0btBIhhEWKZA0JCIEUpMIDFk0hgSkTBmJMJAUCIwSMZMgZQIhaVkiBgEibKSw
gAEmTkmWBBYlUIEiUIiYQAgQAhILhuNEBJHCTBEwTcoWRBKGEAozagGQDRNDSprE
ZQDBiYjIKMgCZZYoLCSncVgwUQkVbCLHSNq2jCRFRoMCRhujkcsOKAjGTAJFUYQQ
iAuIDaSQBdlIKdvICJCyhaGSBcgCaa3JyIu/8HR3n+5neE6TuMyTB8nTCJyk/6Y0
KidBTsm5I+LNgUG/4ME6SdmHZfeU4QR8LQVSwDVEI84SAFzKpB/zwRHANrZ0DOx
JYVHwHv0b26Jyu0jvhmUJMWvs7Kxq/WnthiAjuvqSfQXvJLSGh38z6SUytNuG97g
+Sjo6As441A30ygtGTypeVSfXycTVtOvZb4yKeCx0ioTTYph8+GF1kusxumooEqD
GktF4j0k5k+0cm3t5b4Z7own4t629fblPpB9mP7q0zjt9C6TzOLwQkjuj30Ih9
/FkEN6hrP1B2BAPT+Mpaec2NwB8oBBU+u/OF5r4Wc1WSjOXlNBKkH0wchg950ryy7
XlL9jpUo587NParE8zR233YuQGCh1ivKNnZVqQkiD67XrH9yyawf/9AwmQcPYuQm
LgzjM7soPVyi1ZeZ3lsMzwOrSmeSM2qkhTzdIFPDXTZcwWPH30vdkZKDcvmAyDL
dDVSCtzY0umTWZSY3FKvyjJ70i787HnLTC8StDrgh2MZEULcSwKXUIMmW3zn/2U
hq72j7Lbw6zktSs65KR1dquG0s+NLwAqbIp1tu8IhB2Fdd4P2YhD1BRGrJrQzPLB
CCNznvhvMQk7WLI9/jiUoLGAuFedcaEL5+VwxTd9nUTCvPkzXvCIcO5B6Al4nuNi3
KmEb92vLLm+ms0xZ8+spe2umZanD0oPTr66me25vHsGxJRAQQzjw4N01gEUcx5Lq
6hgE4/jEM9vT4PFZ2K0GXqu5L8iyAP5deccLA5UFLJXWyeH2ZEn+R7/HFwZ4bzjc
tKkDL++g0V6eKeXH1gYypvLvFfheIqg+xsVI/ryS+x+Ameh6jjSpMaJuaXtEhNZ
Uc4eU/lRVyQe+g9oGHS0b+mMAJ6NuWjDwbav13jfeehEzt/BX/2W9ECYVYM9xFP4
MzhUzq/7FaG4dYk51s56vB33U8Eq9QNC70I1Qz/0HOYjCQnhWu2hFpDW5VH9wQAO
XCkKI4JL7GkpdVzJ7asVLDhc0gz9QELiLQy7GjEJHhdNKfJje8xr39UzjIUSW8GV
5dzYY2nN0YPDjz/j9Fqwc6kkcBGWJ/fy7u807Ar3ZJm01nnEpxrUmenMBv8yt47B
MFuWPD2Rqk+wq94F47R22ilfcSVG5s1wWipYEPxtBWCzyvhe5ayykrd4z67zntAV
prD8uK3yFzbghEKNiDv+5R3FmdWLZeRR6Wql8MkTaR0zLuL4JuJ4xgoumBqx8EOG
/STPqg3hNoy8r8PnRJumERasB5GKzSjU5vDYVv8e+r4XBALtQxQiUmTrzXupXLv
2SjvV7Fylq1DnVf04EnGBqjZzm3qgc7XxSra80oz3Neow4Jp2P2/fJ+P60JgGHX/
SVsrwxFlDtBeTmGA8wcVywkhGivlTsGQIPM3wFD4mOD15XFVgQPvVrDWyvNr9fSg
7EhQT/BDQP3/Gv4/nuwF684EHfs0a/rwmURLmsiS0fSjYs+FwvNfrnPOLTsYGDCh
q9eefka0hLpAYX/zwphWQetZo60UsSQeX3IWMF9k17BFw95Y9Stb76MMoe8iXVDE
UXmFBf1cPCX9TDBk01PjiB2mEUv5L0ygiIZBGSn09xg+sB7Eg0Co3GwxobXDpJT2
bV3Svs66CnSZYSkjzm086MRHEM/Agq6InWjJ/QyxJJ2iD5P71PU2r5g4VtgDwi8m
XYxZ0X3eCFHGgpRYRNkyuZBV1sdiiLYE3Ej52H0AbKdfsw/Kclbw4PX7VEi8WfQL
ZjX8hMayI8orgzCvv40f/W20Ceg0lnNUbsAdJGgJaYn0B1DYnJ1Ar9Tcy1ScTnGA
1MhP93Zy85Wjn026PL9v7veyprxFMyzj/S+oCIXwygveXB/7mC6UiaXbVgBh6zX9
Zhg2dBUe/eoZecnn0JjsDMWevvs1PD+TLXPfy6hAF6Trd+841jajon9bYvQib3cS
nCMv+S1V2oQHhY1ubFi1A7dLhbg5de7+gEJLDB+eR+Q8bbjp0FnepMZ0ivi0ykVz
F8gIhSF/PSzPQXsLzLr2+/s40evL+SAnsY0Fb8cn6IQCS4TdXuvDKGqjuDrrBTq7
hqGmP1SZPSsSEszIgZlRhRM86ISGdic0svUCpXDeZ/IFM1RAjvmpce/6+fQJU9R
5LEBz206GCS232X6dpLbUIudb7gALPx4Z8qArtWrPITeSp7nfsS7Pqwp4d7hLm7o
EFGPZxeIBHkwdwIBAQQgo/4BafVr5YW93S3cgyzCmvyHmwFyBXyR3Dosv86fkfyg
CgYIKoZiZj0DAQehRANCAARxy6iZUXq+x1siqMQcgllK2MnQ74X8Cj4KyJsEez2c
GSevPzFDjPohTmNlBn90o6iV77mDENhP2340oF5bb0W+
-----END PRIVATE KEY-----
```

## MLDSA44-RSA2048-PKCS15 (2.16.840.1.114027.80.8.1.22)

Use the following CSR and keys to test the MLDSA44-RSA2048-PKCS15 explicit composite algorithm with the 2.16.840.1.114027.80.8.1.22 object identifier (OID).

- [Sample CSR to test the MLDSA44-RSA2048-PKCS15 explicit composite algorithm](#)
- [Sample public key to test the MLDSA44-RSA2048-PKCS15 explicit composite algorithm](#)
- [Sample private key to test the MLDSA44-RSA2048-PKCS15 explicit composite algorithm](#)

## Sample CSR to test the MLDSA44-RSA2048-PKCS15 explicit composite algorithm

Use the following CSR to test the MLDSA44-RSA2048-PKCS15 explicit composite algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIRQDCCBqYCAQAwSzEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECxmGUETJSHVvi
MSYwJAYDVQQDEx1NTERTQTQ0LVJTTQTiWNDgtUEtDUZE1IFNhbXBsZTCCB1AwDQYL
YIZIAYb6a1AIARYDggY9ADCCBjgDggUHAehgcjlcjE3jlkB8jHMLD7skD0+mGM4e
44uwa+K+EFgg73lj01vp2HBIuBEik5tEVAvL+/x/Dep1dAGeAXkTTvplSNADfxIQ
YmUQwcYNGWYEdpwfWSFE8QS9sQurD5Gb14dvNWFbxeLVpR5uUa15cN90e4xqy4iA
pnh+n0kg0DM1oUD0FIOMzNMkf9KkcK4r5gP3v7bdCATdTUqSWR1KWboeE2WD9CSf
dv1Em3ENcpi2/VtAhlnsihFap8MfkWn+txe/5FvzsN5gZyKyiznR4a4anpH4XGFY
8dIu8Xv+mgZDWJ9kQ5VeXY90I8lKYL2puk+FmkB85z53CZ6Jz0QNSnferqqLoqC
e2YEK5RL+sJjs8R5Ax+OQ0dugFV1NmojQheU0AXcGoxdFjEjZ+ssaCed41JadFW6
hLX9oc/weWsLs8Q3WygdrW4LgV90QQf7thYShSdxAPdT+ZrXH7bLNdSfsqX7H6Pj
humfSRD0SqyVpMgsBBCKybBZCaihK5TXaZL5+HxMw1d2kjftqoxL5UA4bo443wA
dJN0SGfSu4C4v1hNcM7msHUuSR9bgm8uiiLaydiAaB9/NCMMVMQm00aK01eJIm
K1do3r4QJkS1XgASIDJhgVvXfHsLB4xRocLIoYoJX/t9pGJJULCW18o+GE+iWSGL
skGndiIxE/7afaDMwA1SxRI+lg6xs3og66mSULQ0395VkbNHL0jiShj+zhAtgB/6
7fSc2RDGKC5jxMhqzNCD/A5N4qThv3e1pd7Nv3FDH2S1qsM4hrUBtrI5SqNdLtwS
cVgM2W+3K1PKEVIRGNcomUqreqD9iXH6lInSvZg17WjwBvckj0lkgnGMYkZ1wXFY
Bswa9aiNyGQ6XOT/SjqQM4nfJ1fNyrU2JTfGP6vTeYB1smsotCE5i5mWwFCsmquh
FuhsWlexJZamjTvGtZ/BGikzraPopytxodcvsndx/m6JE+lexV21AfM3rPJMMTae
o0Noru/db0S2kzEXxBvG7KdCDqyi08AiWjW9HnmuIbmreLdpNDIGHHFiVXp6pw5A
G/qkfAtrRL4fv/YZTC4evE0ykohWSDVC+SAbPp2jV+0DdTHCty0UT+CpWBncpGkp
plod5MRbLTsklj3kuytC0AKZuv/e9SAAQz7oDCFHSi+f0H0s3mcLhenk69UmlbI
IdRUPvQxPpZAPAcq7sreJ96AnW/0XrrEorB1ACN/yUOGkcPH7BvW5TeMhMmfM2QW
tmFolzLVXrdmlzrBxFejHkC09p1up8PND6c+LGDfWmgEsLD+2jBEinsorCsFis9
T4JD8FIb5COHY9KJmSbjwua4MmTjNUTHtq2WoRMNcp36eIdSj0Boo86hfSPtn9LL
XCrypDgrAKMI3JUG6Gp3+VtdKx88Ijx0ECBCYU+gFzrJ2urNfNFWc7ZZVrfjn6wA
/HFV/nrSdGZU71gbaxdS52hM9Xa75BvD01SVjJLsF2bbhccq5njUTCvU8Pewzn0i
fcv6ALz5urx6t9aLuFAdCeAwcXr6mekrmn4NUlDa5MVry7060i0RhJ2WgCbZa5yr
cL2CI80NagnI4owNesXf6xNkJewSh6MacqTOu1DNdUMolEpsgKcENENVXJsZ04Is
Axbj5UXR0gFUqWlDsgsHTBCNb5At8Q2uTgEEcFlqucXqRMyN5tp+r8WV97pE2c1i
Fr1KZfJEC4Wm3jE+54CbbV/34t/z5n0U+0HrFG57qzWUGKdF3IkoMk8DggEPADCC
AQoCggEBALrTY9cC4IAZkLXeHzCfWGuAWVZsKzPXmmqs/jEexm/ENZA4HJyRIMrf
M+59xBe+mQJxnBm0pFb0tWjFRQuckt1KqkMGJ8bjUBKZYBkk8FHMslKlpQ79k8A
5mYovneBimZqPmd8s/oTkDrBGA+7fBBkONmbLgrvuGIKF9QH6jatUgwpPK/zJ8Gn
sEiTs0n4UvnR0cIRD+qnTK6vIrqIz/z7YZF2C7i3fv5QeZe7o2dfLeecSyYw0tr+
Hr/UogFISx9t0axm2Bl4lWhaW43o99HMPe1ENq597Fgpy3SXqrqWbrCWCvHzRpOT
6icAFVba8LYd5iUGTHEdkkTKR/lcFPkCAwEAaAAMA0GC2CGSAGG+mtQCAEWA4IK
gwAwggp+A4IjdQcjZcAK9+jleELvqjpwbiAZstekD30ui8JvVy60XPRLceH2fg1k
YoWzPBCYSM/VJrCnNxzswUrhcMgds88EYwmce5JDQsLK/8NPihTq06urGqxxKucv
y+jaojEEyU4CSKy+TDJdSXCbWWYpGd1fAgxJMFnr3JVy38Yif1oD5/0o6ljpr2W0
34cm9KF7YcPCFyG/unlhTGZQ+KBe8n/hh9U4ZjAH+UG0JMV+LUcAE0MYSfQkybhY
kbaF6yzzWE+kWA7mIfsGM0GmpBGT8cLr68lmbkUWdUBhuI6vqKmgzSIISHx6Cp3
c6yXKEivAqEiC0WnAtHqeLUnsKMLmIkcNNoYokCI876t3e0W6oHf4JxU6GAQdjE
Ty4UB9pslTg3K00hezcdziHkWz0eBcpLuJj0QwTPqScoXrw4Hbo28YI+GTJr/c5t
```

+0WrJA+Jy2uaCznnKD6LGRH0RyIV1bVLaqiBUZJJufmSalepjfDnTEeH4aUqq23a  
gw7NCIeqt7Nc7tAczrYhndknBiRWTtWMBzFaNUHhYN9JUXprH4QjKV2FGpNYAaSk  
9HKxNRnIDaNsW3J0g5gCpSSxxvQ8viPP8zzAKB/yJ6w9N2Ku+giT+abm/feaZIue  
H1HMzKnQzyo+iOmeq7P3pRLbegbLXMktKHDjSBwGqYP+SA7P/YLXKA0Lo6ev2gja  
yJzABptkP1EvYl/BQwc4muTmd0oDj2xvYLSngRXEY5yxdqSvHouePf1Ja9LtF6p  
ZqS/T98EkLG1LWIljVfEUtV7fnkJd+WBtywyr0vNUAhsKp2avPeto9K/MujicbP4  
xc4k+tn3/ZKZPKHcehF1h/nqyWcqH228ETaDXE7SqVRN7lsWoZ0/R8Hn8tnvjgY4  
eb7bNPaCC1llhxN+AbzB7wNB7qLdn9c70QWhYQ+J3zuiqBjTtTdfZVWiibSp1E+X  
Ze0C6hWzamHYSwTD5IQ7tdgy0MLyBrXSsVSs/ERNc7p1a5HRfmbFuo58vd/cUhXA  
63Y0Lp53+6U66mDLC8q0c02gq7vlt5LqjqDvZSG4UN7h09WNbNcY9uTMmphRGKAD  
Pdh/0b8Ru6NfBDLPW90QqMTLM3hSjzUdu5/w1HgcdWbHPLfQePD60G/LmBH0yW5D  
SpvrE6XVLWFSvN1YjC/cXCm3Zb6iavgRKPxiSxvTGKG2ss7/tSxAkwUJminD05S  
MfGD4GsMoN0I/zyN8mXhTaIuBeMUncTqNe4qhsrINE90frPhcfpyeNON3dT3NIMx  
ID4MNMjc82V6EUREluwF8TSYmBbx/JTfpcTDxhZrFWU1vdPdOCp+LsjPUaj2rNIe  
FIMHHoEKcpGV9b/wM9q0hRtRxem3lRcLBBizh8cxQq/XeizV2pNPATqR0yf/buv6  
uEhxL6nVzQYJoscnuib0krV/nU/wEJrZT4pHEEucnapYiQRgkZpcrGmjy7DpXBJC  
ZFAuyKI fUHo+rKrk9y08FSzfRb9VvRBVFWdNUGNMIRDzahEAzRHabSHBbmrdmiE8  
fJMy2iC+GuZW5uUtv8HIEGnRWV2JFXxoIJzTuoaZ8Q/rCE8KtA04YIjPjtFEJ3cb  
h0hqi+QFudgMDnCFaYi877lrhHSy9ztcp6szKuJzkqQI2u4nDYxLFFivAewVmNro  
qomr5NECCeLLQymz4J5ZjrTxjzxjq8FsiheEJOErZ6B4gKqvLJh0L/LWAnvTX9WA  
BxFjWPL/WkYExDb03NSL3RFpSBmS2eW0q7I4G00i70hFsZhh7UTF1/7guU7N5BKz  
0eH5pjZCCZglwVc0W0fQQbPXuZft1ZeP52nxUcSoPTQ8/1d02xXu2oAkBF66/Lwt  
2qgt12mLEhgH07D5TZKGoZSd2z8jCD8MskU/sZQJ6Xx8lD/qJNVmW8C6qMhLmS8e  
9yCyocsnrU4n4uv5UMqAHKlin8s5cR0aAieyYtqSLHb+Eq9JaYWzszTo3gbmPJLA  
pKts3BCVeysf0IlspPhrLV+GcbWBS07cFicsY2oTn3m74UQak2im3ERnz8rWlIXL  
ez77s/vi4PnoSi9fcWlvt4wZJ4I7gY/DfKE9sd+4cjmPhK0rM2P08yXBsNNE01e  
RZWfwB2+0se0WoFW4f4B8X3z1JGqQ0Qwp7PjXdwfKDOJ0753j/hAA3yR40F9GrnI  
H8kCGpUY1ogMDPMFhi0Nd2dhey80r2H2tZqHeSGY6/PoVsQIPToLQWVTrp8gnd25  
++gcyZDZGR0CusC03C8ht0x3qrtGQUdu6TIJueupZkPe9jAQmL7pIVsUbGUZVgJT  
iEHfjXlR5hCMH0+Uz0eKxlj0syabLM4Ha6SwcEmWzn19Q/fna+PmddZVrfHo5o1  
orwXF1mPMV15UKyCZh4t4HhPmmQAMVPiBb+dbA5LX4c0BZmc8ad9857Aq7P42DjD  
CGhZUHQ530GGM5ysKSF4sXcWbCzK0KEHVwsuAhA3dk6x65GIc/5MnUosb38AUscg  
ahoYTVdSwKcODWzr4KcUQPLXASu3Ek7DEivLkNxzj1gonQ8KB05u/RRY+bh/Hgwe  
L+GepEHZJbcWDHFAxopGVsB9Ztmw6BK2dulKY1AgNodC4bvvyfky7h0LEEnKKEZv  
smypS0N02HU1oEkUJQdt6Ks3dS6S1wNw309Pqy4JDGcLSpWfLUECISXqM30ID804  
SIltOnu9AqENDET7B7wqIvyvM/z5mnT3FJVAEdLToXsLxdEH53txDWmo3oNlyBmE  
RtdEuMZ8TWzoWpUcHtUo/gAlYx0Bhdc/qrm3u2RDfP1rG3wJlf9CiDX0zjF1n+ZB  
Ykv9QYlf72+xYcJckAoTF3wauufE/34SZ6qaoM9PRF0LJKlBdWinl7YW+qVc0+I+  
B88fZ5n3iU0e6+TVonPFR7jogrYTw7n0LFXIySsVMsnKazdW8sWvWNMLTD30bY3/  
C7HLu5u8jzsb7Mo0dtfwRblcx4rxw8xfYmqstNJ7Q4DGaJqFNyA+sRTxkw3jFN+W  
UDZL2uAGvZRZljFy3zLz8akhJ/NJwvdaYtRtJChyLKGi+zDHW4pEq3F0Uy+8VKCK  
wqjsnGRYwgz0KTgm+Uvim0cNWZTL6it3gcVmhs2kfxZEv4s1Ls4AbY+6LBAwRk5o  
e40Gi626vuvvx8xguP1pxdaXL3P40LjxSU1xpiJmbsrPHycrY2+Tm6v4AAQMFKzVm  
Z2lte4ePkp7H2d7j5vT6/gAAAAAAAAAAAAADxkuRQOCAQEAuCI9+M3YV5pwqipS  
NaH0qk1x1+yH3nT14Qzjq//pXhGbSEwC Xu8n0qmk+u1aL7aDpBGxIDZ6/sI/m07Y  
ZKIVQeuf7PKs/NmqPo85JTHRr2G1V9+1iE2PFitYBq8EYWilSWh/LQdSAY/l+ea  
fyYn1XhbfQ/OE8cJrS5mK22UQSMbnTibyRBgE+7BjPtEBK3KTPKBFom5Z7i3bGDF  
o6rJmez5hJ+yYp7yuZUVCKoyqKk8RcIga+3QwPlwpgbTriW0p1oJFLBCL0eskSAj  
4vhLSxrD34PutXq5KjMH8fL9iQp19U2YtmxVbz4Kd4rZHlHKUqAs1EYY4jU6VfnL  
mL05qw==  
-----END CERTIFICATE REQUEST-----



## Sample public key to test the MLDSA44-RSA2048-PKCS15 explicit composite algorithm

Use the following public key to test the MLDSA44-RSA2048-PKCS15 explicit composite algorithm.

```
-----BEGIN PUBLIC KEY-----
MIIGUDANBgtghkgBhvprUAgBFgOCBj0AMIIGOAOCBSEASGBY0UKMTe0UoHyMcwsP
uyQPT6YYzh7ji7Br4r4QWCDveWM7W+nYcEi4ESKTm0RUC8v7/H8N6nV0AZ4BeRNO
+mVI0AN/EhBiZRDBxg0ZZgR2nB9ZIUTxBL2xC6sPkZuLh281YVvF4tWlHm5RqXlW
3057jGrLiICmeH6c6SDQMzWhQPQUg4zM0yR/0qRwriVmA/e/tt0IBN105CxZHUUpZ
uh4TZYP0JJ92+USbcQ1ymLb9W0CGWeyKEUCnwx+Raf63F7/kW/Ow3mBnIrKLOdHh
rhqekfhcYVjx0i7xe/6aBkNYn2TBDlV5dj3QjyUpgvam6T4WaQHznPncJnonPRA2
yd96uqouioJ7ZgSTLGX6yMmzxHkDH45DR26AVXU2aINCF5TQBdwaJF0WMSNn6yxo
J53jUlp0VbqEtf2hz/B5awuzxDbKB1FbguBX05BB/u2FhKFJ3EA91P5mtcftss1
1J+ypfsf0+0G6Z9JEM5KrJWkyCwEEIrJsFkJqKGTlNdpmXn4fEzDV3aSN+02qjEv
lQDhujjfAB0k05IZ9K7gLi+XWE1wzuawdS5JH1uCbY6KItrJ2IBoH380IwxUw5C
Y7RorTV4kiYrV2jevHAmRLVeABIgMmGBVvd8ewsHjFGHwsihiglf+32kYklSUJbX
yj4YT6JZiAwYQad2IjET/tp9oMzADVLGsj6UbrGzeiDrqZJQtDTf3LWRs0cs60JK
GP70EC2AH/rt9JzZEMYoLmPEYGrM0IP8Dk3ipMe/d7Wl3s2/cUMfZLWqwziGtQG1
GLlKo10u3BJxWAZb7crU8oRUhEY1yiZSqt6oP2JcfQuidK9mDXtaPAG9ySPSWSC
cYxiRnXBcVgGzBr1qi3IZDpc5P9K0pAzid8nV83KtTYlN8Y/q9N5gHwyayi0ITmL
mZZ8JKAq6EW6GxaV7ELlqaN08a1n8EaKT0to+inK3Gh1y+yd3H+bokT6V7FXbUB
8zes8kwxNp6g42iu791s5LaTMRfEG8bsp0I0rKI7wCLCNb0eea6IGat4t2k0MgYc
cWJVenqnDkAb+qR8C2tEvH+/9hLMLh68Q7KSIFZINUL5IBs+naNX7QN1McK3LRRP
4KLYGdykaSmmWh3kxFst0ySWPeS7K0LQApM6/971IBpDPugMIUdKL5/QfSzeZwuF
6eTr1SaSVsgh1FQ+9DEWlKa8Byruyt4n3oCdb/ReusSisHUI3/JQ4aRw8fsG9bL
N4yEyZ8zBa2YWiXmTvet2aX0sHEWN6McpzT2nW6nw80Ppz4sYN9aaASyUP7aMES
KeyhFywWkZ1PgkPwUhvki4dj0omZJuPC5rgyZOM1RMd0rZahEw1ynfp4h1KPQGij
zqF9I+2f2UtcKunIMasAowjclQboanf5W10rHzwiPE4QIEJhT6AX0sna6s0U0VZz
tllWt+0frAD8cVX+etJ0ZlTvWBtrF1LnaEz1drvkG8M7VJWMkuwXZtuFxyrmeNRM
JVTw97D0c6J9y/oAvPm6vHq31ou4UB0J4BZzGvqZ6Suafg1SUNrkxWvLs7o6I5GE
nZaAJtlrnKtwvYIjw41qCcjjA16xd/rE2Ql5ZKHoxpypM67UM11QyiUSmyApwQ0
Q1Vcmxk7giwDFuPlRdHSAVSrCU0yCwdMEI1vkC3xDa50AQRwWWq5xepEzI3m2n6v
xZX3ukTZWIIWvUpl8kQLhabeMT7ngJttX/fi3/Pmc5T7QesUbnurNZQYp0XciSgy
Tw0CAQ8AMIIBCgKCAQEAutNj1wLggBmSVd4fMJ9Ya4BZVmwrM9eaaqz+MR7Gb8Q1
kDgcNJEGxf8z7n3EF76ZAnGcGbSkVs63Al9FC5yS3UqqQwYnxuqNQEpLGSTwUcy
wsqWlDv2TwDmZii+d4GKZmo+Z3yz+h0Q0sEYD7t8EGQ42ZuWcu+4YgoX1AfqNq1S
DCk8r/MnwaewSJ0zSfhs+dE5whEP6qdMrq8iuojP/PthkXYLuLd+/lB5l7ujZ18t
55xLJjDS2v4ev9SiAUhLH23RrGbYGXiVaFpbjeJ30cykTUQ2rn3sWCnLdJequpZu
sJYJWHNGk5PqJwAVVtrwth3mJQZMd4MqR0RH+Vx8+QIDAQAB
-----END PUBLIC KEY-----
```

## Sample private key to test the MLDSA44-RSA2048-PKCS15 explicit composite algorithm

Use the following private key to test the MLDSA44-RSA2048-PKCS15 explicit composite algorithm.

```
-----BEGIN PRIVATE KEY-----
MII0zgIBADANBgtghkgBhvprUAgBFgSCDrwgwg60BIIKBASCCgBIYHI5QoxN45Sg
fIxzcw+7JA9Pphj0Hu0LsGviviHBYIMBKoaAl8odQ8Tfy17mXe7+bXrKtMkaLkFsk
TQirgQzxjBv8b2YNfj480CV8rMYuc+/qQGd3IfcR8QI7WbiIcuStrRw+ePenVgmv
LLtcSf1eXh/lpp3YSgaFmEUxriavCOI2EARiImkgSlqogRuzaFkQKcGGiUw4iAy3
-----END PRIVATE KEY-----
```

ZAtCkgMVTlHEa0ISSZBIgKRERhFGbBgIEeLAjYkmLmGQLKKGIYyIUBSGCGPGTRQh  
UtyShQAKihUQKNJaogEbRu1ASRBkSMhMAJEJUwCRMEWBVGUKSMmJQLCTdgYTNsm  
ckIGReNEIsHEIdwQTEsAkPE4ihJDQkqYSGEiaOKkIZgwaNtCkNG0hBoBjRHIUNKw  
JQC5AAGwcJMGMMYCUYswQUCCQR0hCeEGjJuQiQK0AZkoUhLDARmxTB0CjMFCQQpH  
EkAwMMOATAQziFg0TROlcaHGKZNABQknSiMTTRAAMBMyUVMyIQQDDFKYQgqkhcsg  
KcCohENGUtiYjYw0TiKSKi0AadkiYFmYABIkYJmQSRsZaASCaEpGQdpAhECYMJC0  
KKBEUJJITNqkANmUBEnISiigKNFEiiEmCtCSTeM0TRuBUeHAGyOUBQgiIkaQcpSC  
LAsBSUkScECgSQBHicjAABsUMVu4UJSGMVxIASzIEKMYjEGGQAEyLOQmJlkIkBAX  
kAnCZRxAJAWA0aAtDbRyZQdkSbJGESYMiisEEjARGiREkbZGyLUAGYNoEKNMUEgIS  
BJzAEYFIIMyCJQijRjM4kKE2RhPADEzERGAITZEWYBrJcQIohGBCCGQUMRgxLlu2  
gdE4aRKUudg2TkLIJQAigIrEYAI2ZYKACBIjSAuRaRKGBBxAQJvCCVwoILAEZYgg  
QtMmcMu0YJRAJiKImUKI2YtGYZBSgicOERApJEYE0DUg4ZUMAaLAyhmMWQqICCOsO  
DQkojSQ1BSOZiRI5RZCiJKIkTQyjiBkScchCCMMEjcyEjMzGjZgQYsgkAqE4bqII  
bBSjSS0hagNqEgBKIMCQZiPkiCIss4INQkhFigKQQQgOMWafEoBgAFYVUyJZy2CF0m  
TEpAKLSakSQAJIOUIMoUTVskIBoWakJGEEhCIINEEcggjYyyAWOUKa0wSukQSSNG  
bLSmCMygBAE2DYgUUAaiapkoYEmmadwyAg4ewD0Tg5N+Ex6+hUDyLtu1tQnGeOPR  
jzpDuDD0ZU17kzeUebbz5ff5EPrFrX53iyA1NHQ9y6sjsHBCrU9h04F3Cy3dxzWq  
5HQibiNiW1J0Xu3NvBIIBL5U5UozAS5eyffheGc00gtmD3mP89vhPCbYE0xjz0rs  
El12BcxBnDRDPNphtnkWzrDtFbASv0u0wi14HXyGTZaQufiECLUUsD3s0pC2/Ji  
0qsQSnvcQuS2mbMKfUOXeb734rNognmAqD7uaKwqqP26McTzJ00QEa5eIt0kcrZf  
tRNbZMXnEDLJilps9XjWLA+ORhF5qgo8yv6s0bNn9SjfwAsg/BlhIILR/CEgTQn  
XdYmlJDuTexqaTUtu7EA3tVm/mhn9xIqKbVepoySzqDEhz39eQrn3/q9RJiM9mY  
pvWnA0Db3k5KnFMS1J0j68ssoCYjuBeV5ereAPKQHW9YseffjG17xijfv9Z5XHHG  
lorvqUSRiyzU0fKktv5Kj7cKozmfYxmRDodiYg8upvv3frAMy/9xyr0/dDhoeN9uO  
rY0MhipdOhtwekubyG5tjdIrzFr8bZ/Vw54geJ2ZKPmkBowqcsGHtKLYQC0Deaa  
fDPvrLnYb+WzaKiu1pLPrJj1rM9C4SG0eBs4kaW9/c1mzKzmd0VnFBtBC1L5MwVO  
xNHQEii0zQeGY9glwqCIPjXRxffBwvf0FbKzB2aYyW4d6EGb/+6m2YiK/Tw1xwbq  
EBMnvKnbgKYf1uk6h9X6JBTWrA1BPGTI4xUVDHQsBXBuGIPBFRBaH/97UxQBghL  
LwMqwocR13BKGo7Yomy8ZdaPbKQASuwdzmw0xI1QpgpcNx8TP6KHmDqG9KYVrMx  
8EDK3s42TD6Kas/gBy5XtXchtZ8AXE/MQ30DzThKlgwtPSyGrQrj2Fy0EKL56S+d  
xfKrR93Dtw/g8ujkImPCIW0b0A1GpmbmJnmcApdCYW8rIGDkaAntzdZJfy3jFv8U  
to2qzytU/C7i0fnGSuJjppqNvIfS0Boz9Pou1NKawLBnV/UJZl9hENkz8gy3MCkU2  
qMuOGTmWzyPDEYIXSmzmbSkqVv7BzP463VFcJ2i2bUiW1f+qhs46Eu00zix+USb  
gfupeGaCzMEinUM0tVGcqmdPV0WSbrpFzz27XoMIweE34AgoQatXB5GksXUMC2qT  
VW6WCTH1xecpI0xarBC4uGc0g4YfL9sGwBGBHJLJ3GV0+rUx2bT19x7uLYOFTerg  
vYVeniwR6jochK5Iu3XsQISn/T1RG1o1fl6Jd582XojI3JZwJwXNZFJR/nrAqHfH  
gUzJkX1F5zqxsofPKyiNepLr7MXcgZDzQFJmA8WhU+saYSK2qw8806tdUFFWOMEp  
zwWxjZ8GcHgmXNb+tl7McV2p9lXrALwTfvFU9aLN4jf1EyN+ZsebCtUsTBfPvtan  
tQWibdh8+e6T6NhcorcaOXJ8b78HVNfa8uQhH4VGjEcHKDggOPmFH1IsVqAX1X2I  
xauel4Yoc9sapAj5N39I0J+hspThJUrscsx7KcGaGtvihHRRPzpgkbHj420MyrGy  
4+7IYwtYrZN1w4yTbdPS0xx2C/pYQ0h+CEJ60/nPIqQ0t3IuiqEa2H0lxhl054Ka  
2d412oNfLb0WhwgYu9u08N/sHzRsE6fL7VS0nvp++LN+ME9HfL+VrVs+kHednSDU  
FL+s4MDu+RUZ03IorZMTxbRRRfLftBUXDBMNxeiiwjktMxdHSyInrYGe+Xht9+vJh  
yvuZt0ZwOgTmadlnvpd6ikFg/J6DAw3q/WKg8FL613QLc0+a44ciApQAp2ux7aZX  
bDK95YrjLHh181rdMQzpQS7oJNks0bVud6btYuySUUtJhWanYg4KiEbNEAwWyjq7  
gjr7qT7q+0uTrrTkGrbmnuwZyJN65+f1KjLaQsxwZ8owLrMd/Bv+zRF5qq8myF/  
mGZtEzYd7mfs8AsR365HTttJGaSzYQEBB8Gkf0JDoP/YqyvAF2m/TYwFRs3RLxwe  
c5P6YP3RXV0lKcNwTLbiFuzyrf/Z5KWgXWDGwV2cBs17KL59e0K2T9PMPT3pirh5  
32c2DoiYYTNgUgsv0AzUkQ1PXSkA939LUm00LZLfa/2Ikr5a18TK+oZ/7HNp7PjI  
/BPnvinreim0MUQVY0esIMq82mwG9pGxxKIhVpMkW8HqzRUawoGnguXc79xyMCU  
cdwJ85FcBIIEqDCCBKQCAQACgGEBALrTY9cC4IAZkLXehZCfWGuAWVZsKzPXmmqs  
/jEexm/ENZA4HJyRIMRfM+59xBe+mQJxnBm0pFb0twJfRQucktt1KqkMGJ8bqjUBK  
ZYBkk8FHMslKlpQ79k8A5mYovneBimZqPmd8s/oTkDrBGA+7fBBkONmbLgrvuGIK

```
F9QH6jatUgwpPK/zJ8GnsEiTsn4UvnR0cIRD+qnTK6vIrrqIz/z7YZF2C7i3fv5Q
eZe7o2dfLeecSyYw0tr+Hr/UogFISx9t0axm2Bl4lWhaw43o99HMPe1ENq597Fgp
y3SXqrqWbrCWCvHzRpOT6icAFVba8LYd5iUGTheDKkTKR/lc fPkCAwEAAQKCAQBD
w4b0JwP9EsIkQeP4Q+PTYk0F0EjXTf2hccvLTy9UvMtc2y1tkKpc79crSwzEPArN
ux20qVnubp4syxeFJa6Te5CULPhiXLe3d1BG7oIIeYEh2zkqXcmosHvDho/yInF
qgWmjBHOJChT VzP+Alf2rhN8wpVctD6huN15t8E5QTaq8g6Z6uZiuS+10cv0dcVS
x3I46lWa0tIyyV+T/tjzmC+dMKLzQd7kirWxRS1J4iselQnTV606tVqpsapVKkY3
ZjoP778Nj0HwCdrWduYnzx3o7IF5NEXNW6Cwonz2x3MnNbkZM4pr21pNikZhWdf
yG4ZPuX7dfvWIM1iGD29AoGBAMGMG1gv6dRMSz1630xikcPacj99Fwzc3IsgtELy
gqJwsjgkrSoy62xMZ4/i9NU7ri+1I59arjaKrG/6f64HuOnDAgJy48EVwhv0/6aQ
LVecBUJw0/xgUbV4Ai/X1UklFyb9C/kUIIwM6rMnaI2ffSYi4Cu5j+KagsdFxJYL
n/A/AoGBAPccDWbtzcSQLSuGaoMw0EWBHiqkciFkVgSg1ymG0weHPN6EktrZzn8
91opJEGjyX5NWaPVDqkrFTgaHbHfunx4nXlp20lcD9MbZQlFE6RcBKRMr2AvPuNy
57DYyUGro20Nd8hK1MYx3fDfLjktPDw5D2C8SYCohcCHH74zyETHAoGAIHuaLz/D
V60CR6wyHb4hRqAqzHr6/l6m6PaxKjc3M3oEfyWwpk9rcX6VNvHZM1xTzI/zDZCT
gnXdoOGCwjtrjlf7I1wS21oCfNZN06+I3JZDz7W0a5PiwrkEbPELS6Rc8V8wvjnh
iH+2eCDaDELdJz5dLxlyi45w+m68IpLn99MCgYEA3iQevC/9Mb4rWKHG0oN8p68G
V/9mRu+f9l+2LXy5v2S2u/46IgisZInPRwMDL+rwgRVCBzDKHD05wJRhq3ynpau9
wtfPgoEbTLksy/eIH9IE7jpt0fbG/ytVszo/OkT1Blz8GFeFDaLYl0fdIt0v99+H
vnulS/6zNo+CbrCYsXMCgYEA10l05bhwjtftyt9iGIYfHij3Vphe+yZKChxHnLOHT
8a9uKKKoeGkklZEhPaB+00AGxys/8XdTpsShe4kf466C5wzh5LaBwgMQenq0hLxz
xmLVKtFpNSTWblQJpP1XYQwSuZ1BRReE+qrXwTXWkxALcGN+KJv8qX8pvvjJZEFaL
frg=
-----END PRIVATE KEY-----
```

## MLDSA65-ECDSA-P384 (2.16.840.1.114027.80.8.1.28)

Use the following CSR and keys to test the MLDSA65-ECDSA-P384 explicit composite algorithm with the 2.16.840.1.114027.80.8.1.28 object identifier (OID).

- [Sample CSR to test the MLDSA65-ECDSA-P384 explicit composite algorithm](#)
- [Sample public key to test the MLDSA65-ECDSA-P384 explicit composite algorithm](#)
- [Sample private key to test the MLDSA65-ECDSA-P384 explicit composite algorithm](#)

## Sample CSR to test the MLDSA65-ECDSA-P384 explicit composite algorithm

Use the following CSR to test the MLDSA65-ECDSA-P384 explicit composite algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIV6zCCCHMCAQAwRzEQMA4GA1UEChMRW50cnVzdDEPMA0GA1UECxmGUETJSHVi
MSIWIAYDVQQDExLNTERTQTY1LUVDRFNBLVAzODQgU2FtcGxLMIIIIITANBgtghkgB
hvprUAgBHAOCCA4AMIIICQ0CB6EA5PRGIp5KNx0pfWTCrQ7xkuIB5m+KWFVyuwqy
FyDYULnMf0qcZ/6sIf008tzKZVzjaTLQTB8boJGKdg6c0VURJtrE/qiTA6Ro7tAg
FVASwBcKdQLLhf52R57aDtLkJlNharrrtanM/N/v1dB8InwiRbh2V8ZtC0tEmTB76
nDILYKQfH6Crs4dZWpdDin+pqSPaH9y9eFoByI64aF0eW7fIOhR1d+uWdrPABsc8
60lV0SV4+shVy6xdH+niq/GXD1l+4dy9tuz8Zbq84oRy/en31/uhqs3B0PLDWkiV
TOZU6TEfvubwRDMehUokMmXbudMoz6E85ff2t42uKTWEyD/RV6yPsqT6sb4ywlsy
8RAKtMNWRG3nA5fuxyyhkeEfr69z8PYF8cLgWCSec8X9oNbG0t8bAjx5ouTDYwvA
MArFpMhpJwJWNZ26xMKWhG5Es7jwZS6Hqxyse50X0h6Wl0BJ+qehjv03ucFxtI9
mjfbGyDtie8KkGr5sp9CptV/DgGgUc0qbcRd0bDz6YE2UF/rejZi1nFSQQQ94WLz
FYRFaQcPjvSLleSZ86z4Fk/ZxGfHGTawjI9Pho4WlFaPCn9Yz88El0jJDJFYQU76
```

BV85PU0baHV3xBRttVoOxxzIm+K/10yWL9NKlxbCmsnzdNy iX1zyKzQ9/McNrOJ  
8ek1/PsHRdMa7QebgUbGS3G0rqtn2S1lh5jCWu/ZPoL+q6ZVwAbw86z5jux8prRV  
3Ct2aMGhLRcFFgcCqUytPu3/uHWktPpbhTJIElDYAihGF56eZhsXlsoGPgtKbJG  
4yZ7o+AjmcSN2qjppgd+0w3wwghznIHMD8Lfcx03T7n9oKTDfGVlX2F80HeHQkUw  
a9h9D7PJ4gZRHk66bUNGU3uF8lmfjyyYjs2iw6LLVcpLNQRKpTVDeRYXWltR5vVi  
5+A4S8SL5RLkKCaDLQAzm+HCgDVFWMY0QWiQ6fHVQJool1FAwzph3f+2WdZI0WZk  
NIXk780K402/mIq4wGeIMU67MK6RpCs1mIb8zfzvoXg4uBE2/7f01tbIRBu9qmSa  
BiHYFruZEn/6L4AQiFC/nGX02cYMM9EiTESataMp8A14HXKcLwWobZ6tTsF0j0G1  
AyEaXVcsBrfcXwiLCBeLjhtP7WizrFG0q3GhD4IJCEIVNdZ8Luqz4Rs6gON/wUOH  
bIB44+vsQeilhelTfNWKck0uthIo+sHh1ah/UIpmpvsUTUZ4Hy9aJWt4ayK9sTcB  
vktA3vQcTmK5lYE0fQvgvOppTpv4puhi+12v6qZBCZD6l/kjxDp453/9Vx/UpyI3  
Fj/rPztdkUQtB5fkjD6u+dgKNcUs65KSX82wegw5Yzm2DAKiU7tY7ADP5V0ExE4t  
ofrymMBUB3h0FzvLFEZuRxdTj0nGlk8/953EJCWM9NkB9qVSr fogve3UM1/dfITF  
aLgoQivG/tUK/CqJdfze3JruL86fwt65gwfrMyVj4jGJ0YlIBmAlxBDo2TybiUpm  
CfRQBeaolIrEoxBEthDVsj iAyV4+M9oIszB5mzkoS1B2lAoeXaf6/b50l4x0tyAq  
jmLNM/uGutjiFqCDUQR+mBfX4TZYkxzzVr9SKB5H+pLg2f2ZVhqaPSRiOduz7Q  
dkE7cVbtwKDuUvpj70jJBIQ2+/7bo/6cJsVNByqZUbHJc2wVbTH616uLXCxw2T9l  
jhfdls29LIbiE5yFWsgOxBY0hCDa7myN6jdaqe4L3+s84rSixyc2n+5apMeL4bLk  
erDaZUdEeSsgNNLhYd7fGfn2ITC1HgmWsSR2wD+Y7nbbTKFbPBqqMH1EUhiFZZVt  
Hz7nSMZlndA5m7n+fyckP1g8FS1SBCnGYUfwlj9IvUfE5LnOHTc1WuCOgSA4g1k  
YQY76p0i97ARvkMoBU7AMkH88Qxx/dEjV3qaFT3CgXczEsqixQhrUpQg8pDMuOnp  
Szb1Sll9Lg5Hs54XKkyQDmQDiEKvBSsblHq1yXFT6HS0J5s0Wa00CCNGBJg9PAMB  
hee6cj0mhQxQyXgvEkn5GZm/BfoIAoNZ4CEcd60PI3lhF5Cn4NXDtxAKw8k/c0Jg  
g/vuxAmsZl7f0tnrH9020adGT4sy6Cu0YDZHb9f54Riu7IXANHXlQSPT5n+2hmaf  
KxFERL32dsgINW8vH9+nCXdnPU/sxA0j3sh+xJFrjRApLNVGdLUarkUEIt/+HmOZ  
tY7lnmu9CnX1FLbSt+pyqCzChqHcbBNDLdM0n3qwc7RaVfMMst1XPpgFoJD0/Op5  
skYVYo9skDpI2qb5Hnp8wVxNthvYlUTryPnKgrPH4aMeIrUbmGK3VXonlBs0EEwb  
IMb14+c0PDNeABfDaxeB8M3hTLb02uE3gGtQaRcbDI fJ9tRsv82mVY2UkA36g1AR  
mQDH5mN44J1QjXUmlYhhmc9ZKWvgpatqpc3HF8xuMbu3w2LGNsQ9GHAtNzpSWVB  
j4Nq50tWR/1gz0A6VYhTUNgYffsJPkdI4+s2BRSt9/QfINXn3iL1b8DvtG60LMV  
KPFiofNjQOPqtWRte2R2s+2kZ2mxZ6kNtKC3ViYDYS87N+Ph/OSwNw6kxX+MF2ck  
HgsE73QDYgAEDRRxuokt5cSSpnX4DHMD2URAZUZlS iUgd0HyR4QlZVdK9lPmN40Q  
I1lYx+DAorp5YHM+CkLNoZAl5yUIjzhQtm8DjH6FAcQAw98+9nySeeldvMW3eFw+  
uPP/6QU08M9boAAwDQYLYIZIAYb6a1AIARwDgg1hADCCDVwDggzuAMzUv2fgDb33  
H3SjETHos9Pn9MZ/mx0qAKH439KM8XuN45UVgAWOZMNI/VSpPPLWZ9bsDg02eBIX  
UGGbIH+2cGXuY62Vodn3ziG8Zb3DYxHN06kv11vPF0pl3lFC8zkiZDzZNRrs6v  
7ri9YlTfbQxft1cEoisqhFEeyJUcpwcoEfN9aixny8tGNGCD2Jtq5Rnuw1zHdT0A  
UqbiA7lrIX9jsQuEBsMD9qWfX6yQnCTJYr1Jrl9/lTd7finxZ8XthNrUNVXYQEc  
yQenJU1fEW2UuZXIm0KkBWDMFfpPMZqWQpgTo1T+RaKNVafvgiPtenW8t2CGzvHq  
UJibDXJVL4/JduXFQddUn9wPlRPqhCODD0emBb7kadiQxb6v/1Yqu/Qpd0ljMFGm  
e3DpiJmJ4vxQ9vosP9ynUeZKyQptZpp71dI4oTCqUzQs7o6R0kyxzzmkNUSl2Wo5  
XTf7LH7ri/ziWpto7rqbJH0nylM4kM5/nUJoJXdmZ7EH0NgjJaTInxZDQq1MH8/X  
fV7HFxbITabvy2tY5YBhSkuv2ggAL4fBS2spDn4vZ19lxY13HR465fY8GrRq1pW  
4rwiC0MwHqNGuDRI+y+dmCEIcyortYB5hjP/Z4rKT4o4QBAOmFHOWjVoffv9MER  
QOFFwrc5Pfr09X0ch8eoLENhNf+uwFtIloT6r0bgOD8KF0u2bnlI/MUNzTJanQk  
OzwkFZLi1I8BXdx0t4xglLaU3vr+EVogg+z41v5zql8JCrnBRdxB6oKonpOK+kGD  
dzWoqxZlTIKoLu/z1nVa8yUudjnAVscbwIJrR0mnH5RXeXIGFB/uA/Qvzd88n7B1  
2LBK0fz94D0mkKdM+Pe2ITnsTRAQHI3MkKbF0NGtgC1kR134n46/I8L746e1Gkr+  
y3cv6rIqIluaXMeW4cK0WiYC7PD1C1a3mJFpDZ7zvCD6z05oRft/VPDEg2fRWdJm  
JWGkYwKhPlr4xv77soIqrtdsyjrXLFKpQXhln8niAqnlecDlLtLndxNFe3zRoBR  
lNrZK6fdD/TZ7IC7GaiNqx1HM/XqQ9UDpoxZMfCzIJLdPCSDoQ8n8Wdxqt/7N5x  
sUYXKHvp1GPhcU8cNOG89gddYeVpnxII6B9BB2xW/MVvaeiUomCtLZYYzJeRWyY3  
iY0iwY0HYLE6Cm5SdE9RvRmId38X/YulpossgHaEjLiyZ7nKXp+3kARdKHLkXGU9



kaKWryvczfYDi7z8ly23mg4B2WWLnFUcfoUUMWVnn0AmI7KgUFGrvp+i4vJzdyX8  
rDcvp5e32vp8a7L0azUn5qDXq305NwSmX3ha9oXaznxkEQgHVbhpVDN3510YJXHx  
p08F8Tr9kKKoMfFQJ67q6Ljd1km8Y/crtNxcN0KEchYHwcj7w+pJJG47K+DLxjC  
5KnD350YXHMU0eU4FS8ZvW6/ZdVwCAj7w0oBvh15XYn5tU0uMCCYE0+HDlClRzkJ  
xprF2uYD5uZ8W6R438K2iAEm2qYW0ezmmj2B/72mtls10QjsZMcnPnUBdn2hwJVX  
y5xhJ1MuE0o5Y4mgUcCf/hc0KWq9wd+h8NlIyS9b2wgY2d7HDBXJ2Wzh5hQ3xeJY  
E5zyiGwE4mPbvmjaFPuc046Txkv9ZfaSNRNsBtzNht+RVXP46DDIOowPcyAW3kSo  
mUKaUr fuBek9JTpAE48F2Cd6wGsGQmmhR1qX6a9KgPG6ZTQrv0cZPXLgV4I6EfSl  
lcwIl4XAsBb+i98uFr08btDzvPLCK/C7YnBxfi6zLzX06eKo5owtOnv8VQcUNl0b  
IbfV8kL1czBqabvuu1hiGwcJKSFpqCUfZkvJMryWdVUTxQoKfQRZAC5KNsdVP4J  
+rAoWo4v0iBCWXYjG2uJcV0zMSUf86LzBwB6EDli9fez8JKZZy9Rn77s6ptCyAlU  
qr/GZXxtzhPtLJ53a3bDT0g6N9JQqfm7uh02z/RaV4qcN76JwEfZRUVT4DwQRSpl  
kTonv5wV4JAEoQ5jl9/T4VL7tg6JBx78qCvEbLSMYmrIXNZfVIYXLPde9Q6SALNM  
2Q9iEAcLK2yYpqYPLpEX8o5kzQcRDB902ScoxTSZgcT2v7Y2S/0QWRCNU4Qb67XI  
CXpbN0AUcS1T/iw0+hybfnw+f5zn0vnE9Ay8lBGhunvXjorDymthxz/xUl1XmEYI  
ZdVzNtRoo++p6vQS4+AmZgogSd5s0sgq+EKfCmGFpjxyIja0C6mG7IFeOZDRNdLE  
XiILpuYPugK0c+HGXd0artDUS6xD0JsLcUZj1e97QhJca4kuZTgYg03YgRNMLk+O  
x7YGdLSfzFZpGcb6YYyz6w2LfyBVfYX7mrrfGwiH0KN0cB6gLvtSDQBHfb0VMxyQ  
Bg4Te/EcMbr5f49e7kuJ4s4FCLB2WKw0cf2E3xXUPc6C293l0y0+MB9vBk9LrSl0  
xz1aK3pcX5MP0XDJFdQ4r4EZLgfs/uAuSEoPVMQ2jBoF9C1qRfiVkkyaLLzFF5la  
ZLsgnMNnWew/FiknN1kMNC6DE0x/vja7Gjx2k9UsZXRgFrLj4QpruCh8U21xPtq5  
h0BphsGNqmtodEhVzZja0FIHu6Snge18P6SCISldH2Byoa85dV++ejKyp71Z6wM  
PvwQ/H4NeJMff+4HFD0Jm+50viUjp00Ff0EVEba3TpGft+9H2YvcGd7fhj1sB6NF  
xB9Xn5dzztgtn2UWMKVNfZvieQIFsNd/qL44NQ8hoEpRfSgQEKjyLHbPcrchMYx0  
NWMkpQgPOTXFHZZvGwp505ovpLmdWevsY48a9quZ5k5DaaVpVP5Ps1BgDRMYM5VXj  
aeDQ2t1/eBz30C4JT1HwEnH9Y0DBJ0CSyUG0xl7Q5+sNkDHkYqnnW//GcieJ7nQc  
v6Gd4zQ9oJEp8xlrI+jZvWn71qvhqs9LXjJ4EYH09xk0xX4cEaR0QD485FVFPIA  
oyiaH8EBH0xpgqprKKQfW+qnIUBXKZNCuVpztV0emPLxoznIDxUjn77yUpE5/Dj0  
hw9BqlXWjEimD4Jxkh4SwWRGM35jUIbmdZFc7G8k0y8FggGmnxGnqxyNhMWK+iDp  
7IcTdhpk8+pu08/XLIGivp2K36LQUMBxnePtffiHfCsY6mnr9uo62x/3B2J4up83  
gqDeFrrpgvLjtX+0kWTccfXKpB/e4BXDDXHInjeFyXHigGY8No/T0k5wLsizB4tZ  
abR5vj0TRsfpSioL2bLDp0GgYup0iCcjpKqXVCNdET7WQLMVswBE0F7Qk4S9zfIl  
ktuzssfeHsxg1QLfBSG9Hq6u+5U5nmcP5LQ1Qft7/dLJfJv5uK/FMR9TZENrC63C  
J/11Kf4JW+aobt24HhWHK4oHKCLM8hDlMsQMHPtxDnpXgQxkuj/zoCThBblVe5jH  
t3LBhBhkaa+b45YCYtRFuxeS7gOLNvFak3/9tJJ0r74UHUfQOHZFh6pBZzhrGLqA  
gijFdWnYrm8rLhKjBXR07U1pcijDttjKIRzDb80VmoF0KTbheCd4jBORdP0Vig+1X  
i/eyWuVRfgf3jrlq3VqDP2hZk7KCBkG9h4EKIfAcuN42rNIK0zsOLQI8ZqC0rt+c  
QX4cgjJ4f9C8P0PVK0z5ou49SHNgvDRY03c1eDJ/dVNJZy/PNOBGh0Egj7YlgYG+  
v4++hdi0zdGL1xB9CK2HoLGCzx0VTmEEBupikEMM8RFL0JE7bUoYst9bGSwn9ZQK  
sv/rY+zzqZYIbWVRgeFgv/vyrrty5eevwbRAXi0I1BwfrXgD8F37wRE+iVZOUxpz  
NiFSKD9EbXdnazl2v3Ud8A5hLWuQ0oGaFRKudkDhw/VDncKxJca7XfkG3SEnQ5MD  
1K2Z4+3CxEBEU0pXKyG5z6b1d0uS3HBGcYppcbbuEeUrdqBi9BmhEqTmmyeBT8Hn  
XmeI+83nATTTMVZ/I8micNUH2MX9XKrKS8zZGYyD3daYuncZEgn/yHGSJ5/WI5kM  
XNgN+qG5Lb4oYWM/GbGW0q1v/QIm/VnHwkrhen4Gctw+mL9rV/Oka9390+UzhTOM  
lARxDuz1QBTpvkawVWMbs7DZf1bzmj20s6dk8pjnAkC9FX/Iida+KATdN71N2qg  
wWlegrbJsnVKWRhz+gbRzJREV+YmMcequkFsmzx6J+oVU4zrCBYTHoc/lwveKXP  
5QmqhuuGVHbhch7yM5vTZW/9IRivfMTvhQnQbaCKhb0Li/Z0ftF5mNB3Zbg/P/CF  
/S43d0gJRiTk0cSSb9xLfJ4s6+xF8JDb1b+Q6nALRrCa5srZ5Hosv+6L5ViBuh4S  
GQBHERl4jY7/Aygsyk7M6YHuRn9Nx8zuJCxWdXydu9bd8AABEkFSj5+uvdAKCxUe  
HycqVm94tw0w7RE/W8ohmAAAAAAAAAAAAAAAAAAAAAoUHyImKANOADBlAjEA9rLw  
N6BBuj50CpvMgykN9mHnroRxxKF7tiUXHN9ZWAYVlQvvnYUiojeozML6og/AjAc  
y+jfjSgw/wry/3H9gdnacubdVcb6g7jBxTh9ySZuJNwIB01Qw0f4zB3/WZPyVIg=  
-----END CERTIFICATE REQUEST-----

## Sample public key to test the MLDSA65-ECDSA-P384 explicit composite algorithm

Use the following public key to test the MLDSA65-ECDSA-P384 explicit composite algorithm.

```
-----BEGIN PUBLIC KEY-----
MIIIIITANBgtghkgBhvprUAgBHAOCCA4AMIIICQOCB6EA5PRGIp5KNxOpfWTCrQ7x
kuIB5m+KWFVyuwqyFyDYULnMf0qcZ/6sIf008tzKZVzjaTLQTB8boJGKdg6c0VUR
JtrE/qiTA6Ro7tAgFVASwBcKdqLLhf52R57aDtLkJlNharrrtanM/N/v1dB8InwiR
bh2V8ZtC0tEmTB76nDILYKQfH6Crs4dZWpdDin+pqSPaH9y9eFoByI64aF0eW7fI
OnR1d+uWdrPABsc860lV0SV4+shVy6xdH+niq/GXD1l+4dy9tuz8Zbq84oRy/en3
1/uhqs3B0PLDWkiVTOZU6TEfvubwRDMehUokMmXbudMoz6E85ff2t42uKTWEyD/R
V6yPsqT6sb4ywlSy8RAKtMNRg3nA5fuxxyhkeEfr69z8PYF8cLgWCsec8X9oNbG
0t8bAjx5ouTDYwvAMARFpMHPJwJWNZ26xMKWhG5Es7jwZS6Hqxyse50X0h6Wl0BJ
+qehjv03ucFgxTI9mjfbGyDtie8KkGr5sp9CptV/DgGgUc0qbcrD0bDz6YE2UF/r
ejZI1nFSQQQ94WLzFYRFaQcPJvSLleSZ86z4Fk/ZxGFHGTaWjI9Pho4WlFaPCn9Y
z88El0jJDJFyQU76BV85PU0baHV3xBRttVo0XxxzIm+K/10yWL9NKlxbCMsnzdNy
iX1zyKzQ9/McNr0J8ek1/PsHRdMa7QebgUbGS3G0rqtn2Sl1h5jCWu/ZPoL+q6ZV
wAbw86z5jux8prRV3Ct2aMGghLRcFFgcCqUytPu3/uHwktPpbhTJIElDYAihGF56
eZhsXlsoGpgtKbJG4yZ7o+AjmcsN2qjppgd+0w3wwghznIHMd8Lfcx03T7n9oKTD
FGVLX2F80HeHqkUwa9h9D7PJ4gZRHk66bUNGu3uF8lmfjyyYjs2iw6LLVcpLNQRK
pTVDeRYXWlTR5vVi5+A4S8SL5RLkKCaDLQAZm+HCgDVFwMY0QWiQ6fHVQJool1FA
wzph3f+2WdZi0WZkNIXk780K402/mIq4wGeIMU67MK6RpCs1mIb8zfzvoXg4uBE2
/7f01tbIRBu9qmSaBiHYFruZEN/6L4AQiFC/nGX02cYMM9EiTEsataMp8A14HXKc
LwWobZ6tTsF0j0G1AyEaXVcsBrfcXwiLCBeLjhtP7WizrfG0q3GhD4IJCEIVNdZ8
Luqz4Rs6gON/wU0HbIB44+vsQeilhelTFNWKckOutHio+sHh1ah/UImpvvsUTUz4
Hy9aJWt4ayK9sTcBvktA3vQcTmK5LYE0fQgvgOppTpv4puhi+l2v6qZBCZD6l/kj
xDp453/9Vx/UpyI3Fj/rPztdkUQtB5fkjD6u+dgKNcUs65KSX82wegw5Yzm2DAKi
U7tY7ADP5V0ExE4toFrymMBUB3h0FzvLFEZuRxdTj0nGlk8/953EJcWM9Nk89qVS
rfogve3UM1/dfITFaLgoQivG/tUK/CqJdfze3JruL86fwt65gwfrMyVj4jGJ0YLI
BmAlxBDo2TybiUpmCfRQBeaolIrEoxBEthDVsjAyV4+M9olszB5mzkoS1B2LAoe
Xaf6/b50L4x0tyAqjmlNM/uGutjiFqCDUQRr+mBfX4TZYkxzzVr9SKB5H+pLg2f
2ZVhqaPSRi0duz7QdkE7cVbtwKDuUvpj70jJBIQ2+/7bo/6cJsVNByqZUBHJc2wV
bTH616uLXCxw2T9ljhfdls29LIbiE5yFWsg0xBY0hCDa7myN6jdaqe4L3+s84rSi
xyc2n+5apMeL4bLkerDaZUdEeSsgNNLhYd7fGfn2ITC1HgmWsSR2wD+Y7nbbTKfb
PBqqMH1EUhiFZzVtHz7nSMZlndA5m7n+fyckP1g8FS1SBCnGYUfwljj9IvUfE5Ln
OHTc1WuCOgSA4g1kYQY76p0i97ARvkMoBU7AMkH88Qxx/dEjV3qaFT3CgXczEsqi
xQhrUpQg8pDMuOnpSzb1Sll9Lg5Hs54XKkyQDmQDiEKvBSsblHq1yXFT6HS0J5s0
Wa00CCNGBJg9PAMBhee6cj0mhQxQyXgvEkn5GZm/BfoIAoNZ4CEcd60PI3lhf5Cn
4NXDtXAKw8k/c0Jgg/vuxAmsZl7f0tnrH9020adGT4sy6Cu0YDZHb9f54Riu7IXA
NHXLQSPT5n+2hmafKxFERL32dsgINW8vH9+nCXdnPU/sxA0j3sh+xJFrjRApLNVG
dLUarkUEIt/+Hm0ZtY7lnmu9CnX1FLbSt+pyqCzChqHcbBNDLdM0n3qwc7RaVfMM
st1XPpgFoJD0/Op5skYVYo9skDpI2qb5Hnp8wVxNthvYlUTryPnKgrPH4aMeIrUb
mGK3VXonlBs0EEwbIMb14+c0PdNeABfDaxeB8M3hTLb02uE3gGtQaRcbDI f j 9 t R s
v82mVY2UkA36g1ARmQDH5mN44J1QjXUmlyhhmc9ZKWvgpatqpzc3HF8xuMbu3w2L
GNsQ9GHAtNzpSWVBj4Nq50tWR/1gzOA6VQZGTUNgYffsjpKdi4+s2BRSt9/QfINX
n3iL1b8DvtG60LMVKPfi0fNjQ0PqtWRte2R2s+2kZ2mxZ6kNtKC3ViYDYS87N+Ph
/0SwnW6kxX+MF2ckHgS73QDYgAEDRRxuokt5cSSpnX4DHMD2URAZUZLSiUgdOHY
R4QLZVdK9LPmN40QI1LYx+DAorp5YHM+CkLNoZAL5yUIjzhQtm8DjH6FAcqAw98+
9nySeeldvMW3eFw+uPP/6QU08M9b
-----END PUBLIC KEY-----
```

## Sample private key to test the MLDSA65-ECDSA-P384 explicit composite algorithm

Use the following private key to test the MLDSA65-ECDSA-P384 explicit composite algorithm.

```
-----BEGIN PRIVATE KEY-----
MIIQjAIBADANBgtghkgBhvprUAgBHASCEHYwghByBIIPxASCD8Dk9EYinko3E6l9
ZMKtDvGS4gHmb4pYVXK7CrIXINhQuSLGaBCwfHk1aaq82rYGLofZmnKWPYGXZNgN
IEWOHZsRavTXiLNK968NiJovj8kCzBAXlU7CHhEMTbYXUcHjZ5T6Z4dPAoJBr9Du
S8UMazW7cxzjDo04E9yyCs0Cx5TUuWADJzZmcncnNWEFNIBQCAaIijigYzCDUVWC
gBVnMxZBNgVTRARSMGM3ASIQAaJQh4YTN0E2V1Ngg0hjZ2GCRkGIZYBYU0MEJWci
RjESEnaFA2BUMGAxVQGIRDAoA0hhAzMCiAV0gzh4BkMWY3iLEhZkJXKCUHURE4Qx
UAdIEWMjNycDNBYyEiaFh2SEAXGDJxYwGTQFdYUQgCICFRFEVSB0FTUWENDhyZV
gng4QYI4d1dTynMDJzgyUKiYQQAHYRFjMQEwEBQFEENTikRIEUhYVnMRgVRiIEJX
gBKHgUCBEFVLbLE3QVMHM0EHUdFLJkQmYBaHvYf3hhMxZEQWdUfMACAANFY2RgBB
AoRicIEVU0iIBADWJ0JwdDODQxFzSCckNmE2ERRkGDIbCIBxMkUWhAQXJlNwhRQg
iDKFcRhSV1ETVVAhghhGExh0UnBEdmEmVAJnNAREdnQ4gwNoB4h2cSQBYgVAh1iL
VEUXE3J1cAInaEJIZSAXnQFNi3JAIid3UHGHAA4I2ISA1ATRnckcUMkNlVjg4c4B1
JBEQKDYAMyUSHkQBwQyNXhSZQd0N1EnMFGBdQQwBRB2QHGCiQMyFWh1U1Myc4gz
AWSIVVMgJGMjVvcgYlgrN1hmRyYlVTRQVIiAUzYUMSUTJRSHYWhUEDhCMDcgdsG2
MSY0ZIY3UTVmMB0HFnUGcVSGhYI1VWZgc10IhCIiV2EwRgBkJYJwIXRR0EgnQBOC
GIM0AHeII0QxBkMGFRgnBwRUVSSIBHgLNhI0IUYkBiAAKBegYTOFhFVUYTIVR2YV
RDYnNmUDUXcYhVYmYUAVghMiIUQ4Q3NnFjdfBXhFdUuVHqX0ChmF4cTYGJhIAVn
chREdyJQChIWUQJoaAEKhVN4cgDdh1RveBh3eFYQAnFCUChgBAJ4JFZYVhziGBL
IlgAQOm2iIgVNEBxHxMB1dLJQZQR2YHWIMiEXJQg4ZVFCMnRDBDAmQCdScyQzBw
FzdidSABF2Q0EFZCCFUSCBzEocSUiBxAWcII4VoZEiYfyBWYxcXh1MxMmZyYBMw
BnIkMGQxIkV0iHUQcWd0VjAAMjBwcoHGNCEkMgNWJAQBJ4UTMDNXgUhzaERYi1Am
J0c4EBZCEQUHeFnyYyZwQBNXRvVWBXhHileCGBQ4SHd0JziDcwMRNSYAQ3iBV0UD
hhBhB4VEUjNUQ1Ri0EZfIdgETcyYIYyUmQDcANxhLZ0ZHAQd3N0ByZAeBMCEdeA
Q4YDhQIFhnr3ZiImCAIjNEhVRmBSZBzczYcyVYKiaAiEZgcxBjQEV4aIhQQhhoYB
c1JWdBGHUIhVB0NgdWEgOGRnNXgoMwQ2YEUicncXYQVhUFV4Z3Vyd1R0BwCBikRC
MyUmWDcnZWRWQShEEkYhAHRngAKFgRBgh0ImMUViBoYHckZmCDM2dgEEUEJ0Rycx
h1FXgANXVYJBidESd1EFiWhYVWGHbVaHMCcgJUUSdnJCCIFBEYICHfJoUIRCCCHC
hAEIE1AHcnUkVVYVYUieDBWVUhlQDIWUFYTg0B1YwVgZSAAckVgOGZXhjI3SDVF
ZgQBZEIUFEV2eINYJGQkVAYSU0AAUICI2YYdXA4hRE0Y0dihhJBIVBDJmZEUhhBcX
EzhVhDAngh1uY1cBYNNRjJECMHQgiCGCQDUiMDBjgCh1d3QGJkMjgUZGQIVYRzSI
FE0IICJUyImxhUcoQTFSD2YyWEFVhmRYgXQkFgNwRzg3YjYSF2VIYAc3aChneFUn
MEcoYhZGcxJDNoMXBjQ3d2cSNjIgx3NzE3FieAgEhwgWA0godxAmNAAGFkYAFxJi
BhUHRRdVJwcCRXJhKGAHJoVIBnRoJWYVASZhc1QDSDIzJygoJUA+F40nzgs44bUN
fvEqto02c6rvsZ6ldZt5IIWlRFzfc+eAwvSzj8PbKlg3UwkMt54yl5I9qvzNbRsJ
SNn1MD/KfhUjW4XE9A68d1PAg2Kw5ZQiAj8C32Go+YrNzymRwtmj1wwplyK/thhn
JBFTqsSi5Jfr4GydVXnySQqXxSRWYfBILibXecun46W4fgZXuI3Mpodg8oIihXt5
SeRjl3efJmnQsR12BHRtKwN92Yr33Waf2QNbF9kQF3jeQCWYiQrixuc876D2B8m+
Xb4CanpP1Kvcj+i4+Ke5oKdR4gECVj3Jukcq8t9V0x0viL53n0jPT4cpyzcTIQ2S
wqdjh0VxmJb3HaBTu864cdFzw9S5SoD/8BFdlVHL46ulWTWITAp/GZcVn1Fmodwf
4JuaUamMu4q0JqSrph5l6Z0ewkjf1EvQ3TGsZLKvmQPvWl6BGjDtbNjr+SELGs84
zwwlrLNkNxYmVntCipqvCWzQDD/JJ4/I0i7PhzQ1R4zDANQWUvCDu0FLYvjWwZgO
vhU/8PkVgjjvnpB9qRHkLA1o1ryeQPKK04kNeVl6l3AEZiDKIh205tRfQqBqpX0l
g/ET5H9+27RtSj3a8gS2iZeL0iE8PRuTn2SeeQ5//shcjWCB30yWds981R6aD/hG
gU97UpqGHHF5kDkyVrRkci4xTXFY6rrrh99AzY14yrCIbXk/3zApTHl6kYq2iWLM
fhtwMES9ka/gBdSyA2/w6+INm2UjcSABuH0gurSkI+lnBLE0s8NdpbHy70in6op+
9j8c006aZrDR05jFxAESWuVoqnuvWwqM+MPCnqRVx0GQZ5CRhGNKgDsXLcaFAxd
6GoL6cxZVIqlTbqRxrqU11zAvzaiY5Lg0/1zCLgGUMjBU27vxIZWTmKzo5oQxZoU
```

```
rnRrw49Ii+W64CJM2sYa/95qRYk2YFLRK3iFMr23pcchP9pP7pDrJBivlQ+cmsv4
dH5nCJAepAq8AY2cXB3QhiQdLxNiXvLsDuJhTJg+BPD+M8aKIM0gWm75GT8jZTh6
/tRtfeAFXnQURqn0lLoJ3rpIR27hQURyEUBrn7p+w6HZyZ3PPm70Wq3JoH8aPWgN
21AqLyWYim8jqdvI1WZUGEi2ogcYteQ5zrI4U38r5p1jAkGgxTkj3jZdNAOGzDQr
j2SMpBkn7Ke09kSaE/O1oLxBBJmwuk7pFEQ3/D+U5giKBjtH0u+QSBcEF31aSlL
NGu8010Sa/MWnAaGmNEB45K6jWQ/wJg7KQpfm/sLL5Ian1qwys9cvVRfivenFowS
fV6yraqRYfilsIFsDWDPTzR5lhg+EAaw202P0CaJKJqINXKtdeXhki fyvaZ3SMV
iV02ctF4EnpY8TVAD+S/AObtIcP8NabgAM/gnDM3UbfT5AZKjVLz+08Kv0Yig8Xk
Lb5wkk+jUWyY6sbnUVh5LfRr2Y00SEYhM6g4XoWLRAC8kD0icpET0u/5LtQV+J1r
yRXoaDGUS1tBkoyAWE4pFYsOKLROAXDe52ILJhm6ZkK3WxAMzqnSevTnFvnCtjBo
uSq6bFls8+0y4eah0cdFcE4ZoF/Xt0km3JhS17N6U4COVpS80YymWDM+N7eGHFFL
qsLC20mk8DghyMuXTsm5vShdT2r91zT8iRCdmYew25LKmLFUY2DenNk0UGXcku5ZE
xX7IPiGc/zsHAnax5nvcz7S6kVB0IWXOn4PrD4XPrGJpGRodSpDtkcRLu1XszwHa
fyJGB+b08B40klWsm+Q8uRqQTaRz98RcEhZuzUQuH9Wc1nk0yUzXosUR/4AXLrC+
+qGLqEq+WWscXwLcWuEsBcDUgJ4TBjylrtSS7EHkVMMnRZzuyNut/SHj8bcdVck
hSNXAQCdsoQmgJwNVhF0638f2TpNdEEExhSrF0ipWszy2YwrlP5ycDycD8eu3BN8
l0Wy2Gj03Lf9b3wiJ6crF/XZ+nVSljaXIGsAteMNN3TZRkTqvVFWXxlC7M3tsta
IBj9Lqp+z7eJyiwB6NlAn1PZrnwgyanAXF3MTmoDoVJD+/oH/50gExcGL9E0W02sg
LmM9cYmFvEK8xbfAuL0LQrdTLWM10ynX+SJeN9AIJ/8XSPbMnbatKi2pxFr+kVv/
e0wayv/6U8s+DE0YYf9cckNlyspS8UBwfqFpC7Wp+rDlj7IBmHL/6gkwl3eahnxa
tifzi64CpSnXUXs56vG1W2ARuPqqDXIXaDwGbwswS9rtm0aP73NXwj0MyDnOFI7D
Vq2tWErgx+hZmP54IeSqWdy3ecq7u+r8ic8lyF9gGLaYMrFW+BShxwUEstwcNqfZR
jnJXXh68RKvdbBpKrvLnjizdKdhK4N8RNJ1C0dfYYHFVCampw9d0w0MshLCovFM
21uzAD+PFwWDFGpb09lupDIbLUSkfJ2LXpuf/5E8gTV0VwoAQrXMq+o7UQo7l8U7
iQ/JcW8Es1qCuGxQIxmdymU15kiM4jnAQnZf2cixo+anyH8K6cwj+wyd3yYPw+BB
lgJBz72xio+k0P2WSDqhJm9dpxJo04DPXQcn/i/T5aDckBxKN1tPJMFLjsomN7om
eNvaVpSlTJoD5oRPYubt33nymigv6Jh4J16WUyE4aHrvQkRu0ftK93zKWFyM0rP0
LcNSBvsLz/NqH3YvD3FnFpEJzWiZ0CILD9fV3BUR5V1YH6RmkwkMsk1CHmJC+dhz
NPvsaEsHbNxe5xZbngEUDhRfKmdfhm28IJVUvCt+B0lQ56ZoQs8dFSENTpXXv9u
oGj+GfzxBl8070UApRygyiYEHqbT9W5QRG8/j9dMsRIeLuffhWCG+LQ5L2vxBN0V
0YE2cnkbortxTRISpnk8jFE9BcdSLwe06zBSUv+qZph//39Vvx8YNL1j4PgzvRUS
yvfI97qLzN+F+8pAX0TcetThAmgnQXN35kzsNjp4H0LaFf+UIluEzMbEI0ASuBPu
lqgGv0Kesyciqr12Qg7rMuDS+SYd/8nCkeAuWg51LCAkdbrRn1oyNWAX5ryroR0h
AvmUeZWQ8FY+/uazaIIj9BKDBGVHE7IwwTqmZUefZ7xyDcbU03vdFqMFCdQ4BnT1
NNIH/SBMRAljFcspIgxoxvLtwaoSqDugHqU8xoHM265cSuLMDHLsLV11aEy7QPRu
YIDLGBLqclxb0a9DGR8Ve4Ux/1zvdKTN9lr1/F+pF478Yxy0kJgNCKybTffylkic
/dJ+1JarPXj1SS964hSZp30N0njeZpBLRgJKCjffjBM1Rm0VGYHbid86BEaX+Yw0y
5R8cEF+0cSABvQN95tuC8wIrnEC6k30aKJcW0J6JCZBQxfXNjXYEgacwgaQCAQEE
MDjt309p164qWqk/V76DiXxgIfm0QPvAZPjB0epg+C9ZW/Ng+UAjeG2rT90IZoI
56AHBgUrgQQAiQfKA2IABA0UcbqJLeXEKqZ1+AxzA9lEQM1GZUoLIHTh8keEJWVX
SvZT5jeNECNZWMfgwKK6eWBzPgpCzaGQJecLCI84ULZvA4x+hQHKgMPfPvZ8knp
XbzFt3hcPrjz/+kFDvDPWw==
-----END PRIVATE KEY-----
```

## MLDSA65-RSA3072-PKCS15 (2.16.840.1.114027.80.8.1.27)

Use the following CSR and keys to test the MLDSA65-RSA3072-PKCS15 explicit composite algorithm with the 2.16.840.1.114027.80.8.1.27 object identifier (OID).

- [Sample CSR to test the MLDSA65-RSA3072-PKCS15 composite algorithm](#)
- [Sample public key to test the MLDSA65-RSA3072-PKCS15 post-quantum algorithm](#)
- [Sample private key to test the MLDSA65-RSA3072-PKCS15 post-quantum algorithm](#)



## Sample CSR to test the MLDSA65-RSA3072-PKCS15 composite algorithm

Use the following CSR to test the MLDSA65-RSA3072-PKCS15 explicit composite algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIiYOTCCCaYCAQAwSzEQMA4GA1UEChMHRSW50cnVzdDEPMA0GA1UECxmGUETJSHVi
MSYwJAYDVQQDEx1NTERQTQY1LVJQTmWnZiUEtDUzE1IFNhbXBsZTCCCAwDQYL
YIZIAyb6a1AIARsDggk9ADCCCTgDggehAH95+W/h3bdZDShFkwC/NzNTgUPycJ04
nDicyUB1Xi8rp/yN8fNB1T86ZFJ8dUYDBYgVggGjBh9I9BHKFi5T5Y2TevuTeg33
KAnviHaVPeJS8TrU0t20rSHGPYzV1jyITpnX8m0bsoqBP3H9h3QE8xHWYLj90pIK
sS73IUZwkTa2BuIfPbB4cG7puwBBKoUyCpWmJtxkBEUGUR3ykyHoOH8kmhIYjwmw
RjGBIS6jUARxaf7jvdt07phE5PgF02kKQrJl0tkZCGrrM/r/qWIUzJEudxOrZbmr
aSD36rkZrQ18hVAo2UMqjYcmKCWX5DDoZ/trN238wQC6jOMnhre6nCWOIjn4MPaW
21A/uPyENFU7bSN0XEuK3KM5f7PwNNXQ1AgFKiSL+Yb6cbkvwm6VFxoLEKA3J6Vc
IZms6gWhkwp+Buah1SqVFB+VRF552hrX9QLRpVNe5RbyGZv2sGqVnloiri7FuIu/
uSwie8XBHv6aoqeyuF68fn0UGoy3moQSHNRfiTFeDfoo7di6hL/9iFtRH52Wz0rN
Y1RXTonQ/HFPhqhRlB5A8H0kfXW9yxe1oAd5p4gIFLfvhlZN+2fBeFgfy9cvwFTL
52y73vvI6f4r+IivDLEky6gnmmPQADzo0EELAsNLHcwiWhBRwn8Lhd9o7u7ONXSd
PMEgfCB2DlJB1b220zBCZ2kzxfxpD27QhslhEvD193fvg0hQk8sKGKE7LkNgfh
4IxPHT3FMXcI9weVkhS9ymzLn3QWK0egfvQebzXl6G9k026jKPBZ719rpqsDUFzX
jGhC29ehoCPfo/aPShWQ4IME/4hfbpJ4k30sUd+tHqce0qe47P1n3xLY5nH/rLMG
6T2KIvdvhgxnTyM6rAqfFHSa4ZHA+KJhLKCLXGdzbdWP6jH5uGr8ZAURPS82D3
GoII8E61GCE8kz9EVHRse8mvByR/ExPOCrbiIBCb5c3dYJewngOYx5H6ohbfeok
l6FpCc7KB7/LfU7KBv1G1RQIyA/8Bgbctz7H1bBJeanDnsYYuRB6U6zMtI+yAYa3
PBuEGAE4MvdjeHwt101ZZP3R6QhsijfC8cp0rMlh9/VXkZ4j9I2G9l4J8UTWij7C
wWKIyDaKkEZysczRCNDIyQLstwl43LAiG9RiA2nDkDALBcn0fZo79ArRHsN1vR5j
9LCT3kKDKsw8FZEy3PGKdrL0TTa+ZDBp6Dik4Ade00z70h70P3QbbB+/YZD+HHmT
P1qiW03Mfy2DDavpK+KUN9Xo+8zNJl54CN/qOU8gDJIEdGrT7/DF9A1arMAJb5I5
60BeoWAEoVLKDBKajJDGBq1xtFMXutb6tPaIWivy01WUouWz4tx0vI9sxT2EqXy0
48GjUijKjeiyt4775eIQ+Bkt/vBg7BbjCwcWNNCYN+NPbk3SX0FGYWzagTyrfWk
fFC4s44UHS6rJMOqMfW30LigGHZJLXi5wlan2dXaSds45tSf6LuqBp9ih7kHC2L4
55Dr79H+3uN//ZrD60DYNVNlRnXv0DK1YgDZFaKL2YUH5L6e827ch6/v9G+pS9iG
GIzRKQA80vG5uVumzC6+uMam/NTd8x2U62NzyipqJPWwhA9mVGdId0CDy9rU/rg5
lh08LOXFarcPdn0+ipdDajnu0byDxK15oG0klk06fgsC0GsEJMMjkRwvB/vXRa79
TB35c+AZJ80ovcQNukSQVMJ56xb/+55H6AZEVI7kCL5s2pI5WOMLRWLgMwvNkKMs
K/JDapZiS0Z7b16y3iRj2xtXSbIBPn3y4q8FSuUqQ/Fe6u1M0AhJh6noNY74K5OG
iaez9Q42rPaueHmQglMXcjH1j0LGDpVCMzGcv1X0ft5UVzpNtVy5Hc+1ZFwzn5DV
wr0j2AcSA9+ev79ANQx6p8EhwaLcdLX5wH072Uy96o100TkzHwZOMmKnW+2dcPeX
hm1ANhdMqTez/SMaon3zQW4JdjWiT5DWrllFX9IulW0Egphq5jSh48cVDFUQR5ZV
bmTcJLWjssuJRyZJuK83piQFuJTL8oK/VkXY4a0H/+YztJN0uoNsXzizqsY00UbuU
Iil5c80Ejt6r5QRpf5jQx/AAf06kMwxcGYKs9bKaSE9ufXi7X4D3DiGp5PJ/vAGK
eZ4nf5I/s7bDxLqV8ybx+/HVU474mkNv5560YybQFQwXI0tiM09DWys1RRQTRBnp
hlGXGL7BwmnghASaWpNsSMk0C0rLElcQLqrg1iQ3IQE5+eyS4X+2Z/edadKw24mD
asdKnyYJf5Embum4o+jSEn1kABTEvPI5yIUMPZKrS65AXj0Ef0EYJxskEsCWhod
AofJH1rYYH1P6EMkU5DtK6Ds56drEPZ41wKIHHKWtUz8u0oQiAgUFAKg0qi69IMk
ckvWtZdyFr6JzEULL8ab4Mdp9nlnRun6Y8Yy22iMF91l+nIHM2EFKJfjafH/2yvu
D2UGPTtT/jNkm30m1vIjpZAZk+HzVfAhJnJtEeyh2mtXvP1fH6qnvLdspaVer3j4
fUS/dLT+GCYKZWTvUyx46913LF060JQR7Ri4D7WkFsJG5p8ds+30Ic63cnsIlvmt
y8ok8rFRfCSX1A4IBjwAwggGKAoIBgQDf2nh7tjyKgeBsQSxCVyUheLo1xfE+I1nS
Q5MBrF07vhVL1wjK6e7U69HNFvN/46uC810403AESzAjEcAs/8HKf36wP6me0nx9
eA67gWAP6IdnDi4f2thBaDMJVGRzKqX60FqNeknYT5KtRCyZ9hFxEbRbQkY7bidO
Ci1dW2mXEv0S0xhVqYeeMhLFSB60H25k5UJQVMPZ5zP2KnZkjkn2yI0qWaegz4r
```

5rhkwRG2lPa/R2Lfc3AwAd4U+l+rWpNnqfIYjd3LSDOficszuvTvTp3aVHqDn+oS  
j8BIXDTWOKE19n1/bHDFWarn0tFf/DA0Uoe2S24X11Dsrs14/Q0i0VY91odAlWCP  
y17g3zBskYDT2MSmjLEOV/Ptu5fq8iIrAdsewDtXiIG+QF+btyl7AmYSR4SZyW  
tWgM9v4aRET+wKUKjppq8RI4Fj0QDWJTZQAVYF6UKyR5efivJ4grZg7SrQRf0v7wV  
SQEn06MZZLYeaIyqzkRJA1/wHXJo5hcCAwEAAaAAMA0GC2CGSAGG+mtQCAEbA4IO  
fAAwgg53A4IM7gB+VU3W0jM54imd2PLz0DAVtMwLXiHkgsppR8AafkCUK3Agyc0l  
jwYnAcndydw0ueymAfBTSM7bzigtKadD6gm0+wJFPHqfIWP7kpQjYpLXuv5zsNgn  
j+A3pDCRBmoWpD9qukd0y2TdykpFbM2A/VCr70BybWV4DFmrHm7Qrj+61fgsz0k1  
AYERa1Ka/YVHZCZ4tGK76PtgbPRCejMorT101MaN8TudyW5Mkvdx0YTMERR0z4lb  
3jc5l2bBvA5lZb7DARntzwniWf+7LxuihvhaWGUyfwjQz2Akp3lbd6Z3MJC0Dq4  
cCXr9zEfxdsTsKQW1PconkMRk+cyISJ5FU2+8fNUEKYlBTM+gocdfU3sIz4+iLk0  
MLiZqhHdID+1oszQRMD6CQLGtwcp/RfyZ/+EFf0x/AKLQZ27u7iFgQyJv3tYbkLm  
zv76ahCohLud8DgVkh3LrUq3iQt3DD4LLt6pkvto/+oiyogNZRwkJ/cGzgVsJF+x  
vaiER+i3JH7kvXs1ZdneN6JgbZoHIUvOAhk10N6s5V5ivxydAueEELIDsoQHwc9L  
llspPa4jVfH8NgZ7OzyUw6TQmYx7DHYHW2V9fJlqyjBp5wk0wchXhSRvUiugtV  
EA MwZyUMN1RiTaPtoW8/Y6btxHvU9+UUsE/Za/hW2LN//w9dLPYcL3cX9q9scRTiPh  
LD80N9jYYdKFEtLLpg/KHx3s/9PW4dfMRd6o1ya19ZEarFR/B6V3xUYhXj0gr/K3  
QPV5JH0ETkLha5CrP0ZDu3Nf9CFfdu7XWiXpE6vi0E1Exm5Qf0KNdaUElRrQ08N  
h8GM7/6sJaRDCoBW8bHyLU9Xm+2tAcB3oMXySRkULWimp4vEqC8ki2UrmTmPprMn  
TwsrV1KSWlVs/r2DctVsVU68w/1jkqoMep1DxbED/WjYRkzEmlBz9fbQxfkMFpT  
LOGF9y731TssxvG0GJ5SvLBbXNUQE3sv7lq0CUARAqseMSbQ6a/qcUXDnriDfN8r  
KAR/qeTDO/k/Dftz5M9c+DiUQGNC7WbLTjHIFPau6KNivAEaPoYGqkFZZcsmN5xS  
FR3ZzYInoa3DS0qri0AkyRihe8A/VXpOyppi7JsSsAnRubWYgwBl/Wp3uB1/8JrL  
Z/bcefxV+JT0R9SGcIeM92R9x9qAjUHLW8Qru1bQjdq4iV/Z/IpZvJsuu6eM6nZfc  
XVlXlrei8g+dGbzMqfeUt6o8/46LXWcZiszPg+XvBbwCxrU4YeR7b70HW/Fz5vzx  
hqpFhFR8pmPBospf8gOEGRReri9fw6MbAcHojkEyA7x6mF0w+V0gEGXiQRRzF7II  
Z63/aUsIj7pFrRdg+g2N2NWm0D7lTa2FPfD7L5gJ4LHtj9EmaqZ18Xxdbz4Tx9LH  
Uy44LGiNrcR3YMBDCrcQEnPbZx4AyPA1cSCpkxFguZDzHbQsaCBb9uZYHhANhrYE  
48aWei0W9uoR3YMBDCrcQEnPbZx4AyPA1cSCpkxFguZDzHbQsaCBb9uZYHhANhrYE  
QCmBGBb7r8FcoYgPJw7QZoxKjj3DEkiRUU5bYKpMYBv0u3VvMmIE/mYCuxbeA/0k  
Uwp3VDyYgfcBpH4eIASosNg4mxX4CZbSn0UmWarNwGZAf3MRuVzNjAZE8DTzJ1S  
UeWinj97jz6WXXNWioalXAUN7LO8EW4cLEk8ZN7zLSBxuF00b4B15wdsf/lmIn9p1  
mcii40SMefBoqxboak6zAAQVKdyW8wLLshHqnESy1pnWAK8xXupDr7QJAoQVfLKP  
7CN2kKJ3CfWf00dVoho9Xj5EDaxMhFLtA0du5rMyyi+DERb47kKLTh8hv05pEScg  
uKfoK0qh0HEk2WuF0cTswU8PJzDNtJy0EMbK83C5g7ZGLU3b1QyOq8uVhPD3DSPH  
fvKciZG86GpxWMB6zPBL/LEVp3eP/z/tFg0+QM/x0rylNUSSLBgIXpPeax0Cxb1q  
VUzVbHFXNGNT+UDCzznURQXcauuA0kF6Ho3QQwsj44mPzKPhE+e0RZZJCa20BPhR  
YCRiXo8GFNSjNl31LLXK6vthCMragf/ZN/FIZ16Gpuz8Hazi7erMEkJuFJh3Tr1y  
78YoYPIqPw38CRJZF0YcEmrrqxs5jaTfag5B3BNRZwmcE1Qmbb59Hj5TRzGwMgS  
ntrXf9ekGkv5GfCgXhK45znvVix3A7qmPsbkTZlrys/Y903u6KT0qQZPj1qzsxoE  
ovW0hqifFucVMQqpnky4bWrmrKp5KU3sBu9UoILhCzd4arP4ni01f6jP3dGkw5ao  
OURnh3WVvrqgLXxvd6/voDh5RKVQfibi2zuZLX1gl9JAEqc/CdWH+fjJ0ey9JtBFA  
JtG9nExAdNsZ/D9Ia0gzVDDDuZmM8/K0gtdd14T1uP7v3SfSsUUBuRgB8oLG8AYs  
rLlwg0hWmviLD3qYYAttInuaK9fcnQFvawAAS7ZF6TW+Zwe8CebnT1xf8cLOTvRE  
D5GCxkYhsBrt/uC/60I1aEX6lrqEbOWeQ0VcONHJwewzo7PmAbp52LRxmnopH8BN  
y9WqLo6J1wcT1amxmZxDMHx5JCguC0g6QM/u9EBBu60UbyQPst5osSLY+7YXZYvi  
s8EbmZUHJUPYtzpvlQ8WqdzpngzWTiWp2xwfqQ9iNWLPrZAdqG897LdNLQb5H5Vi  
j+fC0pyV2jN0ReHUc8uOy0W4BkHYhYPTHubHXhkzsKyt6lrQ+Uv4vz6RfCNWSTdn  
bC2PPY0hOstghB21dDzIvyHtGHhesrNdxtT2/w45FiLnhurJj6B4carT1+VQgiL  
HnNDWcvaFk4Woqv7AMmzuR/FCxJ3zx/oS2vhNpgJpWkLeR4m5UWedHcNoF48EfWw  
r1ylqfhtCjRokuFbim6uiyHG5EazK8K1EgiuBaxdrzG0H1voCuK7Nu1Ahm7we7L  
y4lqGXNWu1w0g5N+RezJptYV9wZNDEmbA32sMU04kJ8dT7E4smeewhp89lkE7tH4  
fWnVoXMTGKxiZWID5F3K89mSEzxLD9IEzVTLMBC2N/uPKiFU1ncKtF9eIeriJA5J

```
RdDzmkGUUKx0VGd300CksZZiCQ9Mq/FA9QkUseIhNhVU9VLHU+5d2l06UzQt7JUA
i200PzNuHG6zXD+1K8CvA06+Rbbg/AAvLVdYmt555dL80H/31Bb7Tc2d/eLSUCTO
uaWUICnzrs7dsCA6rTnwzASe6+4oQYVUeZm+S1WhaOc97oyp1N9hmbhMhm+sHtTy
J97sYwHMOHRW0HAhVZjhv4i5xHjTbLtcqw859177VWj0R0r01CwLA1YrZKsdY3vH
gfjxvXhuV1SPQnQ767+Nm8iiz75cJ2cM3VhMt7RAVurFwoq0k9pZKzEaLt6fI1Fi
Y6R+IfZ094q0503BlfXwHCYjjc5DoF9vKNtQUKnr98PWHakS206w3XhqM4gtNjay
CxrWvHTdKJ+Bm0vPaFSiEJgNKUuJRabkmSfCR0p+mXwoTiOm+GHA1KOK71EXYz2d
xr0tkLRR7auDyMBWe2IT8tcg19Bj1tSYF0K3+LXj9RM7QWPoqPWPuAuG41ayURaOM
+01d0uroWQ1PTL6zwhgR9fU28ml3WVXnvee5ZUPPm2rsBTlhWJuTiUCNGnqvb4K
y/wjvzi/YFZBYR3cuKkahg9c0TER+toNH3c9Hl0+bTXLU6fm2V+SeTQ5vs4Fm8g
T/kzaC6Gge8HIRp1JBS0FivYgaMDi5Ru9v1KM2vLVF3DzHDS2qgpXfPXLQXN5wgt
ztsaYw81qAH0qVdFm4CyQHypfRhOgjRLujl69AWYYTcwujay+nujwnMWR+OGEM
00xPS5S7WhsgkHtdfYkLuzWtUcZeD//Bn+5hdqXg6Gpu+cssN6JCEPtFtZcTz
KbBw80pnKRjjTRIZFqckCT3Y9h9zyU0ewK4ju4FiyadlvhF+D2uQqdGecjwxRXBY
Tp5i30pBiPlVtVkt0+LuhJGQetrhYge5HfLw4MVZho0KE1m29I/b90R8R+G04r
H6xNqEJzdLArE75MQok0t4XI2mJhR75B+0aXDSDTKwLJQRx7UQbpwNbACBmqw7Uj
UyK9hI2Wswj94napZT4whddSF6jooN1LXDAf0a+lfYuGA7PZ22iF8fMVYiNLYoSH
cobrw2VVH2UuDsJ4KXrF3LfTEAnmosxCUQBqcKz599BLi4ruEqNoGUffM8BTmRKE
acjzrsYJQwgtSjdHivqWvv0L9gr4tw9/uwtTru0pabVhto0AFZFRgXKZ0J3EU3dU
AtXhEL7+dJh5tHhzhZomeN8A8IIraSuS9iUl2zxo/lo9TuQmfdi/pLRiXB1nJ3W
4zKbKX6Qnvv/hZegrL0Jg424/BVeik26AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAGCA4TGB0DggGBAMkyqcX7oXTRtZ0EsIGbXG734y4XTGdkF2WoBoiXwoXvAeFI
g/hWAGX1i3I8VpmuA7Nhr0eT1XCJR6JQY80HgLM6AhaPnEhMgGE+0I0rUHVMeD
vRupIoov2VxMSvibeNUK1o7X/9LybOMV3T0LKjczRhIsGZTZzh40UZODRH4gBhv
uUkdarLV8fTH3iqGrhKjuz2xbBeyU1IYdvQIql2f/2/YWF4lklIz1SJrisn4Leut
vT9jzN8oWhofJa7JT0a6sePTjG3QLntkmNcs9IY1DM66e8ZNUckn/CjK2Zh06uUW
kryg4u0kcS3nS6D/98KcKw++Wgs0VeJLzcEho760l10+yfX1GctkwteVuFOTMq8N
veyu0hoTMQBx5GTiXu0aUXMPPV0nELHhzmHDyYR4PbMK8Zd8/XvcmZiAXPg0UVw9
7ja0K2GFgu6YAIGS29IcQ8Sj4yFSOnQIsNqAqPYAQ2U4t9iZmzddLpIXyBEefpLZ
9G8VR2Jlz/GmReG/Yg==
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the MLDSA65-RSA3072-PKCS15 post-quantum algorithm

Use the following public key to test the MLDSA65-RSA3072-PKCS15 explicit composite algorithm.

```
-----BEGIN PUBLIC KEY-----
MIIJUDANBgtghkgBhvprUAGBGwOCCT0AMIIJOAOCB6Eaf3n5b+Hdt1kNKEWTAL83
M10BQ/Jwk7iC0JzJQHVeLyun/I3x80HVPzpkUnx1RgMFiBWCAaMGH0j0EcoWLlPl
jZN6+5N6DfcoCe+IdpU94lLx0tTS3bStIcY/Jm/WPIhOmdfybRuyioE/cf2HdATz
EdZguP3SksgqXlvchRnCRNRYG4h89sHhwbm7AEEqhTIKlaYm3GQERQZRHfKTIEg4
fySaEhiPCbBGMYEhLqNBHfP/u0922jumETk+AU7aQpCsmXS2RkIausz+v+pYhRk
kS53E6tluatpIPfquRmtDXyFUCjZQyqNgKYozJfkmOhn+2s3bfzBALqM4yeGt7qc
JY4i0fgw9pbbUD+4/IQ19TttI3RcS4rcozl/s/A01dDUCAUqJIv5hvpXuS/CbpUX
GgsQoDcnpVwhmazqBaGTcn4G5ofVKq8UH5VEXnnaGtf1CVGLU17lFvIZm/awapWe
WiKuLsW4i7+5LCJ7xcGFxpqip7K4Xrx+c5QajLeahBic2sWJMV4N+ijt2LqEv/2I
W1EfnZbPsS1jVfD0g1D8cU+GqFGUHKDwfSR9db3LF7WgB3mniAgUt++GVk37Z8F4
WB/H1y/AVOXnbLve+8jp/iv4iK8MsSTLqCeaY9AAP0jQOSUCw0sdzCJaEFHCfwuF
32ju7s41dJ08wSB8IHYOUkGvVvbY7MEJnaTPF+nGkPbtCGyWES8PX3d++DSFCTyw
oYoTsuQ2B+HgjeE8e3cUxdwj3B5WQez3KbMufdBYrR6B+9B5vNeXob2TTbqMo8FNV
X2umqwnQXNeMaELb16GgI9+j9o9KFZDggwT/iF9ukniTfSxR360epx46p7js/Wff
```

```
EtjmcF+sswbPpYoi92+GDG0dPIzqsCp8UdJrhkcD4omEsoItcZ3Nt2JY/qMfm4av
xkBRE9LzYPcaggjwTrUYJ7yTP0S8dGx7ya8HJH8TE84KtuEiIEJvLzd1gl7CeA5j
HkfqiFt96iSXoWkJzsoHv8t9TsoG/UbVFAjID/wGBty3PsfVsEL5qc0exhi5EHpT
rMxMj7IBhrc8G4QYATgxV2N4fC3XTVlk/dHpCGyKN8Lxyk6syWH39VeRniP0jYb2
XgnxRNaKPSLBYojINoQQRnKxzNEI0MjJAuy3CXjcsCIb1GIDacQMCUEKfR9mjv0
CtEew3W9HmP0sJPeQo0SzdWVl5jc8Yp2uU5NNr5kMGno0KTgB1447Ps6HvQ/dBts
H79hkP4ceZM/WqJbTcx/LYMNq+kr4pSf1ej7zM0mWzgI3+o5TyAMkh4MatPv8MX0
DVqswAlvkjno4F6hYASHuUQMEpqMkMZurXG0Uxe61vq09ohaK/I7VZSi5bPi3HS8
j2zFPYSpfLTjwaNSKmqN6Ji3jvvL4ior4GS3+8GDsFuMLBxY00LI3409uTdJfQUZ
hbNqBPKt9aR8ULizjhQdLqskw6ox9bc4uKAYdkkteLnCvo3Z1dpJ2zjm1J/ou6oG
n2KHuQcLYvjynk0vv0f7e43/9msPo4Ng1U2Ws3FXQMrViANkVoovZhQfkvp7zbtYH
r+/0b6Ll2IYYjNEpADw68bm5W6bMLR64xqb81N3zHZTrY3PKKmok9bCED2ZUZ0h0
4IPL2tT+uDMwE7ws5cUCtykM3T6Kl0Nq0e7RvIPeRxmGY6SWTTP+CwLQawQkwYOR
HC8H+9dFr1MHfLz4Bknw6i9xA26RJBUwnnrFv/7nkfoBkRXXuQIvmzakjLY4wtF
YuAxa82Qoywr8kNqlmJLRntvXrLeJEnbG1dJsgE+ffLirwVK5RCr8V7q7Uw4CEmH
qeg1jvgrk4aJp7P1DjAs9q54eZCCUxdyMfW0gsY0LUIzMYz/Vc59PLRX0k21XLkd
z7VXkD0fKNCXs6PYBxID356/v0A1DHqpnwSHACVx0tfnAfTvZTL3qjU7R0TMfBk4y
Yqdb7Z1w95eEzUA2F0ypN7P9Ixxq3fNBbgl2NaJPKNauWUVf0i6VY4SCmGrmNKHj
xxUMVRBHLlVuZNwKta0yy4lHJkm4rzemJAW4l0Xygr9WRdjhrQf/5j00k066g2xf
OKqxjQ5Ru5QIKXlzzQSO3qvlBGL/mNDH8AB/TqQzDFwZgqz1sppIT259eLtfGpC0
Iank8n+8AYp5nid/kj+ztsPEupXzJvH78dVTjviaQ2/nnrRjJtAVDBcjS2IzT0Nb
KzVFFBNEGemGUZcaXsFaaCEBJpak2xIyTQI6ssSVxAuqDWJDchATn57JLhf7Zn
951p0rDbiYNqx2SfJgl/kSZu6bij6NJIQ3WQAFN688jnIhQw9kqtLrkBePQR/QRg
nGyQSwJaGh0Ch8kfWthgfu/oQyRTk00ro0znp2sQ9njXAogccpZNTPy46hCICBQU
AqDSqLr0gyRyS9a1l3IWvonMRQsvxpvgx2n2eWdFSfpjxjLbaIwX3WX6cgczYQUo
l+Np8f/bK+4PZQY901P+M2SbfSbW8i0lkBmT4fNV8CEmcm0R7KHaa1e8/V8fqqe8
t2ylpV6vePh9RL90tP4YLIpLZ09TLHjr3XeUU7rQLBHtGLgPtaQWwkbmnx2z7c4h
zrdyewiW+a3LyITx9EVxJfUDggGPADCCAYoCggGBAN/aeHu2PIqB4GxBLEJXJSES
WjXF8t4jWdJDkwGsU7u+FUVXCMrp7tTr0c0W83/jq4LzXTjTcARLMCMRwCz/wcp/
frA/qZ46fh14DruBYA/oh2c0Lh/a2EFoMwLWBHMqrHo4Wo16SdhPkq1ELJn2EXER
tFtCRjtuJ04KLv1baZcS+hI7GFWpgR4yEsVIHo4fbmTLqLBUw9nnM/YqdmS0Senb
IjSpZ6DPiVmuGTBEbaU9r9HYt9zcdAB3hSX6vA+c2p8hiN3ctIM4WJyz069090n
dpUeo0f6hKePwEhcNNY4oTX2fX9scMVZqufS0V/8MDRSh7ZLbhfXU0yuzXj9A6I5
Vj3Wh0CVYI/LXuDFMGyRgNPYxKaOYsQ5X8+27l+ryIisB2x7A01eIgb5AX5u3KXs
CZhJHhJnLA01aAz2/hpERP7ApQqOmrxEjgWPRANYLNLABVgXpQrJHl5+K8niCtmD
tKtBF86/vBVJASfToxLkth5ojKroREkDX/AdcmjmfWIDAQAB
-----END PUBLIC KEY-----
```

## Sample private key to test the MLDSA65-RSA3072-PKCS15 post-quantum algorithm

Use the following private key to test the MLDSA65-RSA3072-PKCS15 explicit composite algorithm.

```
-----BEGIN PRIVATE KEY-----
MIiWzQIBADANBgtghkgBhvprUAgBGwSCFrcwghazBIIPxASCD8B/eflv4d23WQ0o
RZMAvzcZU4FD8nCTUJw4nMlAdV4vKyghwQ0lNcCI6CPEb3CsCXYP0tZAY0CV0TaJ
a/e921VSHvSJE+gqgySrSkpxRiw7P+KR97HESpbmvRtPl//iYwl+0j5Ldr/CJAU+
/95z8W6RPJXXgNa56cisYh4wzsnTcjMghIN3dzcheQVmfXB3ZXh4dgGEMhU1MYAW
EEJzITIRgVMAIVmVVGEEARhTUiyXVScRI1NzcSY3hENTZGZzMRAXJoBmATZDhm
GBhnAUzZEAVUQ1aAVhUhd3N4ZUZBMFIIB3MwZVNCgyBUZzcAWBUVhQFWKEBYd2EY
MBIDSEBCBTGHcyRRFESBVWYycFUxN4MjVwAEZgBwDBFWMQV3cVIYIjUCJkY3AKA2
gogUhrQBRoAgJ1djRSU2hBJ1BANnZyI4cEQYWFYjcgAXVHNBEhMBUjGDZiVgaHhW
```



JoZfVWViiVJfUFASdVYoNiiB0RgQVdSIIRLZ1RjYYAyF3U2Iogmd0N0gYJVEUUF  
gAJoc2WEcmFzVScBigrJh1Fic0FQNFJkGAh4N3ETEnM4GAIRhhzR0cGiAUkVyg0  
QVZTE2cEg3RzMwcZQUUAJXFXZ3ZoZyFohHNBh4UgJWgH0AJXdwI3AHdAhAaHQzhi  
ZhKCBIdTGAY4UxNRQTRlChI1E2MmUXg3gjNnGHdwUBYAdBMBYFQjIliFMQQWQQVD  
EwdjQIhocyAIaIhyQgMyUnYFRlFid1WDZSETJwESiDdiEdGN1U3NBVIUoQYYhJR  
CCN1dEBRVyBVJoM2cgVmUSYEZyYYN0IFByAoGEKEhgNYMTNkeBQiBBKHAYcTVLAT  
R3FBdnJxdAQwISZmRWKAUARYZ3R3ZKEHIShgUGaIAGUhhivGgFFQiCGDdERAcYOD  
AHcxFDAHB1WFZgIBiCdGQjE4SGWHMUNiaId0ADECC4QzKAZmFnA3JSdReEFihkNo  
iAFiUSQIhlg4GIEgYNEETyLB1dmSEhHMERnQkFUKegjJyWGiCQVdCRlBBBUAWgi  
Y2hUfLOFY0CGHbUTQRQEIgRiI1iEMWU0E4VjIBEHMWSDJAZCNSiHAIiJIXBWhgZB  
A4KBM3KBCHF3hAAFEyJiM2dzdFZjZXgwU4RxNjFYFWREQgFVZ2hBGCizVyYXJDBh  
dRWHQjGIKAMAAMeONGg4ZHNQEyVAeEBCQVAGhyGGYiQkMBAUYRVkEnEAVnGIVCNh  
YTZ1I1EXhEdGZ3IBFSIjUWRxQAQYOFZIOEckFRUTciJVJEgDIiNhNQWajgVkyTFA  
aAE4VQBjGFMQFXBSQQFoZXJHEmhoNkhGg3IBVoUyFwgkGAVHgARwd1WGAHZ4GDgy  
gSVQNHgGSBN2hyYhVUBBgHdHhGeGF30IALdBQXJUJnYTiHV2QgFgEjRhBOCVwQD  
aGFhcFQIUUMWgCNXAGSAKABwNEZ1UTgGcDZAF2SGREhIhINoFEZBNEQxA1hkUwAT  
WAVwdodW1InycyRyFkIIdnSFIiFRcQd1VmGHR1E1dDVYdTR4QUcVOIJIIVFTJyEj  
VCWFZiIiFI3WIEAFVJSQZ2JXUSYRQjA0F3dzRmFVZRgmV0QHE10HgSNIB1J4ZCI0hj  
iIYkd3dFKGMBcUEYUkA2JnVlIoJoYwFhg4BDFXIkZ4hiRoMTaIBTOGADJkgwdYKF  
VYA0iBQ1FHMzF1cyGGJic2ZzZlKAeHZGgWAFgyhBiAhUMjNhxzATFgM3MWJjEGVC  
ghWHZSZl3gExAUAFJDIVFgIKRXVlNxAgd0NTYEdGYAMRFVBxUVBhiEJWcUADCHIX  
N4YXEDRYRCJWRWBoUCFGeDQlNjczUBCIMAB4QkdEaDgiglQ2ExcoZgMydjcvGFUF  
NXJRQWRxcVdxAzcdUdkNEOHMoSBFSEidIBQhycUJkFgBlNxI3dnQ4FkYxRyEjJQWC  
JUCEYAdTUGUAIyhydGFDVoAAZAWIgxZ1UoQGZyMUREIAdQNHYxVlhIVUg2RjNYYA  
R1aDMhBwcBfOEYBiBzKHJwd1M1IkJDWAAEMjNUZGVUNVQIcCCCMILsGp58wjH1Aw  
Z+9PhxPuiiNTkdRgexiB5Uy1AjRsCTWwwBnLDwecADj+G16A5gTN5sqFMRLPhUdw  
94Zj6cidUvpYSEH9PAQNdxS8PUEBRORUZeI7wZA0onyHbqNGRwzutjfm8boe0yOv  
yJ9GoZdL0dehk1sQBQIygcIWINE9eLsoi41UYnm4rdDTysKeAI0q3zBG9w/yU1bu  
800hppqPRZi0G0hQ5bHwJhJhSozM7leUf+l2JGAcOJe2kfSmWXQ7eLJqZdOgdRb  
ETIMc9y8AWYa8i8n4SxxLpC5h+i4+FgYv/DKxgspS+qf2plxqy8jv+EIY91md9Fh  
jGi78Waf1QXiFVR/q06pDSz0cdHPMBVH/bFbsaQVb72wIXA4zZPY4hSYNi7I78hg  
6GDWwy63U+RaDxUiwbCMdTdC6t21GW1LKQdsV8dkAOLZV6/2Dc9YOFtjWt0j/tZ1  
pmy4SAsQw1tViutKVrc+pJHigSoCidHF7sM7ab8IK7QoyPTTf15BSfCgmnMV7hN4  
xmAgE2aVphPTYibUnai2H6pDPIfWVD3j6oQqbyAd9nWu6gybSNUb1YolbAJLkT0h  
qIHghdnPoByYWMFCD5Vcn/bFAGzWCKKUXQt03kh/HeIWUEoaCpu67Cs4mtwA09ad  
FaZUQQtA8gCvVYA9EGP1eCzyt7vXgQGC+KBIDFgZ05Vn7JQgEHUW+ErnmpqgnHLA  
0hBSxxbzhLZjmc73fDMVVQW0llsrVgBwIqZOVWtWv2zp51q+F+UrwUwwTDVPYRPL  
b00tJ6yobuQZ+6Ucji845jLUPAjAZwy7nXLKSLGjMjIe04c+ih1JgbncpK+ZYUHa  
c784ZTMgyaUKVgpUGz+SmaIziHTpvM36kS/H+x+3j6tKhVF63IKV3JVNK/6/gXwN  
0YKAbed8gHlFTp8KpKm0uXcq1dkGUTw2zeQU7DzQ5XALF1QEN/MLTjk7/XF/A6N3  
cKCQUTtP9LIEsYV/txcl8/Jer0kz6k/tsD35MpJZKJj239PVOn3grduT6zMY1097  
3DIqyNI9K5ARIGiUuxAQoiAUbpdWLAdYxFK36MskBXAat4HTsMEkmBHARMuZXzc1  
hpr87MqABTNhwrL7Y0gPfDY6FaelLxnWlc0o1uCp9zmH+uyGP4oxazCTijjz5eov  
dlwDfVZ3WAp62ZQBHG0DRESW30CugAUNyryYQsWv2up6tAw/Hj71tzK4j8UceBC  
fPc8gIxxBr0i3GRn0y/S7QYpFX+OMf70hAcvGrwEe6R8IKytKMUBxAuArB/spkB  
vLXkIpq4an0+NU0Ssk7a1rqiKufIK6Em0hLtoWxl0pdTREsei7DHDQplRm0UE08  
WPcK6Udt3BRoUQH4iuv8f0LXsI6lmvFbBVbL7mcMMj0h35ZLI90cAbVvo5aiZ0F1  
k+4yrPLUDtxjzSAMRQ1vSa9Z5kJUeP0kNqRojEN5/y407sdP0Se8aC/2Ebj6IXBZ  
EvsDBAKXqpnNg2/3QIT77Ff0+AYJK7QeegitiBduEbriERNjPwQuQDa3kYciDld  
tEvM5XhAcBhDIKvk4MyJutC24+qUikx5GLddVVL0xjqKSzgy0SU0015EVV5NDDcb  
n9S2DGr70J1l7EAjjoqjg02yHkzodiUUtWIKfx5uX/KEkDdGSLvFvSxE3kAhbTxk  
8BsxcisgmQbgfdaFskSVcV/JqQ07uma0CKXxl7FuVe0zkL7SjTIYt30EZhjKq8hA  
CiAGhcBhD48Hi5l0oemRR/kkNMFTRWndLGH8EAQIF+Vb3BdnRPcV4083Sk7iZack

CapszRq2jBoSgxYyuoNPhQc80sRt3Vi8lDMDauJ9HIn4TzMb+dY+DKKNNCTAJMJ  
0jNheCtQpJ0vpoRPU5LCBFfBeq5nntbG0xJJtrkM4dgFB2BUqJSDG1a2U4aMd9Zi  
rca9pS35TU6LTkm0ZJZnGR0VvLCOME4IckKzyYUbRme37UwUK0RRdwJiRoM77XNW  
e0zKNLtnLJr4RNB+QR3lvwAD8SePDiqueu2fWkNeSmhhNucmrW+FF0IcMpjrGRGzO  
/SUiqudfGZMq+SAFNLj2T/SzRujWntFd1r/jE0XMidzCLVT0Mg0BBxKLxUtZEDog  
XGq4kGrbAkCRvC2+2n0rm/MLEk0Z1St+TSou0yJ1ZQwLEwzubEgwb4v7orvwCYIP  
+slwQVbtDw2SkWoKN2KiPS93bsBFbm9wQn9EN6eNQSyAytioUjF97ueR1tEvV0W  
K/9kXt1co5FwvZ6k9ttipHwofZLRBNk34kVAFpZ0op4F0ryPo3WCewfM19MjARCh  
/DwEMaox1/hQphFDWoepBLEQw9MX9er7tZ3EjXn9Z02o3trsXDFsVN8wy8gW0JSt  
P9FmOmEeosUX6xIg+twzJB3YJ4uuVXT9Epr00a9SgKyMH7H+XdILQpF1XruYSm5L  
t0w0i1igdqCt93qS9yokMiA30bFjo9s8yI1NG4syF7hriQYsKGrITOR/hmmy  
Ddh+eNQkhh27tpe53ZwD4pKPPQB6dPVLupnpaCGG8nesGrzoiqpONwft419PIhU3  
Ia6U74FHL0E/fdA81GVjamLT4icGoLSFIqS1CjprRhP6EFYtavXbLv0XSP8RKzfFQ  
XqH1pLug9Xcixuuu105AHpqdV4Ln8BNKDvuiZRdu+5A6F21QUMZx/+0lRplQERnY0  
R7fVubxEmScfFX/gEW7qtDbNepskncp+816pii3P4AbSQJUA0AmPuzAzJrvaLnDa  
VsQHBtXhjXJd7vmKd5Xw9NlmoHrL+X1XdaREqjKNNZph1MTfYGy2yExtpjW7zk3  
V2I4xYe4VmkcDUu3G/MZHwmcohNltD2Rez7DF0JUUnldx320hZdcZyZ2tejzGA5ka  
EgNPQCFVKbzRLRdZ3CXVVMF9CxbZlkfIqGGeDxi3Z0lrnpdydTb019w/rnSVxQT  
L8zCFEA0y0L1giBv9TXUQi21srd4guV2FHEq69xCeMV3pZH4xf5sbnA0j99mjIPB  
pA2qSujdMmyTRkf+pN11AfIUTYrGhCGL+DkIq5N61YFUijksGZk7W3As+118+JSa  
B89vgv2EoFrFrJyZy3ct0Pvr01jKgw30nQ9Ww61L+spZF06NG/YQuRVwR2gpaClGa  
Vkwpkb0N+ITqqjzo8ILXJT94ruE2DQ09ImF5sSsGxtBqz4JVcsE+JZ2n+/CeMjy  
iDHvg1U3ziV5uZRGMMpU0IXmkwXRTYd2rlwaYZRRFL3Hw088lagH6sLF5MaYEAn  
iXcaC/m7PoYttHr+A4gCFBs2mmknJIQTM306nIZ8uHp92Ty0i2IEggbnMIIG4wIB  
AAKcAYEA39p4e7Y8ioHgbEEsQlclIRJancXxPiNZ0k0TAaxTu74VS9cIyunu10vR  
zRbzf+OrgvNd0NNwBESwIxHALP/Byn9+sD+pnjp8fXgOu4FgD+iHw4uH9rYQWgz  
CVYEcyqsejhajXpJ2E+SrUQsmfYRCRG0W0JG024nTgotXVtplxL6EjsYVamBHjIS  
xUgejh9uZOVCUFTD2ec29ip2ZI5J6dsiNKlmnoM+K+a4ZMERtpT2v0di33NwMAHe  
FJfjQ83zanyGI3dy0gzhYnLM7r0706d2lR6g5/qEp4/ASFw01jihNfZ9f2xwxVmq  
59LRX/wwwNFKHtktuFgDq7K7NeP0DojLWpdaHQJVgj8te4N8wbJGA09jEpo5ixDlf  
z7buX6vIiKwHbHsA7V4iBvkBfm7cpewJmEkeEmcsA7VoDPb+GkRE/sclCo6avESO  
BY9EA1iU2UAFWBelCskeXn4ryeIK2Y00q0EXzr+8FUKBJ90jGWS2HmiMqs5ESQnf  
8B1ya0YXAgMBAAECggGANKkP0Mh31Ar89q0zbP8fJ08Da2juQ0hnuvLeQpic0bme  
Bn9GRZcHcSEjBr5bHJeEn0QPRlmYH6JwMQD7/q2jPE1A1tMJejKqv+6efAA64IC+  
XVKGAvmawfo/7jKq75bYrub9pr0Snt/NLTGMM2YGASqNV1gyGfVzmKxJfg+mApn6  
hPNJynRJJuJ3iCW+c4VBkABnMxBhaSnyUEE1p2qba69hVajnuheBD8neIHf7oIcPs  
NqTEKHylLBM2PP4+XjZ2aKGVCV21TJDnFRNnEdGKmF+Uv3XfItT0SxsizEYBSVhV  
7gUA1w27/L7v72Y+xSFvCnIV8hRUz7MEpjDZb2ZaRbA+wJwunqIjzJmBY4PLAsn0  
1byfDH63N/jMgy4gD+Wuv9Ad3Qx+xFBMmLntuKvrx9PQiUqxAXikUMRZ3I9SPu8S  
SfQ0ZqiAjsdH+qBlcSaPpmJ6xPfWkHdXbMMFHLjtQXNebTL1U6Ae1Wodd4FZhZbH  
+nl4ddB4588r9vJmZLTpAoHBAPb/OGJU2G2n3jPNf5jSj1IzL45vVeuqQJnc9jpp  
Pnc8GHcAXC2NGlahE6Z+fBFFS3TmqVLtXIKkpNbv/Qs8p+xdDoYuMH0kp5Vg2fby  
df8cH8TXF3XZdAocVgeEkY+Mht44BP0aUmckbprKb5bc7YQScfJoL/u43aLC8t8o  
7GAUR58eLFdZXwU1PkNb07bff8ewSwZd03s1BsnH+RSQ2Te10fszs90hPQyPMraa  
UpBwPt2dWC/JINfRmn8YxW7YmwKBwQDoA0sId04T4on88GTZbSfkZkY6RI21Y8LP  
zC00/1L3+9Is4bEUjqMLVeNLWHQ+dBsLPHk2gMQ3iMdJmqyYl/+j/iEoR50LZHA  
YhQ1L0i1zRucBbT36ixT9T6NHQP5fRZbvKXBLac5wM30PL71oC0SLlRuc5XdG/  
JoH8am4VuPdZUJS5NaopRCH3QP0yWrCzx7tb6YmFsJrCsSyLVmtOxmW0bWPWeG0h  
Of06q4SUE7J2AaZwJgCxeqVu+5oACjUCgcEA2oYG3ogHqjSALJhVMWoxzM5/Rxn  
ie7A5N/nQNpoF5mlk3NQgkTibo5oEj+JiN0kpzKD0AiMdLEwPbFp0Q1DDA1wkio/  
YBiT48ciUCdHWgMJ4F7KNLHEXkU3n8Mb/UJc9QHe+AbXrMVAzdYYUAL6aITftyjS  
ewSdoiUM/fC2WZXz2EkncTGFBd9FJ8jeoHWTvedq05N8o2BifhQWG+mnnFQa8zc  
buG/X2M53PA/5+ZG2E8i/HQXiJm69IN3+Y/NAoHARNQFRG0wQ/HmoaTnJiFdvkIg

```
/1Qq/e62X/fgSWKdSHfqJ+pkUAbom0DZhxacLZJ4IxnHk8WrcBYhmNJL+tfoRmQL
fT0W/bww+JigCg5iktXgHm8K+qj7sYSFo/04V0cREB79wjiU1N2LI75wLGW7PC6y
vXXFTp1ohd50nV8tfUA8EMD664PiEQ/nS6R3JygEV7EfAetMI77aLqJNhtnBh2R
0m9hONTM+XhqBVGWqSPxE1T1/Tso5X306he13eEpAoHAKwQRFxqHKWBJcsibflm0
wwTkE0U10F0cnSI5p/ZycTkY377UqbMrTbCvrxFKCMWlWmmyBimgkR5twRjs1JMf
hfX+A6T4wGRqQyzr9N3DwR/O+QQcjneU4WqE0LUXVNmp2znpNP0zHSjj/4R9+Cy
OH/Drh6Nrrbbi06SWZwxE945ZrsR0hKjYC849H7yPBs00pFfbTLfqMAD7IpdrnOV
qHvbdUKK20qpnLsHNHei6Xy/qQJQ0oiv/oCoyTTsun88
-----END PRIVATE KEY-----
```

## MLDSA65-RSA4096-PKCS15 (2.16.840.1.114027.80.8.1.35)

Use the following CSR and keys to test the MLDSA65-RSA4096-PKCS15 explicit composite algorithm with the 2.16.840.1.114027.80.8.1.35 object identifier (OID).

- [Sample CSR to test the MLDSA65-RSA4096-PKCS15 composite algorithm](#)
- [Sample public key to test the MLDSA65-RSA4096-PKCS15 post-quantum algorithm](#)
- [Sample private key to test the MLDSA65-RSA4096-PKCS15 post-quantum algorithm](#)

## Sample CSR to test the MLDSA65-RSA4096-PKCS15 composite algorithm

Use the following CSR to test the MLDSA65-RSA4096-PKCS15 explicit composite algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIZOTCCCiYCAQAwSzEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECxmGUETJSHVi
MSYwJAYDVQQDEx1NTERQTQTY1LVJQTQwOTYtUETDUzE1IFNhbXBsZTCCCAwDQYL
YIZIAYb6a1AIAASMDggm9ADCCCBgDggehAPxkh1CJ8pm3VQB+Xmu7WBivB0asomNa
eaK9sSVV8z/eUHNzKJsVU0DK7UrBXeL7if8dhwroJQ1jCepx+z+ViQLV6oRT90zn
3Ue80R3sBDd4S59i/noUmZT0IxjtN5CEati77zpL37LCHQkhRnClv5a+srA+GI4i
wZcWiaNFFLOmrTWOCY7a6bTqBHZ/fAS83KFngyE3YHGTH0Fbu9odQFRmeZieeoZ
3FXFPXYGss0hQe2+Gvca74t582DIgb8x+8T2/EshaoGc8rkQDNMLLeJPCnWwyN5L
NCwgzL623jetuqn+MSBQgXXK7jdxg7LiDr+X+WMvu5kDmbPq7F9gK2j3/zYt3mYP
rrIgnptHjAsDYyEpQ6jH+/gtQoRV8WgJveoBBQ78mBXQRnRWmauZEDn0kvuy9qic
eFBzLZ78cwCirl4NFu2jo0aTwzvPIWwjIF6P00Y6D1wZqkv6GWRM9Yrvqmig3/r+
OKSMw2iEdQu9G565ImKM0hp1diy2EqU5Tqi9wNTW6sqblKxiJLeo5KP2me6GTqdf
7e1wd9x8oG/8Xi2ef0wGU0fxJdrDWwv+N4GrQaQnl80GXpSA/xnNnYssU0lFiOm
7113pDsZgnFt1od5Rsn+g2PxV1KKn2/YcMVICybtImdYet2d80zf7eeZ0KSnAMK6
uhNMQZ49AbZnHrikiSQEyvEJnmVdHtPRNPd9FbYj9nBqDmLIpa4BAnCKA9r6qd/F
wgM0ecItfMzUyXTK61BgfQmjmmZ2HcQWlhULTlhL4uSlxhhpJr6pBeViKjtMOSFN
t4PwnhaeXKn0IBl04R4IPi9yW3fXefsIoKAm0wrXqw+iSAMmx+GZHP7Unf+e36a/
yKtew6INaQ0fYu7QgabfrJjAYd53MEluCJ6wwq0KajYsvoae3gEnhdFr08ZFEYM8
muHswqSmgxcLZggig0HeftW/TAqNf9brz0OCftq9c4+hbMf4PtqaAydDq10D2T/J
E4dzzdJ0k4KpusX0Klu6eDRptkqTxLjr36Jo8U6yYM50rpy0LhJUBwPiP64SbrJ
Aet93aBdiwQ4y55t3uowlasDpyDf43ljeLkq1/DVA4Pt0sRzuR7BCTRdANJk76Jw
EVQQmage9ljz4uHdiRHec5BgfZiWUEHQoMD0zKCC807vN9JDHZwe1qRKQTM6hgUg
7X7CqULexLA8aZ4wvaDy6LSRKpD08ZCu8lHnGAwRye4tgGRIeK5AbsDjt4IYj71b
f3dpmD/EaoDFV2W3wU9WdezdoezXwou00RoE1C0BcjsSoslkDbtTvJokIIRk68Hm
QcfS0JgLEyRLAHx+d/Q7E3V8bnKnBixPKPvBSiLOagnF0patmBjZ6Xb+31EXHPaj
ByLFGFTxoZEQkzRMQgKKdt/73UHVJkZob6Qjt0uhqetYXFLlCeij8hDatj8yEvfJ
0E5wABtt0Zrppw1L9vZGBSuTHfFK+5gWzX0brt5C5n26arPBmthM4t4kcU9JDtrU
Y3BkSI48EcPlXn05W53jE8514Qz+Md/D9gVbH59UTMFxzDgaaB6m6VtX4+trcqQ8
```

EdJLibsw4XlokMG1BbXpUtbASeurRxIh251m4im3jEcCRYUa8llsV9/xaT58yoIU  
ox5cWtEEBL9/MjbdSQ9/vtMVND0beT90AqbtIXP9uYRWro1x+GF8tAZZ8bDMLIFL  
Th0vWGF1U2vgGUujILGM6y09/RuXF0RizlCMvAs2ilcg+vjVcr/CRd5Kz9McF95o  
4JayMblX/E/eMV2iSXZ2DX276WeTXAuKtu6CV3CTqP+T6gQUgbkdSwEFUt1bYsnH  
wdxTsnNw+N0nPaJEGTSlyt6TweEpWkYe0b2cntCSeVSPHApIsF/cr89J1GGaH3ul  
wIGAV7qfQQkLBiUHN/DxNqcH9oyXFrnKZqD8j+WJGzBV3RSy3EHIq+MkMDAH/6cN  
vXVwvN5c0cOz0ygijsdu+vbNwAIrYbY9HSfJs/+K5qQ7D00GVJzfbm9JHyGoWUPY  
g0acTNvg5gj33BXxpDywlRHAYXs3NpZEkg08CYJY98WUnGJoLRVwc1s/9wSsFIXX  
IoAsvpjQ8EgUbq6TJglei2cA4LbDXJrLEkgYyxbeInkJw/TQ9IEJiFLE0HhlcP  
C1cos7DaG2VaICJ30Rga75e6/ncIZuAYdqLPxKGvjxRWdZh3zUdO9XC03Pl9tQXI  
qZVenFdQHvcG25r69cZwkt9ISqrUEDvHdPT3B1F0u2/kDYPBeaYmHmTRAUGyGHNR  
Xolj/TUOF2Pg02rxE7aWoRSyHtGL2PKR3lj2Yv1L6hVDlwMK49UXDuaESjnzbcFD  
DTA26F8f1/Ncr3nw9TTKhhNNGu52umUoMJCWNkJVtIpzim3VgDPXuYEP3/nt791BX  
kp0Lp7WKppUcnjgpARaWyOPdaa2HuMznucWyqyNBjoj05C/XVASaJ/VaHx1Xhma3  
qZEA9keMohpQNBV3/SuHNKL93KZg92X7WqtaJuyr1v8m580vPx03ZFGgf/Z/the  
LecY+a7+YwDFDEpv2lgEVK0/4JWWTmhxL0ak9KbwMg0rrHB/Yw6Wd+p+0b3SSZ+X  
SPDEJ307uLgWA4ICDwAwggIKAoICAQDJ663UCqGVlqMpRV/Y7p4Y75wPPIJGZGcx  
H+z5tGpaYea/vvWbbQKzdIj/9kGIzC4eTCYg30ElpHu9h/bVqTdxH048x2meEyK3  
Qw/ZG3t/iQvYb0vuRHPMXwHbrfdKDD8yZux3Jp18VeKMHSXJu2gyigzCSNi/PvLG  
sIQVTYzYeiYbYqXigG5607bLnhCS07rib/GX0VSwA/ibTHlHnuJA0B0Qg0r1UJ49I  
Hr70i7/ud19k2X1rqK2hdDl6jSlHdAlaflMva6pDtB7b8B/7P1h+AkP5HJC0Tydb  
r+kT0NZaXKFC2YRhHkEmucEGvpmug2aFIXgZv9CTjU8b5BxkvV4Qck2vMZ+Q5K9  
q3s3QqEY/g7iVc3x76WpSES4o/es6N8+cK0prumsKn0qACUd3bhG3ttVTwPcaDma  
TQu4vJ00aBXKn6GUJDOXYS7GLCRwWG4AdEPsZ6T71NHBW/cD82JUWQR5TZGaapGm  
VwTDhZ4YPJztMmhvjeNL0hCMInvHzBQI09W6FIEAFh2H9X7phAzcdHZ0M1UpytGR  
n9Ra6/brjl6rVfTvP/XTEi3A+LZgDe3Q0gsex5f0mVlClDeQ2iCzHfCP0wWQ0zny  
k0xltz8dxNtZTDhHieF9qUi9nlmPjL8at5v9rkWJULALfjKrSpaCcYXQKcyfR+Sg  
8yGk8dUASWIDAQABAAwDQYLYIZIAyb6a1AIASMDgg78ADCCDvcDggzuAK9Nc53q  
TLf3wM9mDpvsNBZLxBILPzGPDqVeQC30Vh07Pg0l6ZTEY0qiVi+fk8amiHh5ymL0  
pSNZgJ59g4enw04/0ESdmEaUoIqdHyof1jTeadArC8eYGL8bkWZgizy+/BGLAvA  
9vpNsac3ymK2RllGwooe+zWwwq0KMFAtp0wN4fghSQPFibEj2V3PCquqCEwtLe0  
G+3uHoFG7UYmTbXDwGgnA+fXW25SCyvduaCWKxaAIXJmY6n1LtejVJ0FmsyGSW5  
/SJIBtLLjiTGwkfdWv9lDpGEQiRD2e7I13x7de387JGXzvDovE9g8b23Wh02qEu  
bMbGDxaLi6RI8Qe/6giicoREb/LGuGlaplbs77GyQaL6sdAyllKd5P00b9T6N1ap  
Tq+0JC7FstGy5Ap1xAn9J92aG/Hp1wwg7m/VCHvQFd0FRyNMfLYYx23wN2UnajmM  
0WzlddzFtnicATJ0U1qqbiM10kVdI2+V3by/bonZRCrHr/t0opD0fL1/wz5Av40r  
Y34Qo4fLyyBxaGxJJSC556ilG6I+Xi7YBdMA6v+FTpwmhIp+w+j/Gca4+9eUdYPC  
7cNF/aWvPCM1Um4rTv8yF9JG9W/f930t83/BKN4BcAvMgn5/u9S51NqTnGY/bMYC  
GK8cJiT/qeXqqzgu9Q5o4WPRmQGbQELsTxnpA0ZHnI/GCd7ZYWaBw1Jiq8oHTQVW  
4NmXkm0v3NonXobEyE+ccv/T9/QV0ajT02qidRc/5Si4VFqwZEhQ156jHAoKCxOr  
EcjPjXkBO4laDHC3AksmsbikkqLDnTTLCXyQt010IAK0Kdkp9jNfgSvPyLPglQaX  
49B7PUXLeDw0VeKYcGs06tiLwcsWp2mlZfVVRsUydy8ZQk9jTVBhnAFazBGo5k1Q  
pYRV4Df9EzoikSWCJ/z4vnnmtrZ3fh8qAd6W0Uy5XsS/4anW6tevcWgBd78uTum  
ny1UpC0FaTUp7UEbDEg2KJo7d824rM41tH8keHHAijQAcdvZaFUE05Ra9QptMjQF  
UFep+wS/UITd+6iqzt+dvIu3e02KqFaB17TNzN23FoWAs3gLrJ07z3EQ0Ckl9csB  
ldheReQlNhB7tEkqMtjt9ayymxPD4c3NZHM9SozsR4GB/VEKhllMsGALLr94/BH  
lyblXyLbII7IjqLX0AuLaGrK7QKEK26Fd7DmsKEc6V0329Icm0zwdA8yNEdXQG++  
uQXcnoD7tqpZSDiYjzjgPvbgDzwfMTEYpJzeU2S8HYhJ3j+P+2fWnDERNDx1Pj7L  
/NMAJvy7nd3VbeGGips8qdP+9bGnY8eLS0u/8KRUMlX7rLa8duvVo9XP6zvRnDns  
N8U1J14uFwuoVW/urLsYHPmZRv7VSCF5hGAzyqPcEDVh9630tL2pFHllf9LXPBX  
ep/2yG5FBPqnQe8ApZF2WmDYCRWtn+u+DsRdZr1ucwmu51MHByluc9XW/j6pdNBp  
fz2lq6phxFxAXn7no0Jm6oKo5CsTtE30gVn13HRJeyuZdSQ9FvSmFkhMW0EUdRy  
gFkSxcw7bnxVD65H0UNSyuv8dVI+WJZcrEtfsb/m1i0rhKtM9H1AC9zPTcGEqe6I



lBsFaA19pvn8i6ry0WdIqf+KGUVvxonFmA4v29Jt6iQrFpfb08uqXogeDlioE+3  
jkhDBBI7vyLKmBiClyDS0ho2vC0v7nomqCpXD460Ks8Ka54Ux+JbivoZk8K+5YSZ  
6pzuEOIJerYy86l65v90LgwnmhrbewF9PC2wGusuiLzZrkFb/001lBlfV7/nzL/N  
7a3cWQYPgn5HcvxchgGVZMuIMnW0ikFG1XN28BIU0n/y9Cvk2+V6a6j8dBsD62p3  
mLQtA4EEQEmvA+JeivzP/+XzPdGXv/fVju91HH09keNKdIr0NWWd6iWN/OwtQZW/x  
7StNYV6lVJhbHMD0vu3GxhWCEmLKT2WW+KXgTwT3kfRYCL9wYTRSfPtv9ZYEadYZ  
Pwrd1BJWBrxQ/RmqudHE+ufNRx8rigR4UjWDpm5cE3E4HeZY4ceGKugi2+WUup+D  
bySFuxYzWtyCzweoUhvNuM+SKRXWlqRs2pNvjSlS+Kdkv5+A8tx1DU1N7rBE/2l  
yPsAtE2BoXXSke04e9DARENVgK+Mh8485YdD1na0di5rc8Q3bDjqbDyfhW2DvTKQ  
cijRgeHPA44TyqTafTv8kL2L6aHU+Dt1ku6Yq5sQxhuK/585nH6BPAaKC4FNXpl3  
x8ZjwyZ7I0sfN22DyXblPXwyByALjQF9xPrUzRavnMkhc/V9ePzhdJ0KlF7xMTw  
g+2m+gI9MczD+x6tMHfVLALM6aUaua8fJMI6iUt/Kcwnlwf2wnw8Vm1HkUzmIcMF  
585D7xY8YxWFRn2U7WUJhnE5nfjg3IMjmJRZE5Fx2tzC00/bkqlWHyY3isDTPNyH  
/U+PVMQpBe15cNgFm3G5H6eWpZv6QHqfzLiUpV4aTy+ZnkkwAB1z7p5FGHB5zI1  
C9DWCQ0ESBAnseUHkV34frs5R7gLYe8xVSNhufkpW/D9WZo/V8F+h23dRmWL1ba  
B0mlURVXhLPJxPgUDoiHjMmlpYAXGhPCDnik/Dk093N72AQNuvmMiaZ9rA4iQriW  
ShwKyFwvYkrhN11cIJBzVwLbrOrqTxSCx+xMKj0+jgMJo8xMIqJbMSHaVnRxrZnJ  
x2yyJWQ4kbrEOoepMJQuJvVunI5G1tmBEglzKCq8uEvUYa0e16+qR9FANG+sHa15  
HSnMIEmWu3y3aSdgtTZS9Q6mn+iT0B3vZ53WglfpTV30JNk74DQ9pAhCNNoUq/Nc  
8267hNDBFQ4ZoykBgXq5pCU3Nzy8g3nEIMNGpbYvxW8PDdyZ2h0OVGQAMYh66CgN  
v2TW9qYeqYUGM0Whl3/MjbsLhPS3glGz67iWtfPGL1TrBRbm2kk6tGJI1RP3L/4u  
RMlGAt1usZSNFPNfWsbFaUxqabduET1tFkmWk10ou3xWi7nxHOK+Ie5AVMJUGXTm  
RiKpDFYDPTbmrktdCrcHuqVpyfxMqeq/LLUx30g53DHHeAvISQJZr1AlDbrio7MY  
82TILcLWPKetBt/CQSwjDf+kw1ZQnjy8Z33H/udkgudDir0MDDBUrsbZvCuUACi4  
TbY3tmy3NNR02yLLZV3XsHhjv2g/l/cRqEXGJnS5l7WLDy+ObEl1btj21QrHP2WE  
quFm4U+4mdRzDbeS10U4L/lwipwxZ/RG6tAfCd853iSxwALL0ZWVgcL7LP+ORrGP  
foBJzro0UvHp0g0jFP200qncEV5mfBh1DrvtVIUjvz9PMznR0g3ZdLU0cI1TSsWZo  
LbvQg4o4cW2qUrc03pEtNuxSqN4bYrjneM8RVLZl76CpmpFWg8UNCBHC4oH03Vg  
ljL0s2o04Bi1QUfum4nRCFF7G1QLb9TdAEViggdNW/QDqzZ9FfxvFNkRLeHb8HpF  
5/7HVJFBsV73wtwMEznUdP8FBExOp9VqGMUfu9YseYma0l6QDw4Y+CiHzqSWE6C  
LgooK/qSdc7+5q+SwRMGuoBHDU0EIfSfgVMWDEzt8o1lc1fQcG7X/nY3DE8x8uFf  
+uca9EchVe9jck5yb5gPGYaFdw9lXzJLSy4PsoRGE0SEKv6MPAexkd1nUDs2JiVn  
6VZyXoXjYVAG4KM280aHU9k/Src01eb3tpe585xBpRrRsWMJ3YQidBCKljKqYH6N  
V4NDHvs5YpKxyVDOP7EL5Ro2c85reUsIm4mK+0WhNnorKenKM1moQ7ubxLk9m1cQ  
+92nQ7bT8s10BQOwE+0EY8I8Cljk/6sefB0DuyBah64ALDNxYmVdEb7n1Pf1VG/  
65sB9p2CwuzxR0mLITFYaGmeuX34h5sRKPrvejJJo8PEoh9lBLQBBMn3xFeUBZ1w  
OTxpwiBz5HNboaWwUC+bYVd4BozRsCc/DFGSUB4VfVr/SReNYOyo73QtIAd0cZfq  
H0ReCdFAH0jJp++BvOXmLOCAgBkGf31VLn7f6nwUwS85y8FjpIFLYEvN4kpViIYE  
UtD5FGCDLZ++8xrapn4LxVLSscX+/8ToOfk/9C62vZUIjHmYknnIeS/dYuMELXZ  
HJ8ku16XuIXYQZ90b68lI6T+0KA/Fsavhh0aWim5TzbJtUer4uQK3ZFckL30PkFl  
mWp3wJr2Bccfb6k3vZv/SvWx15kMMSyoJ8YDP6hbv07eAduok4P7KiSVMLFXN/fb  
rB8VozmUN1PCaE2sWSUCHF7KKG6H02dSNQF3AhijGq4iLRsvnxPfxZjBhyc0cIsX  
IyJZoXZSszvhg++jhy7KuWUARLmQ08Sr8tkvDDQ5PWQDJzlBr7XIzdzoGDhGvufs  
DVmEj8TQ8WwsxuMIF1SAnJ3DxdPa9wAAAAAAAAAAAAAAAAAUPFRwgKw0CAgEAsz57  
EUlGZTAX9SQ4anltbmPglj856iuJg0rWMMsCwUzs5dANULLVP1xRYrH6doDPislt  
Ttlkf33bF5ths8PF2XhA8j00dG9FEwVsXjmu0ud1ufb7pqmB/V8rh5zNtrjS8tvL  
CkDeIYZcRh71ttDG0fYl8oPlBTtF6Km3SYsa0dgFog60aVqP87xWM+psXB6Pb95j  
+ytRhg2930BJrAs9xAUBcxEbwwdo2KnYqcfZiwgfYgyJfb021pzxcB4d+NtAB3ru  
VCUf1m6RMm2Q1fGEXP73LWC5FiBapCiXIJarAaFB7YTP2wApiWX6geeZQlTuZyiy  
PN2JDBLL56gKlHifu/YZ0U+nqruSY0u6ZARftJ62nqXYjGPd8vNUBhcQgzd1LWS9  
4xH7XJvj10qtmzxc652GazQNIhrwtERILPvEHuxXrYaem0iweiqsVjfi+IooYXw  
tYh8+JFMADvrInbpQTz13X1vMjLC61yI+p0Mk/LQq/n99WTjHsVVxkisw+RDId/4  
sTDnogujMNM4ZkP/QywYgGy1Z5V5r8sbNtXfLc08/tc9nuon3Dbd3PIiS51u5Ya

```
wkHL4Ve/IBhyzCAAELvBwH4wSTbD0yVU0JNW3j5Yng68xMxZqg5DFDb0JbDopPfI
JxKovy8JJrdW7Hid2wtg9vm9V5a23AtWoLdpZwc=
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the MLDSA65-RSA4096-PKCS15 post-quantum algorithm

Use the following public key to test the MLDSA65-RSA4096-PKCS15 explicit composite algorithm.

```
-----BEGIN PUBLIC KEY-----
MIIJ0DANBgtghkgBhvprUAGBIwOCCb0AMIIJuAOCB6EA/GSHUInymbdVAH5ea7tY
GJV55qyY1p5or2xJVXzP95Qc3MomxVQ4MrTssFd4vuJ/x2HCuINDWMJ6nH7P5WJ
AtXqhFP070fdR7w5HewEN3hLn2L+ehSZLPQjG003kIRq2LvV0kvfssIdCSFGcKW/
lr6ysD4YjiLB1xaJo0V8s6atNY4Jjtrpt0oEdn98BLzcoWeDITdgcZMgfQVu72h1
AVGZ5kh56hncVcWldgayw6FB7b4a9xrv3nzYMiBvzH7xPb8SyFqgZzyuRAM0wst
4k8KdbDI3ks0LCD0XrbeN626qf4xIFCDFcruN3GDuUh1H5f5Yy+7mQ0Zs+rsX2Ar
aPf/Ni3ebKmusiCem0eMBJ1jISldQmF7+C1ChFXxYa096gEFDvyYFdBGdFaZq5kQ
0c6S+7L2qJx4UHMtnvxzAKKuXg19Ta0jRpPD088hbCMgXo/Q5joPXBmqS/obBEz1
iu+qaKdf+v44pIzDaIR1C70bnrkiYozSGnV2LLYSpTl0qL3A1NbqypuWReIkt6jk
o/aZ7oZ0p1/t7XB33Hygb/xeLZ587AZTR/El2sNZZ6/43gatBpCeXw4ZelID/Gc2
dhKxQ6UWI6bvXXek0xmCcW3Wh3lGyf6DY/FXUoqfb9hwxUgLUJu2Ix1h63Z3w7N/t
55nQpKcAwrq6E0xBnj0BtmceuKSJJATK8QmeZV0e09E0930VtiP2cGo0aUg9rgEC
cIpr2vqp38XCAzR5wi18zNTJdMrrUGB9Ca0aZnYdxBaWFQt0WEvi5KXGGGkmvqkF
5WIq00w5IU23g/CeFp5cqfQgGXTThgg+L3Jbd9d5+wigoCbTCvGrD6JIAyBH4Zkc
/tSd/57fpr/Iq17Dog1qo59i7tCBpt+smMBh3ncwSW4InrDCo4pqNiy+hp7eASeF
0Ws7xkURgzya4ezCpKaDFwtmCCKDSER+1b9MCo1/1uvM44J+2r1zj6Fsx/g+2poD
Js0rU4PZP8kTh3PN0nSTgo+6yBc4qW7p4NGm2SpPGUmvfomjxTrJgznSunLQuELQ
HA+I/rhJuskB633dof2LBDjLnm3e6jCVqwOnIN/jeWN4uSrX8NUdg+06xH05HsEJ
NF0A0mTvonARVBCZqAT2WPPi4d2JEd5zkGB9mLBQQdCgwPTMoILzTu830kMdnB7W
pEpBMzqGBSDtfsKpQt7GUDxpnjC9oPLouxEqkPTxkK7yUecYDBHJ7i2AZEh4rkBu
w003ghiPvVt/d2mYP8RqgMVXZbfbT1Z17N2h7NfCi7Q5GgTULQFy0xKiyWQNu10+
0iQgiuTrweZBx9LQmAsTJEsAfH539DsTdXxucqcGLGko+8FKIs5qCcU6lq2YGNnp
dv7fURcc9qMHI8t8YVPGhkRCTNEXCAop23/vdQdUmRmhvpC03S6Gp61hcWUsJ6Iny
EMC2PzIS98nQTnAAG23RmunA/Uv29kYFK5McV8r7mBbNfRuu3kLmfbpqs8Ga2Ezi
3iRxt0k02tRjcgRIjJwRw+Vec7lbnemTznXhDP4x38P2BVsfN1RMwVfM0BpoHqbp
W1fj62typDwR0kuJuzDhewiQwbUFtelS1sBIS6tHEiHbnWbiKbeMRwJFhRryWwX
3/FpPnzKISjHlxa0QQEv38yNt2xD3++0xU0PRT5P3QCpu0hc/25hFaujXH4YXy0
BlxnsMyUh8t0HS9YXXVta+AZS6MiUYzrI739G5cXRGLOUIy8CzaKVyD6+NUKv8JF
3krP0xwX3mjglrIxuVf8T94xXaJJdnYNfbvpZ5NcC4q27oJXcJ0o/5PqBBSBuR1L
AQVS3VtiycfB3F0yc3D43Sc9okQZNXK3pPB4SlaRh45vZye0JJ5VI+ECkiwX9yv
z0nUYZofe6XAgYBXup9BCSUGJQc38PE2pwf2jJcWucpmoPyP5YkbMFXdFLlcQcir
4yQx0Af/pw29dXC83lzRw7PTKCKNJ2769s3AAithtj0dJ8mz/4rmpDsM44ZUnN9s
z0kfIahZQ9iDRpxM1WdmCPfcFGkPLCvEcBhezC2lkSSDTwJglj3xZScYmgtFXBz
Wz/3BKwUhdciGcy+mNDwSBRurpMgmCV6LZwDgtsNcmssSSBjLft6WeQnD9ND0gQk
iIUsQ4eGVyKLVyizsNobZVogInFRGBrvl7r+dwhm4Bh2qU/Eoa+PFFZ1mHfNR071
cLTc+X21BcplV6cV1Ae9wbbmvr1zNaS30hKqtQQ08d09PcHUXS7b+QNg8F5piYe
ZNEBQbIYc1FeiWP9NQ4XY+DTavETtpahFLie0aXY8pHeWPzi/UvqFU0XAwRj1RcO
5oRKOfntwUMNMDboXx/X81yvefD1NMqE02C7na6ZSgwLxY2QlW0inOKbdWAM9e5g
Q/f+e3v3UFeSk4untYqmLrye0CkBFpbI491prYe4xme5xbKrI0G0iM7kL9dUBJon
9VofHVeGZrepkQD2R4yiG1A0FXf9K4c0ouT3cpmD3Zftaq1om7KvW/ybnzS8/HTd
kUaB/9n+2F4t5xj5rv5jAMUMSm/aWARUrT/glZZ0aHEvRqT0pvAyDSusCH9jDpZ3
6n45vdJJn5dI8MQnc7u4uBYDggIPADCCAgcGgIBAMnrrdQKoZWwoylFX9junhjv
```

```
nA88gkZkZzEf7Pm0a1pgRr++9ZttArN0iP/2QYhkLh5MJgbfQSWke72H9tWpN3Ec
7jzHaZ4TKTDD9kbe3+JC9hvS+5Ec8xfAdut90oMPzJm7HcmnXxV4owdJcm7aDKK
DMJI2L8++UawhBVNhnJ6JtipeKAbnrTtsueEJLTuuJv8ZfRVLAD+JtMeUee4kA4H
RCDsvVQnj0gevs6Lv+53X2TZfWuoraEN0jqNKUd0CUB+UxVrqk00HtvwH/s/WH4C
Q/kclw5PJ1uv6RPQ1lpcouLZhGGEqYS5wYSBWma6DZoUheBm/0JONTxvkHGS9XhA
Kta8xn5Dkr2rezdCoRj+DuJVzfHvpa1IRLij96zo3z5wo6mu6awqfSoAJR3duEbe
21VPA9xo0YBNC7i8n05oFcqfoZQk0hdhLsaUJHBYbgB0Q+xnpPvU0cFb9wPzYLRZ
BHlNkZpqkaZXBMOFnhg8n00yaG+N40vSEIwie8fMFAjT1boUgQAWHYf1fumEDNx0
dnQzVSnK0ZGf1Frr9uuOXqtV908/9dMSLcD4tmAN7dDSCx7Hl86ZWUKUN5DaILMd
8I87BZDT0fKQ7GW3Px3E21lM0EeJ4X2pSL2eWY+Mvxq3m/2uRYLSUAt+MqtKloJx
hdApzJ9H5KDzIaTx1QBLAgMBAAE=
-----END PUBLIC KEY-----
```

## Sample private key to test the MLDSA65-RSA4096-PKCS15 post-quantum algorithm

Use the following private key to test the MLDSA65-RSA4096-PKCS15 explicit composite algorithm.

```
-----BEGIN PRIVATE KEY-----
MIIEZEWIBADANBgtghkgBhvprUAgBIwSCGP0wghj5BIIPxASCD8D8ZIdQi fKZt1UA
fl5ru1gYlWzmrKJjWnmivbElvfm/3vzIMDJj/jhAQUldbvoeMgtBaid5tSg3WcLk
8l8IcmU2ZE5b60NubqWP861lXrmK3+3PB2T4tpLLRsGQXGSuHa3yDhjBz0fpc/K+
bYEW/sMZEplxr0VgZLmaJVpRnvwOenYWMUBYZgFBFGUlQyAhAAg0Y4E2EUAENQB
JxhQABFXdFmYJWSGQmFgdgUWFiuARSJ1dXUzRiJUE4MQBWh1NDR3EwgCgSGIJnY2
IhgmUnN1RnQhECNVZjgUF4KFEHiCNEaIYZAzAGMUJkIhQ4ciJRaFMQBeyhUWMTVS
BGCDF4BGdjQCJTEIziASgGVLAGBodZijhXUxhIEmEXVDF0ZYaDMFUEUD0IKDgndI
MnR2gzeCJBRzSDBACDKBI4WEgXNCYQWQSCMYRkZwg0QkMnQmQiQiRYYSV0hFeCdE
AxGDNXczUjUYEwFjGCAhIFREA4VFaEFkWDYCFxNSH2RkQAjNgAgHeEhARCYHBIQx
hXNCQAgUCDMYzWMDNUWAN2dlYRF3YhE2eFE3AxIBFFhjRcnh3VQAHdxURBiQxVi
dDGGNQABVzEgRwEyCEJCilhhIXYCJHFHR1JRGBGHRShACINUMoMDOBJYZihmISgC
AVUQglJ4SGJLM4UYcyACSBFCIAEHvjRBNAckAyhQEaAHVkdNBmUicodkcXKDGfGg
MBYhJhEEA3YXeB1N0BnUmYxBChgUDVoBEU4I3dGiAhUgWRXUHNXULRIREVxRDSI
YTSFVQfHBQCAEIqjJWYXIRYYg0dzMUAKYzQyRgaCALZEgwd2MCOAZHJTMWQHUQRn
OBcwcFI2Q0YSNUNwVRVGMjRiIDJiIERhMwVUDZAGEVBVFAVh0NXRjMFUWN1NmFF
dQM4ZDgARmMncISHZ1UyQ3ACULZlFRGEclA0FiMkJRARRoICJ1NQCBrGnH0EhmJl
UFdSVAhRNDZBKAZQFgVTECMYdBhUBXNhYwKHA1cjQnJhZlJhaBgDM4dmQDVkdzUw
cwcFmifBFSgXUHCfg0JEBBETgmYUUER0QmSDMVKAdgRVc0Q4dXIAhGVUAoWHgHcQ
NFcyMiIVOHMxBVFQQWRhJoZBZkYCM2QRMiYlZUeDVhBhWDFhAGRVeFMihQMHIWgS
FlUxBHBwRmZTilBHOCOGcDgViAYDFldXdhACSBVXMXQQYDFWc3NoMCUHALJwR3UV
ISYIA3gwAURXMAEkUQQBYnZTWAUmUnBgZCFHNxg1B0FHdlRyGDANG0IRJzQnZLER
BDB2EmdCQzITCANTZURhFmhoJWFGEUURBhBSZgNGEiFDd3g2VYAoY0CHVWJEAfZI
ZRgCARJlJAR2aGYxY0ImOCMngFWCVIAxh2gSCAVXSDMYhYNxSEEnCIAkUzFVBFAW
GCRjBXR4gCSBgndkYgKBB3VxSANDEAY0YHRiITc0gVgwWCVEQGRXUghBdmVYdVdI
IlVHYjhN0Y3clBxcUBkYAJgmikaKfYRJTbzSCUDUWgTdnRQhHNydQhQgxdgFTEH
MjcxQA0BWBVQI4E1IDJQdhE0JBY1AxKAVwiEIYhCNWR4gyY1ABZQRHI4JlcrVUE2
BhRVFYVIANfDsoANlADQ40GNQVnRHEBBjEQUWMSHxKHQhVUGBJwV3VhNmZxVyOA
c2cYUkaFFRaFWBUAhyRwdmE3aDAwJUhlFDVkh4UzYjJHYLYaifhwYjY2aEVXV4JV
aAdKETJ4FVBEJhWdKAZkN1iHFMTFHNouRVxIYJzMwNnYiWgQLJDVnKHAWYRQxE0
R0KIg1QgQAhLqjRGfXVCZncHBCIFelDcdZaoZhQIRIQgEcCEaEGECHRMNadiJiFS
FYg0BzIgNDMDEiEBZVFfCTRHaBeDYgIRWBINTAWU4UkERGjBRFWGdQFSQXYgMY
U0N4VoAkFnMjkhJQInVkImJCdoZUEXWBgNAwECY2JxWHAiKBBWgxBRaBRDUhKFUj
djJDA4VjAYJyGDBHgIJlZydSfDAEJFF2h0eDJwMVQkg2dzQEh3B5Fewdj82jWr71
```

N7Gv+X09RN4dV+FTn2TSH9Gdk+cbLdvC3EcMrLMb3ndkcwTa0VZ+K4CeH2G0QuVP  
AKaY90TUULr fibos91PLLR5bfwV0WkMdX6G4j6Wm5IgNA+MEotDNZkh7ehAHZkxK  
5XZua6G6kvY6ZyH/+7wtUbzqaxUdDffTCY/LRIHRgzIkIR900saR2T2qggN3cB7o  
3vW67CE0zyl0j+P5kMZt66KfMjEc97ELdTifq861q7f5WdEKwunjPAK+cXAAT/7z  
Q/opERRYkkX4dQnsdQyf6SANT6AFbU1+Wxan54dW+N32iLu/g7DnAzN1/U0JLgrR  
uBwkqW51og5HZ8TcPnHYidmNXdUHILQ/YmYlci6vpdkrGR/dK0qaLg8X3qF8dg8p  
zFPpKlzE05hcxq2Ir10EJM6x7fkTaDwpgPzDBBz3ZP5Y2VqYfWFTnn8YUF+bCxUw  
m1h648pMTkVfaI9ti8rt62orOmRUMzxfrDX0jf7acpwpGqeWmHiHNNhm2rTvHhCW  
t/1RAsr7te7WvriLA0TZ5y0ZKwiGAjx5yvUMTi7rUrEu2oSvAoW5Pfxixiz19LJxk  
YLXlmdC9hYd+EVmSdELWzR92E/GE23rLpAVKXPJDhQyzMJZBftP3GF94tDpBjBBW  
6u16U9ne2AgzUzxIjYLPShPZ7FXvsxwmHKAAILsIIViYwRtisVZkbMgAm3zhFwF  
4kfPFUftfKp4vDBfyyBjux7sT6dsRpcMMDC3T8IvfwWNyKcQlH3ypSQ9kEor0dzF  
mdkDWylJuGtdAX/SNIWdvvesB2EG+llaxz0gEcFOA7o0Cq2xUrZzCtZXpteu+Ic  
KtiW2Y2lepLy75aa1QsX6ycd7kcEtMC76qmc5TSKlJ8XoVKpjs5lc2R5JmtRLk8v  
2vKJEilnCRsoc/yIwQGUehCKfhxCwHdnC4hy6n0zYVY5VURkBPE5yGs2LJ/9Nccg  
7zZLLYIT2DJ0S1sVdZrr6bnm4u5bXzg+ONGQYu0/SiNBcju45rJtCLOZQN25TRqz  
Rz7MpnA7+rMKzStml8P7ZHOymUUX3nX90abBApbXvA8q4u6Y81Nqfd6c59CEgXIE  
F+VLL0M3zGxj/g2Lfy+6NBoJqp9TrEBgohS/57CpZTm/MDcn7HJMGgL2M1dYQE0X  
g03Fdm0DdmhjX9SLf2t5LYXam0m9mFgPWMS0pNTiiPSstaI+nyfxOGZkIYA5kuoS  
S0/S+cu9VdIeQk+huedJ9kYpyXIdKEY9j0l1qtRPsWCLBPCg7V7T87Axx+DE9L9Z  
tEag1ZQK/Lc8uvZ5KGO5F/5JjgTga6fmfmadYp0kZFs69ldXs0vAe9i8Uy/YMpdKM  
C+QemMHwizSnRs1ihLSHUT+OJd2ElDtjZ3NNcNs0OSDLJzrXw0HEYHxftPVVwBA  
1R1LH/mXV5W/NYcTGIAMWbKt/Ks3mfZTXIpGKq+iRfzrl0fuRemfSxxkVW8yMK3uS  
Z2vU4yCqpCXxTM4WfZYP0GrPw/RD7OqN0rYjgCbLXkrjigctfIZA++PiYdl6MM9  
bB+L4dq6I/1kxBbnSwgm3WV2moj+AcNl7re/h7ywLbtH1zdYrWQBtgZINyRvgj4T  
+d2UdWuzVvd2oBCbRZbfNzxBLAMv/zP/9TZ2X+0frDwJ98+bui5da+xwVocQqYxf  
bNoA2b01QfbxyH21JPoiSWIxxku24MTUQ2BakdJpXBjwQcnwam29kxzHehBunPIem  
pTztjmtZLATfVU0oj+eFU1eGb9U0W8wsTGnozW/h9ZL+CzVYcjhDu0HoSPAb/9Sv  
Suc0KENh9QSFxNb0z8R3WzmKSDtCktKJ5YmnWTi5BIVd6aw87P2eIbjoCBNH7ioF  
bYMF82UMdcFmpmidn2QhioBND96d0f+B39jf+5sR3D7N0iTOPQrVLZnncLqEyYNY  
bTQLdLEY17kZcYzZh4uFeaTAU99AETXafYyBDi0K4WmQYc70z9VH7bbsaCNVLXh  
s13ckkStQL2rCjdnrcZvdyme/dK0Kq7nLyih70iy7LeW5cUdCcXjQ+8XudtGzNOv  
5Xo10FqDut4hwa0jPjaQr82ztYliIhhWov/qKTexDZ7N3JvjoZe43PfqB4sTSnDc  
dNdbDdic9ubN2cz4V7cKSjiEAP2InRZGml6ldhYBunR/g0rpAG/Eq4zTSfpFm+rSz  
JYkS/J+lvqRN1yFCULWDXDZJqcrYkTqG4B5HdLuRwXcXVd3A9P7vwETpq9ecaBLwb  
AwzKYxibSy6r04onpnUugNk0Xghwuob9YHbPsgdApUaLOFrGf63itiC2RZdeN4CX  
rX9tougX61U6mF/e7WNLTiSiurzGLASPvYYLDZuM19Iqhqt8GA0dWT7ynMexV5Q  
PEl4QJv1ZNUgEkpz7ktu4lKkWnMh37v6nhe0NLQ8RI0p7fBdnjYdpd47j0vIpJsN  
bboyotaINK7X4EYsWyNj2Uhr4RNUvJeh20oUkCFsK8Ms8cgDU3IxN4wa4V7PGUKo  
y+rUs3d37+A1DwmJq34uir38Iv60fv42N5xJUDtcwPd5BEBZ78WUj5/dvMGjgnuB  
HzJgcf/m9yUvdvIzFX0zjneEQIhvwWED0Yk7vZID9+XT+j3dhqsmblf1gUjv4kk9U  
p/OL9St5qYamIFvitTIAuI6PVuv2sEyrCmf0lPr500i6um5Q4oBorxE6CAzjhYEE  
tI05UNs3pgmQ9QtT5WkQC0zrNe5m3pZ7JZ2uEr4umrPh71g243xZad+T9hd14AMA  
VPvdELg/d4ze2rcuHrvFFw/hoA0w6u4EFmAddmPtEANuWjHWPAGgTdR9MCzwnCxQ  
+QHU1zHxZiZaXwDxN0WR/L6wG3UmmAw48r/tGnnMCG/HJjpzIXfMMtD0mKr0ArG  
/5G82V0RP3NCM4z3YeugTPudzCXXfBelhMlsGU0aUF0Ftj9AelU6EorxgVvJ4IVR  
tjGWSXeI/kce6mLYJm+N0ovDUDemaLXXBbQgsWfehWiQMgzBbHmFlyHCAULBM0G9  
CF6plKmrhRDRp0KoElT0qgu2f6B5d+peNhdwhES8gDfL92jNvnfhfzZEkg9Rs8Yy0  
ZNdM097t1xK3x2FN6z2wh7IUK2doR3YHWH7NV60dmQKxaUYSxsRkK6XxmAZVMkjC  
lez0bzldYwfp1lEeTxqYhWCZaLAIs4ng/pb0xs9CHDJr2u4yE1xXHdwCC7dsfswi  
FNGy+50FpIioV5GGAbC2WS0qPF3Qk3URJLkQDb490BK3bx90v0Gcw7SP0nQfSFG  
ah/Jq66J4H6KyCvCvgEvBjn8eUrQRdh8ajrBEc1nvF1ddwAY0XIEggktMIIJKQIB  
AAKCAgEAYeut1AqhlZajKUVf206eGO+cDzyCRmRnMR/s+bRqWmBGv771m20Cs3SI



```
//ZBiGQuHkwmBt9BJaR7vYf21ak3cRzuPMdpnhMpN0MP2Rt7f4kL2G9L7kRzzF8B
2633Sgw/MmbsdyadffXijB0lybtoMooMwkjYvz75RrCEFU2Gcnom2Kl4oBuet02y
54Qkt064m/xl9FUsAP4m0x5R57iQDgdEINK9VCePSB6+zou/7ndfZNL9a6itoQ3S
0o0pR3QJQH5TFWuqQ7Qe2/Af+z9YfgJD+RyXdk8nw6/pE9DWwlyhQtmEYYSphLnB
hIFaZroNmhsF4Gb/Qk41PG+QcZL1eEApNrZGfk0Svat7N0KhGP404lXN8e+lqUHE
uKP3r0jfpnCjqa7prCp9KgAlHd24Rt7bVU8D3Gg5gE0LuLydDmgVyp+hLCQ6F2Eu
xpQkcFhuAHRD7Gek+9TRwVv3A/NiVFkEeU2RmmqRpLcEw4WeGDyc7TJob43jS9IQ
jCJ7x8wUCNPVuhSBABYdh/V+6YQM3HR2dDNVKcrRkZ/UWuv2645eq1X07z/10xIt
wPi2YA3t0NlLHseXzplZQpQ3kNogsx3wjzsfkNM58pDsZbc/HcTbWUw4R4nhfalI
vZ5Zj4y/Greb/a5FiVJQC34yq0qWgnGF0CnMn0fkoPMhpPHVAEScAwEAAQKCAgBi
mtj0Z4ypBDsBeINp6H0EKf7Jgf8MaROLhc+v0U7ue32RPaurDvz2rb4JYTR3apSq
7vzS9ktWGPdi6Xa8uDn+3uXogGkvbKP//JvMpgMVMN08Cf3GiV8TOoIpyTatznU+
I8zuEsLtn0TgNhnP0GPDKNWbUSLgDEz0BgIXyd81/IIdBoX9eT27e0j6gAS61Dz
u7n+K2mlwnCr0e89fX+7mgjHDqKuafMqgPkk3FIKHfLTwnHhFSpVL+6t8SlrX1r1
R7tDBQtLEzb0Q0C1TSXlwy12hW0u9TB/MdRcf0twjT0i9Z4UETjH0/8ouhJvgAQm
bmFCSIn200JkFQcwr1d3VrTpGzSUHbnZQhTPo3u9u10Tqy2EGvmQgf3i7yJ0UVjk
wQeeNj2zLN2ZRN+ECXa+Uxfa/0bB7M6kqRr73GLXjv+w6B/JwzbZUPx3H68URsjH
Cwu4lMqCMBitnibTiRghcHwh+e0woT4aUsx8Ffuxok10nVhUxgSihF2HWEp0ABLR
8iznf4Qbdjpjz70RKBGLML/dJIfWx5NNFmpwb+X5UDxrI6j5Zm2Qq0mqZ0tlIwY
EKwPCOrKMLb90m2vQjs3KLDFV03xlaGxKhps62idkj+2HVnW3T5VIVkLnt8sB0sP
SXANXuITApunbVEqIquqDF93uZ4yQ+ckDNjhmXupIQKCAQEAzwBoTHqFwjyLOT36
F3QiEawBNuERO2QRhd9774hs5JF3YYd/vybLXwX00+CipQsrX75gnemxnp6vWA6k
jo5ihhbY+CMiVkpVmdqBcBFvKaJYrUR9jNxfQyTIwUWT9Ci5Rd+dX4jaMeJ9ox75
ts9gDDRge10sJ8VReaeQV0vma9CRkfABSA7vfS1qM2on3jcg8OPDyGUKh/vYzH
xK04zVzwfApNZEPdNePcZhZwigTPBnhf0Fr8530lePQYghUUXA8L5I7raw1uL+5
cj5raR2hC3b0f0nWmUoOgkyqt3dJiqy7t8vS7MWBjATnk59RNn++3KaGliIr6JLw
Ze0jFWKCAQEA+bdhz7IDVjQUFSVzWGDBohnhV72fsauRV0sBR7N4TKMYFuoACfd3
3ACBhC+tn5D4LJwnu3ykJt5ZGhtW3UovKN9+HkHszh3cGYaRIVZCshLDV+K0HzLI
TLi0Nc5hYByQq9D6V2+I18lvz1PLPZyFVNw9aGLPz4ArWu/6H+e8Nk5IQYZ58dlI
py4zvmIbVsT4zFquReRsCMDbNql/arKhEcII0EBP9MLBLSCTW2nPUUMo9UoY0TBR
NqoBq/D/qXH621Kd6i4uoHzzDBusxIKwSacxD7Sm+8a10T0InnnI+hV0iCkVfzLj
47ZLCLsw80uwIFvhTHYmwX2JxlWjA1Mc7QKCAQEAuB/OpihdMXSLChcuvvryfhL
ZDsyazl5dLDjFp8s70qPW8sg0DB7uVv7Ku+moT3rydAXNJ9IBKV1pkfwC3WPIWJ1
P9JQmpb2zktj0wF09a0YaRaA7qiee6TehTuUbRtEIWjUHMqoATNL0as1x2wSLQjx
wQEeIooa/LEVatQqXXNM6iKsJGMC/pClk5G96S88/plxuhbECj620S3GC5ztpo3C
wzKPHOBiHcTWqF+6cB0hbtY+g+j3UszvX9wx40Ez0GaiglX6i3KgnmK7W2k2NVvL
gd0ff3SoE9WRrkjvmR2b5qPanZPJXB4aKye5rM+Ld4SNisr879IZaFg7SQ5zpQKC
AQAQ13FdVKAs/C4ujuwTmXL1v9EW3c8baHrQw1i+wTfn00gYo4eFJI+M4uvZQm3v
SR0zzoRPFMSFapGP1TAylIJBu3ECEWgrLpBdmFnJacvtvw5vqvaC9CXWQm0LA/RF
Syfmrp1zsC4CLq3+4aWgViIX6xKpLBEZ6YcDBxRTEomTEAyHfs5SpVql89PBj1RQ
sdAl2CfQxusSXA9szFmvlISQcgmuiEhcliAzLvNBQw2caW8lu+20TdfsW+Lo+cQE
ZY+JozTlSnoSkNrDgkpQpo/FJ+WDLafLayxbw6H/Li+DzLQRktPEVGZSQUUmPZm7
jus+A3Rad819Vz4nhjcMTlqxAoIBAQCjYdSM0lEot/q8s+wp60sCsnL6BxPqVTSW
TrMfIguP3edeNkvblLYnqTwkZxbkkqnzkZTJuLHqgeRy2pdCvPHKVgxnw48osrOV
cyXTtshVG3SVyZw8yqKV8xwh8w4scbk0TlaDivP3b1LZzCAR9EM/zaLd9EyA0THL
77M6Ht2qbX6STKVfVH1ZyFMZydrZBroQTx/jBN/u2zwyRhAhCIESNL5J0h0VqeSw
2KB8mPvjwuxg9mn76D2soY1hq9uWU5selv+2CNniS7Xu8Sn7pBPBfnFCD0G5t5F6
M1bYisNGSlnBsAtaMdhHE0X6PEDuYKJ/xTiQ3T7u5IFc8mJCGSm5
-----END PRIVATE KEY-----
```

## MLDSA87-ECDSA-P384 (2.16.840.1.114027.80.8.1.31)

Use the following CSR and keys to test the MLDSA87-ECDSA-P384 explicit composite algorithm with the 2.16.840.1.114027.80.8.1.31 object identifier (OID).

- [Sample CSR to test the MLDSA87-ECDSA-P384 composite algorithm](#)
- [Sample public key to test the MLDSA87-ECDSA-P384 post-quantum algorithm](#)
- [Sample private key to test the MLDSA87-ECDSA-P384 post-quantum algorithm](#)

### Sample CSR to test the MLDSA87-ECDSA-P384 composite algorithm

Use the following CSR to test the MLDSA87-ECDSA-P384 explicit composite algorithm.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIdkTCCCvMCAQAwRzEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECXMGUETJSHVi
MSIWIAYDVQQDExlNTERTQTg3LUVDRFNBLVAzODQgU2FtcGxLMIIKoTANBgtghkgB
hvprUAGBHWOCco4AMIIKiQOCCiEAK7u9rNJO4TTLy7wPSB8H6ggu0le3IzKk/Lzs
3n0vwn5p000UaQ60xM+agtgLkYgLF32ZV0gLYZqzhPhPODaTgcCp01P2gw9vhrWq
snZn6tpE5cwaVrnkKmlWI/4aR17opeLT9zfwH7uYVpB0K53h9lDRu8/Lj/bhh414
Q4g+3dxEc7Pw65m1vBRJg3088aWKWDQ/axoAtiMmfac9Jp0tdLEej5+8Yh3bNycE
7zN/sjZShZ7sHBlN2cK6Z8cc/86+SxSWImS6rEgQUs2V+WU9PbhuSJn9in9NbL2
KSm9y9MSTw6Z6NcG0PZ3cCr96L2hgEQVhEuqs31ft8sRBm7uIOA/N0UuCsSek+hk
MwH/WnBmQJL7s7p4wtYvX0JaL6t3MQstp6awihjVc4dFS+cj8Sl8LqLyeuqQ2PbL
TY8P5IF84PNv33aDGiCSLTMKiXquhcuLE5y/004bDi0hAT2E1r2bCdPtB3qgsIgS
n46mBcJMqdjnqseJ2Gh02hyQ06J5AenvL4JsiAWaJExdm23WfwRnKtTzxF1NrAvx
Jp25k5f57qBbiACzZvP97aZfAu534QwQnW5JlsvH053WjpidGTBKKPKhG0I1vtH
04RqtD5m4Fp70xr7J+BrcmsqonnLGLJN9avUMdeAhcavm0e3w0oa2GmrgSLfDV5d
3Y2VVZQm0k1sG1hLd9xhRircAYgmQjbyaPKZ+dTiDcsRV+9tQqrXsx9gdQFrKS5
S2zTy3p1KnwbyDCxYMGKXtfVVgrvX22D3uvNMYPpmN4XFix0ot42Lp02L1mrPi8i
IBPgSksljzVeg6wMDKTwx7f8eAvL5zKJGan8xhCeUJjCHAZoHU/HtLQwBq5/Yb1G7
8auxz5aQjbAlKSRreknCppyLX7Qr9N3rSSnx08UDJkSM728w31zj+fd7Hb2x0d00
Y6DuWcWdH50D9SLUuiv89l4Qt1ksIHv1+6LCKpXg3WBKYZx37IJuRkFakPt8SCIO
ZpPdF3stI8EzHbJg+KNDcx8xv3/pjQe8mH5fNzF1fwwwHxqJR7qIyHVKqIghKqQD
mba/WCJXhgGf2DxMxJCQBQn/1uhskM1lBZPw5KuXly1Paty01XvWcpk0gVH27jXG
SpYEhDlyS9S3jaCXhRpyqKHeu+XqqyJden6HwUgtpd61TmG+++yvA2swmQR1J8o4
qe/x9fAqmrwfp4K8HhL02W5e20pBEBxUTBr2Ycvf+zpb51dPFWSN2bzMqYzCSX1g
91hau1iZ2W2/JEaRfHc1WXhRAB70D3cdUbWlJTEE4BsYi14KJ0D5aglhVmvDum67
YXDuUUnyJ3alExRmDoLFa2JLTDDKGiQWhhVVFSp2n8avyB70mjHwz8gKM4v9daWz
GLHyApTWYm0Jg2V56B9IXRS6qpJC14JCW7kRig11Cv3HLvUvPt4cdmCGgHsI9Dly
UAZb8nziSrCY3aNA645qYzIB0bnd57j3s6aHP/Q5yRIQkEWabA8vUORsHMP70KP58
kumQIcku9Sgr+trksp3HiAIOpCHLSRnDZAoRi6jw1T7PPGB8y3BMAZTMNB1PwVZ
hdQg+LaxGMAVG/GKxrYbhkQK28Muj+I8LBp4r9ZUwLm6KH/i2mmYc8CjdNiBjYky
hM1AiNFAwzCx9+UHbbhILVwB6hT9tGQQJxmuI8CHdtZw6gYzEcyWhiaYmUDKXQ+q
xTnVblxKcNNDzsstUX/HdHpfsvibCNThKBM8Ci0sWmKcxvMPOU/uUqZlcwOwQ28S
dT7NyjpY7PWSjKYyukssZoMvyPhcsDEPVhNa+fo00+mHEg6kmXH3Fdtlu4DPb4qF
b9zAupGB26HIDgVvRYRP9A/JMarJUnOYSupC9kUxyMPGjpeEBcucoBb7u4yLmZpb
i2QF/KfvPNApC9irlXv/vMDMV9yFQHAY8iv0zZc1LaATWDBa903xN09sSSDaDCHz
bLVXlSL5g8oV01/o09LLg0bQq9jTEU0b6LXpYXTZWvW//SpI8PjiDu2D0BS49sUk
4lsWHPKf0v1+/ThPiQPsHZlgRXToq/ujcoYTHr2/ES59vVsGxdrUwsBy/Y+uMfqo
hpje/vS3JdfdeAWHqq3U+52EK4UEJG1DHWpnsV9KsXLMYFMmi9U2AgrG4L4DzxT9
Pl526/9aVfrsDL+Pj0HZNVm2qJh1iXhbc9EbahRgHpxydkRMLrvRUPuTSp86M+OH
o0dqXniUENo1t0ccjnk1FuiUcmNkdCHLk4S2AKeN9D2GMMQsJpZeXXXoLQ09CZ1U
```

4rQjx9zNqm9EDTMVRfTuEWSpEpQfUcNvB8lIbBINP1ZTDHfrKmuuOtcwShEi1GoC  
e0oCVmiNDumwE6jw++gc0d5XzH90HvJaChnBBCCf73ZybzZrKDRddAUlRLSiGjSF  
siZcQMIBpbTGLIyhwyve/NagR+OYHlsuNEyJJ0FEGK3xVlsyNJ8y+DJZwz3usZ0f  
WZRY4NUZzV6eJCTap6HVmdYmvs4lGd9lWL8i0RC/BQe9lvUycVdqSnPkef/d01Xy  
bv006TLMqsHzH2rbkC3SLMtQ0Ax7FxE7y6+0SZ/lCujQoBV14ggBuoFgDtfl2EB  
XRsf/x/z+0t9p+TTXL5yM2953o9Q6aD8tLhXE6GazN1AodTlpu8VsnY4LrBP/yW  
4+KuREHj64FKSSv82q6jT3rfbmtW1aSWMVpUe3anLN2gjn/1po3/MAJsa68akIXm  
ntn7AjWjURnoKmlxEy64AzFeo9xI1JVL69Xa05DNRMW+JtiTsm+LN8cwjqbdiMNS  
eKd37anyX4C74sEbxQM2K101PJMKGci554CGqES4Qgt8fis+260Wwk09N++JSt+B  
eKYp5EpRI+drwbsqeqH88GXj6KyGtJET/hUC7nTkEMGVYfYKD63YNA3ozjF8VMle  
/ZYQ8l3eX8YbwoocZmr5oWGDgeQ0Y5rYRqI4SbVfIhx6hwJIHBMgj iexX/F73BRP  
9JZ32hTpyvg0b6p4zghDPrSOR1Ra5+oCp87mlmh6uVjSXXflbDBXs60UH7UwXTAC  
rr9aeR6yMQLtUcIx2CnJqJoBNbG3C5fujc3jeZAWc7r0Wadc6uA204ZKXoE1kNhe  
0zqdrmmWZ26m6aNdKJ0+dr/tTODh00IWkTIACwv1BtVSboMwaevrfAwn/9T1LlHC  
407HPrmQJAFqbgCDJ8aFD7ga0vm/hw5e/LeUMqNp/CCX889m5kJjwXawVsGpRpbrC  
GNuKtR+RIbKZSdAh77wzpnRDUPq2EYV0kaqwXxKA8Jq0Knl1JNu5pYJtpngg7dc7  
4MvzpcA0nHrZbbnR1fHiDhaK+C4a97MN03ETL0ggbkWl/QahYfjBPcF1trLkaMWk  
0Wz1YR6jePQn/Fu+Vxd2EVKB+i6enEb9GYQS/lqs/1PzKWzrAdSE6FqJr6eI57Hk  
4T+GGkj+UwA4zzv1KerQROQJti5yA2IABCHyu6g4zZjaZQiSolrMkLL0dviU63jg  
fyz6sJ9GPLwMC+3GA4YJ7m4xU1Sy0eGU//57s2Yy1xWv4zXTThLYX754ThB0wg4u  
kwXzAajU0H0aeuLL5tqFE4kC2cugJbLMpKAAMA0GC2CGSAGG+mtQCAEfA4IShwAw  
ghKCA4ISFAAPQdDYKr7L9QTCBvYwc5PeOFInevA0+0t1U46xJz84Fb0h6fSLVroN  
GRiitiz/8HV5g0MCj/OQs1BmgEx0gBiHkenMWckAtBF1ySwmb6DdScEF3aG3dMX5  
SNNYq7fph6WttJQTCkmu6QoPgjzsknSPZxFTs/wFknTwXJGDOcz6DWCWUl7dthPP  
4IWRbG8ROW1C+wwmZ7+2c+2o8cpMON4IJKmsBQN3U0IRNXurLFDagJ6A3yveem8J  
jUGjKD5dCM0f61mEnNjDprbEBkQ8052UDPrKWtPXRIDyvj4rAFfHSCop3tz0rX9S  
2IREtU3RhJCVS19c0sGh027ojVZX9AN3dXdVze47erHB9qWES8vmu0RoBMLEQ1jn  
xd3ibLQWwb8H5az/8waoRR48LB+VMKHjnKPXhSBQ9m9UViWmq/WmT5Kc/40u9an7  
fVsD61tWwBjU/9J5TGQKdRGkdFxxthnAyDU/5YGy+j5ysVQXjZ815MguwY2yqL8+  
nNb2bdJdq148c75Vo0XR5KmGA0xIAPAgUVgjKabuIJSQza2kmQgYc0QaDDUQc4zj  
Gh7Tnnd49W9uuvws8kwadWeUDftooMmXToYtKMmT2QHqG4hIpFI4+/UrP9Bfr8ZKH  
QqJrS3lAO/JooGEGJoAE/8ktG2LY8mwqQvJPWBkxD2qjVdfqT4hOnXrbdL/1E3Qg  
s10WTXsdKSZeTP9s9u5IqcYoeQj/4QrEHZq28Izg89664v1BzK0tppH2kCvlo0Hy  
Ps/0IKhgCK0viK0oesB090yhNXetKBMFdt+Bcfdz+xNGtOgtLMHTK8FCv9JmifXH  
V9R0hJQxTDEVncofsw3fsjmduw9dmlim0kqKZasK8zrAQeYZpLMrhidj4+DgAQhI  
Kf2NGXuGHwKdv3xTxQx9uTxetdvKZDqR/+ufQu0MIYQJpPJY9Q1XNYs7EWuWQ1F+  
UugoXlnUn6glCwuFU45wzUL0BlbWAFearg8WsMQANNQRDXU7QIjpw+Q0u/g9/1cg  
ZQMDLxPA2FpLeH4nlFbJAfGh8FqW3NrdT0T2a1upsWhA+3oMLFMrhMWduJqKdso  
85NEXIj0Vo6AGvrkBGcyuqA+Vi4zJ2uxL2zwhhFDb5gMkHrLZxDeiTUIdCALOguj  
u8/gz53dNRpWdKa2xPGJNX68/mVMc7cXk73fx7faJ45N25hEHnGta6RR+8D95dPe  
DKlfBCAtBybbag0XJzREsomeKfKz4GMFRGzVfa6lMLHJLRDoFWoun+0TTSmf3C68  
X/gYAjVJ1KClmG0D181YEDn5p076kiRBYa5afYiy0+gY08dwaVQIE7zBrAevVZfi  
HwiQByuqTpaPLUAkEL+1pXjxDH4e4K1E6dFShtfwxdS2KIJgsU7tmiCuJo4Fkqno  
dcM3zyZQz2rLAGFIwoiFTm0AuuEEe5aVdJeQLLt/UEjhl76XbV7cpE1vbV/SbJOS  
/tNjj6YwrD1Q+kW0GVxMvRiqS6JlKxehy00kPAGPXnLP0tpmrm0BBqhfr65xS8bn  
FVcsptFfinTM7GZE9G7Wj9A+eHVV2ixFYz2rA1heE7yMAZ2wf+kGHg+j17Lf5jPE  
l1N/mLuuHrAqjqkFSnZshkHquspQfflSeCsRA2oMZPri2Ljycg00eayM823CEAMR  
AIVIuuK956I848t67yg15V4G/1irg2h9rdw4j29jmh3RxxAwavC6eBuJncyJRkWh  
7R/E/kX3K3h0Parlq4Tfupdg+0BiJhsymR0LMLyE953BrpHcsmAg27lbyfW9rchp  
Q5BwtNgay3G/auJ4i/YfYhsxT0CtsuEBhLbNjqpn7xvd9E1guAx7SzEzccLEcxjD  
+fpVsEizogFtQq7HMCA9mskKibNm4QbDwfSd1/MeKrxY7wFhwINoK5BLuNiXmVMS  
xGmCUK74u4AcvvekC1dMktazTz+m/a6MY/mH+5ikIiXQxTq3hC3zDG1ctoEV6aik  
VGr2wocqCk0cZN+gHNIXtKvuBh0/UiZtz4S089g3bytynIPPPiK9np83HMq/eFPg

2BzvMLdi9MJwA3QJquG5l7DZiDIFmRwr/Pc/gZ5iu1LgRPMut+SJJgtnQUpXeaQh  
NSOI+zY+tHRfkK/jgsuQ3rbagUCxAZjsqK5UsDL2Srxn+R00Vs95YXhSULhRJfUu  
y2W4MNYwZOzjLGkY1lAgK0JKfWWyrD05yH0DRrz4gkuDN26CxXb9fSmMZgwRUTX5  
siU3vpPWAHq8pgIslkoSy8vg5RsTN7J64H+ZCze0WJHQXUKba/cus7iRKcdr6iea  
a/xZuKx0zK+wtyibH4W1LQrcWIXH44RJDLetoJn/7qGxKvzZ8yz3LLwio/gpGDSI  
sosJyrnVUrP2RYj5lNRZS1v07Y2SWPnbwgyubL50szPhejKt/2DntGtLr6mtXVtd  
DCn/xpU80/E5Mw8E2a/y9PbJKAI2/rewak16+Ro1qCBvsCXy57qc0gLoZ9709UMa  
Ehelj4vm0u0xq2+335Vh/r0NIJZD+yc2LR7wGaPTYqWaEYWanqVvtNXFIXZxU6nK  
sT8ZHam3ULeEA0ZwX0vbLUd8sg8e7AT7+8MJUE+HdxmX0o7qKeAGazrPfDHCKs5n  
rqf1VMf13bz772MUSiCXzsUBpycDkuYte/D9SQ0sDH/vQ0cdBefb3u2VJPUfyD+1  
/UHCyZm66bD16dACiLeUW+59G0yjjccabDJ4002eYN/VtxBmM9w35eR9Suam6ZVfH  
G2CXfGJU6BBs1Toa4PK9G+tErEcjR36kR1uidooNiaLhs6e3CUyeUppqdv1t65E  
QTxcY0tpg5XyLqdf2IAt9jSxaxerHk44RPGlTWtb9fEYw+VZRYGuIeIJCyoFoZnZ  
KUVsB8YA+9J0dtZLnnU2tKXZ7X1hrLUWPoyRI4uEGo2HxzPUnfPSXSE3d7gTS1w  
9Py47lRbTfHwiF0rAH8bDsrR8XDKNGWc03boV2RtPEssNiiQ9GPzaPqt1spTaMwq  
uChzfPXuQu5RWE128dC5jZEViyFo+b0HX3nomcWQT/YZcfrDdzYwmeUNvYno0NE  
qVKOMDL0SRodeGERv3Dn+H+3q2Psd7I/JSUKZJxcG275qICB6Xnkr6EMMZhdPdCA  
g22yIXS4uNLU8AbTKbv7q+8s6cn+MJ+Xku42NY8nTLXg+LyPuXwbCZMLDa5hp/0p  
p2f00KIdfMJXjMwGhLKvgUYyLthVqZxisHtWjb774LI2swcK3038kiZEexpsQ8yi  
6tvlvLTZ2bsp3c/Ap9AHbu5DzU7cgxZKEEkNjiW+i0OKTtx1LXnfSt1K6C8NSilae  
Iy69uNQ8dtUPXZLnhAwVL+J6lsYnjMPEo/FPvCfPzLeN70Q0ITKxaVcqdiB+7KyP  
cd5mKjasSdg47Rn1NeNrTcCIM1pRszqV27FTpxPExRwFixsFDtTiW0a5QLNm6V1FM  
lvjKsm2kanhinZByLy5e01SV5iuuudyQXNtqEGfA3xKat0kuGUaGXUYDn7HkjL+w  
ZJhpnS5C8Pnt3pgrWRDQl1/qFtBPfEjXppbKZ2w3IgVSRk0ZWUVFMB4C73Fp+HQ6  
5nh0ZfQvMW6QtZXi0vIkdrVXVciqvj16UMiZPBiVL3DQ2NTnds9deufau4/s0e+L  
UWjr/nDyVgcY1/ox2p59si0jet6+fhghQ5uzYRBcehlIp3+2yd7ptcstfLNbn001  
SPT/YgTwzlc7SRJ0r4NapgZMZoJRH4QIrbLt0a0ssw89fLXKGDahCykc/qb1VBEH  
jet6GW3AEJtIzHqswueAUJNWXiLTyjqg4ZESIOWUCwwjF8QhrWw1i0XvYBTki+LU  
nTICEczMx2246AQxotl8kYKfRh+bXtP4fm+JsJ5DFL7ni7JWzi15LUApbVKsGbBq  
Jz3Lp8n1CGRVftjNt10tXN3eS6ioE1PR6Q+F4VEt/g+Alm/F0kVoUzQvq9ioELg  
CtQ8DLN9VJuydr13w/symES34jJ+NBx+zaTUD2A6XTzmyeSlKofbgcscG9rHglp  
29bIPTcjFntDt9+hWegluouy/1PHqtlCxjGEvLwJPF/Oji/L3MRT2GjYICKkH0on  
9C4RwZDR+IE6ThaCnctJ84bvRTw+otciv8S9FDDpKrtzGIKI3UCXQ3YoSf5SFKIs  
un2esTUMeQDeQ51/jyfdA2wSY5K4iBLIZNvJLnqm4pTmJX0d6rDrRbL8nf19IobB  
oojqdtft+kNk5xUjCcNv4+heLRYw6qoH5IP0/B+9CP7iQ5Bc29Fh35s3bgmcBwm0  
iRw7GDwTSfLaAa0JRuNMAwon0mwgJjyM16VZ0h217DxqNJ/ewANOrERVfQc25j4  
BkjIHeP5s45T4BhrbXGmX+K6kvVkyUzAQ8rHMS5AsTQBPwbEf0SJHFvqQlwdEd1  
0jpMHWoBa3qZgK2+0SF0ABsgRBRiDS3Ehb01Jd35seiMFTkzDHdEmzw+ZwSl/XMo  
4vB6N9vs7g5uL443KVWyl/kVhTviRghTKhNYzvLQvY9+fwrRtJSpTPgdNj6uKy+  
+fmsk/jfCDfzhAvsSlV78wNDva/KNm/KUdw78d+pvd9ztdLMH+z4IojwyVITTvc4  
lukiSqbN1EMa3NUfua9UmuHHWxr62W+qhiBYp7uHKgod5Lyx7Mlo2Jn4fWNbva/v  
Dv8uKBdAAR7e3N6WD03LY1tC2QsQhklvQMeFsbz74HJIdQtWkw98cjjyA+q0zB+Mj  
wdkYymyAajv5V9IM4optTlIxojY5M96LtiEw+mg6wf00wP4tsml3/mae9VdiQeC  
1mPitVGg3qfQamBxTxY7aBY9srzfg8dvasD4U4IWnVNhf4z3r0Cbmo5p9dhRqkew  
VJHz9+c/oyFsFvecvBVjygmrow12yYFonB3btszbCiD2yAVAVEf/QurBhwxC2XGo  
sHsJt6HE02U7/UIohoILqrRfxChm9rio9PqJT6pMu1/LEPfs1Rwidkdb0T64Hgaf  
v1F/A8zA5+6qQvATwCnYH845Xv45AFXDBBCJNU2uMb57nF5/uXrojtLtqyg6ouob  
hoc26yHMCZmVr8m8EPg13fK5tT+SS4hg+L5c7DwGaMZ6NSd+ufUAA7Q06Sc2nqEc  
gFndeY0180Z96BwlsvsR7J4LaIoganbPNEUyFH+aLHaYt6VF91Q+41/lyEyG4zmJ  
9hcZg8VOM0xoTN+Z0aGPwnmzmFpSv4aNdmq/MavKVcNu0qAQLDYGKDq03iPoKQI  
3jEZSBR68LDmjwoEok4iNIIaU8gBQnNC3cHNk4u1suQqu2YDc2HdKByzfW1VVTOP  
F8igPbDw2owHYJi0S0YRC7J43UTnkIi7Z0VwquOCzsQgYFyvB9GQlnGTuMmRzKia  
sBXsk5YAInqCFEztcfA2R8JF+fGgYoz5zKMpUhTmhooP7Yu+Pp/kbUyYfDmGa6tG



```
Tz08QGp1hWuIjYyVP8FebrRHTMSbcRqkMPWbbR1gtu2mY/Fd3zJPLy0yyh+SWXm
No4X+ESMYxailVDFj0iUswH68IVp0hmtjt04vCZunFhnXWcSoyhGLCxLpUTELXFP
gYr30gVCxLf5fhQYtM0RkE1yLgmosbXNqVX/k6cjkz1vG0Wazk8M2/m/VDPDKh9a
0tNFA1BiVZ96hWqqngtPb7lhV8ldWoIXdrIJHjsjsAiQWauXJD9VS1vhpr0edsHy
diR1AN5NXP0EztJYsyzteLC53LKMwCGqYoGtppbPKEg7ravBL0SPJcVDsM6+Anpp
Kp5jZaISazkNCMP0Rl3rvyek0P1etxp54bf9r69s1dv0Q9S51gHotjKXe432JP19
pBVZIIj0/Lhq0izgb6Pkq94x072CGiJIYizjgR0F3tPmSpJkuScMMdLuLSw+nAmf
r0jPtQjq2we+HQP60k39w47viGuQQvXsDa0Cm0WtX+gqinzKf4TcwcPkkuLYnW/z
kAmgjk2i2Uzu+R596G6j1HE7ielNyALZI79ubLFLY6gkLkm/B5xYLSGZkDoo214o
07dDUybITkxe0UrtJGysB/rCFyxEOmm9lLlMxA01uJnrW+85bfNyuB1KTmueHzJH
o7y90Q8bstHiGkaktiArOkWdHYfC6yRQWHW7v+cKEBM1Njg/f7G0u8YRs97i9gAA
AAAAAAAAAAAAAAAAAAAAAAAAAUMERUEJTE2A2gAMGUCMGVHdV0PT0+2u+WuBsJZ
kTlCZ2GVGemFv2ZsrjV2KdikOmKAWAWuG31m80/QDFYqIgIXAKfEWo2lEWa/VQT3
5701G2mackohVuS8fzL0JzEiP8/eqDQRbYgtm+FUY+D5AsCdTg==
-----END CERTIFICATE REQUEST-----
```

## Sample public key to test the MLDSA87-ECDSA-P384 post-quantum algorithm

Use the following public key to test the MLDSA87-ECDSA-P384 explicit composite algorithm.

```
-----BEGIN PUBLIC KEY-----
MIiKoTANBgtghkgBhvprUAGBHwOCCo4AMIiKiQOCCiEAK7u9rNJ04TTLy7wPSB8H
6ggu0le3IzKk/Lzs3n0vwn5p000UaQ60xM+agtgLkYgLF32ZV0gLYZqzhPhPODaT
gcCp01P2gw9vhrWqsnZn6tpE5cwaVrnkKmlWI/4aR17opelT9zfwH7uYVpB0K53h
9lDRu8/Lj/bhh414Q4g+3dxEc7Pw65m1vBRJg3088aWKWDQ/axoAtiMmfac9JpOt
dLEej5+8Yh3bNycE7zn/sjZShZ7sHblN2cK6Z8cc/86+SxswImS6rEgQUs2V+WU
9PbhuSJn9in9NbL2KSm9y9MSTw6Z6NcG0PZ3cCr96l2hgEQVhEuqs31ft8sRBm7u
IOA/N0UuCsSek+hkMwH/WnBmQJL7s7p4wtYvX0JaL6t3MQstp6awihjVc4dFS+cj
8Sl8LqLyeuqQ2PbLTY8P5IF84PNv33aDGiCSLTMKiXquhcuLE5y/004bDi0hAT2E
1r2bCdPtB3qgsIgSn46mBcJMqdjqseJ2Gh02hyQ06J5AenvL4JsiAWaJExdm23W
fwRnKtTzxF1NrAvxJp25k5f57qBbiACzZvP97aZfAu534QwQnW5JlsivH053Wjpi
dGTBKKPKhG0I1vtH04RqtD5m4Fp70xr7J+BrcmsqonnLGLJN9avUMdeAhcavm0e3
w0oa2GmrgSlFDV5d3Y2VVZQm0k1sGhLd9xhRircAYgmQjbyaPKZ+dTiDcsRV+9t
QqrPxsx9gdQFrKS5S2zTy3p1KnwbyDCxYMGKXtfVVgrvX22D3uvNMPpmN4XFix0
ot42Lp02L1mrPi8iIBPgSklsjzVegwMDKTwx7f8eAvL5zKJGan8xhCeUJjCHAZoH
U/HtLQwBq5/Yb1G78auxz5aQjbAlKSRreknCppyLX7Qr9N3rSSnx08UDjKSM728w
31zj+fD7Hb2x0d00Y6DuWcdH50D9SlUuiv89l4Qt1ksIhV1+6LCKpXg3WBKYZx3
7IJUrKFaKpt8SCIOZpPdF3stI8EzHbJg+KNDcx8xv3/pjQe8mH5fNzF1fwwwHxqJ
R7qIyHVKqIgHKqQDmba/WCJXhgGf2DxMxJCQBQn/1uhskM1lBZPw5KuXLy1Paty0
1XvWcpk0gVH27jXGSpYEhDlyS9S3jaCXhRpyqKHeu+XqqyJden6HwUgtpd61TmG+
++yvA2swmQR1J8o4qe/x9fAqmrwFP4K8HhL02W5e20pBEBxUTBr2Ycvf+zpb51dP
FWSN2bzMqYzCSX1g91hau1iZ2W2/JEaRfHc1WXhRAB70D3cdUbWlJTEE4BsYi14K
J0D5aglhVmvdUm67YXDuUUnyJ3aLExRmDoLFa2JLTDDKGiQWhhVVFSp2n8avyB70
mjHwz8gKM4v9daWzGLHyApTWYm0Jg2V56B9IXRS6qpJC14JCW7kRig11Cv3HLvUv
Pt4cdmCGGhsI9DLYUAZb8nziSrCY3aN645qYzIB0bnd57j3s6aHP/Q5yRIQkEWab
A8vUORshMP70KP58kumQIcku9Sgr+trksp3HiAIOPCHLSRnDZAoRi6jw1T7PPGB8
y3BMatZMNb1PwdVZhdQg+LaxGMAVG/GKxrYbhkQK28Muj+I8LBp4r9ZUwLm6KH/i
2mmYc8CjdNiBjYkyhM1AiNFAWzCx9+UHbbhILVb6hT9tGQQJxmuI8CHdtZw6gYz
EcyWhiaYmUDKXQ+qxTnVblxKcNNDzsstUX/HdHpfsvibCNThKBM8C10sWmKcxvMP
OU/uUqZlCw0wQ28Sdt7NyjpY7PWSjKYyukssZoMvyPhcsDEPVhNa+fo00+mHEg6k
mXH3Fdtlu4DPb4qFb9zAupGB26HIDgVvRYRP9A/JMarJUUnOYSupC9kUxyMPGjpeE
```

```
BcucoBb7u4yLmZpbi2QF/KfvPNApC9i rLXv/vMDMV9yFQhAY8iv0zZc1LaATWDbA
903xN09sSSDaDCHzbLVXLSL5g8oV01/o09LLgObQq9jTEU0b6LXpYXTZWw//SpI
8Pj iDu2D0BS49sUk4lsWHPKF0v1+/ThPiQPshZlgRXToq/ujcoYTHr2/ES59vVsG
xdrUwsBy/Y+uMfqohpje/vS3JfdfeAWHqq3U+52EK4UEJG1DHWPnsv9KsXLmYFMm
i9U2AgrG4L4DzxT9PL526/9aVfrsDL+Pj0HZNvM2qJh1iXhbc9EbahrGhpxydkRM
lrVRUPuTsP86M+0H00dqXniUENo1tOccjnk1FUiuCmNkDCHLK4S2AKEN9D2GMMQs
JpZeXXXoLQ09CZ1U4rQjx9zNqm9EDTMVRfTuEWSpEpQfUcNvB8lIbBINP1ZTDHfr
Kmuu0tctwShEi1GoCe0oCVmiNDumWE6jw++gc0d5XzH90HvJaChnBBCCf73ZybzZr
KDRddAUlRLSiGjSFsiZcQMIBpbTGLIyhwvye/NagR+OYHlsuNEyJJOFEGK3xVlsy
NJ8y+DJZwz3usZ0fWZRY4NUZzV6eJCTap6HVmdYmvs4lGd9lWL8i0RC/BQe91vUy
cVdqSnPkef/d01Xybv006TLMqsHzH2rbkC3SLMtQ0Ax7FxE7y6+0SZ/lCuJQoBV
14ggBuoFgDtf12EBXR8f/x/z+0t9p+TTXL5yM2953o9Q6aD8tLhXE6GazN1AodT
lpu8VsnY4LrBP/yW4+KuREHj64fKSSv82q6jT3rfbmtW1aSWMVpUe3anLN2gjn/1
po3/MAJsa68akIXmntn7AjWjURnoKmlxEy64AzFeo9xI1JVL69Xa05DNRMW+JtiT
Sm+ln8cwjqbdiMNSekD37anyX4C74sEbxQM2K101PJMKGci554CGqES4Qgt8fis+
260WWk09N++JSt+BeKYp5EpRI+drwbsqeqH88GXj6KyGtJET/hUC7nTkEMGVYfYK
D63YNA3ozjF8VMle/ZYQ8l3eX8YbWoocZmR5oWGDgeQ0Y5rYRqI4SbVfIhx6hwJI
HBMgj iexX/F73BRP9JZ32hTpyvg0b6p4zghDPrSOR1Ra5+oCp87mlmh6uVjSXXfl
bDBXs60UH7UwXTACrr9aeR6yMQLtUcIx2CnJqJoBNbG3C5fujc3jeZAWc7r0Wadc
6uA204ZKXoE1kNhE0zqdrmmWZ26m6aNdKJ0+dr/tTODh00IWkTIAcwv1BtVSboMW
aevrfAwn/9T1LLHC407HPrQjAFqbqCDJ8aFD7ga0vm/hw5e/LeUMqNp/CCX889m5
kJjwXawVsGpRpbrcGNuKtR+RIbkZSDAh77wzpnRDuPq2EYV0kaqwXxKA8Jq0Kn1l
JNu5pYJtpngg7dc74MvzpcA0nHrZbbnR1fHiDhaK+C4a97MN03ETL0ggBkWI/Qah
YfjBPcF1trLkaMWk0Wz1YR6jePQn/Fu+Vxd2EVkB+i6enEb9GYQS/lqs/1PzKWrz
AdSE6FqJr6eI57Hk4T+GGkj+UwA4zzv1KerQROQJti5yA2IABCHyu6g4zZjaZQiS
oLrMkLL0dviU63jgfyZ6sJ9GPLwMC+3GA4YJ7m4xU1Sy0eGU//57s2Yy1xWv4zXT
hhLYX754ThB0wg4ukWxZaAjU0H0aeuLL5tqFE4kC2cugJbLMpA==
-----END PUBLIC KEY-----
```

## Sample private key to test the MLDSA87-ECDSA-P384 post-quantum algorithm

Use the following private key to test the MLDSA87-ECDSA-P384 explicit composite algorithm.

```
-----BEGIN PRIVATE KEY-----
MIIT7AIBADANBgtghkgBhvprUAgBHwSCE9YwghPSBIITJASCEyAru72s0k7hNMvL
vA9IHwfqCC7SV7cjMqT8v0zefS/CfkLubLCwYE/8DDeGmIDT+8Eg17JDnQYarvQf
ra1cMcSXm7tXNRp94xuGoEo1CUyIOciLw1xToWS7Dy8A82W7yAgNT4J0FnfcioqC
TKekbVhFMFFYwR5dwjZ9dnMXcy0m0Qm0aUQ2jRgIBhOWAVRASaIIZIIyQNSEBASy
ZeSIjeK0aQo2BUmybeQsBgICbplGglLEjBOFCUSQKE00EQvAkMmmYFvCcEgwJZEg
bhI3iUwACQ0wBkZcQE0hociUWCAQQwJCiQyagizLRkJAJsiASGJQQkBcqQmiRC2
LMLGACTGTWI0kAtIbhxiEPkIKNSQTRPABQQFghQBECIGRRM4CQuRbZsiAQiiYOEY
ZqHGMACCMOCGRAMWAQkZAKGGJBwjEpACjW0iBF0gZRS3DdkIiUJIQEkmcOKohGOI
YNMgThwRDJACMBSwSAGRQcgEaiGXYYSLhADMhQESosSBpFGLZA0jBEAIAGAUBFE
aJxAUIkWcSIBMICCTQSYUCEzQlvCKRuBAFsCEAMkcRiwMaKCUAwhkgGlcAnHjQJA
QQQ3KlsAhMAQUVHCABJFSJE0ZeIGbiAGitEohREDUZICYJnGBNqyRZSwbRsABuNG
cAGTcAKBjYgZAAVgCNBziKjEVKIhdTGiqgAShOnYRQzIAAQJAm2DRgWUcLGhNtA
LZSwMZRGgVyGbMOSjZoCiHsFBjMETCIISoAYIFAiJhEBSYgIEAgZALGAOREEQE5
RZPIRETGMCHGKKE2AtTEDBNGcZuYgYgkjNgQMdMGKS0k0NJAkWSEYzsmRguHRRio
MOEoBIGQhRk1MQQhMRyxaUQGQZkoACExKBGShRiPSBMBTdpGjloibhKFEZwkTAgH
ImEgTWE0cuGYDZg0LJySYMMACIM0TAo1gsEgTsBIghQ2CtI0ktqAJFomkgASCcSA
hQG5aRsHTANELdumJCKxEIAyKOMmICRGkGOSUOMoMtQYUUQ2DaKyECKEHdg4YFsI
```

UJoYCEy0JQomUZtAhgFFJJUeMUqmTdIWbaMiTtrAUUFIQFokMsREEsKgIqA4MBun  
DQuJgBkohNkwt00UOKQDeMcAaFPGYaG4kVq2IVtITAIAkYQEAIugJMOQCNgCkMyW  
jUK0hMsGBEyKTCkoAKOETOKYgAtBitQSghuXBCIJiRGYbMOUDGTCUFISCSMCLiIH  
gNgITFESDjgkSBAGLWCWLMaKEZwoZoNGQpimDCASKAADhgGJIAImQhIAbAsiUqE4  
EkqyIIiKCNKsBRgEQAM3Qck4KhypSIKQkKiCpw4isoyUAjCZUE2bQojYRwzcUwS  
TNJAEAGyJVMIRQiXbdQCTcwSBswYEIACStMoUIJCTgvGEBIQKiGjjNykcYDIBIOU  
BAQGSMSkhGRjJoEUW0obBpDEgrBLFoYCECKMmIYASECBkAIhquAi1gNiSDMG2  
DVMECCeWDEvAIOEWKQXJBghEAJwAbYNCKBCBACHJbaQoYqLAREmwUJxITpsWCQsQ  
gQw0cuKEJBilLcSGKNOWLMKyQRO4hdwgClgEDVq4DYEQUBOSEFvIKYLACFEKIJ04  
KdMobt04LVSABckESFKUaeMoEpSCRakhMoAwCBJIMQwwYcpGMPiGEJuIMQAhaLO2  
haKWUcowsICkYkkjZK0iQLHcRNAsmRsJEhGOUUUaOTBqmCdzASBM2UBwpQGAW  
QNAiYBQzBBnBYFpICAEiksgwaFmyielCbEsWbdhGECK4YOKwSNKoQZuyYMwwKCGE  
UEMGJYPAbBI2jEPIKQq0IIy2QNGyYAOWCNggk00mgSKFhRoScFpGrpIYLNQIUVC  
hZugTRuIbUhRCEJLog2UkKmJODGJcoogoKADYughQQ5MqNABRLGgqKyAeEgSA03  
hYEQcgS5SAu0hZC4hEKiTNLIZIPCjeMGTgMWDSEUKOQwjRGEZBwUSIMSSYFAZmGk  
gSQyQhsxkoK4jQRHagwIHgKoKFsmchEHEFQwbNMmTpTElCNGMEuICAK2ZookbGCY  
iJsYhVwmRBwmDcQYMQM3CqCwcdi0ETynna4h0gvu6H2su5THKoH4Iq4Bp7W8cLYN  
FVEZrknpbKJTPBWBtJRrsjxYDC8nZ3DFwgMmTeFHW9Q800UT0BSN0qZrrfL5Ju1n  
2U3aPgJU9K2VBCWRrtfTh7au+pD6XHE5RJHk/FqzD7PZeEVz5xHBBZ3UD6hQOni  
a+o/N6N0tnH4e1XYAVLlMwZqrndOghmnD7Fjaacm0crh4ia4mex3NedqvUJEIsB7  
EGJPPRND0qFti+yDsTqX7yj12ydMrtonfAEk4fCpGJL3ruy+Wd4ayKegzzg/HcPm  
Eu/09jjgR3PPhmsswmUIMPT/6cRBLSuGcfMMq5E+xsN5u0jjZRwJBC3Ke3JLk6  
gIxxv8ReKIIsX+im6ffoK3IZB8GLBIL9FXcJ/IwUY949L0ADZzvGwmfAXJ9X4/u06f  
N1HPIM6n4rvNNrXVh8l3w+L2mW9eks3jrVaG370eBiqiWdx7nL5CJzfx6BM493z  
Ca5LRf9RR2sxQbq1q0emqF8IJ1ENthvSdBfZvrWbu26Sodwz+c5SYsn+bJcVQy  
C7YZLlNMcyzhEaw9nE/G4ukAc2NCSftEwQpKl2MfBfbwjy6+TrHorBbi9jSNW+E  
bzPQbKRiKmanfNZEHksptHzdG0mWRsVjLak4xBvitnPC7YHdTH8AL3Nrn/VD+wqZ  
SLZ8EqlhC/a/agkNVVT8n05T4hQ7BgNFhDBWlsGiXzgcsAIwrWMNYUxd4Yp32QDh  
4MhCFz0802ad2VfEKFV5TYkUS2YciMpL0urvR4wGbZFktEcy2/YbLZAYdMuN4Y  
de28DeRaVvQSa1f65Z0q57f3zdJM0dZ8CcVh5iTwrmSsU38I78/BDpi8dl8E7YLw  
CMG69v64+xK92ZH3uvpEFxBsaMhsOuVILtjjdBWjTKldR5jvR4o7yGPT9yl6dH0b  
jdvxU1ka176hFtHBKovwr4z8THRSFRzp/WYeSzxv89CYU1inY2CXo0TuKXB1SjW  
K09q05RGNWQeVkyngxbroX9D9vfl+uB9Mia4sufltrVobL+ReTPS47XYFU74Uyzy  
0tE0tbBk+Gb8Cj1jtnzmusU+9bo4r8A6jA0knhImsex11EeaTOvejA92KmrAAsGX  
YXtTUK6qAID08CthqSsJEIdK7rOYq0AvHSXILdD4HsCsbNmj2+NaxB26wly5gTj7  
yxLQu/7cm4FEYS1VC5vKm9qD99kVmwBouth9U0ZEHdN9sdHPE8NexUEqzGvdYNO  
9KTFu2HstAgLB6h18XHgPnC4tp/2kjxkv+PKx3WzsGi3AvI7LZRzfdlx0CfImTr  
2iaqqSG4kXoaAt7rVB07kMiAb0V178PIF4XYKFdIGR4MFPkcCmLBwbakELIXK82D  
nR4QzbmSNkh9owBKLy9GLVES10ewA5DD9RnIp/7Ej0B0UGnimRlaI8rd/UHQnjLK  
CvBkfQ40XbZ9d93NK46pDMnrm092/dzBmFeJW4uwuFBQyTFe1P/MsekNFQjuo83D  
KltZFkEg7Mz24N5n2uK5bnw0Zi5v+9j5Ha9gjdscfJv0orJYShtDdqIoaVh41yv  
2JHMGBOsFLYGu/SQrwLd/x0LCjKZYz8Zduj1/un5BSWRK28k896qWl9Spc99rAqp  
T4PQ78UCS3jfyQifkr166GFxpKrhvmHOjUZoMnfmwAiRq4mqZdiv/R3ztQ9psVQw  
aiKdIMWZv+Uft4VmltYYP9NALV1SuY9arPH+gPDeBqcYTv33Jqj3SRR+Qj5Fk3wU  
vzQWAEGEswJYhLz9EIVL9izPS4/viIBkSgkKbPdVYUQFMnocyrkXgBSJk1yfCgAv  
95881zhfmrdrFrIJHUApZ00RsMA0ZtMPLvH/Cs7ivb+r1T3qTBsy26wkPdY7f2TB  
BLTTik/3CNf0hgX0XBwNp+hIN64lfbSeuomnDNYUmXj+QoudIpCr1Aj0LYyZ4RES  
2d44cw04oozjCZJqDZ/zmfMgUVh3LshfDtf5qk73dFgZvDhpBwChyj6YFkmuQgh7  
C9d/8wyuLcSGeXn40At+Iw23wcvS0p4GhtIeW9uJVSt+9dIXEBI6mZHNCy4RGG9R  
exF0yfgquLoWAHfTbzIea8ZtLoUYzLUQEFdLC6cpxpZJyuoYN/a04PEQ5YUjSIsA  
YoCPpstcYB+4jE0EIF4wAoX50K1xwRjTrFug8u4QIE6GVlzM7662y8MzRJoIbfMZ  
HJuNp10sg7vkhPDRd9MoxAlSrmQvKptzbf0QFRSRazN0ZPRCFxx5B32zhBeIq0zt  
mAueqqlxc7Bmp/VhC10Xx1DCzGUGCvqLV4iiZ1mAjft61kv+9j41pgKCepgJiLUF

```
kXH0GBxgG+L9dloRdrsbFaar5/0/Zew+duaWbey9VJejmfzc/nh0Gz2geVT9AXBv
qUzV2odkdaea+voN83py4RXwv7Hco1W+PMc1ogSWgAqY09hJiiwXaGlhSd3/FSeY
oWsrDYaEmWb8v9UUp0VWVW0GKgYmLwD0mSghw3j5yob0pe0kp8hmM60kzs4u1sfX
uHesJlmjiZ+ppaxKZig+S5AV4yvLZi95nck3J0JXII6Df9tKa6FQneVHMx4NPHcr
VfJ0ZmqTLluscDyJbRI+P/csNZvClT9nTepybZqFq49lWankESybMN5agxh4Yb5l
aj8oWgbXVd0XvXsHAzsXqvd52N0ylCYarc77cE7rii+A5+0LMBdzYcoJ/6lPu0VD
osEm9hGvohXI2p2rReXjGBoe1GJGJOiuBt8VQ0wp+TFVDvWI0Ygg4UpfN/YjAdnf
nVzDLkS4mxjy0ViDGXxmVrMrbfPBmq0E68PIGs8JcPh3BdF2Z0xwM4VHjUWzH/xT
uPga4V93cL9/HaCgTu2S4nojApeV11Rvwm5rShMY0uCM3ix0jj8+EC+yfdC+g8yW
0LVNDPUjx05l9ivZTpFzU+wF7YIs3LF+xxJB1wJC40lWfy5TeSDj4kHchrIfx83q
J1zFtQm0BID8FY0/JbZHeC9ozAbsGGds+F0sivrAJbZ+zvr30lTtzSymn2gbkUR+
JOuNYUcmQQP2+uwNdTKh57SXmHT5tnKMat+8NIMD4ni3jucGxenKI4cevMEHkh6A
o0VgTAHbLz+BTl4pW86qtLkY3VSmJxKd0ss0At9Plhx9j+kyA9mWcSRttLiY00yl
mmBCz/x20cp8utigki+w1krLqv/HupmD1hs7qAtlywgZwELHbwZnWow7fyunPqLW
e1wwPAQn7PcKZ0McSvWRB3JskxFx0iIgUHZBICoUDtjTApHuTZqWJGLzNhuq0E
CNtsh8vBleKXtWtyXxKdLpUHK9Q15QkqyAUQtWFrzZNY3XnE+EGY0F//rucAZXhq
ptQrbRR9N6t2FoYwRfLpQcQ0uAjS5YqI02/PsykuSwtbuCT5aHWVaUcc8eUefW1m
kRkiYRnHtEQqYU0oGok/i6pme8PAjJgkHKCjJQ7mBBjDci3TcPxMisVLgVcr9kqD
K/1vm1+Hq3LizLMTPLOR2lwm0bIt14bqK30KURcAV2wvIstbca3VFhcrp/uSjJU
m1azVhopDOKPqIvFDt+cB0xgaE9fAZaiyKETuKhk6Qidb18M7InD0tTQxzBH6yU
BXv1nXf7fPoir2i6YIL4GvcptYvLPgHNpCZCZqDgmdynL8rWNAQk51WEfIkizBd
8fRmiHLHKf4DynoirBmpC88HcMprX0kKvJ2ZNU6qgEuMpA+PpWGrXNLowgKuloQ3
4jDXv6Ek/BZ7bLLMsA2iob7Gsw/AKf63mJMe3Rl73nYCPHJZoEISdNsdHu2W5MGc
vQ0VTaY0+gyGoQneBK0YxRPzdBzcAsmpFjY8ejrYi55ZceWVHJoJq8UxfZghbyH4
CuPWQy3xns009764j14JlXr/BH1ipuYZFWKYhxdRM70a29VDdjFW+4sEUpwUgFjU
olcIos3oXvhGWpsslUa8dbFoBz4wXG8xBkLLPt6Bp7AGy0kAqABIj8bILr/pKejs
a21jnVktv/xmnbI8djph4VN+wRcv8AQU+uoZebmbPx0hKcgqlaT7geX8lp3gvZQR
6cIvu55FADzYhrTiLiBvFSn/xLIuK1oA+/oX3dQHoM9qUERD2GAAGxY+fkrMZrTt
bxThjev0zqz3YDA65h1FYUIBVtmvI5p4rfwR+AdTNIkrR0N7stt+pkPgG+kXUTY7
BWvrOSv5HfQa4yggkBBYfyD8U/qZMLiM6twrgYhXjnFFYGwpyvto0EaK0ngP0qgc6
zDaYmb46wSBfS20Ea0lcduEce6JvctZpq39HmK4PBn+Lmd1BPHcMyxsQsGkKrvet
hLEWQpXZ22tI1xdPw1RM/4xAIgp3edKS4juMM8k6tuG2tmILZizU2Ei4UHfQHPUw
iF/nUj6qrtLy8ViA+BetAMrdjSDMXM+X03o8nPbIm+Ii9c4ziAcEgacwgaQCAQEE
MG8Ju+kDMxlk1Qfi6mVRD7WH7iw04Fgx1Kr0tleWmVo0yqDigiFz2VgYdBjbeBZg
GqAHBgUrgQQAIqFkA2IABCHyu6g4zZjaZQiSolrMkLL0dviU63jgfyZ6sJ9GPLwM
C+3GA4YJ7m4xU1Sy0eGU//57s2Yy1xWv4zXThhLYX754ThB0wg4ukwXzAajU0H0a
euLL5tqFE4kC2cugJbLMPA==
-----END PRIVATE KEY-----
```



## 25 Integration report

This section provides a complete integration report for Cryptographic Security Platform.

- [Base installation integration report](#)
- [CSP CA Gateway integration report](#)
- [CSP Certificate Authority integration report](#)
- [CSP Certificate Enrollment Gateway integration report](#)
- [CSP Certificate Manager integration report](#)
- [CSP Timestamping Authority integration report](#)
- [CSP Validation Authority integration report](#)

### Base installation integration report

Regardless of deployed solutions, all Cryptographic Security Platform installations share the following integration report.

- [Browsers supported by Cryptographic Security Platform](#)
- [Cryptographic Security Platform internationalization](#)
- [Cryptographic Security Platform upgrade](#)
- [Cryptographic Security Platform versions](#)
- [Infrastructures supported by Cryptographic Security Platform](#)
- [SIEM supported by Cryptographic Security Platform](#)

### Browsers supported by Cryptographic Security Platform

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         | Windows                                                                                                                                                                                                              | Mac OS        |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Apple Safari    | 5 or higher                                                                                                                                                                                                          | 5 or higher   |
| Google Chrome   | 8 or higher                                                                                                                                                                                                          | 8 or higher   |
| Microsoft Edge  | The stable versions listed by Microsoft in <a href="https://learn.microsoft.com/en-us/deployedge/microsoft-edge-support-lifecycle">https://learn.microsoft.com/en-us/deployedge/microsoft-edge-support-lifecycle</a> | Not supported |
| Mozilla Firefox | 9 or higher                                                                                                                                                                                                          | 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.

### Cryptographic Security Platform internationalization

Cryptographic Security Platform is released in English.

 As explained in [Changing the keyboard layout](#), you must set the system locale `en_US.UTF-8` during installation.

## Cryptographic Security Platform upgrade

This product release only supports upgrading from CSP 1.0.0.

## 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
- Proxmox
- VMware vSphere

See the Cryptographic Security Platform guide for the required installation steps.

## SIEM supported by Cryptographic Security Platform

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

- [Splunk](#)
- [Syslog](#)

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

### Splunk

Cryptographic Security Platform can forward logs to the following Splunk services.

- Splunk Enterprise
- Splunk Cloud

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

### Syslog

Cryptographic Security Platform can forward logs to Syslog-compatible services like Datadog.

**i** As explained in [Log Server](#), Cryptographic Security Platform supports the [RFC 5424](#) and [RFC3164](#) implementations of this protocol.

## CSP CA Gateway integration report

A Gateway is a lightweight, container-based module implementing a CA-agnostic Certificate Lifecycle and Policy Management API. Using CA Gateway, your applications can implement certificate issuance, renewal, and revocation actions across all your Entrust-supported Certification Authorities (CAs). 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** CA Gateway supports easy upgrades using container technology. We maintain backward compatibility on the API so you can upgrade CA Gateway without worrying that consuming applications will encounter API problems.

## Certificate Authorities compatible with CA Gateway

CA Gateway is compatible with the following Certificate Authorities.

| Product                                          | Version             | Support Notes                        |
|--------------------------------------------------|---------------------|--------------------------------------|
| Entrust Certificate Authority (ECA)              | 10.2                |                                      |
|                                                  | 10.1.1              |                                      |
|                                                  | 8.3                 | The Events API is not supported      |
| Entrust Certificate Services                     | Service             | TLS certificates are supported       |
| Entrust PKIaaS                                   | Service             | CSRs must be provided on enrollment. |
| Microsoft Active Directory Certificate Authority | 2019, 2016, 2012 R2 | CSRs must be provided on enrollment  |
| AWS ACM CA                                       |                     | CA Plugin for cert operations        |

## CSP 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 n-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](#).

- [Hardware secure modules supported by CSP Certificate Authority](#)
- [Entrust products compatible with CSP Certificate Authority](#)

## 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 [Administering nShield HSM integration](#).

See the following table for supported versions.

| Hardware                   | Client driver                              | Firmware           |
|----------------------------|--------------------------------------------|--------------------|
| Entrust nShield Connect XC | 13.7.3 (FIPS 140-2 Level 3 mode supported) | 12.60.15 & 12.60.2 |
| Entrust nShield 5c         | 13.7.3                                     | 13.2.4             |

## Entrust products compatible with CSP Certificate Authority

Certificate Authority for Cryptographic Security Platform 1.1.0 is compatible with the following Entrust products.

- Certificate Manager included in Cryptographic Security Platform 1.1.0
- Certificate Enrollment Gateway included in Cryptographic Security Platform 1.1.0

## CSP Certificate Enrollment Gateway integration report

CSP Certificate Enrollment Gateway automates user and device enrollment based on the Entrust next-generation microservice framework. When deployed on Cryptographic Security Platform, this Entrust solution adds the following to the [Base installation integration report](#).

- [CSP Certificate Enrollment Gateway localization](#)
- [Databases supported by CSP Certificate Enrollment Gateway](#)
- [Enrollment protocols supported by CSP Certificate Enrollment Gateway](#)
- [Entrust products compatible with CSP Certificate Enrollment Gateway](#)



CSP Certificate Enrollment Gateway integrates with Entrust CSP CA Gateway to provide certificate enrollment capabilities.

## CSP Certificate Enrollment Gateway localization

The current CSP Certificate Enrollment Gateway release only supports English localization.

## Databases supported by CSP Certificate Enrollment Gateway

Certificate Enrollment Gateway data must be stored in a database. Certificate Enrollment Gateway supports the following databases:

- internal database in Cryptographic Security Platform (HSQLDB)
- external Microsoft SQL Server database
- external PostgreSQL database

For information about deploying an external database for Certificate Enrollment Gateway, see [Deploying an external database for Certificate Enrollment Gateway](#).

## Enrollment protocols supported by CSP Certificate Enrollment Gateway

See below for details on the CSP Certificate Enrollment Gateway support for enrollment protocols.

- [CSP Certificate Enrollment Gateway support for ACME v2](#)
- [CSP Certificate Enrollment Gateway support for CMPv2](#)
- [CSP Certificate Enrollment Gateway support for EST](#)
- [CSP Certificate Enrollment Gateway support for Intune](#)
- [CSP Certificate Enrollment Gateway support for MDM](#)
- [CSP Certificate Enrollment Gateway support for MS-WSTEP](#)
- [CSP Certificate Enrollment Gateway support for SCEP](#)

### CSP Certificate Enrollment Gateway support for ACME v2

See below for details on the CSP Certificate Enrollment Gateway support for ACME (Automatic Certificate Management Environment ) v2.

- [ACME v2 version supported by CSP Certificate Enrollment Gateway](#)
- [ACME v2 clients tested with CSP Certificate Enrollment Gateway](#)
- [Load balancer support for ACME v2 enrollment with CSP Certificate Enrollment Gateway](#)

ACME v2 version supported by CSP Certificate Enrollment Gateway

CSP Certificate Enrollment Gateway supports the ACME v2 version described in:

<https://datatracker.ietf.org/doc/html/rfc8555>

ACME v2 clients tested with CSP Certificate Enrollment Gateway

The CSP Certificate Enrollment Gateway 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 Certificate Enrollment Gateway

ACME v2 enrollment with CSP Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

| Load balancing layer | Supported |
|----------------------|-----------|
| 2                    | ✓         |
| 3                    | ✓         |

| Load balancing layer | Supported |
|----------------------|-----------|
| 4                    | ✓         |
| 7                    | ✗         |

## CSP Certificate Enrollment Gateway support for CMPv2

See below for details on the CSP Certificate Enrollment Gateway support for CMP (Certificate Management Protocol) v2.

- [CMPv2 version supported by CSP Certificate Enrollment Gateway](#)
- [CSP CA Gateway version for CMPv2 enrollment with CSP Certificate Enrollment Gateway](#)
- [Load balancer support for CMPv2 enrollment with CSP Certificate Enrollment Gateway](#)

CMPv2 version supported by CSP Certificate Enrollment Gateway

CSP Certificate Enrollment Gateway supports PKIX CMPv2 ([RFC 4210](#) and [RFC 6712](#)) for:

- LTE (4G/5G)
- VPN

CSP CA Gateway version for CMPv2 enrollment with CSP Certificate Enrollment Gateway

The CSP Certificate Enrollment Gateway support of CMPv2 is tested with CA Gateway for Cryptographic Security Platform 1.1.0.

Load balancer support for CMPv2 enrollment with CSP Certificate Enrollment Gateway

CMPv2 enrollment with CSP Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

| Load balancing layer | Supported |
|----------------------|-----------|
| 2                    | ✓         |
| 3                    | ✓         |
| 4                    | ✓         |
| 7                    | ✓         |

## CSP Certificate Enrollment Gateway support for EST

See below for details on the CSP Certificate Enrollment Gateway support for EST (Enrollment over Secure Transport).

- [EST version supported by CSP Certificate Enrollment Gateway](#)
- [EST clients tested with CSP Certificate Enrollment Gateway](#)

- [Load balancer support for EST enrollment with CSP Certificate Enrollment Gateway](#)

EST version supported by CSP Certificate Enrollment Gateway

CSP Certificate Enrollment Gateway supports the EST standard described in:

<https://datatracker.ietf.org/doc/html/rfc7030>

EST clients tested with CSP Certificate Enrollment Gateway

The CSP Certificate Enrollment Gateway support for EST has been tested with the following clients.

| Client                            | URL                                                                                                                                             | Comments                                                                                                                                                                 |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LibEST<br>3.2.0                   | <a href="https://github.com/deviance/libest/tree/feature/opensslv3-compat">https://github.com/deviance/libest/tree/feature/opensslv3-compat</a> | Requires compiling Uriparser-0.9.8 ( <a href="https://github.com/uriparser/uriparser">https://github.com/uriparser/uriparser</a> ) before compiling and building LibEST. |
| GlobalSign<br>EST client<br>1.0.6 | <a href="https://github.com/globalsign/est">https://github.com/globalsign/est</a>                                                               | —                                                                                                                                                                        |

Load balancer support for EST enrollment with CSP Certificate Enrollment Gateway

EST enrollment with CSP Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

| Load balancing layer | Supported |
|----------------------|-----------|
| 2                    | ✓         |
| 3                    | ✓         |
| 4                    | ✓         |
| 7                    | ✓         |

## CSP Certificate Enrollment Gateway support for Intune

See below for details on the CSP Certificate Enrollment Gateway support for Microsoft Intune.

- [Intune versions supported by CSP Certificate Enrollment Gateway](#)
- [Load balancer support for Intune enrollment with CSP Certificate Enrollment Gateway](#)

Intune versions supported by CSP Certificate Enrollment Gateway

CSP Certificate Enrollment Gateway 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 Certificate Enrollment Gateway

Intune enrollment with CSP Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

| Load balancing layer | Supported |
|----------------------|-----------|
| 2                    | ✓         |
| 3                    | ✓         |
| 4                    | ✓         |
| 7                    | ✓         |

#### CSP Certificate Enrollment Gateway support for MDM

See below for details on the CSP Certificate Enrollment Gateway support for MDM (Mobile Device Management).

- [MDMWS version supported by CSP Certificate Enrollment Gateway](#)
- [MDM clients tested with CSP Certificate Enrollment Gateway](#)
- [Load balancer support for MDM enrollment with CSP Certificate Enrollment Gateway](#)

#### MDMWS version supported by CSP Certificate Enrollment Gateway

CSP Certificate Enrollment Gateway supports the following version of the MDM Web Service (MDMWS) protocol.

- v8
- v9
- v11

#### MDM clients tested with CSP Certificate Enrollment Gateway

The CSP Certificate Enrollment Gateway support for MDM enrollment has been tested with the following clients.

- VMware Workspace One (Formerly 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 Certificate Enrollment Gateway

MDM enrollment with CSP Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

| Load balancing layer | Supported |
|----------------------|-----------|
| 2                    | ✓         |
| 3                    | ✓         |



| Load balancing layer | Supported |
|----------------------|-----------|
| 4                    | ✓         |
| 7                    | ✓         |

## CSP Certificate Enrollment Gateway support for MS-WSTEP

See below for details on the CSP Certificate Enrollment Gateway support for MS-WSTEP.

- [MS-WSTEP version supported by CSP Certificate Enrollment Gateway](#)
- [MS-WSTEP requests supported by CSP Certificate Enrollment Gateway](#)
- [MS-WSTEP domain enrollments supported by CSP Certificate Enrollment Gateway](#)
- [Windows products supported for MS-WSTEP enrollment with CSP Certificate Enrollment Gateway](#)
- [Load balancer support for MS-WSTEP enrollment with CSP Certificate Enrollment Gateway](#)

MS-WSTEP version supported by CSP Certificate Enrollment Gateway

CSP Certificate Enrollment Gateway 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](https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-wstep/4766a85d-0d18-4fa1-a51f-e5cb98b752ea)

MS-WSTEP requests supported by CSP Certificate Enrollment Gateway

CSP Certificate Enrollment Gateway 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 Certificate Enrollment Gateway

CSP Certificate Enrollment Gateway 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 Certificate Enrollment Gateway

The CSP Certificate Enrollment Gateway 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 Certificate Enrollment Gateway

MS-WSTEP enrollment with CSP Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

| Load balancing layer | Supported                                                                            |
|----------------------|--------------------------------------------------------------------------------------|
| 2                    |  |
| 3                    |  |
| 4                    |  |
| 7                    |  |

## CSP Certificate Enrollment Gateway support for SCEP

See below for details on the CSP Certificate Enrollment Gateway support for SCEP (Simple Certificate Enrollment Protocol).

- [SCEP versions supported by CSP Certificate Enrollment Gateway](#)
- [Load balancer support for SCEP enrollment with CSP Certificate Enrollment Gateway](#)

SCEP versions supported by CSP Certificate Enrollment Gateway

CSP Certificate Enrollment Gateway supports the SCEP protocol described in;

<https://datatracker.ietf.org/doc/html/draft-nourse-scep-23>

Load balancer support for SCEP enrollment with CSP Certificate Enrollment Gateway

SCEP enrollment with CSP Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

| Load balancing layer | Supported |
|----------------------|-----------|
| 2                    | ✓         |
| 3                    | ✓         |
| 4                    | ✓         |
| 7                    | ✓         |

## Entrust products compatible with CSP Certificate Enrollment Gateway

CSP Certificate Enrollment Gateway 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

Certificate Enrollment Gateway for Cryptographic Security Platform 1.1.0 is compatible with CA Gateway for Cryptographic Security Platform 1.1.0. This integration supports the following protocols.

- WSTEP
- ACMEv2
- Intune-SCEP
- SCEP
- MDMWS
- EST
- CMPv2

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 AD CS 2019 and 2016

### Entrust Certificate Authority

Through Entrust CSP CA Gateway, CSP Certificate Enrollment Gateway 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 Certificate Enrollment Gateway 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 Certificate Enrollment Gateway 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 Certificate Enrollment Gateway integrates with the Entrust Certificate Services (ECS) to support the ACMEv2 protocol.

### Microsoft Certificate Services

Through Entrust CSP CA Gateway, CSP Certificate Enrollment Gateway integrates with Windows 2016 and 2019 Microsoft Certificate Services to support the ACMEv2 protocol.

## 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](#)
- [Databases supported by CSP Certificate Manager](#)
- [Plugins supported by CSP Certificate Manager](#)
- [Standards supported by CSP Certificate Manager](#)

## Entrust products compatible with CSP Certificate Manager

Certificate Manager for Cryptographic Security Platform 1.1.0 is compatible with CA Gateway 3.x (the version included in Cryptographic Security Platform 1.1.0).

## Databases supported by CSP Certificate Manager

The external CSP Certificate Manager database must be hosted on PostgreSQL 15 or higher.

## 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 for external IdP providers | Notes                                    |
|----------------------------------------------|---------|--------------------------------------|------------------------------------------|
| OpenID Connect (OIDC)                        | 1.0     | ✓                                    | OIDC 1.0 is a layer on top of OAuth 2.0. |
| Lightweight Directory Access Protocol (LDAP) | v3      | ✓                                    | Includes Active Directory.               |

## 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.

See the following table for supported Hardware Security Modules (HSMs).

| Hardware                   | Client driver                              | Firmware           |
|----------------------------|--------------------------------------------|--------------------|
| Entrust nShield Connect XC | 13.7.3 (FIPS 140-2 Level 3 mode supported) | 12.60.15 & 12.60.2 |
| Entrust nShield 5c         | 13.7.3                                     | 13.2.4             |
| Thales Luna HSM 7          | 10.7.0                                     | 7.7.1-20           |

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](#).

## 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](#).

- [Certificate Authorities supported by CSP Validation Authority](#)
- [Hardware secure modules supported by CSP Validation Authority](#)
- [Databases supported by CSP Validation Authority](#)

### Certificate Authorities supported by CSP Validation Authority

Entrust CA is currently the only issuing Certificate Authority supported by CSP Validation Authority.

### Hardware secure modules supported by CSP Validation Authority

See the following table for supported versions.

| Hardware                   | Client driver                              | Firmware           |
|----------------------------|--------------------------------------------|--------------------|
| Entrust nShield Connect XC | 13.7.3 (FIPS 140-2 Level 3 mode supported) | 12.60.15 & 12.60.2 |
| Entrust nShield 5c         | 13.7.3                                     | 13.2.4             |
| Thales Luna HSM 7          | 10.7.0                                     | 7.7.1-20           |

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](#).

## 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 |