

Cryptographic Security Platform 1.3

Installation and administration guide

Document issue: 1.1
Issue date: January 30, 2026

© 2026, Entrust. All rights reserved

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

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

Contents

1 About this guide 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

Cryptographic Security Platform 1.0.0 release notes 13

Cryptographic Security Platform 1.1.0 release notes 31

Cryptographic Security Platform 1.2.0 release notes 47

Cryptographic Security Platform 1.2.1 release notes 59

CA Gateway 3.4.0 release notes 59

Certificate Manager 4.3.1 release notes 61

Cryptographic Security Platform 1.3.0 release notes 64

4 Requirements 78

Required number of nodes 78

Machine requirements 78

Network requirements 80

Software requirements 87

HSM requirements 101

5 Starting up CSP 103

Downloading the installation files 103

Verifying the downloaded files 104

Installing the image 105

Installing the cluster 167

Joining nodes 169

Replacing the default TLS certificate 169

Configuring the proxy 170
Selecting the keyboard keymap 171
Selecting the operating system timezone 171
Configuring time synchronization 171
Manually starting the chrony service 172
Configuring an nShield HSM 172
Configuring SNMP Authentication for MIB information access 178
Replacing the initial password for the Management Console admin 180
Setting the license 182
6 Managing identities 184
Roles 184
Users 205
Sessions 213
Events 215
Settings 218
Authentication 222
Identity providers 225
User federation 231
7 Managing CA Gateway 242
CA Gateway architecture 242
Obtaining the Gateway server certificate 243
Integrating Certificate Authorities with CA Gateway 247
Configuring and deploying CA Gateway 284
Issuing public trust certificates with CA Gateway 339
Administrating CA Gateway 341
CA Gateway endpoints 342
CA Capabilities reference 360
8 Managing Certificate Authority 379
Configuring and deploying Certificate Authority 379
Creating partition administrators 383
Creating partitions 383

Onboarding and adding partition administrators 384
Using Certificate Authority 386
Changing the HSM vendor 428
9 Managing Certificate Enrollment Gateway 430
Certificate Enrollment Gateway overview 430
Preparing to deploy Certificate Enrollment Gateway 430
Issuing TLS certificates for Certificate Enrollment Gateway 469
Configuring and deploying Certificate Enrollment Gateway 477
Enrollment URLs for Certificate Enrollment Gateway 500
Integrating Certificate Enrollment Gateway 505
10 Managing Certificate Manager 695
Certificate Manager architecture 695
Configuring and deploying Certificate Manager 696
Using Certificate Manager 700
Certificate Manager API 886
Certificate Manager error reference 887
Migrating Certificate Manager database to an external host 908
11 Managing Timestamping Authority 910
Timestamping Authority overview 910
Loading the HSM configuration on Timestamping Authority 910
Generating a timestamping key pair and certificate 910
Configuring and deploying Timestamping Authority 913
Testing the timestamping service 920
12 Managing Validation Authority 922
Validation Authority overview 922
Loading the HSM configuration on Validation Authority 923
Initializing the Validation Authority database 923
Configuring a certificate information source 926
Generating a VA certificate and key pair 927
Configuring and deploying Validation Authority 929

Testing the OCSP Responder 946
13 Managing Log Forwarder 949
Log Server 950
TLS 951
14 Administrating 954
Administrating nShield HSM integration 954
Checking the node health 955
Checking the persistent volume disk usage 955
Managing the etcd database 956
Managing the retention policies 957
Recovering from disaster 957
Restarting the nodes 958
Updating DNS resolution 958
15 Browsing logs with Grafana 960
Updating the Grafana initial administrator 960
Browsing and exporting logs with the Grafana Loki Dashboard 962
Browsing log file contents with Grafana 964
16 Backing up and restoring 968
Backing up 968
Restoring 969
17 Uninstalling 972
18 Command reference 973
clusterctl backup create 974
clusterctl backup restore 975
clusterctl certificate 975
clusterctl database info 977
clusterctl database set 977
clusterctl help 978
clusterctl install 979
clusterctl license import 981

clusterctl node add 981
clusterctl node info 982
clusterctl node join-token 983
clusterctl node user create 983
clusterctl node user delete 984
clusterctl node user info 985
clusterctl node user modify 986
clusterctl proxy clear 988
clusterctl proxy info 989
clusterctl proxy set 989
clusterctl retention config logs 991
clusterctl retention config metrics 992
clusterctl retention info 993
clusterctl solution config export 994
clusterctl solution config import 994
clusterctl solution deploy 995
clusterctl solution info 996
clusterctl solution secret set 997
clusterctl solution upload 999
clusterctl uninstall 1000
clusterctl version 1000
clusterctl volume capacity 1000
clusterctl volume info 1001
evactl check all 1002
evactl check cert-source 1004
evactl check db 1005
evactl check hsm 1005
evactl create-csr 1007
evactl create-key 1009
evactl delete-key 1012
evactl enroll 1014

evactl export-nshield 1015
evactl import-nshield 1015
evactl import-p12 1016
evactl import-thales 1017
evactl list-certs 1019
evactl list-keys 1020
evactl load-oracle-wallet 1022
evactl reenroll 1022
evactl stop 1023
tsactl check clock 1024
tsactl check hsm 1024
tsactl create-csr 1026
tsactl create-key 1028
tsactl delete-key 1031
tsactl export-nshield 1032
tsactl import-nshield 1033
tsactl import-thales 1034
tsactl list-keys 1035
tsactl stop 1037
19 CIS benchmarks 1038
Linux CIS benchmarks 1038
Password policy CIS benchmarks 1040
Kubernetes CIS benchmarks 1041
20 Troubleshooting and technical assistance 1049
Generating technical assistance reports 1049
Troubleshooting CA Gateway 1051
Troubleshooting Certificate Enrollment Gateway 1051
Troubleshooting state restore issues 1052
Troubleshooting Timestamping Authority 1052
Troubleshooting Validation Authority 1053
21 Licensing 1054

Customer license 1054
Third-party license acknowledgments 1058
22 Certificate profiles reference 1059
Basic authority certificate profiles 1059
Intermediate authority certificate profile 1060
External subordinate CA certificate profiles 1062
Subscriber certificate profiles 1069
23 Post-quantum key types 1130
Pure post-quantum algorithms 1130
Explicit composite algorithms 1219
24 Integration report 1254
Base installation integration report 1254
CA Gateway integration report 1256
Certificate Authority integration report 1256
Certificate Enrollment Gateway integration report 1261
Certificate Manager integration report 1269
Timestamping Authority integration report 1270
Validation Authority integration report 1272

1 About this guide

This guide describes installing and managing the Entrust Cryptographic Security Platform (CSP) 1.3.x releases

- Revision information
- Documentation feedback

Revision information

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

Issue	Date	Section	Changes
1.1	Jan 2026	Managing certificate authority instances	Update the **Signing Key Type** table of supported key algorithms
		Deleting or disabling users	New section
		Logging	Add a description of each log level
1.0	Jan 2026	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) software solution has the following software 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 software uses:

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

CSP Public Key Infrastructure

This feature provides embedded internal **PKI** software to create, manage, and distribute digital certificates across an organization's eco-systems. Optional add-on functionality includes:

- Out-of-the-box enrollment protocols
- 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. CSP Certificate Manager software includes:

- At all subscription levels, **Discovery** capability to find and discover certificates across diverse platforms, and Control capability to issue and manage certificates.
- At the Enterprise level, **Automation** 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:

- **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 software, 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 software, but whose metadata has been imported to be included in the CSP software's cryptographic inventory and/or used in compliance assessments.

3 Release notes

See below for the Cryptographic Security Platform release notes up to 1.3.

- Cryptographic Security Platform 1.0.0 release notes
- Cryptographic Security Platform 1.1.0 release notes
- Cryptographic Security Platform 1.2.0 release notes
- Cryptographic Security Platform 1.2.1 release notes
- CA Gateway 3.4.0 release notes
- Certificate Manager 4.3.1 release notes
- Cryptographic Security Platform 1.3.0 release notes

Cryptographic Security Platform 1.0.0 release notes

See below the new features, fixed bugs, and known issues for Cryptographic Security Platform 1.0.0.

- Platform 1.0.0 release notes
- CA Gateway for 1.0.0 release notes
- Certificate Authority for 1.0.0 release notes
- Certificate Enrollment Gateway for 1.0.0 release notes
- Certificate Manager for 1.0.0 release notes
- Timestamping Authority for 1.0.0 release notes
- Validation Authority for 1.0.0 release notes

Platform 1.0.0 release notes

See below the release notes common to all Cryptographic Security Platform 1.0.0 installations.

- Platform 1.0.0 new features
- Platform 1.0.0 fixed bugs
- Platform 1.0.0 known issues

Platform 1.0.0 new features

See below the new features common to all Cryptographic Security Platform 1.0.0 installations.

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

Integration with Compliance Manager (ATEAM-17848)

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

1. Meet the Compliance Manager requirements.
2. Start up CSP Certificate Manager as explained in Managing Certificate Manager.
3. Integrate Compliance Manager with CSP Manager Certificate as explained in Compliance Manager.

Log forwarding uses proxy configuration (EDM-10449)

The SIEM solution described in Managing Log Forwarder uses the proxy configuration set with the clusterctl proxy set command.

Docker Registry update to 2.8.3 (EDM-14214)

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

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

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

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

Upgrade from EDM 2.0.2 (EDM-14996)

Cryptographic Security Platform 1.0.0 supports upgrading from both:

- Entrust Deployment Manager 2.0.2
- PKI Hub 1.0.0

EntrustOS packages updated (EDM-15602)

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

No proxy (EDM-16084)

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

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

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

> After upgrading from earlier versions, Cryptographic Security Platform 1.0.0 does not enforce this requirement for legacy passwords. However, when renewing them, you will be prompted to create passwords that meet this minimum length requirement.

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

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

Platform 1.0.0 fixed bugs

See below the fixed bugs common to all Cryptographic Security Platform 1.0.0 installations.

- User names are case insensitive (ATEAM-17300)

- Old credentials on certificate renewal (EDM-13524)
- Unintended use of network interfaces (EDM-15095)
- CVE-1999-0524 vulnerability (EDM-15379)
- CVE-2008-5161 and CVE-2015-4000 vulnerabilities (EDM-15388 & EDM-15397)
- Failed solution deployments (EDM-15800)
- Solution deleted on update (EDM-16127)
- Online registration error (EDM-16154)
- Deployment process not interrupted on failure (EDM-16961)

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.

Old credentials on certificate renewal (EDM-13524)

The Helm component uses old credentials when renewing the K3s client and server TLS certificates.

Unintended use of network interfaces (EDM-15095)

Under some circumstances, K3s and Calico components use network interface controllers.

CVE-1999-0524 vulnerability (EDM-15379)

CVE-1999-0524 vulnerability in the firewalld service.

CVE-2008-5161 and CVE-2015-4000 vulnerabilities (EDM-15388 & EDM-15397)

CVE-2008-5161 and CVE-2015-4000 vulnerabilities in the SSH server.

Failed solution deployments (EDM-15800)

Some solution deployments fail with a "DeploymentNotFoundError" message.

Solution deleted on update (EDM-16127)

When a solution update fails, the old version is sometimes deleted.

Online registration error (EDM-16154)

When an HTTP proxy is configured, the online license registration fails with an HTTP 404 "Not Found" error.

Deployment process not interrupted on failure (EDM-16961)

When a solution deployment fails, the deployment process is not always interrupted.

Platform 1.0.0 known issues

See below the known issues common to all Cryptographic Security Platform 1.0.0 installations.

- Occasional restore failures of single-node installations (EDM-16171)
- Session expiration does not redirect to the login page (ATEAM-17362)

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.

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 for 1.0.0 release notes

See below the release notes of the CA Gateway version running on Cryptographic Security Platform 1.0.0.

- CA Gateway for 1.0.0 new features
- CA Gateway for 1.0.0 fixed bugs
- CA Gateway for 1.0.0 known issues

CA Gateway for 1.0.0 new features

See below the new features of the CA Gateway version running on Cryptographic Security Platform 1.0.0.

- SPKAC support (ATEAM-15658)
- Deprecated cipher suites removed (ATEAM-17303)
- Policy OID listing (ATEAM-16004 & ATEAM-16005)
- New endpoint for license validity monitoring (ATEAM-16023)
- JDK replaced with JRE (ATEAM-16045)
- SID extension support (ATEAM-16815)

SPKAC support (ATEAM-15658)

CA Gateway now supports Signed Public Key and Challenge (SPKAC) requests.

Deprecated cipher suites removed (ATEAM-17303)

This release removes support for the following vulnerable cipher suites.

- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_AES_128_GCM_SHA256

Policy OID listing (ATEAM-16004 & ATEAM-16005)

This release adds the following API endpoint to list the certificate policy object identifiers (OIDs) supported by Entrust Certificate Authority.

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

Other CAs may support this endpoint in future versions.

New endpoint for license validity monitoring (ATEAM-16023)

This release adds the following API endpoint to monitor the license of Docker deployments.

```
/v1/license
```

JDK replaced with JRE (ATEAM-16045)

This release replaces the JDK (Java Development Kit) with the more lightweight JRE (Java Runtime Environment) for Docker and appliance deployments.

SID extension support (ATEAM-16815)

This release adds support to handle SID (Security Identifier) extensions.

CA Gateway for 1.0.0 fixed bugs

See below the bugs fixed in the CA Gateway version running on Cryptographic Security Platform 1.0.0.

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

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

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

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

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

Mandatory Subject Alternative Name not enforced (ATEAM-16170)

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

Invalid date format for expiry date (ATEAM-16797)

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

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

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

Wrong spelling of UserPrincipleName (ATEAM-17046)

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

Role selection not supported (ATEAM-17182)

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

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

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

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

```
Extension of certificate lifetime beyond policy not permitted.
```

Unowned files (ATEAM-17355)

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

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

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

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

Invalid bitwise OR example in documentation (ATEAM-17501)

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

Missing filter-list setting (ATEAM-17650)

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

Non-documented parameters (ATEAM-17651)

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

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

CAA filter bypassed (ATEAM-17708)

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

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

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

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

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

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

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

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

Mandatory subject variables not supported (ATEAM-18126)

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

CA Gateway for 1.0.0 known issues

See below the known issues of the CA Gateway version running on Cryptographic Security Platform 1.0.0.

- 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 for 1.0.0 release notes

See below the release notes of the Certificate Authority version running on Cryptographic Security Platform 1.0.0.

- Certificate Authorities for 1.0.0 fixed bugs
- Certificate Authorities for 1.0.0 known issues

Certificate Authorities for 1.0.0 fixed bugs

See below the bugs fixed in the Certificate Authority version running on Cryptographic Security Platform 1.0.0.

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

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

> Organizations with a name exceeding 14 characters are unusable.

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.

Certificate Authorities for 1.0.0 known issues

See below the known issues of the Certificate Authority version running on Cryptographic Security Platform 1.0.0.

- Datadog errors in logs (ATEAM-17270)
- HSM configuration requires an RFS server (ATEAM-17470)
- No error message when losing the database connection (ATEAM-17478)

Datadog errors in logs (ATEAM-17270)

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

HSM configuration requires an RFS server (ATEAM-17470)

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

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

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

Certificate Enrollment Gateway for 1.0.0 release notes

See below the release notes of the Certificate Enrollment Gateway version running on Cryptographic Security Platform 1.0.0.

- Certificate Enrollment Gateway for 1.0.0 new features
- Certificate Enrollment Gateway for 1.0.0 known issues

Certificate Enrollment Gateway for 1.0.0 new features

See below the new features of the Certificate Enrollment Gateway version running on Cryptographic Security Platform 1.0.0.

- Support for the EST protocol (CEG-1003)
- Support for the CMPv2 protocol (CEG-1006)

> See Enrollment protocols supported by Certificate Enrollment Gateway for a full list of the supported protocols.

Support for the EST protocol (CEG-1003)

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

Support for the CMPv2 protocol (CEG-1006)

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

Certificate Enrollment Gateway for 1.0.0 known issues

See below the known issues of the Certificate Enrollment Gateway version running on Cryptographic Security Platform 1.0.0.

- Configuration backup is only supported in single-node deployments (EDM-704)
- Unsupported ACMEv2 features (PKI-30901)
- Unsupported Intune-SCEP operations (PKI-28149, PKI-31351)
- CSRs sent from ACMEv2 clients cannot have an empty Subject DN if they will be sent to Entrust Certificate Services for processing (ECSPR-39482)
- CSRs sent from ACMEv2 clients cannot have an empty Subject DN if they will be sent to a Microsoft CA for processing (PKI-32853)
- Authentication error message is always logged when enrolling for a certificate with a Cisco LibEST client using basic authentication (CEG-3287)
- Certificate Enrollment Gateway will log WARN messages during startup when attempting to create database tables that already existed (CEG-3392)

> For other known issues with Certificate Enrollment Gateway, see https://trustedcare.entrust.com/TrustedCare/_ui/knowledge/ui/KnowledgeHome

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

Certificate Enrollment Gateway deployments on multi-node installations do not support exporting the configuration.

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 faied.Reason:Access to EST operation:simpleenroll must be
authenticated  ]
```

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

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

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

Certificate Manager for 1.0.0 release notes

See below the release notes of the Certificate Manager version running on Cryptographic Security Platform 1.0.0.

- Certificate Manager for 1.0.0 new features
- Certificate Manager for 1.0.0 fixed bugs
- Certificate Manager for 1.0.0 known issues

Certificate Manager for 1.0.0 new features

See below the new features for the Certificate Manager version running on Cryptographic Security Platform 1.0.0.

Key backup options for Apache and Nginx destinations (ATEAM-18409)

The Apache and Nginx destination configurations now include the **Backup Path** and **Retain Backup Files** options to customize the backup of the deployed keys.

> See Creating an Apache web server destination and Creating an Nginx web server destination for details on these options.

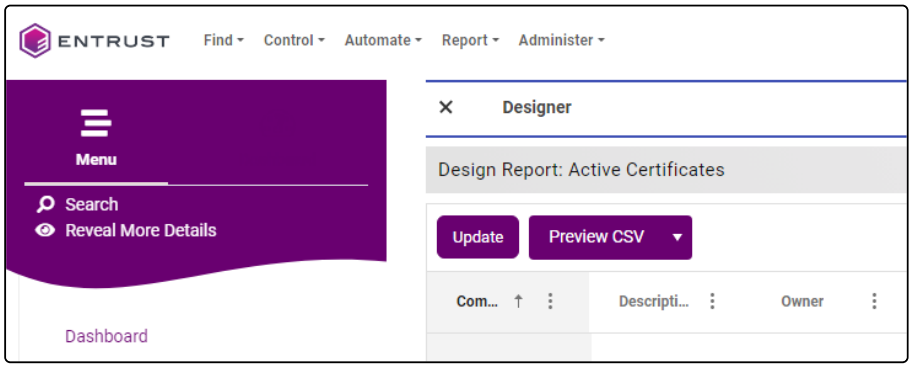
Certificate Manager for 1.0.0 fixed bugs

See below the bugs fixed in the Certificate Manager version running on Cryptographic Security Platform 1.0.0.

- CSV preview command fails on extensive reports (ATEAM-17431)
- Certificate issuance fails on web server empty folders (ATEAM-18214)

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

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



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

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

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

Certificate Manager for 1.0.0 known issues

See below the known issues for the Certificate Manager version running on Cryptographic Security Platform 1.0.0.

- Error when taking certificates off hold (ATEAM-1445)
- Issues when changing the display order of custom fields (ATEAM-15463)
- Some endpoint filters display invalid results on report files (ATEAM-15933)
- Certificates without names not synced from source (ATEAM-16039)
- Out-of-memory error when generating reports with many certificates (ATEAM-16346)
- Wildcard certificates not recorded (ATEAM-16436)
- 'Manage Schedules' option disabled in non-scheduled reports (ATEAM-16910)
- Buttons language not affected when switching language (ATEAM-16920)
- Owner grid column not populated when accessing reports (ATEAM-16923)
- Labels not affected when switching language (ATEAM-16942)
- The Verify button does not trigger a verification without additional changes (ATEAM-16950)
- The public key ID can refer to the private key ID (ATEAM-16982)
- Error when selecting the Domains widget (ATEAM-16986)
- Archive certificates option missing with FIND licenses (ATEAM-16988)
- Incomplete CA certificate chain (ATEAM-16997)
- Verification fails for IIS destinations (ATEAM-17030)
- Certificate creation fail (ATEAM-17063)
- Web server request fails (ATEAM-17070)
- Python requirement not documented (ATEAM-17072)
- Not found error messages during deployment (ATEAM-17230)
- 502 status code when selecting Preview CSV for a report (ATEAM-18121)
- Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)
- Manual upgrade required for supporting Sectigo CA (ATEAM-18790)
- "Weak Hash Algorithm" filter requires resetting before generating a report (ATEAM-18804)

Error when taking certificates off hold (ATEAM-1445)

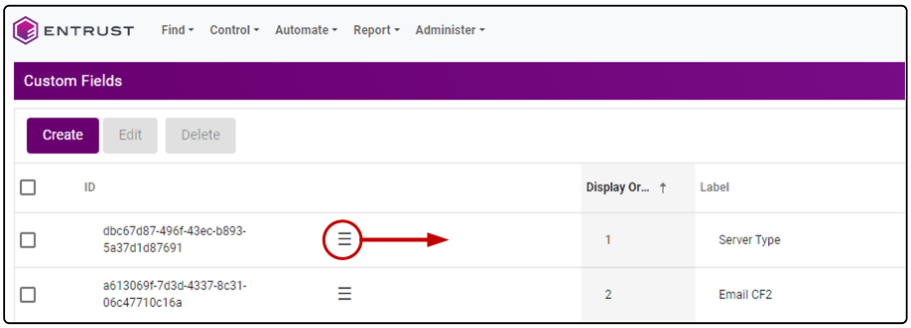
For certificates with **Revocation Reason**: **On Hold**, attempting to unhold the certificate may fail, or the **Unhold** option may be absent from the **Actions** dropdown.

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.

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

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

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

Wildcard certificates not recorded (ATEAM-16436)

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

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

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

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

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

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

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

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

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

Labels not affected when switching language (ATEAM-16942)

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

The Verify button does not trigger a verification without additional changes (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 creation fail (ATEAM-17063)

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

Web server request fails (ATEAM-17070)

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

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

Python requirement not documented (ATEAM-17072)

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

Not found error messages during deployment (ATEAM-17230)

When deploying, you can safely ignore the not found error messages like this one:

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

502 status code when selecting Preview CSV for a report (ATEAM-18121)

Certificate Hub can return a 502 status code when exporting a report to CSV. That is, when:

1. Navigating to **Report / Designer**.
2. Selecting the **Design** action for a report.
3. Selecting **Preview CSV** in the menu bar.

Workaround:

1. Log in to the machine hosting the appliance or the Kubernetes deployment.
2. Run the following command to edit the `acm-api` configuration file.

   ```
   sudo kubectl edit deployment/acm-api -n certhub
   ```

3. Add `-Xmx4g` to the `JAVA_OPTS` setting.

   ```
   env:
     - name: JAVA_OPTS
       value: -Xmx4g
   ```

4. Run the following command to make the changes effective.

   ```
   sudo kubectl rollout restart deployment/acm-api -n certhub
   ```

5. Run the following command to edit the `scheduler` configuration file.

   ```
   run ssudo kubectl edit deployment/scheduler -n certhub
   ```

6. Add `-Xmx4g` to the `JAVA_OPTS` setting.

   ```
   env:
     - name: JAVA_OPTS
       value: -Xmx4g
   ```

7. Run the following command to make the changes effective.

```
sudo kubectl rollout restart deployment/scheduler-n certhub
```

Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)

Pushing a certificate to an SFTP destination may fail with an error message that includes the following:

```
Caused by: java.lang.UnsupportedOperationException
```

Workaround: This error may occur if the plugin manages an outdated hash of the destination SSH key. To resolve this issue, please follow these steps:

1. Edit the SFTP destination as explained in Editing a destination.
2. In the **Edit** dialog, click **Verify** to force an update of the destination SSH key hash.
3. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
4. Click **Save** to confirm the changes.

Manual upgrade required for supporting Sectigo CA (ATEAM-18790)

Certificate Hub 4.2.0 does not support requesting certificates from a CA Gateway 3.2.0 instance integrated with a Sectigo CA.

Workaround:

1. Log in to https://trustedcare.entrust.com
2. Download the solutions installers with `.sln` extension for:
   - Certificate Manager 4.2.1
   - CA Gateway 3.2.1
3. Copy these files to any Cryptographic Security Platform node – for example, using an SFTP client.
4. Run the clusterctl solution upload to upload the solution files.
5. Run the clusterctl solution deploy command to deploy the new Certificate Manager and CA Gateway versions.

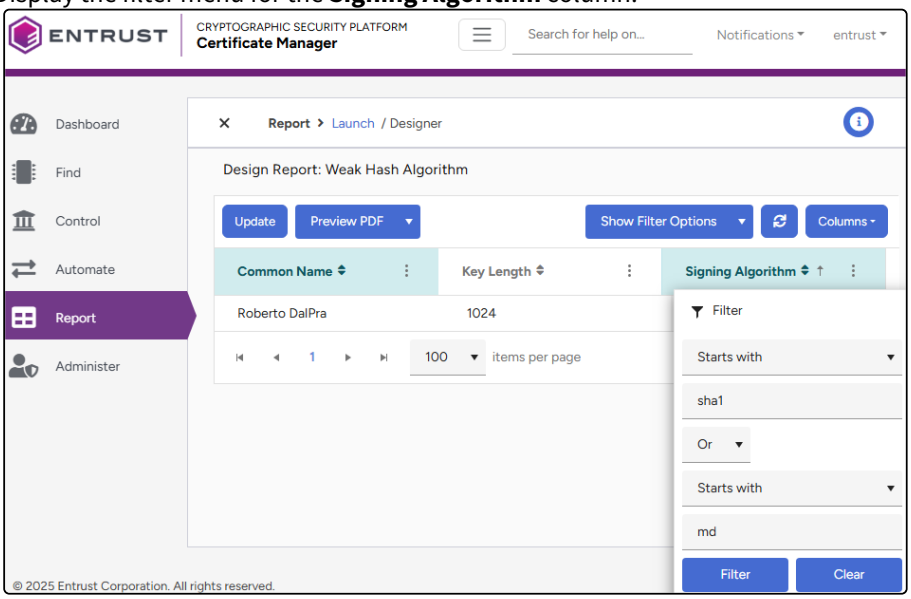
"Weak Hash Algorithm" filter requires resetting before generating a report (ATEAM-18804)

When using the **Preview** button to export the contents of the **Weak Hash Algorithm** system report, the generated report file includes more certificates than just those with a weak hash algorithm.

Workaround:

1. Log in to the user console of Certificate Manager.
2. Navigate to **Report > Designer**.
3. On the report grid, click on **Weak Hash Algorithm**.

4. Display the filter menu for the **Signing Algorithm** column.



5. Click **Clear** to remove all the filter settings.
6. Click the **Update** button.
7. Set again the initial filter configuration:

> **Starts with**
>
> sha1
>
> **Or**
>
> **Starts with**
>
> md

8. Click the **Update** button.
9. Click **Preview** to confirm the generated report only includes certificates matching the filter.

Timestamping Authority for 1.0.0 release notes

See below the release notes of the Timestamping Authority version running on Cryptographic Security Platform 1.0.0.

- Timestamping Authority for 1.0.0 known issues

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

Timestamping Authority for 1.0.0 known issues

See below the known issues in the Timestamping Authority version running on Cryptographic Security Platform 1.0.0.

- False alerts of failed deployment (ATEAM-16344)
- Large kmdata files not supported (ATEAM-16338)
- tsactl logs not forwarded to Splunk (EDM-13275)

False alerts of failed deployment (ATEAM-16344)

After a successful TimeStamping Authority deployment, the Management Console may occasionally display an error message that misleads the user into believing the deployment has failed.

Workaround:

1. Log in to any of the Cryptographic Security Platform installation nodes.
2. Run the following command line.

```
sudo kubectl get pods -n tsa
```

3. Verify the TimeStamping Authority pods are running, in which case the deployment has been successful.

Large kmdata files not supported (ATEAM-16338)

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

tsactl logs not forwarded to Splunk (EDM-13275)

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

Validation Authority for 1.0.0 release notes

See below the release notes of the Validation Authority version running on Cryptographic Security Platform 1.0.0.

- Validation Authority for 1.0.0 known issues

> The Validation Authority release for Cryptographic Security Platform 1.0.0 focuses on dependency updates, not adding features or fixing bugs.

Validation Authority for 1.0.0 known issues

See below the known issues in the Validation Authority version running on Cryptographic Security Platform 1.0.0.

- 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)
- tsactl 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.

tsactl logs not forwarded to Splunk (EDM-13275)

When integrated with a Splunk server, the platform does not forward logs recording `tsactl` commands. However, these logs can be browsed using 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
```

Cryptographic Security Platform 1.1.0 release notes

See below the new features, fixed bugs, and known issues for Cryptographic Security Platform 1.1.0.

- Platform 1.1.0 release notes
- CA Gateway for 1.1.0 release notes
- Certificate Authority for 1.1.0 release notes
- Certificate Enrollment Gateway for 1.1.0 release notes
- Certificate Manager for 1.1.0 release notes
- Timestamping Authority for 1.1.0 release notes
- Validation Authority for 1.1.0 release notes

Platform 1.1.0 release notes

See below the release notes common to all Cryptographic Security Platform 1.1.0 installations.

- Platform 1.1.0 new features
- Platform 1.1.0 known issues

Platform 1.1.0 new features

See below the new features common to all Cryptographic Security Platform 1.1.0 installations.

- 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 Hardware Security Modules.

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 Hardware Security Modules.

Grafana upgrade (EDM-12811)

This release upgrades the Grafana portal to version 12.0.1.

> See HSM requirements for the list of supported Hardware Security Modules.

EntrustOS component update (EDM-17549)

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

> See HSM requirements for the list of supported Hardware Security Modules.

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 1.1.0 known issues

See below the known issues common to all Cryptographic Security Platform 1.1.0 installations.

- Installations with Certificate Enrollment Gateway cannot be restored (CSF-704 & EDM-18536)
- Occasional restore failures of single-node installations (EDM-16171)
- Session expiration does not redirect to the login page (ATEAM-17362)

Installations with Certificate Enrollment Gateway cannot be restored (CSF-704 & EDM-18536)

Cryptographic Security Platform installations with a deployed Certificate Enrollment Gateway do not support Restoring the state.

Workaround:

1. Contact Entrust support for a new version of the `csf-backup-restore.sh` script
2. Open a user session in any of the Cryptographic Security Platform installation nodes.
3. Run the following commands to install the script.

```
sudo cp --force csf-backup-restore.sh /opt/entrust/scripts/rhel/
sudo chmod 550 /opt/entrust/scripts/rhel/csf-backup-restore.sh
sudo chown sysadmin:edm /opt/entrust/scripts/rhel/csf-backup-restore.sh
```

4. Follow the steps described in Restoring the state to restore the state.

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.

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 for 1.1.0 release notes

See below the release notes in the CA Gateway version running on Cryptographic Security Platform 1.1.0.

- CA Gateway for 1.1.0 new features
- CA Gateway for 1.1.0 fixed bugs
- CA Gateway for 1.1.0 known issues

CA Gateway for 1.1.0 new features

See below the new features in the CA Gateway version running on Cryptographic Security Platform 1.1.0.

Cache management (ATEAM-17140)

This release adds support for enabling and disabling CA Gateway API caches.

Sectigo CA support (ATEAM-18339)

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

- See CA Gateway for 1.1.0 known issues for how to work around the ATEAM-18782 known issue.
- See Integrating a Sectigo CA for selecting a Sectigo CA in the configuration settings.

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.

Multiple KeyUsage on request (ATEAM-18374)

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

CA Gateway for 1.1.0 fixed bugs

See below the bugs fixed in the CA Gateway version running on Cryptographic Security Platform 1.1.0.

- Error when revoking certificates without Subject (ATEAM-11625)
- Missing HTTP Strict Transport Security header (ATEAM-16176)
- Missing Content Security Policy header (ATEAM-16215)
- Unspecified validation error (ATEAM-17472)
- Sectigo CA not supported (ATEAM-18790)

Error when revoking certificates without Subject (ATEAM-11625)

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

Missing HTTP Strict Transport Security header (ATEAM-16176)

CA Gateway does not add an HTTP Strict Transport Security (HSTS) header to responses.

Missing Content Security Policy header (ATEAM-16215)

CA Gateway does not add a Content Security Policy (CSP) header to responses.

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 ("-").

Sectigo CA not supported (ATEAM-18790)

Certificate Hub 4.2.0 does not support requesting certificates from a CA Gateway 3.2.0 instance integrated with a Sectigo CA.

> ⚠ To fix this bug, you must install Certificate Hub 4.2.1 and CA Gateway 3.2.1.

CA Gateway for 1.1.0 known issues

See below the known issues in the CA Gateway version running on Cryptographic Security Platform 1.1.0.

- Mandatory parameters are mutually exclusive (ATEAM-16246)
- subject.certificates field omitted (ATEAM-16264)
- Slashes not supported in passwords (ATEAM-18325)
- Sectigo plugin invalid name (ATEAM-18782)
- Sectigo CA profile synchronization requires redeploying CA Gateway (ATEAM-18819)

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).

Sectigo plugin invalid name (ATEAM-18782)

The **Connector Name** selector of the Management Console lists the Sectigo CA plugin as **com.Sectigo** instead of **com.SectigoCA**.

Workaround:

1. Export the CA Gateway configuration using the clusterctl solution config export command
2. Replace `com.Sectigo` with `com.SectigoCA` in the following files.
    - `config-schema.json`
    - `sectigo-schema.json`
    - `application.yml` (only if CA Gateway has been deployed with the Sectigo CA plugin).
3. Apply the new configuration with the clusterctl solution config import command.
4. Deploy or redeploy the solution with the clusterctl solution deploy command.

Sectigo CA profile synchronization requires redeploying CA Gateway (ATEAM-18819)

Changes to Sectigo CA custom fields are not automatically effective in the `requestedProperties` field described in Sectigo CA profile properties.

Workaround: redeploy CA Gateway using the Management Console or the clusterctl solution deploy command.

Certificate Authority for 1.1.0 release notes

See below the release notes in the Certificate Authority version running on Cryptographic Security Platform 1.1.0.

- Certificate Authority for 1.1.0 new features
- Certificate Authority for 1.1.0 fixed bugs
- Certificate Authority for 1.1.0 known issues

Certificate Authority for 1.1.0 new features

See below the new features in the Certificate Authority version running on Cryptographic Security Platform 1.1.0.

Support for 3-tier PKIs (ATEAM-18489)

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

Certificate Authority for 1.1.0 fixed bugs

See below the bugs fixed in the Certificate Authority version running on Cryptographic Security Platform 1.1.0.

- 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:30000/pkihub/init-attila:v202503271109\":
rpc error: code = NotFound desc = failed to pull and unpack image
```

Certificate Authority for 1.1.0 known issues

See below the known issues in the Certificate Authority version running on Cryptographic Security Platform 1.1.0.

- Datadog errors in logs (ATEAM-17270)
- 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.

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 Enrollment Gateway for 1.1.0 release notes

See below the release notes of the Certificate Enrollment Gateway version running on Cryptographic Security Platform 1.1.0.

- Certificate Enrollment Gateway for 1.1.0 fixed bugs
- Certificate Enrollment Gateway for 1.1.0 known issues

Certificate Enrollment Gateway for 1.1.0 fixed bugs

See below the bugs fixed in the Certificate Enrollment Gateway version running on Cryptographic Security Platform 1.1.0.

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

Certificate Enrollment Gateway deployments on multi-node Cryptographic Security Platform installations do not support exporting the configuration.

Certificate Enrollment Gateway for 1.1.0 known issues

See below the known issues in the Certificate Enrollment Gateway version running on Cryptographic Security Platform 1.1.0.

- Unsupported ACMEv2 features (PKI-30901)
- Unsupported Intune-SCEP operations (PKI-28149, PKI-31351)
- CSRs sent from ACMEv2 clients cannot have an empty Subject DN if they will be sent to Entrust Certificate Services for processing (ECSPR-39482)
- CSRs sent from ACMEv2 clients cannot have an empty Subject DN if they will be sent to a Microsoft CA for processing (PKI-32853)
- Authentication error message is always logged when enrolling for a certificate with a Cisco LibEST client using basic authentication (CEG-3287)
- Certificate Enrollment Gateway will log WARN messages during startup when attempting to create database tables that already existed (CEG-3392)

For other known issues with Certificate Enrollment Gateway, see https://trustedcare.entrust.com/TrustedCare/_ui/knowledge/ui/KnowledgeHome

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. The cloud-based Entrust Certificate Services require 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 faied.Reason:Access to EST operation:simpleenroll must be
authenticated  ]
```

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

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

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

Certificate Manager for 1.1.0 release notes

See below the release notes of the Certificate Manager version running on Cryptographic Security Platform 1.1.0.

- Certificate Manager for 1.1.0 new features
- Certificate Manager for 1.1.0 fixed bugs
- Certificate Manager for 1.1.0 known issues

Certificate Manager for 1.1.0 new features

See below the new features of the Certificate Manager version running on Cryptographic Security Platform 1.1.0.

- 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 for 1.1.0 fixed bugs

See below the fixed bugs in the Certificate Manager version running on Cryptographic Security Platform 1.1.0.

- Matching tags not sorted (ATEAM-18116)
- 502 status code when selecting Preview CSV for a report (ATEAM-18121)
- Missing keyboard accessibility options (ATEAM-18302)
- Mandatory fields not validated (ATEAM-18315)
- No charts dislayed 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)
- Manual upgrade required for supporting Sectigo CA (ATEAM-18790)
- "Weak Hash Algorithm" filter requires resetting before generating a report (ATEAM-18804)

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.

502 status code when selecting Preview CSV for a report (ATEAM-18121)

Certificate Hub can return a 502 status code when exporting a report to CSV. That is, when:

1. Navigating to **Report / Designer**.
2. Selecting the **Design** action for a report.
3. Selecting **Preview CSV** in the menu bar.

Workaround:

1. Log in to the machine hosting the appliance or the Kubernetes deployment.
2. Run the following command to edit the `acm-api` configuration file.

```
sudo kubectl edit deployment/acm-api -n certhub
```

3. Add `-Xmx4g` to the `JAVA_OPTS` setting.

```
env:
  - name: JAVA_OPTS
    value: -Xmx4g
```

4. Run the following command to make the changes effective.

```
sudo kubectl rollout restart deployment/acm-api -n certhub
```

5. Run the following command to edit the `scheduler` configuration file.

```
run ssudo kubectl edit deployment/scheduler -n certhub
```

6. Add `-Xmx4g` to the `JAVA_OPTS` setting.

```
env:
  - name: JAVA_OPTS
    value: -Xmx4g
```

7. Run the following command to make the changes effective.

```
sudo kubectl rollout restart deployment/scheduler-n certhub
```

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 dislayed 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.

Manual upgrade required for supporting Sectigo CA (ATEAM-18790)

Certificate Hub 4.2.0 does not support requesting certificates from a CA Gateway 3.2.0 instance integrated with a Sectigo CA.

Workaround:

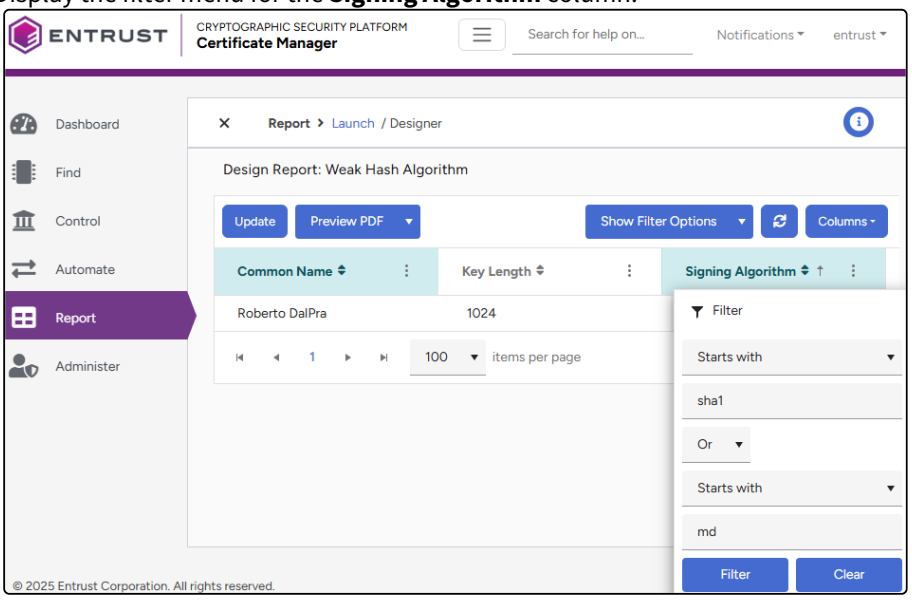
1. Log in to https://trustedcare.entrust.com
2. Download the solutions installers with `.sln` extension for:
    - Certificate Manager 4.2.1
    - CA Gateway 3.2.1
3. Copy these files to any Cryptographic Security Platform node – for example, using an SFTP client.
4. Run the clusterctl solution upload to upload the solution files.
5. Run the clusterctl solution deploy command to deploy the new Certificate Manager and CA Gateway versions.

"Weak Hash Algorithm" filter requires resetting before generating a report (ATEAM-18804)

When using the **Preview** button to export the contents of the **Weak Hash Algorithm** system report, the generated report file includes more certificates than just those with a weak hash algorithm.

Workaround:

1. Log in to the user console of Certificate Manager.
2. Navigate to **Report > Designer**.
3. On the report grid, click on **Weak Hash Algorithm**.
4. Display the filter menu for the **Signing Algorithm** column.



5. Click **Clear** to remove all the filter settings.
6. Click the **Update** button.
7. Set again the initial filter configuration:

    Starts with

    sha1

    Or

    Starts with

    md

8. Click the **Update** button.
9. Click **Preview** to confirm the generated report only includes certificates matching the filter.

Certificate Manager for 1.1.0 known issues

See below the known issues in the Certificate Manager version running on Cryptographic Security Platform 1.1.0.

- 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)
- The Verify button does not trigger a verification without additional changes (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)
- Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)
- Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)

Error when taking certificates off hold (ATEAM-1445)

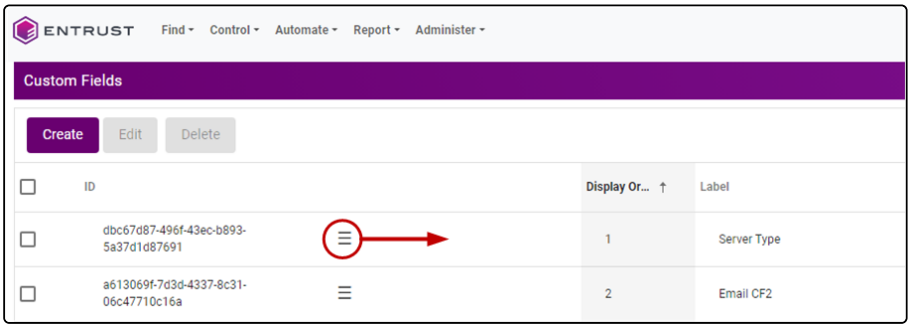
For certificates with **Revocation Reason**: **On Hold**, attempting to unhold the certificate may fail, or the **Unhold** option may be absent from the **Actions** dropdown.

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.

> 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 **Destinations** page.

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

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

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

The Verify button does not trigger a verification without additional changes (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
```

Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)

Pushing a certificate to an SFTP destination may fail with an error message that includes the following:

```
Caused by: java.lang.UnsupportedOperationException
```

Workaround: This error may occur if the plugin manages an outdated hash of the destination SSH key. To resolve this issue, please follow these steps:

1. Edit the SFTP destination as explained in Editing a destination.
2. In the **Edit** dialog, click **Verify** to force an update of the destination SSH key hash.
3. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
4. Click **Save** to confirm the changes.

Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)

The Certificate Manager console may display a blank page when manually renewing a certificate issued by a Sectigo CA

Workaround:

1. Reload the page.
2. Repeat the renewal operation.

Timestamping Authority for 1.1.0 release notes

See below the release notes of the Timestamping Authority version running on Cryptographic Security Platform 1.1.0.

- Timestamping Authority for 1.1.0 known issues

> As explained in Platform 1.1.0 new features, this release updates the HSM client software.

Timestamping Authority for 1.1.0 known issues

See below the known issues in the Timestamping Authority version running on Cryptographic Security Platform 1.1.0.

- tsactl logs not forwarded to Splunk (EDM-13275)
- False alerts of failed deployment (ATEAM-16344)
- Large kmdata files not supported (ATEAM-16338)

tsactl logs not forwarded to Splunk (EDM-13275)

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

False alerts of failed deployment (ATEAM-16344)

After a successful TimeStamping Authority deployment, the Management Console may occasionally display an error message that misleads the user into believing the deployment has failed.

Workaround:

1. Log in to any of the Cryptographic Security Platform installation nodes.

2. Run the following command line.

```
sudo kubectl get pods -n tsa
```

3. Verify the TimeStamping Authority pods are running, in which case the deployment has been successful.

Large kmdata files not supported (ATEAM-16338)

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

Validation Authority for 1.1.0 release notes

See below the release notes of the Validation Authority version running on Cryptographic Security Platform 1.1.0.

- Validation Authority for 1.1.0 new features
- Validation Authority for 1.1.0 fixed bugs
- Validation Authority for 1.1.0 known issues

> As explained in Platform 1.1.0 new features, this release updates the HSM client software.

Validation Authority for 1.1.0 new features

See below the new features in the Validation Authority version running on Cryptographic Security Platform 1.1.0.

- 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 processing signed OCSP requests.

> Entrust Validation Authority does not validate the OCSP request signature, as OCSP services are supposed to be free and available to all PKI subscribers, just like CRLs.

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 for 1.1.0 fixed bugs

See below the bugs fixed in the Validation Authority version running on Cryptographic Security Platform 1.1.0.

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 for 1.1.0 known issues

See below the release notes of the Validation Authority version running on Cryptographic Security Platform 1.1.0.

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

tsactl logs not forwarded to Splunk (EDM-13275)

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

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

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

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

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

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

1. List the pods.

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

2. Kill the dead pod. For example:

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

Newly deployed status after command execution (ATEAM-16337)

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

Large kmdata files not supported (ATEAM-16338)

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

Database validation error (ATEAM-17466)

The Management Console displays a validation error when:

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

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

Cryptographic Security Platform 1.2.0 release notes

See below the new features, fixed bugs, and known issues for Cryptographic Security Platform 1.2.0.

- Platform 1.2.0 release notes
- CA Gateway for 1.2 release notes
- Certificate Authority for 1.2 release notes
- Certificate Manager for 1.2 release notes
- Timestamping Authority for 1.2 release notes
- Validation Authority for 1.2 release notes

Cryptographic Security Platform 1.2.0 does not upgrade the versions of the following solutions already distributed with Cryptographic Security Platform 1.1.0.

- Certificate Enrollment Gateway 2.1.2.
- Log forwarder 4.0.2

Platform 1.2.0 release notes

See below the release notes common to all Cryptographic Security Platform 1.2.0 installations.

- Platform 1.20 new features
- Platform 1.2.0 known issues

Platform 1.20 new features

See below the new features common to all Cryptographic Security Platform 1.2.0 installations.

- Support for new TLS algorithms (EDM-17844)
- Server name removed from HTTP responses (EDM-18199)
- SNMP monitoring (EDM-18341)
- ECDHE-RSA-AES128-GCM-SHA256 TLS cipher suite deprecated (EDM-18453)
- Configurable JWT expiry (EDM-18527)

Support for new TLS algorithms (EDM-17844)

This release adds the following supported algorithms for generating the TLS certificate.

- ECDSA curve NIST P-384
- ECDSA curve NIST P-521

Server name removed from HTTP responses (EDM-18199)

For security reasons, the server name is no longer disclosed in the HTTP responses.

SNMP monitoring (EDM-18341)

This release adds support for SNMP monitoring of the Cryptographic Security Platform nodes.



See Configuring SNMP Authentication for MIB information access for how to enable SNMP access.

ECDHE-RSA-AES128-GCM-SHA256 TLS cipher suite deprecated (EDM-18453)

Cryptographic Security Platform no longer supports the ECDHE-RSA-AES128-GCM-SHA256 TLS cipher suite for TLS connections.

Configurable JWT expiry (EDM-18527)

This release adds support for configuring the expiry of the JSON Web Token (JWT) granted to the console user.

Platform 1.2.0 known issues

See below the known issues common to all Cryptographic Security Platform 1.2.0 installations.

- Session expiration does not redirect to the login page (ATEAM-17362)
- Installations with Certificate Enrollment Gateway cannot be restored (CSF-704 & EDM-18536)
- Occasional restore failures of single-node installations (EDM-16171)
- Installations with Certificate Authority do not support upgrading (EDM-19202)

> ⚠ As explained in Certificate Manager for 1.2 known issues, after installing Cryptographic Security Platform 1.2.0, you must manually upgrade Certificate Manager and CA Gateway if you want Certificate Manager to support a Sectigo CA.

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.

Installations with Certificate Enrollment Gateway cannot be restored (CSF-704 & EDM-18536)

Cryptographic Security Platform installations with a deployed Certificate Enrollment Gateway do not support Restoring the state.

Workaround:

1. Contact Entrust support for a new version of the `csf-backup-restore.sh` script
2. Open a user session in any of the Cryptographic Security Platform installation nodes.
3. Run the following commands to install the script.

```
sudo cp --force csf-backup-restore.sh /opt/entrust/scripts/rhel/
sudo chmod 550 /opt/entrust/scripts/rhel/csf-backup-restore.sh
sudo chown sysadmin:edm /opt/entrust/scripts/rhel/csf-backup-restore.sh
```

4. Follow the steps described in Restoring the state to restore the state.

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.

Installations with Certificate Authority do not support upgrading (EDM-19202)

Cryptographic Security Platform 1.1.0 installations with the Certificate Authority deployed solution do not support upgrading to Cryptographic Security Platform 1.2.0.

Workaround: Skip the 1.2.0 release and upgrade Cryptographic Security Platform 1.1.0 to 1.2.1

CA Gateway for 1.2 release notes

See below the release notes in the CA Gateway version running on Cryptographic Security Platform 1.2.0 & 1.2.1.

- CA Gateway for 1.2 fixed bugs
- CA Gateway for 1.2 known issues

CA Gateway for 1.2 fixed bugs

See below the fixed bugs in the CA Gateway version running on Cryptographic Security Platform 1.2.0 & 1.2.1.

- CA lookup fails when the DN includes tildes (ATEAM-18768)
- LDAP and LDAPS port incompatibility not documented (ATEAM-18779)
- Sectigo plugin invalid name (ATEAM-18782)
- Sectigo CA profile synchronization requires redeploying CA Gateway (ATEAM-18819)

CA lookup fails when the DN includes tildes (ATEAM-18768)

The lookup for a CA (Certificate Authority) fails when the DN (Distinguished Name) of the CA contains tildes, like in "MODERNIZAÇÃO".

LDAP and LDAPS port incompatibility not documented (ATEAM-18779)

The user guide does not properly outline that the **LDAP Port** and **LDAPS Port** settings are mutually exclusive.

Bug resolution: add a warning note to the com.entrust.SecurityManager section.

Sectigo plugin invalid name (ATEAM-18782)

The **Connector Name** selector of the Management Console lists the Sectigo CA plugin as **com.Sectigo** instead of **com.SectigoCA**.

Workaround:

1. Export the CA Gateway configuration using the clusterctl solution config export command
2. Replace `com.Sectigo` with `com.SectigoCA` in the following files.
    - `config-schema.json`
    - `sectigo-schema.json`
    - `application.yml` (only if CA Gateway has been deployed with the Sectigo CA plugin).
3. Apply the new configuration with the clusterctl solution config import command.
4. Deploy or redeploy the solution with the clusterctl solution deploy command.

Sectigo CA profile synchronization requires redeploying CA Gateway (ATEAM-18819)

Changes to Sectigo CA custom fields are not automatically effective in the `requestedProperties` field described in Sectigo CA profile properties.

Workaround: redeploy CA Gateway using the Management Console or the clusterctl solution deploy command.

CA Gateway for 1.2 known issues

See below the known issues in the CA Gateway version running on Cryptographic Security Platform 1.2.0 & 1.2.1.

- 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 for 1.2 release notes

See below the release notes of the Certificate Authority version running on Cryptographic Security Platform 1.2.0 & 1.2.1.

- Certificate Authority for 1.2 new features
- Certificate Authority for 1.2 known issues

Certificate Authority for 1.2 new features

See below the new features in the Certificate Authority version running on Cryptographic Security Platform 1.2.0 & 1.2.1.

Updated user interface (ATEAM-18496)

This release updates the Certificate Manager user interface with features such as:

- Certificate profile customization
- Client certificate renewal
- Ed25519 elliptic curve algorithm support

See HSM requirements for the list of supported Hardware Security Modules.

Certificate Authority for 1.2 known issues

See below the known issues in the Certificate Authority version running on Cryptographic Security Platform 1.2.0 & 1.2.1.

- Datadog errors in logs (ATEAM-17270)
- 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.

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 for 1.2 release notes

See below the release notes of the Certificate Manager version running on Cryptographic Security Platform 1.2.0 & 1.2.1.

- Certificate Manager for 1.2 new features
- Certificate Manager for 1.2 fixed bugs
- Certificate Manager for 1.2 known issues

Certificate Manager for 1.2 new features

See below the new features in the Certificate Manager solution distributed with Cryptographic Security Platform 1.2.0 & 1.2.1.

- Custom layout for email notification (ATEAM-17499)
- JWT security enhanced with cookies (ATEAM-18693)
- Apache restart without sudo permissions (ATEAM-18827)

Custom layout for email notification (ATEAM-17499)

The new Email configuration setting allows for the definition of a custom header and footer for the notification emails.

JWT security enhanced with cookies (ATEAM-18693)

The security of the JSON Web Tokens (JWTs) granted to console users has been enhanced by using browser cookies.

Apache restart without sudo permissions (ATEAM-18827)

The Apache web server destinations add support for restarting the Apache server without sudo permissions.

> See Creating an Apache web server destination for details on this destination.

Certificate Manager for 1.2 fixed bugs

See below the fixed bugs in the Certificate Manager solution distributed with Cryptographic Security Platform 1.2.0 & 1.2.1.

Filters do not support custom rules (ATEAM-18762)

The automation rules do not support custom rules.

> See Rules and Actions for how to create automation rules.

Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)

Pushing a certificate to an SFTP destination may fail with an error message that includes the following:

```
Caused by: java.lang.UnsupportedOperationException
```

Workaround: This error may occur if the plugin manages an outdated hash of the destination SSH key. To resolve this issue, please follow these steps:

1. Edit the SFTP destination as explained in Editing a destination.
2. In the **Edit** dialog, click **Verify** to force an update of the destination SSH key hash.
3. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
4. Click **Save** to confirm the changes.

Certificate Manager for 1.2 known issues

See below the known issues in the Certificate Manager solution distributed with Cryptographic Security Platform 1.2.0 & 1.2.1.

- 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)
- The Verify button does not trigger a verification without additional changes (ATEAM-16950)
- The public key ID can refer to the private key ID (ATEAM-16982)
- Archive certificates option missing with FIND licenses (ATEAM-16988)
- Incomplete CA certificate chain (ATEAM-16997)
- Verification fails for IIS destinations (ATEAM-17030)
- Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)
- Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)
- STARTTLS not enabled when "Use TLS" option is checked (ATEAM-18848)

Error when taking certificates off hold (ATEAM-1445)

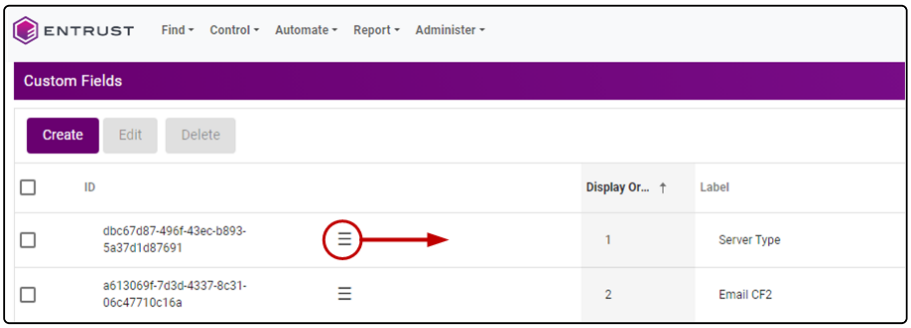
For certificates with **Revocation Reason**: **On Hold**, attempting to unhold the certificate may fail, or the **Unhold** option may be absent from the **Actions** dropdown.

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.

> 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 **Destinations** page.

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

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

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

The Verify button does not trigger a verification without additional changes (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**

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
```

Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)

Pushing a certificate to an SFTP destination may fail with an error message that includes the following:

```
Caused by: java.lang.UnsupportedOperationException
```

Workaround: This error may occur if the plugin manages an outdated hash of the destination SSH key. To resolve this issue, please follow these steps:

1. Edit the SFTP destination as explained in Editing a destination.
2. In the **Edit** dialog, click **Verify** to force an update of the destination SSH key hash.
3. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
4. Click **Save** to confirm the changes.

Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)

The Certificate Manager console may display a blank page when manually renewing a certificate issued by a Sectigo CA

Workaround:

1. Reload the page.
2. Repeat the renewal operation.

STARTTLS not enabled when "Use TLS" option is checked (ATEAM-18848)

The **Use TLS** option of the SMTP plugin configuration does not enable STARTTLS.

The STARTTLS command upgrades an SMTP communication channel to a secure, encrypted connection using TLS (Transport Layer Security).

Workaround:

1. Log in to the Certificate Manager user console.
2. Navigate to **Administer > Settings > PLUGINS**.
3. Edit the **smtp-notification-plugin** configuration.
4. Activate the following options:
    - Use TLS
    - Use SSL
5. Click **Save**.
6. Edit the plugin configuration again.
7. Disable the **Use SSL** option.
8. Click **Save**.

Timestamping Authority for 1.2 release notes

See below the release notes of the Timestamping Authority solution distributed with Cryptographic Security Platform 1.2.0 & 1.2.1.

- Timestamping Authority for 1.2 new features
- Timestamping Authority for 1.2 known issues

Timestamping Authority for 1.2 new features

See below the new features in the Timestamping Authority solution distributed with Cryptographic Security Platform 1.2.0 & 1.2.1.

- Support for Thales TCT (ATEAM-18526)
- Post-quantum cryptography support (ATEAM-18750)
- Support for RSA-PSS (ATEAM-18753)

Support for Thales TCT (ATEAM-18526)

This release adds support for the Thales TCT (Trusted Cyber Technologies) HSM (Hardware Security Module).

See HSM requirements for the list of supported Hardware Security Modules.

Post-quantum cryptography support (ATEAM-18750)

This release supports Thales Luna and Entrust nShield HSMs (Hardware Security Modules) with PQC (Post-quantum cryptography) drivers.

- See tsactl create-key for instructions on selecting a Module-Lattice-Based Digital Signature Algorithm when creating the key for signing TST responses.
- See HSM requirements for the list of supported Hardware Security Modules.

Support for RSA-PSS (ATEAM-18753)

New **Use RSA-PSS** option to enable RSA-PSS (Probabilistic Signature Scheme) when signing TST responses.

See TST profile for details on this option.

Timestamping Authority for 1.2 known issues

See below the known issues in the Timestamping Authority solution distributed with Cryptographic Security Platform 1.2.0 & 1.2.1.

- Large kmdata files not supported (ATEAM-16338)
- False alerts of failed deployment (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.

False alerts of failed deployment (ATEAM-16344)

After a successful TimeStamping Authority deployment, the Management Console may occasionally display an error message that misleads the user into believing the deployment has failed.

Workaround:

1. Log in to any of the Cryptographic Security Platform installation nodes.
2. Run the following command line.

```
sudo kubectl get pods -n tsa
```

3. Verify the TimeStamping Authority pods are running, in which case the deployment has been successful.

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 for 1.2 release notes

See below the release notes for the Validation Authority solution distributed with Cryptographic Security Platform 1.2.0 & 1.2.1.

- Validation Authority for 1.2 new features
- Validation Authority for 1.2 known issues

Validation Authority for 1.2 new features

See below the new features in the Validation Authority version running on Cryptographic Security Platform 1.2.0 & 1.2.1.

- Support for Thales TCT (ATEAM-18526)
- Post-quantum cryptography support (ATEAM-18750)

- Support for RSA-PSS (ATEAM-18753)

Support for Thales TCT (ATEAM-18526)

This release adds support for the Thales TCT (Trusted Cyber Technologies) HSM (Hardware Security Module).

Post-quantum cryptography support (ATEAM-18750)

This release supports Thales Luna and Entrust nShield (Hardware Security Modules) with PQC (Post-quantum cryptography) drivers.

- See evactl create-key for instructions on selecting a Module-Lattice-Based Digital Signature Algorithm when creating the key for signing OCSP responses.
- See HSM requirements for the list of supported Hardware Security Modules.

Support for RSA-PSS (ATEAM-18753)

New **Use RSA-PSS** option to enable RSA-PSS (Probabilistic Signature Scheme) when signing OCSP responses.

> See OCSP Responder for details on this option.

Validation Authority for 1.2 known issues

See below the known issues in the Validation Authority version running on Cryptographic Security Platform 1.2.0 & 1.2.1.

- 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
```

Cryptographic Security Platform 1.2.1 release notes

Cryptographic Security Platform 1.2.1 only upgrades the version of the PKI Hub kernel.

- Platform 1.2.1 release notes

Platform 1.2.1 release notes

See below the release notes common to all Cryptographic Security Platform 1.2.1 installations.

- Platform 1.2.1 fixed bugs

Platform 1.2.1 fixed bugs

Cryptographic Security Platform 1.2.1 fixes the following bug listed in Platform 1.2.0 known issues.

Installations with Certificate Authority do not support upgrading (EDM-19202)

Cryptographic Security Platform 1.1.0 installations with the Certificate Authority deployed solution do not support upgrading to Cryptographic Security Platform 1.2.0.

Workaround: Skip the 1.2.0 release and upgrade Cryptographic Security Platform 1.1.0 to 1.2.1

CA Gateway 3.4.0 release notes

See below the release notes for the CA Gateway 3.4.0 independent release.

- CA Gateway 3.4.0 new features
- CA Gateway 3.4.0 known issues

CA Gateway 3.4.0 new features

See below the new features in the CA Gateway 3.4.0 independent release.

DigiCert CA Support (ATEAM-18568)

CA Gateway 3.4.0 introduces support for issuing DV (Domain Validation) certificates with DigiCert certificate authorities.

CA Gateway 3.4.0 known issues

See below the known issues in the CA Gateway 3.4.0 independent release.

- 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 Manager 4.3.1 release notes

See below the release notes for the Certificate Manager 4.3.1 independent release.

- Certificate Manager 4.3.1 new features
- Certificate Manager 4.3.1 fixed bugs
- Certificate Manager 4.3.1 known issues

Certificate Manager 4.3.1 new features

See below the new features in the Certificate Manager 4.3.1 independent release.

New renewalSerialNumber enrollment value (ATEAM-18902)

When requesting a certificate renewal from certificate authorities like Sectigo, the enrollment API will include the new `renewalSerialNumber` value.

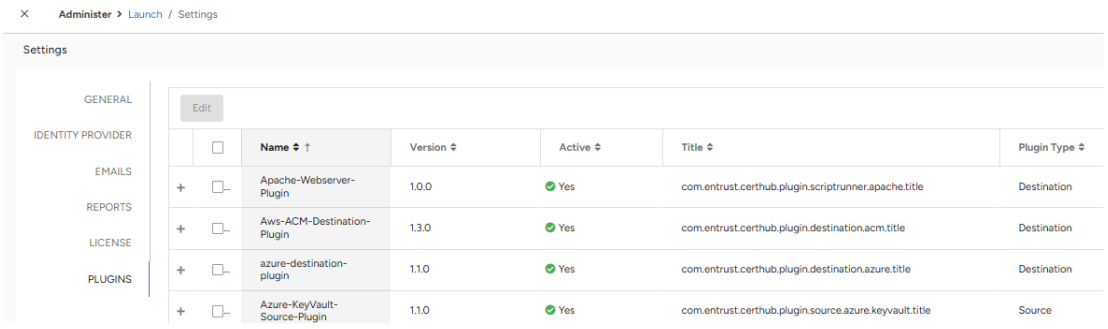
Certificate Manager 4.3.1 fixed bugs

See below the bugs fixed in the Certificate Manager 4.3.1 independent release.

- Plugin titles not properly displayed (ATEAM-18894)
- Error when issuing a certificate for an Apache or IIS destination (ATEAM-18895)
- Error when verifying access and credentials for an Apache or IIS destination (ATEAM-18904)

Plugin titles not properly displayed (ATEAM-18894)

The **Title** column of the plugins grid shows the keys of the plugin titles instead of the real titles.



Error when issuing a certificate for an Apache or IIS destination (ATEAM-18895)

Certificate Manager returns an error when issuing a certificate for an Apache or IIS web server destination.

Error when verifying access and credentials for an Apache or IIS destination (ATEAM-18904)

Certificate Manager may return an error when verifying access and credentials for an Apache or Microsoft IIS web server destination.

Certificate Manager 4.3.1 known issues

See below the known issues in the Certificate Manager 4.3.1 independent release.

- 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)
- The Verify button does not trigger a verification without additional changes (ATEAM-16950)
- The public key ID can refer to the private key ID (ATEAM-16982)
- Archive certificates option missing with FIND licenses (ATEAM-16988)
- Incomplete CA certificate chain (ATEAM-16997)
- Verification fails for IIS destinations (ATEAM-17030)
- Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)
- Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)
- STARTTLS not enabled when "Use TLS" option is checked (ATEAM-18848)

Error when taking certificates off hold (ATEAM-1445)

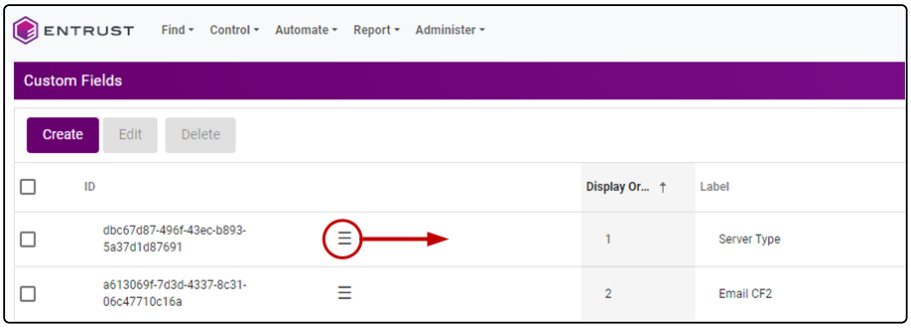
For certificates with **Revocation Reason**: **On Hold**, attempting to unhold the certificate may fail, or the **Unhold** option may be absent from the **Actions** dropdown.

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.

> 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 **Destinations** page.

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

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

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

The Verify button does not trigger a verification without additional changes (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**

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
```

Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)

Pushing a certificate to an SFTP destination may fail with an error message that includes the following:

```
Caused by: java.lang.UnsupportedOperationException
```

Workaround: This error may occur if the plugin manages an outdated hash of the destination SSH key. To resolve this issue, please follow these steps:

1. Edit the SFTP destination as explained in Editing a destination.
2. In the **Edit** dialog, click **Verify** to force an update of the destination SSH key hash.
3. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
4. Click **Save** to confirm the changes.

Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)

The Certificate Manager console may display a blank page when manually renewing a certificate issued by a Sectigo CA

Workaround:

1. Reload the page.
2. Repeat the renewal operation.

STARTTLS not enabled when "Use TLS" option is checked (ATEAM-18848)

The **Use TLS** option of the SMTP plugin configuration does not enable STARTTLS.

> ⚠ The STARTTLS command upgrades an SMTP communication channel to a secure, encrypted connection using TLS (Transport Layer Security).

Workaround:

1. Log in to the Certificate Manager user console.
2. Navigate to **Administer > Settings > PLUGINS**.
3. Edit the **smtp-notification-plugin** configuration.
4. Activate the following options:
   - Use TLS
   - Use SSL
5. Click **Save**.
6. Edit the plugin configuration again.
7. Disable the **Use SSL** option.
8. Click **Save**.

Cryptographic Security Platform 1.3.0 release notes

See below the new features, fixed bugs, and known issues for Cryptographic Security Platform 1.3.0.

- Platform 1.3.0 release notes
- CA Gateway for 1.3.0 release notes
- Certificate Authority for 1.3.0 release notes
- Certificate Manager for 1.3.0 release notes
- Timestamping Authority for 1.3.0 release notes
- Validation Authority for 1.3.0 release notes

Cryptographic Security Platform 1.3.0 is a greenfield release that does not support upgrading from previous versions.

Platform 1.3.0 release notes

See below the release notes common to all Cryptographic Security Platform 1.3.0 installations.

- Platform 1.3.0 new features
- Platform 1.3.0 fixed bugs
- Platform 1.3.0 known issues

Platform 1.3.0 new features

See below the new features common to all Cryptographic Security Platform 1.3.0 installations.

- Different ports for administration and end-user services (EDM-17153)
- New user management console (EDM-18229, EDM-18230 & EDM-18231)
- Hardened operating password policy (EDM-18608)

Different ports for administration and end-user services (EDM-17153)

This release sets 8443 as the port for accessing administration services. For example, the URL of the management console is now:

```
https://<machine>:8443/management-console
```

End-user services will continue using ports 80 and 443.

New user management console (EDM-18229, EDM-18230 & EDM-18231)

This release introduces a console for registering users and managing user settings, such as permissions, credentials, and session timeouts.

- See Cluster database requirements for the database requirements of this new feature.
- See Managing identities for instructions on using this console.

Hardened operating password policy (EDM-18608)

Cryptographic Security Platform 1.3 hardens the following settings of the operating system password policy.

Setting	Cryptographic Security Platform 1.2	Cryptographic Security Platform 1.3
Password history	5	8
"Reset account lockout counter after" period	15 minutes	24 hours
Lockout duration	10 minutes	24 hours

Platform 1.3.0 fixed bugs

See below the fixed bugs common to all Cryptographic Security Platform 1.3.0 installations.

- The management console does not populate already set passwords (ATEAM-18773)
- Some commands prompt for confirmation of existing passwords (EDM-18424)

The management console does not populate already set passwords (ATEAM-18773)

When viewing the configuration of a successfully deployed solution, password fields may appear empty instead of displaying asterisks. If you attempt to navigate to the next configuration page, the management console displays an error message incorrectly indicating that these passwords have not been set.

Some commands prompt for confirmation of existing passwords (EDM-18424)

Some `clusterctl` commands prompt the user to enter and confirm a password that has already been set, instead of prompting for the password once and validating it.

Platform 1.3.0 known issues

See below the known issues common to all Cryptographic Security Platform 1.3.0 installations.

- Session expiration does not redirect to the login page (ATEAM-17362)
- Installations with Certificate Enrollment Gateway cannot be restored (CSF-704 & EDM-18536)
- Occasional restore failures of single-node installations (EDM-16171)
- RTC configured in local time instead of UTC (EDM-19299)
- Upgrade from previous versions not supported (EDM-19933)

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.

Installations with Certificate Enrollment Gateway cannot be restored (CSF-704 & EDM-18536)

Cryptographic Security Platform installations with a deployed Certificate Enrollment Gateway do not support Restoring the state.

Workaround:

1. Contact Entrust support for a new version of the `csf-backup-restore.sh` script
2. Open a user session in any of the Cryptographic Security Platform installation nodes.
3. Run the following commands to install the script.

```
sudo cp --force csf-backup-restore.sh /opt/entrust/scripts/rhel/
sudo chmod 550 /opt/entrust/scripts/rhel/csf-backup-restore.sh
sudo chown sysadmin:edm /opt/entrust/scripts/rhel/csf-backup-restore.sh
```

4. Follow the steps described in Restoring the state to restore the state.

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.

RTC configured in local time instead of UTC (EDM-19299)

The system RTC (Real-Time Clock) is configured in local time instead of UTC (Coordinated Universal Time).

Upgrade from previous versions not supported (EDM-19933)

Cryptographic Security Platform 1.3 only supports greenfield installations, that is, it does not support upgrading from a previous version like Cryptographic Security Platform 1.2.

CA Gateway for 1.3.0 release notes

See below the release notes in the CA Gateway version running on Cryptographic Security Platform 1.3.0.

- CA Gateway for 1.3.0 new features
- CA Gateway for 1.3.0 fixed bugs
- CA Gateway for 1.3.0 known issues

CA Gateway for 1.3.0 new features

See below the new features in the CA Gateway version running on Cryptographic Security Platform 1.3.0.

- Support for renewing Sectigo-issued certificates (ATEAM-18908)
- EJBCA support (ATEAM-18931)
- Entrust CA support for post-quantum cryptography algorithms (PKI-42161)

Support for renewing Sectigo-issued certificates (ATEAM-18908)

This release adds support for issuing certificates issued by a Sectigo CA.

> See CA enrollments endpoint for considerations on renewing Sectigo-issued certificates.

EJBCA support (ATEAM-18931)

This release adds support for Integrating an EJBCA CA.

Entrust CA support for post-quantum cryptography algorithms (PKI-42161)

This release adds support for Entrust CA post-quantum cryptography (PQC) algorithms. Specifically, when Integrating an Entrust CA, CA Gateway supports the following algorithms.

- Module-Lattice-based Digital Signature Algorithm (ML-DSA)
- Module-Lattice-based Key Encapsulation Mechanism (ML-KEM)

CA Gateway for 1.3.0 fixed bugs

See below the fixed bugs in the CA Gateway version running on Cryptographic Security Platform 1.3.0.

- Unexpected warning logs (ATEAM-18776)
- URL not hardcoded on Sectigo configuration (ATEAM-18856)
- Error when renewing a Sectigo-issued SSL certificate (ATEAM-18858)
- Sectigo plugin requires profile synchronization enabled by default (ATEAM-18863)
- Failed deployments reported as successful (ATEAM-18893)
- Digicert CA with Certificate Enrollment Gateway not supported (ATEAM-18920)
- Documentation does not describe the risks of enabling SAN attributes on request (ATEAM-19009)
- Error when enrolling certificates with a DigiCert CA (ATEAM-19060)

Unexpected warning logs (ATEAM-18776)

CA Gateway records unexpected warning logs triggered by the Spring framework. For example:

```
Check the corresponding BeanPostProcessor declaration and its dependencies/advisors.
If this bean does not have to be post-processed, declare it with ROLE_INFRASTRUCTURE.
```

URL not hardcoded on Sectigo configuration (ATEAM-18856)

When integrating a Sectigo CA, the configuration settings require entering a URL setting. However, this URL value should be hardcoded, as is always the following.

```
https://cert-manager.com
```

Error when renewing a Sectigo-issued SSL certificate (ATEAM-18858)

CA Gateway returns an error when trying to renew an SSL certificate using a Sectigo CA.

Sectigo plugin requires profile synchronization enabled by default (ATEAM-18863)

The `enable-ca-profile-sync` setting defaults to `false` for all profiles. However, the Sectigo configuration requires this setting to default to `true`.

Failed deployments reported as successful (ATEAM-18893)

When a CA Gateway deployment fails, the management console incorrectly displays the deployment as successful, even though the process has failed.

Digicert CA with Certificate Enrollment Gateway not supported (ATEAM-18920)

Certificate issuance fails in the following situation:

- The Certificate Authority is Digicert CA
- The client application is Certificate Enrollment Gateway
- The enrollment protocol is ACME

Documentation does not describe the risks of enabling SAN attributes on request (ATEAM-19009)

The CA Gateway documentation does not clearly explain the risks associated with allowing Subject Alternative Name (SAN) attributes in enrollment requests.

Bug resolution: A new section in Enabling SAN attributes in the enrollment request describes the risks.

Error when enrolling certificates with a DigiCert CA (ATEAM-19060)

CA Gateway returns a "cagw-5000" error when using a DigiCert CA.

CA Gateway for 1.3.0 known issues

See below the known issues in the CA Gateway version running on Cryptographic Security Platform 1.3.0.

- 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 for 1.3.0 release notes

See below the release notes of the Certificate Authority version running on Cryptographic Security Platform 1.3.0.

- Certificate Authority for 1.3.0 new features
- Certificate Authority for 1.3.0 fixed bugs
- Certificate Authority for 1.3.0 known issues

Certificate Authority for 1.3.0 new features

See below the new features in the Certificate Authority version running on Cryptographic Security Platform 1.3.0.

- Updated user interface (ATEAM-18496)
- More post-quantum algorithms supported (ATEAM-18983)

Updated user interface (ATEAM-18496)

This release updates the Certificate Manager user interface with features such as:

- Certificate profile customization
- Client certificate renewal
- Ed25519 elliptic curve algorithm support

More post-quantum algorithms supported (ATEAM-18983)

This release introduces support for the following post-quantum cryptographic algorithms, with software and hardware cryptography.

- ML-DSA
- SLH-DSA
- ML-KEM (with bare CSR)

Certificate Authority for 1.3.0 fixed bugs

See below the bugs fixed by the Certificate Authority version running on Cryptographic Security Platform 1.3.0.

- No error message when losing the database connection (ATEAM-17478)
- Missing CRL and OCSP endpoints on redeploy and regeneration (ATEAM-19046)

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.

Missing CRL and OCSP endpoints on redeploy and regeneration (ATEAM-19046)

The CRL and OCSP endpoints are no longer available when redeploying or recreating a certificate authority.

Certificate Authority for 1.3.0 known issues

See below the known issues in the Certificate Authority version running on Cryptographic Security Platform 1.3.0.

- Datadog errors in logs (ATEAM-17270)
- Broken links to documentation (ATEAM-18997)
- Error on logout (ATEAM-19055)

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.

Broken links to documentation (ATEAM-18997)

The Certificate Authority user interface includes broken links to the customer guide.

Error on logout (ATEAM-19055)

Clicking the **Logout** command in the console results in a "Page not found" error under the following conditions.

- The Certificate Authority solution is enabled
- The user has the PkihubRole role

Certificate Manager for 1.3.0 release notes

See below the release notes of the Certificate Manager version running on Cryptographic Security Platform 1.3.0.

- Certificate Manager for 1.3.0 new features
- Certificate Manager for 1.3.0 fixed bugs
- Certificate Manager for 1.3.0 known issues

Certificate Manager for 1.3.0 new features

See below the new features in the Certificate Manager solution distributed with Cryptographic Security Platform 1.3.0.

- Serial number added to certificate issuing notification email (ATEAM-18345)
- Support for custom service names (ATEAM-18601)
- DORA-compliant password policy (ATEAM-18829, ATEAM-18830 & ATEAM-18831)
- Truststore format selector (ATEAM-18880)

Serial number added to certificate issuing notification email (ATEAM-18345)

Emails notifying the successful issuance of a certificate now include the certificate's serial number, allowing it to be easily tracked on the user interface.

Support for custom service names (ATEAM-18601)

This release adds support for using custom names to differentiate `httpd` services.

DORA-compliant password policy (ATEAM-18829, ATEAM-18830 & ATEAM-18831)

This release hardens the password policy to meet the DORA (Digital Operational Resilience Act) official EU Regulation 2022/2554.

Policy setting	**DORA-compliant value**
Minimum password length	15 characters
Password complexity	zxcbn score 4
Account lockout threshold reset counter	24 hours
User lockout duration	24 hours
Minimum password age	24 hours
Password history	8 passwords

Truststore format selector (ATEAM-18880)

A new selector in the Certificate Manager user interface allows you to select the format of a truststore before importing it from a file. Supported formats are:

- PEM
- PKCS#12

Certificate Manager for 1.3.0 fixed bugs

See below the fixed bugs in the Certificate Manager solution distributed with Cryptographic Security Platform 1.3.0.

- Server details disclosed on response (ATEAM-18719)
- Create button only displayed on page refresh (ATEAM-18882)
- Truncated CN on CSR (ATEAM-18909)
- License issues (ATEAM-18921 & ATEAM-18940)
- Password-type values displayed (ATEAM-18981)
- Destination automatism requests for unnecessary CSR (ATEAM-19016)

Server details disclosed on response (ATEAM-18719)

HTTP responses disclose internal information as the name and version of the server.

Create button only displayed on page refresh (ATEAM-18882)

After adding a CA Gateway instance, the **Create** button for creating a certificate is only displayed following a page refresh.

Truncated CN on CSR (ATEAM-18909)

When completing the CSR creation form, the **Subject DN** field updates before you can finish typing the Common Name (CN).

License issues (ATEAM-18921 & ATEAM-18940)

The user interface may show blank pages due to license issues.

Password-type values displayed (ATEAM-18981)

The user interface displays as plain text the values of certificate fields defined with the "password" type in the certificate profile.

Destination automatism requests for unnecessary CSR (ATEAM-19016)

When issuing or renewing a certificate on a destination, the automation requests a CSR (Certificate Signing Request) even when the destination is configured to provide one.

Certificate Manager for 1.3.0 known issues

See below the known issues in the Certificate Manager solution distributed with Cryptographic Security Platform 1.3.0.

- 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)
- The Verify button does not trigger a verification without additional changes (ATEAM-16950)
- The public key ID can refer to the private key ID (ATEAM-16982)

- Archive certificates option missing with FIND licenses (ATEAM-16988)
- Incomplete CA certificate chain (ATEAM-16997)
- Verification fails for IIS destinations (ATEAM-17030)
- Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)
- STARTTLS not enabled when "Use TLS" option is checked (ATEAM-18848)

Error when taking certificates off hold (ATEAM-1445)

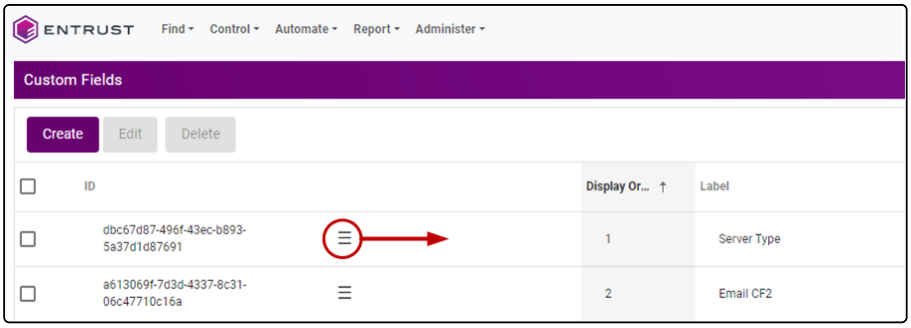
For certificates with **Revocation Reason**: **On Hold**, attempting to unhold the certificate may fail, or the **Unhold** option may be absent from the **Actions** dropdown.

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.

> 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 **Destinations** page.

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

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

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

The Verify button does not trigger a verification without additional changes (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**

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
```

Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)

The Certificate Manager console may display a blank page when manually renewing a certificate issued by a Sectigo CA

Workaround:

1. Reload the page.
2. Repeat the renewal operation.

STARTTLS not enabled when "Use TLS" option is checked (ATEAM-18848)

The **Use TLS** option of the SMTP plugin configuration does not enable STARTTLS.

> ⚠ The STARTTLS command upgrades an SMTP communication channel to a secure, encrypted connection using TLS (Transport Layer Security).

Workaround:

1. Log in to the Certificate Manager user console.

2. Navigate to **Administer > Settings > PLUGINS**.
3. Edit the **smtp-notification-plugin** configuration.
4. Activate the following options:
    - Use TLS
    - Use SSL
5. Click **Save**.
6. Edit the plugin configuration again.
7. Disable the **Use SSL** option.
8. Click **Save**.

Timestamping Authority for 1.3.0 release notes

See below the release notes of the Timestamping Authority solution distributed with Cryptographic Security Platform 1.3.0.

- Timestamping Authority for 1.3.0 new features
- Timestamping Authority for 1.3 fixed bugs
- Timestamping Authority for 1.3.0 known issues

Timestamping Authority for 1.3.0 new features

See below the new features in the Timestamping Authority solution distributed with Cryptographic Security Platform 1.3.0.

- HSM support for high availability (ATEAM-15728, ATEAM-18949 & ATEAM-19020)
- Epicom support (ATEAM-18822)



See HSM requirements for the list of supported Hardware Security Modules.

HSM support for high availability (ATEAM-15728, ATEAM-18949 & ATEAM-19020)

High-availability deployments of the Entrust Validation Authority and Timestamping Authority solutions are compatible with all supported HSMs (Hardware Security Modules).



Although not officially reported, this support was already present in former releases.

Epicom support (ATEAM-18822)

Support has been added to Timestamping Authority and Validation Authority for Epicom Hardware Security Modules (HSMs).

Timestamping Authority for 1.3 fixed bugs

See below the bug fixed by the Timestamping Authority solution distributed with Cryptographic Security Platform 1.3.

False alerts of failed deployment (ATEAM-16344)

After a successful TimeStamping Authority deployment, the Management Console may occasionally display an error message that misleads the user into believing the deployment has failed.

Timestamping Authority for 1.3.0 known issues

See below the known issues in the Timestamping Authority solution distributed with Cryptographic Security Platform 1.3.0.

- Large kmdata files not supported (ATEAM-16338)
- tsactl logs not forwarded to Splunk (EDM-13275)

Large kmdata files not supported (ATEAM-16338)

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

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 for 1.3.0 release notes

See below the release notes for the Validation Authority solution distributed with Cryptographic Security Platform 1.3.0.

- Validation Authority for 1.3.0 new features
- Validation Authority for 1.3.0 known issues

Validation Authority for 1.3.0 new features

See below the new features in the Validation Authority version running on Cryptographic Security Platform 1.3.0

- HSM support for high availability (ATEAM-15728, ATEAM-18949 & ATEAM-19020)
- Epicom support (ATEAM-18822)

HSM support for high availability (ATEAM-15728, ATEAM-18949 & ATEAM-19020)

High-availability deployments of the Entrust Validation Authority and Timestamping Authority solutions are compatible with all supported HSMs (Hardware Security Modules).

> Although not officially reported, this support was already present in former releases.

Epicom support (ATEAM-18822)

Support has been added to Timestamping Authority and Validation Authority for Epicom Hardware Security Modules (HSMs).

Validation Authority for 1.3.0 known issues

See below the known issues in the Validation Authority version running on Cryptographic Security Platform 1.3.0.

- 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
```

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 `wal_fsync_duration_seconds` 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.

Specifically, to ensure optimal fsync latency, we recommend either:

- Allocate dedicated IOPS
- Use storage QoS

Do not:

- Overcommit storage on the hypervisor.
- Use storage features that introduce unpredictable delays, such as deduplication or tiered storage.
- Use virtual machine snapshots or disk-level backups, as these mechanisms rely on copy-on-write techniques, which can lead to additional latency and result in an inconsistent state.

> ⚠ Use the built-in Cryptographic Security Platform backup feature instead of disk-level snapshots.

- Run real-time antivirus or file scans on data directory, as these processes may lock files or slow down I/O operations, causing latency spikes.
- Move a Cryptographic Security Platform node to a different host (for example, using vMotion or live migration), as this can introduce I/O latency or disrupt clock consistency. If you need to move Cryptographic Security Platform nodes, migrate one node at a time and wait for it to be fully available on the new host before migrating the next one.

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 device show
```

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 port mappings for internode communication
- Required ports for outgoing traffic
- Solution-specific port requirements

> ⚠ After installing Cryptographic Security Platform and the solutions, run a scan to ensure that the ports open to external and internode traffic are only the ones detailed in this section.

Required ports for incoming traffic

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

Source	Protocol	Target service	Target port
The IP address of the Cryptographic Security Platform administrator	TCP/SSH	SSH	22
The IP address of the SNMP manager	UDP/ SNMP	SNMP	161
The IP address of the end-user-facing services users	TCP/ HTTPS	End-user facing services	443
The IP address of the Management Console, Identity Console, and Grafana users	TCP/ HTTPS	Management Console, Identity Console, and Grafana	8443
The IP address of the Cryptographic Security Platform administrator	HTTP	Health endpoint (see Checking the node health)	15021

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

Port	Protocol	Source	Destination
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
9295	TCP	localhost	localhost
10250	TCP	localhost	localhost
15014	TCP	All nodes	All nodes
30000	TCP	localhost	localhost
51820	UDP	All nodes	All nodes

Required port mappings for internode communication

Once installed, the Cryptographic Security Platform and the solutions map the following ports to random ports.

- 80
- 443
- 9444
- 15021

Run the following commands to discover these random ports.

```
sudo kubectl get service --namespace istio-system istio-ingressgateway
```

```
sudo kubectl get service --namespace istio-system additional-ports-service
```

For example:

```
$ sudo kubectl get service --namespace istio-system istio-ingressgateway
NAME                   TYPE           CLUSTER-IP    EXTERNAL-IP      PORT(S)
AGE
istio-ingressgateway   LoadBalancer   10.43.86.11   172.21.233.131   15021:23369/
TCP,80:12858/TCP,443:42086/TCP  139m
```

```
$ sudo kubectl get service --namespace istio-system additional-ports-service
NAME                       TYPE           CLUSTER-IP     EXTERNAL-IP    PORT(S)
AGE
additional-ports-service   LoadBalancer   10.43.27.236   10.1.141.139   8444:3863/
TCP,9444:63608/TCP,1443:1412/TCP,7443:9108/TCP,8880:21277/TCP,4443:9048/
TCP,7773:24560/TCP   62d
```



Ensure that these random ports are not accessible from outside the cluster, as they are used only for internode communication.

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 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.

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

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.

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

Port requirements for Certificate Enrollment Gateway

The Certificate Enrollment Gateway solution adds the following port requirements.

- Incoming traffic to Certificate Enrollment Gateway
- Outgoing traffic from Certificate Enrollment Gateway

Incoming traffic to Certificate Enrollment Gateway

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

Source	Protocol	Target service	Target port
EST clients	TCP/HTTPS	Certificate Enrollment Gateway EST service	1443

Outgoing traffic from Certificate Enrollment Gateway

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

Source	Protocol	Target service	Target port
Certificate Enrollment Gateway (all services)	TCP/HTTPS	ocsp.ssl.com	443
Certificate Enrollment Gateway (all services)	TCP/HTTPS	crls.ssl.com	443

Port requirements for 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.

Source	Protocol	Target service	Target port
Timestamp client	TCP/HTTP	Timestamp responder	80

Outgoing traffic from Timestamping Authority

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

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

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.

Source	Protocol	Target service	Target port
OCSP client	TCP/HTTP	OCSP Responder	80

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 Validation Authority. However, remember to deploy or redeploy Validation Authority after the changes to make them effective and to automatically open the ports.

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

Reserved subnets

Reserve the following subnets for Cryptographic Security Platform use.

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

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

Software requirements

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

- Certificate-issuing authority requirements
- Compliance Manager requirements
- Database requirements
- SIEM requirements
- Web browser requirements

Certificate-issuing authority requirements

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

Compliance Manager requirements

Cryptographic Security Platform 1.3.0 integrates with Entrust Cryptographic Security Platform Compliance Manager v 10.4.5.

See Compliance Manager for the integration steps.

Database requirements

See below the database requirements for the cluster and each solution.

- Cluster database requirements
- Certificate Authority database requirements
- Certificate Enrollment Gateway database requirements
- Certificate Manager database requirements
- Validation Authority database requirements

The databases for the cluster and the solutions can be hosted on the same DBMS. However, do not merge tables from different solutions into a single database. Both the cluster and each solution require their own dedicated database.

Cluster database requirements

The user functionalities described in Managing identities require a database with the following properties.

- Database management system
- Database storage
- Database platform
- Database user permissions
- Database allowed incoming connections
- Database supported number of connections
- Database TLS certificate

The databases for the cluster and the solutions can be hosted on the same DBMS. However, do not merge tables from different solutions into a single database. Both the cluster and each solution require their own dedicated database.

Database management system

Certificate Authority supports the following Database Management Systems (DBMS).

DBMS	version
PostgreSQL	15+

Database storage

Calculate the required database storage based on the expected data.

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, ensure that you install the following extensions.

Extension	Description
lo	Large objects extension
pg_trgm	Trigram matching for string search
uuid-ossp	Universal unique ID generation

To install the PostgreSQL extensions

1. Run the following command on the server hosting the database.

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

2. Connect to the database as a user with permissions to install extensions.

```
psql -d <db_name> -U <username>
```

3. Run the following SQL commands to install the extensions.

Although usually optional, the quotes around the extension identifiers may be required in some environments.

```
CREATE EXTENSION IF NOT EXISTS "lo";
CREATE EXTENSION IF NOT EXISTS "pg_trgm";
CREATE EXTENSION IF NOT EXISTS "uuid-ossp";
```

4. Run the following SQL command to check that the extensions are installed.

```
SELECT * FROM pg_available_extensions WHERE name IN ('lo', 'pg_trgm', 'uuid-
ossp');
```

Database user permissions

The database user must have permissions on the public schema. The default permissions assigned when creating the user should be sufficient. For example, to create a PostgreSQL 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 mydb;
\c mydb ${POSTGRES_USER}
CREATE EXTENSION IF NOT EXISTS pg_trgm;
```

Where:

- `${POSTGRES_USER}` is the database user name.
- `${POSTGRES_PWD}` is the database user password.

Database allowed incoming 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 supported number of connections

The cluster database must support 20 connections.

> ⚠ To calculate the number of connections your database must support, include those required by the cluster and any installed solution. For PostgreSQL, set this final value as the `max_connections` parameter.

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.

Certificate Authority database requirements

When deployed, Certificate Authority adds the following database requirements.

- Database management system
- Database storage
- Database platform
- Database user permissions
- Database allowed incoming connections
- Database supported number of connections
- Database TLS certificate

The databases for the cluster and the solutions can be hosted on the same DBMS. However, do not merge tables from different solutions into a single database. Both the cluster and each solution require their own dedicated database.

Database management system

Certificate Authority supports the following Database Management Systems (DBMS).

DBMS	version
PostgreSQL	15+

Database storage

Calculate the required database storage based on the expected data.

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, ensure that you install the following extensions.

Extension	Description
lo	Large objects extension
pg_trgm	Trigram matching for string search
uuid-ossp	Universal unique ID generation

To install the PostgreSQL extensions

1. Run the following command on the server hosting the database.

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

2. Connect to the database as a user with permissions to install extensions.

```
psql -d <db_name> -U <username>
```

3. Run the following SQL commands to install the extensions.

> Although usually optional, the quotes around the extension identifiers may be required in some environments.

```
CREATE EXTENSION IF NOT EXISTS "lo";
CREATE EXTENSION IF NOT EXISTS "pg_trgm";
CREATE EXTENSION IF NOT EXISTS "uuid-ossp";
```

4. Run the following SQL command to check that the extensions are installed.

```
SELECT * FROM pg_available_extensions WHERE name IN ('lo', 'pg_trgm', 'uuid-
ossp');
```

Database user permissions

The database user must have permissions on the public schema. The default permissions assigned when creating the user should be sufficient. For example, to create a PostgreSQL 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 mydb;
\c mydb ${POSTGRES_USER}
CREATE EXTENSION IF NOT EXISTS pg_trgm;
```

Where:

- `${POSTGRES_USER}` is the database user name.
- `${POSTGRES_PWD}` is the database user password.

Database allowed incoming 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 supported number of connections

The Certificate Authority database must support:

- 272 connections in single-node deployments
- 544 in multinode ones

> ⚠ To calculate the number of connections your database must support, include those required by the cluster and any installed solution. For PostgreSQL, set this final value as the `max_connections` parameter.

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.

Certificate Enrollment Gateway database requirements

When deployed, Certificate Enrollment Gateway adds the following database requirements.

- Database management system
- Database storage
- Database platform
- Database user permissions
- Database allowed incoming connections
- Database supported number of connections

- Database TLS certificate

Database management system

Certificate Enrollment Gateway supports the following Database Management Systems (DBMS).

DBMS	version
PostgreSQL	15+
Microsoft SQL Server	2019+
	2022+

Database storage

Calculate the required database storage based on the expected data.

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, ensure that you install the following extensions.

Extension	Description
lo	Large objects extension
pg_trgm	Trigram matching for string search
uuid-ossp	Universal unique ID generation

To install the PostgreSQL extensions

1. Run the following command on the server hosting the database.

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

2. Connect to the database as a user with permissions to install extensions.

```
psql -d <db_name> -U <username>
```

3. Run the following SQL commands to install the extensions.

> Although usually optional, the quotes around the extension identifiers may be required in some environments.

```
CREATE EXTENSION IF NOT EXISTS "lo";
CREATE EXTENSION IF NOT EXISTS "pg_trgm";
CREATE EXTENSION IF NOT EXISTS "uuid-ossp";
```

4. Run the following SQL command to check that the extensions are installed.

```
SELECT * FROM pg_available_extensions WHERE name IN ('lo', 'pg_trgm', 'uuid-
ossp');
```

Database user permissions

The database user must have permissions on the public schema. The default permissions assigned when creating the user should be sufficient. For example, to create a PostgreSQL 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 mydb;
\c mydb ${POSTGRES_USER}
CREATE EXTENSION IF NOT EXISTS pg_trgm;
```

Where:

- `${POSTGRES_USER}` is the database user name.
- `${POSTGRES_PWD}` is the database user password.

Database allowed incoming 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 supported number of connections

The Certificate Enrollment Gateway database must support 10 connections per node.

> ⚠ To calculate the number of connections your database must support, include those required by the cluster and any installed solution. For PostgreSQL, set this final value as the `max_connections` parameter.

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.

Certificate Manager database requirements

When deployed, Certificate Manager adds the following database requirements.

- Database management system
- Database storage
- Database platform
- Database user permissions
- Database allowed incoming connections
- Database supported number of connections
- Database names
- Database TLS certificate

The databases for the cluster and the solutions can be hosted on the same DBMS. However, do not merge tables from different solutions into a single database. Both the cluster and each solution require their own dedicated database.

Database management system

Certificate Manager supports the following Database Management Systems (DBMS).

DBMS	version
PostgreSQL	15+

Database storage

Calculate the required database storage based on the expected data.

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, ensure that you install the following extensions.

Extension	Description
lo	Large objects extension
pg_trgm	Trigram matching for string search
uuid-ossp	Universal unique ID generation

To install the PostgreSQL extensions

1. Run the following command on the server hosting the database.

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

2. Connect to the database as a user with permissions to install extensions.

```
psql -d <db_name> -U <username>
```

3. Run the following SQL commands to install the extensions.

> Although usually optional, the quotes around the extension identifiers may be required in some environments.

```
CREATE EXTENSION IF NOT EXISTS "lo";
CREATE EXTENSION IF NOT EXISTS "pg_trgm";
CREATE EXTENSION IF NOT EXISTS "uuid-ossp";
```

4. Run the following SQL command to check that the extensions are installed.

```
SELECT * FROM pg_available_extensions WHERE name IN ('lo', 'pg_trgm', 'uuid-
ossp');
```

Database user permissions

The database user must have permissions on the public schema. The default permissions assigned when creating the user should be sufficient. For example, to create a PostgreSQL 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 mydb;
\c mydb ${POSTGRES_USER}
CREATE EXTENSION IF NOT EXISTS pg_trgm;
```

Where:

- `${POSTGRES_USER}` is the database user name.
- `${POSTGRES_PWD}` is the database user password.

Database allowed incoming 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 supported number of connections

The Certificate Manager database must support 120 connections per cluster.

⚠ To calculate the number of connections your database must support, include those required by the cluster and any installed solution. For PostgreSQL, set this final value as the `max_connections` parameter.

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 cause issues when mapping to a name with uppercase letters.

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.

Validation Authority database requirements

When deployed, Validation Authority adds the following database requirements.

- Database management system
- Database storage
- Database platform

- Database user permissions
- Database allowed incoming connections
- Database supported number of connections
- Database TLS certificate

Database management system

Validation Authority supports the following Database Management Systems (DBMS).

DBMS	Version
Oracle	21.3.0
PostgreSQL	15+
Microsoft SQL Server	2019 CU15
	2022 CU13

Database storage

Calculate the required database storage based on the expected data.

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, ensure that you install the following extensions.

Extension	Description
lo	Large objects extension
pg_trgm	Trigram matching for string search
uuid-ossp	Universal unique ID generation

To install the PostgreSQL extensions

1. Run the following command on the server hosting the database.

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

2. Connect to the database as a user with permissions to install extensions.

```
psql -d <db_name> -U <username>
```

3. Run the following SQL commands to install the extensions.

> Although usually optional, the quotes around the extension identifiers may be required in some environments.

```
CREATE EXTENSION IF NOT EXISTS "lo";
CREATE EXTENSION IF NOT EXISTS "pg_trgm";
CREATE EXTENSION IF NOT EXISTS "uuid-ossp";
```

4. Run the following SQL command to check that the extensions are installed.

```
SELECT * FROM pg_available_extensions WHERE name IN ('lo', 'pg_trgm', 'uuid-
ossp');
```

Database user permissions

The database user must have permissions on the public schema. The default permissions assigned when creating the user should be sufficient. For example, to create a PostgreSQL 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 mydb;
\c mydb ${POSTGRES_USER}
CREATE EXTENSION IF NOT EXISTS pg_trgm;
```

Where:

- `${POSTGRES_USER}` is the database user name.
- `${POSTGRES_PWD}` is the database user password.

Database allowed incoming 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 supported number of connections

The Validation Authority database must support 192 connections per cluster.

> ⚠ To calculate the number of connections your database must support, include those required by the cluster and any installed solution. For PostgreSQL, set this final value as the `max_connections` parameter.

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.

SIEM requirements

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

- Splunk
- Syslog

> ℹ 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

> ℹ 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.

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 an issue arises, we will address it using the latest browser version compatible with the operating system.

HSM requirements

See the following table for the Hardware Security Module (HSM) versions supported by each solution.

Hardware	Client driver	Firmware	Certificate Authority	Timestamping Authority	Validation Authority
Entrust nShield Connect XC	13.9.0 (FIPS 140-2 Level 3 mode supported)	12.60.15 & 12.60.2	✓	✓	✓
Entrust nShield 5c	13.9.0	13.2.4	✓	✓	✓
Epicom	EP990 v1.08-1	—	✗	✓	✓
Thales Luna HSM 7	10.8.0	7.7.1-20	✓	✓	✓
Thales TCT	10.8.0	7.7.1-20	✗	✓	✓

General considerations:

- 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.
- On high-availability installations with a cluster of several HSMs:
  - You cannot use HSMs from different providers simultaneously, meaning that nShield and Thales HSMs cannot coexist within the same deployment.

- Entrust Validation Authority may experience the Thales TCT limitations described in the *Thales TCT Universal Client Plugin Additional Information* technical note dated May 28, 2025.
- Solutions using the HSMs must be redeployed after any loss of connection with the HSMs, such as after an HSM reboot.

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 the cluster
- Joining nodes
- Replacing the default TLS certificate
- Configuring the proxy
- Selecting the keyboard keymap
- Selecting the operating system timezone
- Configuring time synchronization
- Manually starting the chrony service
- Configuring an nShield HSM
- Configuring SNMP Authentication for MIB information access
- Replacing the initial password for the Management Console admin
- Setting the license

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 Hub installation files
    - Cryptographic Security Platform Compliance Manager installation files
    - Cryptographic Security Platform utility files

Cryptographic Security Platform PKI Hub installation files

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

- Cryptographic Security Platform 1.3.1 - PKI Hub 1.3.1 for Amazon Web Services
- Cryptographic Security Platform 1.3.1 - PKI Hub 1.3.1 for Azure
- Cryptographic Security Platform 1.3.1 - PKI Hub 1.3.1 for VMWare vSphere, Hyper-V and Nutanix

Cryptographic Security Platform Compliance Manager installation files

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

- Cryptographic Security Platform 1.1.0 & 1.3.0 - Compliance Manager 10.4.7 ISO Install
- Cryptographic Security Platform 1.1.0 & 1.3.0 - Compliance Manager 10.4.7 OVA Install
- Cryptographic Security Platform 1.1.0 & 1.3.0 - Vault 10.4.7 ISO Install
- Cryptographic Security Platform 1.1.0 & 1.3.0 - Vault 10.4.7 OVA Install

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

- Cryptographic Security Platform 1.1.0 & 1.3.0 - Vault 10.4.7 Upgrade ISO
- Cryptographic Security Platform 1.1.0 & 1.3.0 - Vault 10.4.7 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-1.3.0.iso SHA256
SHA256 hash of c:\Users\john\Downloads\pki-hub-1.3.0.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 ISO image on Nutanix
- Installing the ISO image on Proxmox
- Installing the ISO image on VMware vSphere
- Configuring a 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 virtual machine on Hyper-V
    - Configuring the boot mode on Microsoft Hyper-V
    - Starting a virtual machine on Hyper-V
3. Configure the image installation as explained in Configuring a ISO image installation.

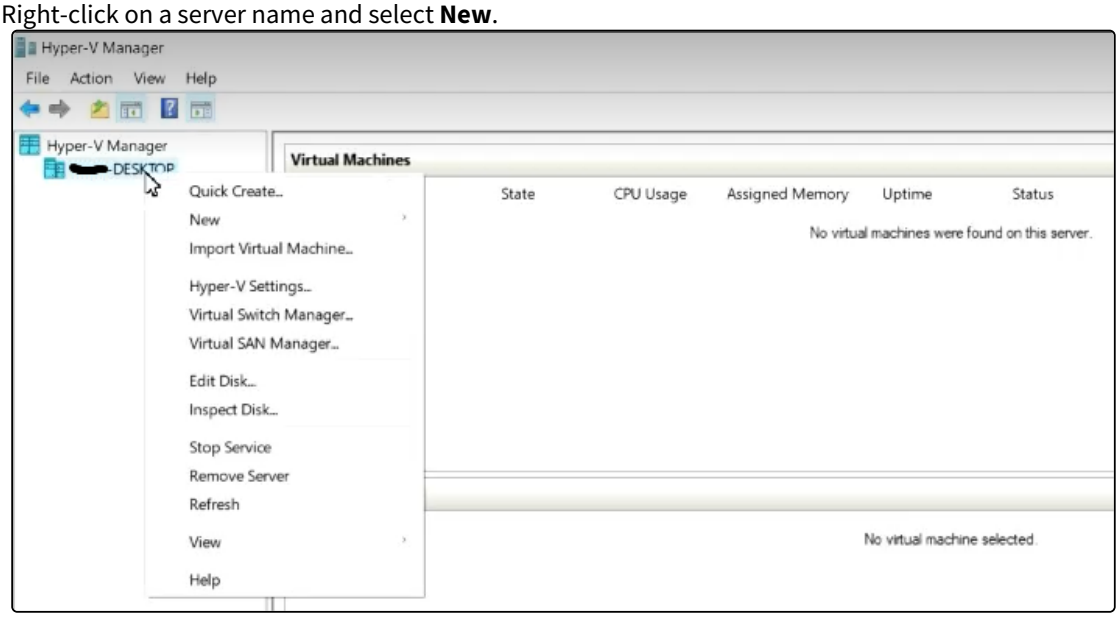
Creating a virtual machine on Hyper-V

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

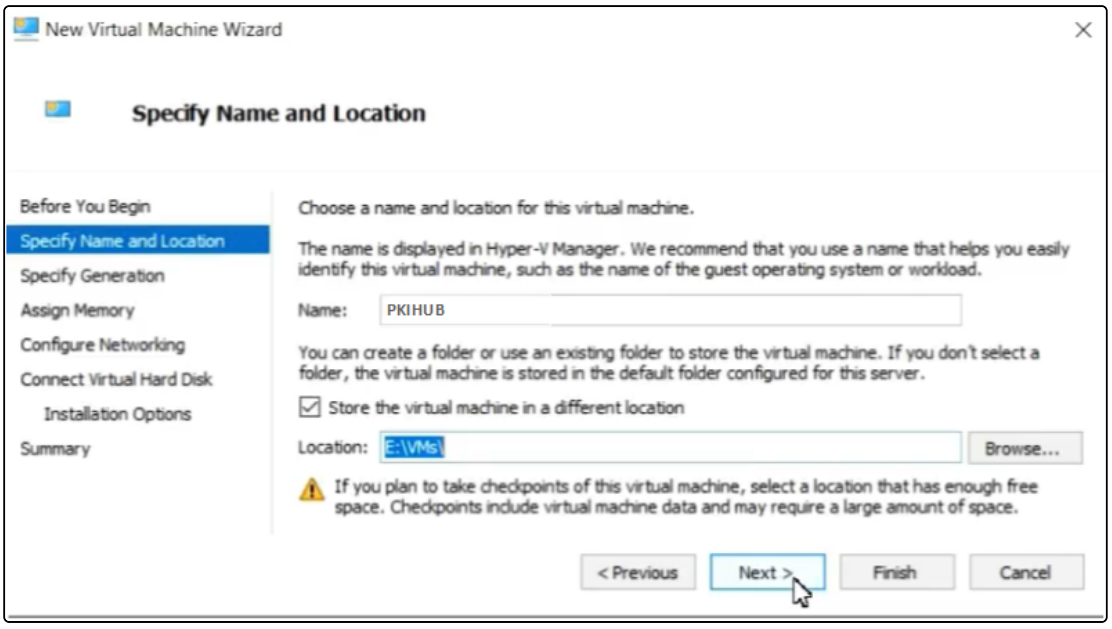
To create a Cryptographic Security Platform virtual machine on Hyper-V

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
Disk type	(discretionary value)	Fixed size

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

Installation Options

Configure the following settings.

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

Summary

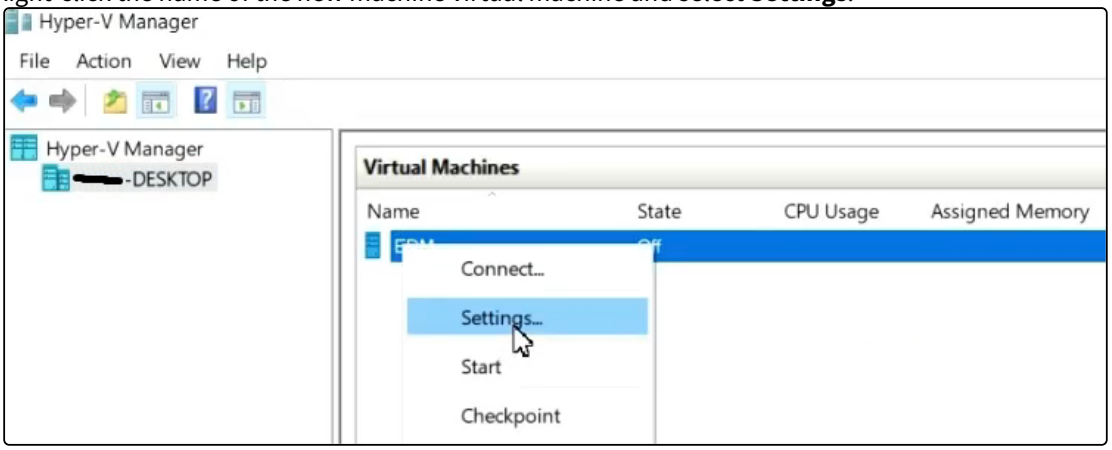
Review the selected settings and click **Finish** to complete the virtual machine creation.

Configuring a virtual machine on Hyper-V

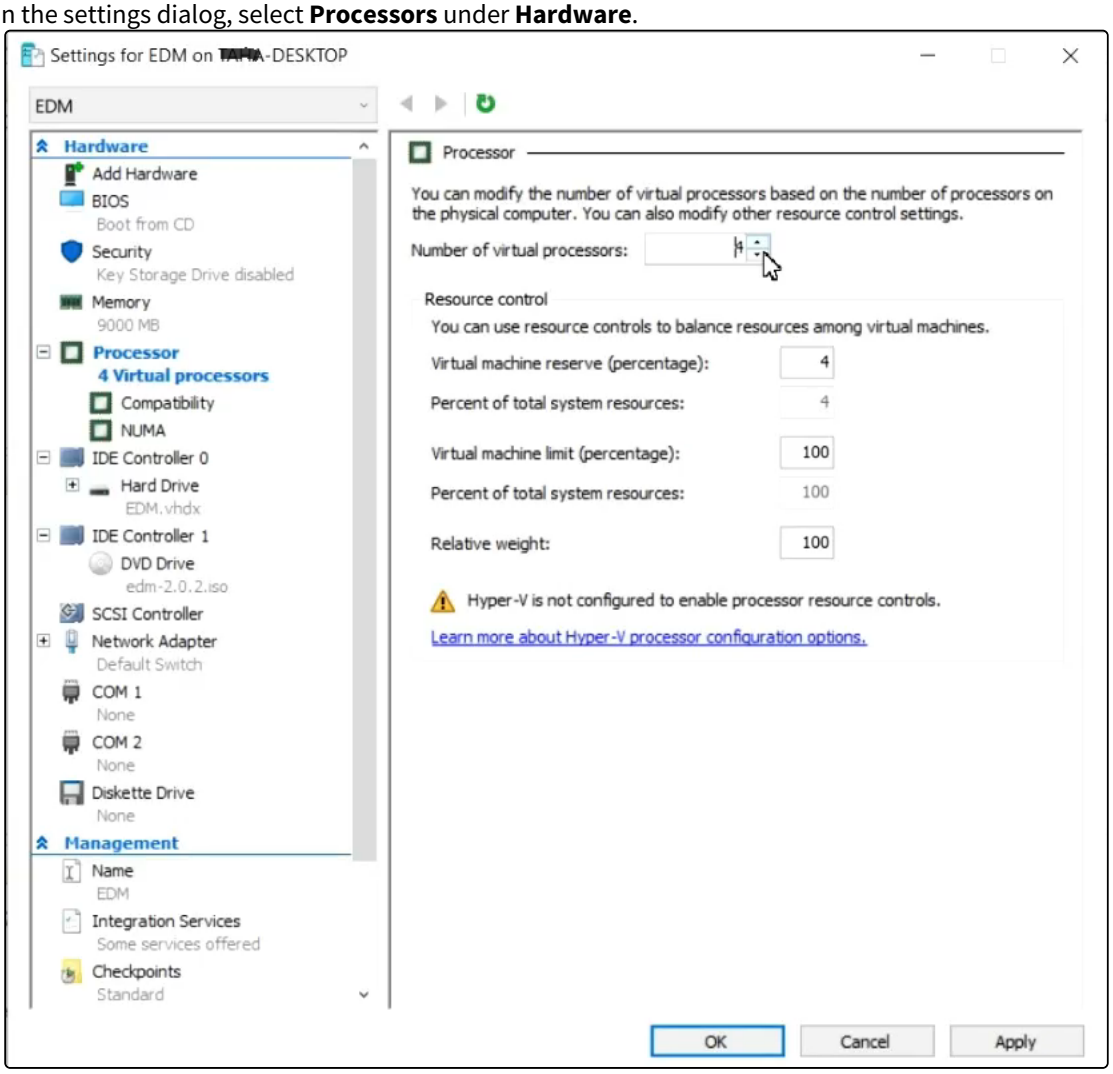
Once created, complete the new Cryptographic Security Platform virtual machine as follows.

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

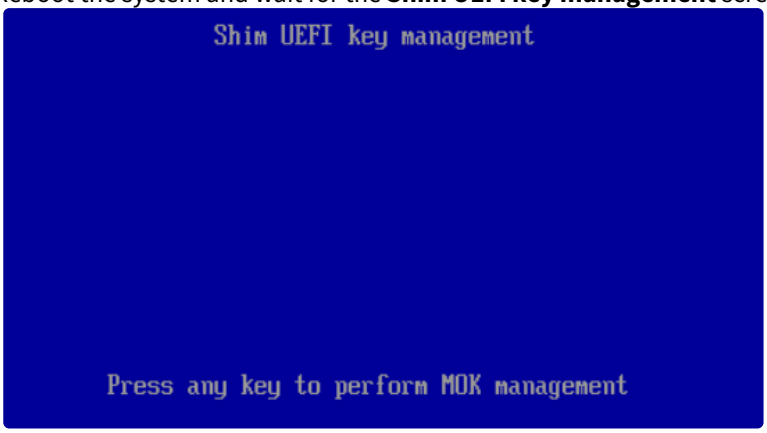
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

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

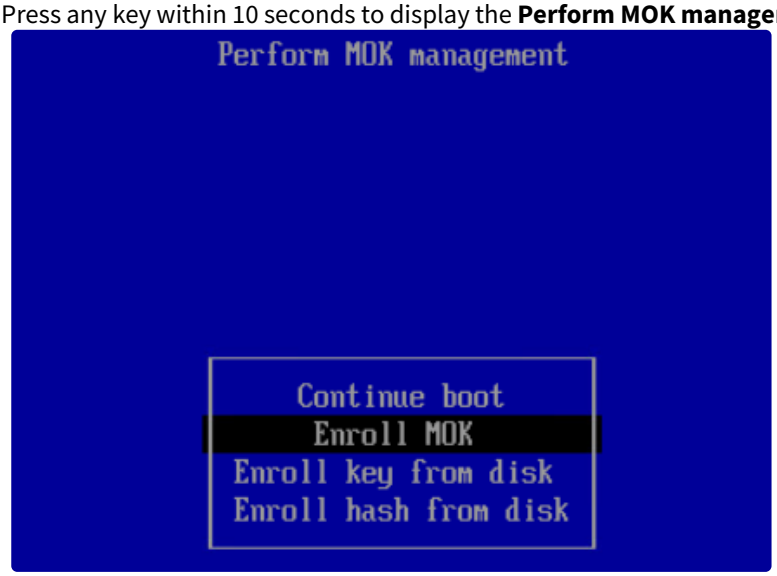
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

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

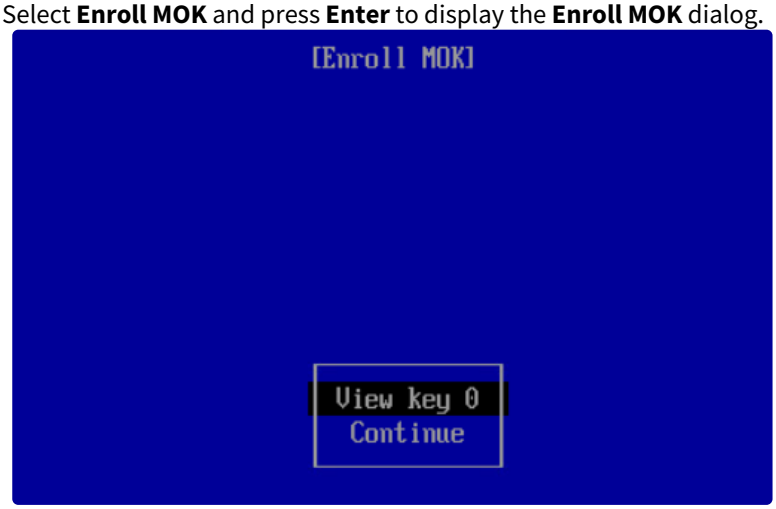
6. Reboot the system and wait for the **Shim UEFI key management** screen.



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.

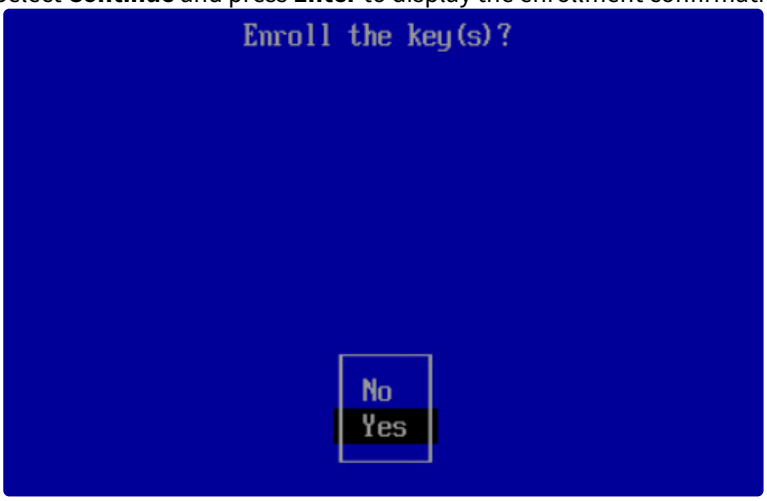


9. Select **View key 0** and press **Enter** to display the key information.

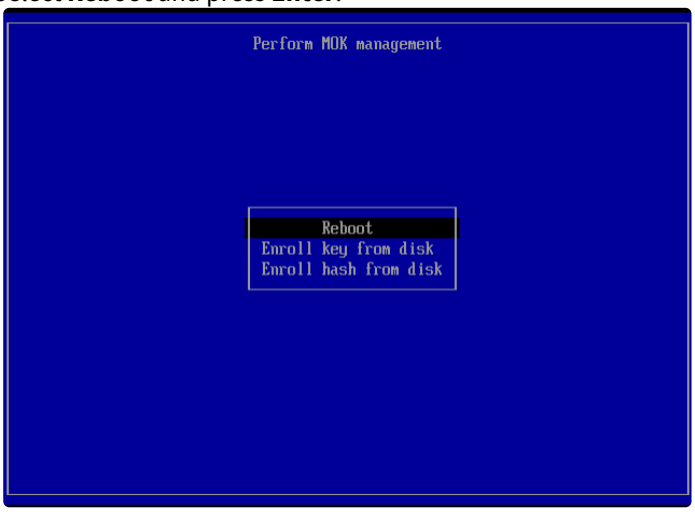


10. Check that the serial number is `0xe9d471cfb4fe136c`.
11. Check that the SHA1 fingerprint is `e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7`.
12. Press ESC to return to the **Enroll MOK** dialog.

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**.



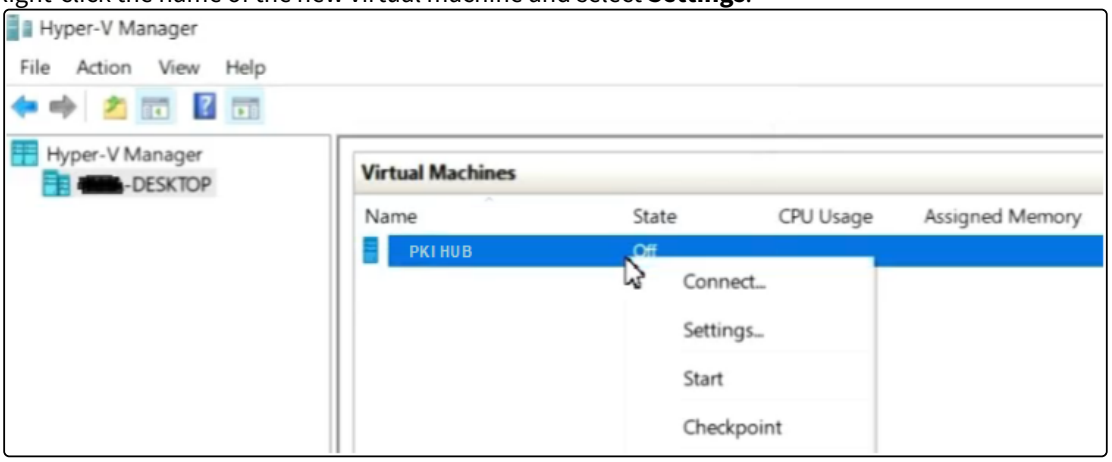
Starting a virtual machine on Hyper-V

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

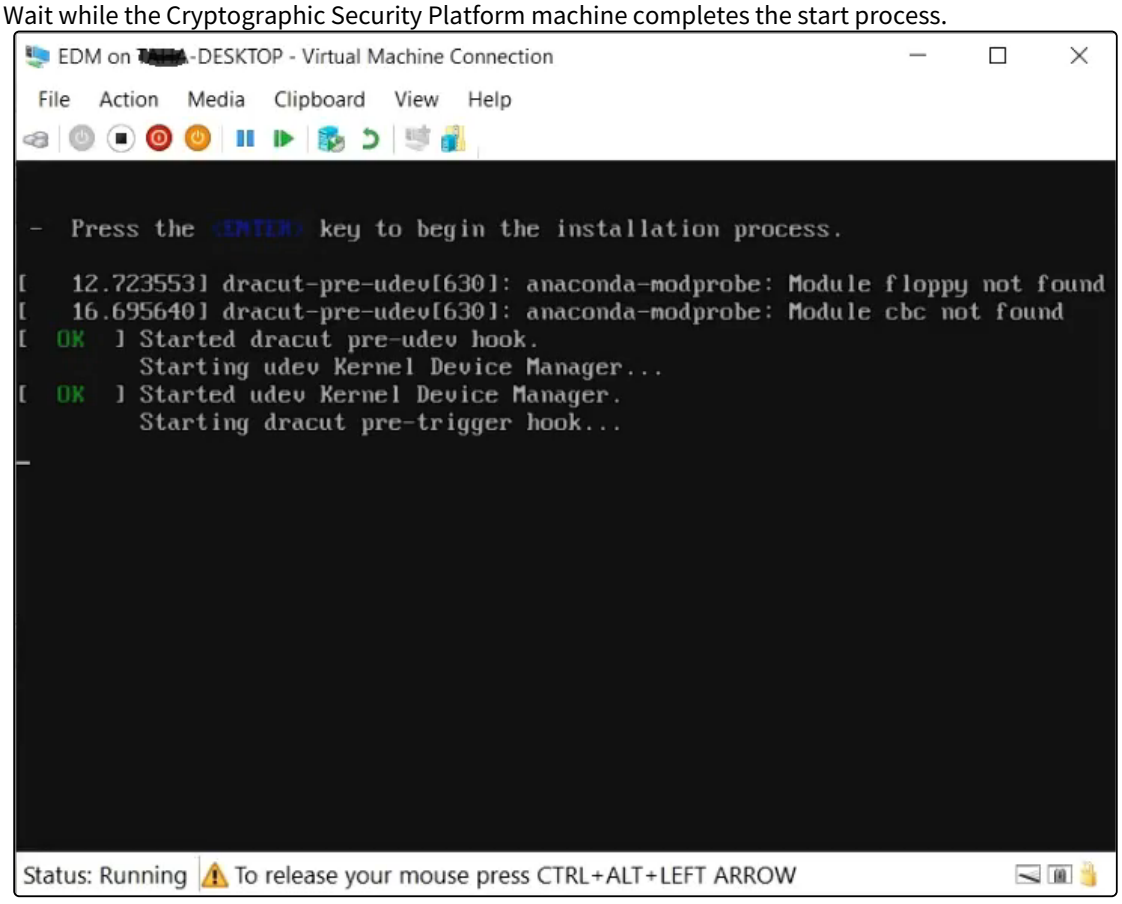
To start a Cryptographic Security Platform virtual machine on Hyper-V

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

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



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



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

Installing the ISO image on Nutanix

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

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 ISO image to Nutanix
    - Creating a virtual machine on Nutanix
    - Configuring the boot mode on Nutanix
3. Configure the image installation as explained in Configuring a ISO image installation.

Uploading the ISO image to Nutanix

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

- Uploading the ISO image with Nutanix Prism Element
- Uploading the ISO image file with Nutanix Prism Central
- Importing the ISO image to Nutanix Prism Central

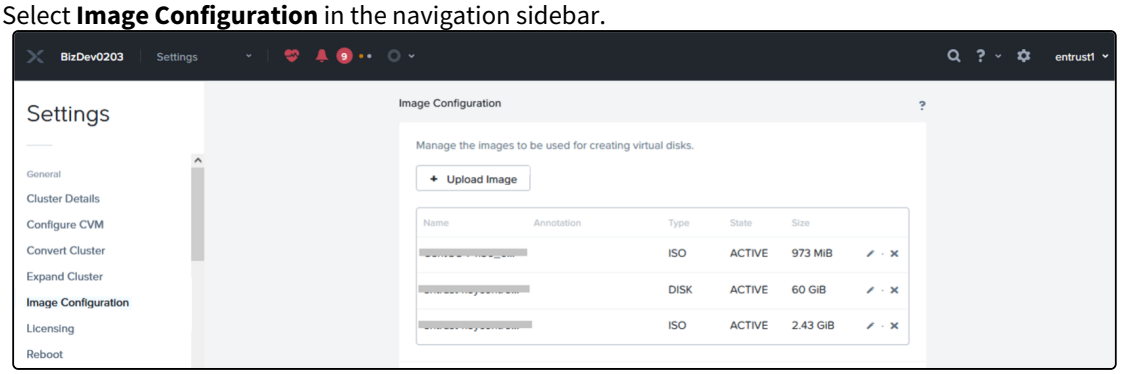
As explained in Creating a cluster with Nutanix Prism Central, uploading the image to Nutanix Prism Central allows you to create a cluster of Cryptographic Security Platform machines.

Uploading the ISO image with Nutanix Prism Element

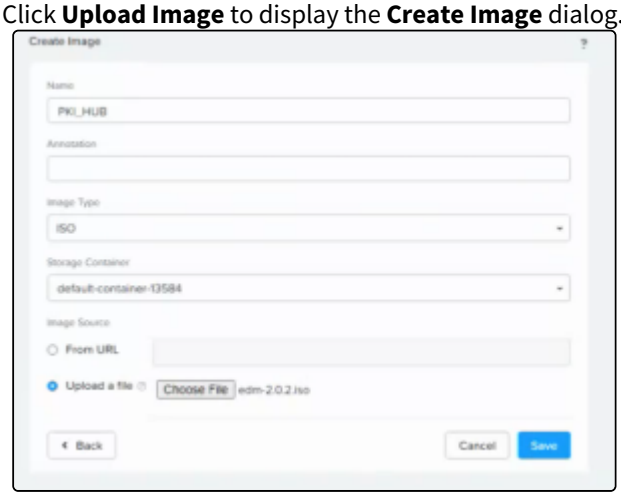
Follow the steps below to upload the Cryptographic Security Platform ISO image using the Nutanix Prism Element portal.

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.



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



5. Enter a unique image name in the **Name** field. For example: **CSP**.
6. Write an optional description in the **Annotation** field.
7. Select **ISO** in the **Image Type** field.
8. Select the required container in the **Storage Container** field.
9. Click **Upload file** and select the file with ISO extension obtained when Downloading the installation files.
10. Click **Save** and wait while the file uploads.

> Do not refresh the page while the file uploads.

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



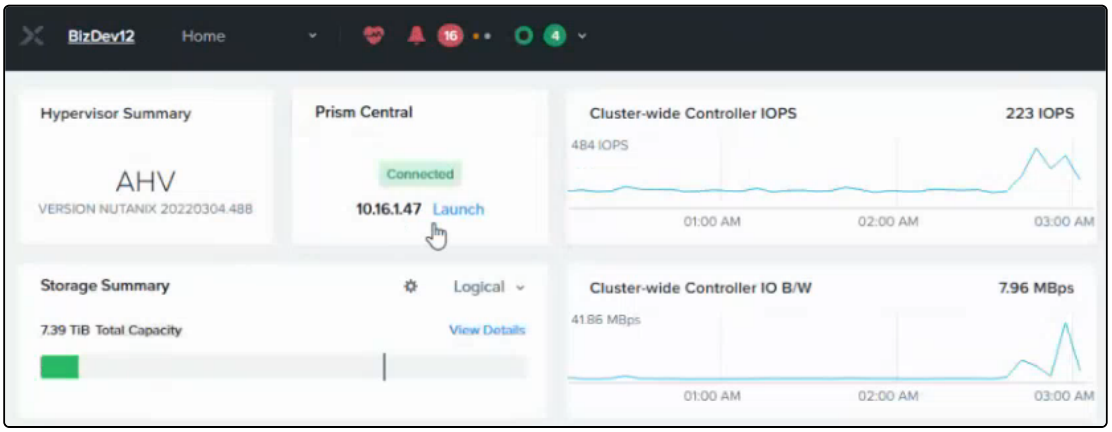
Uploading the ISO image file with Nutanix Prism Central

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

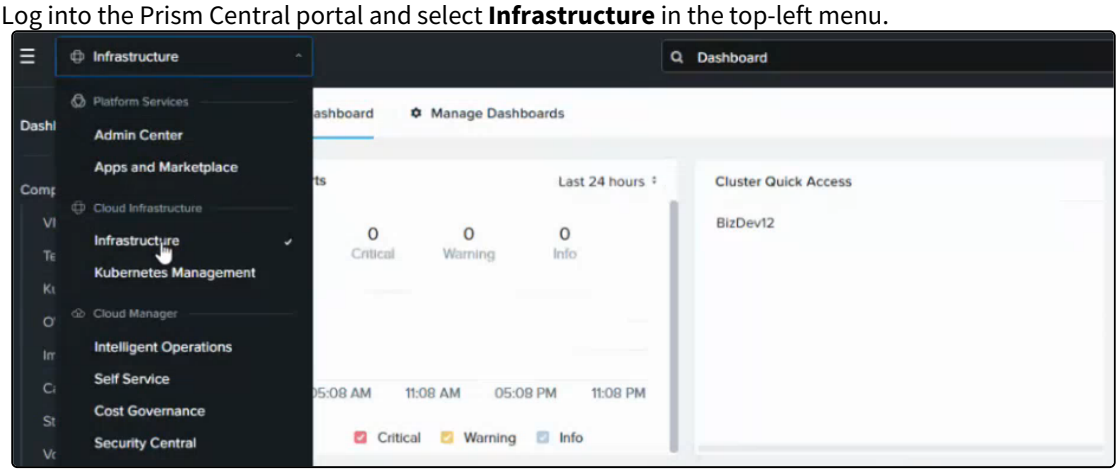
To upload the Entrust Cryptographic Security Platform image file with Nutanix Prism Central

1. Log into your Nutanix Prism element web portal.

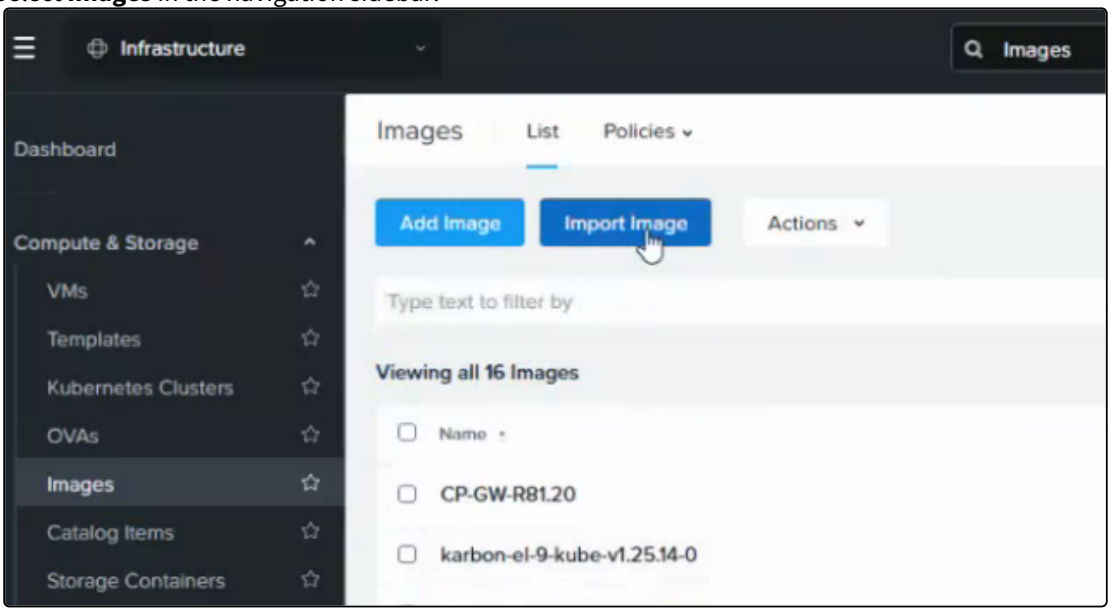
2. Click **Launch** under **Prism Central.**



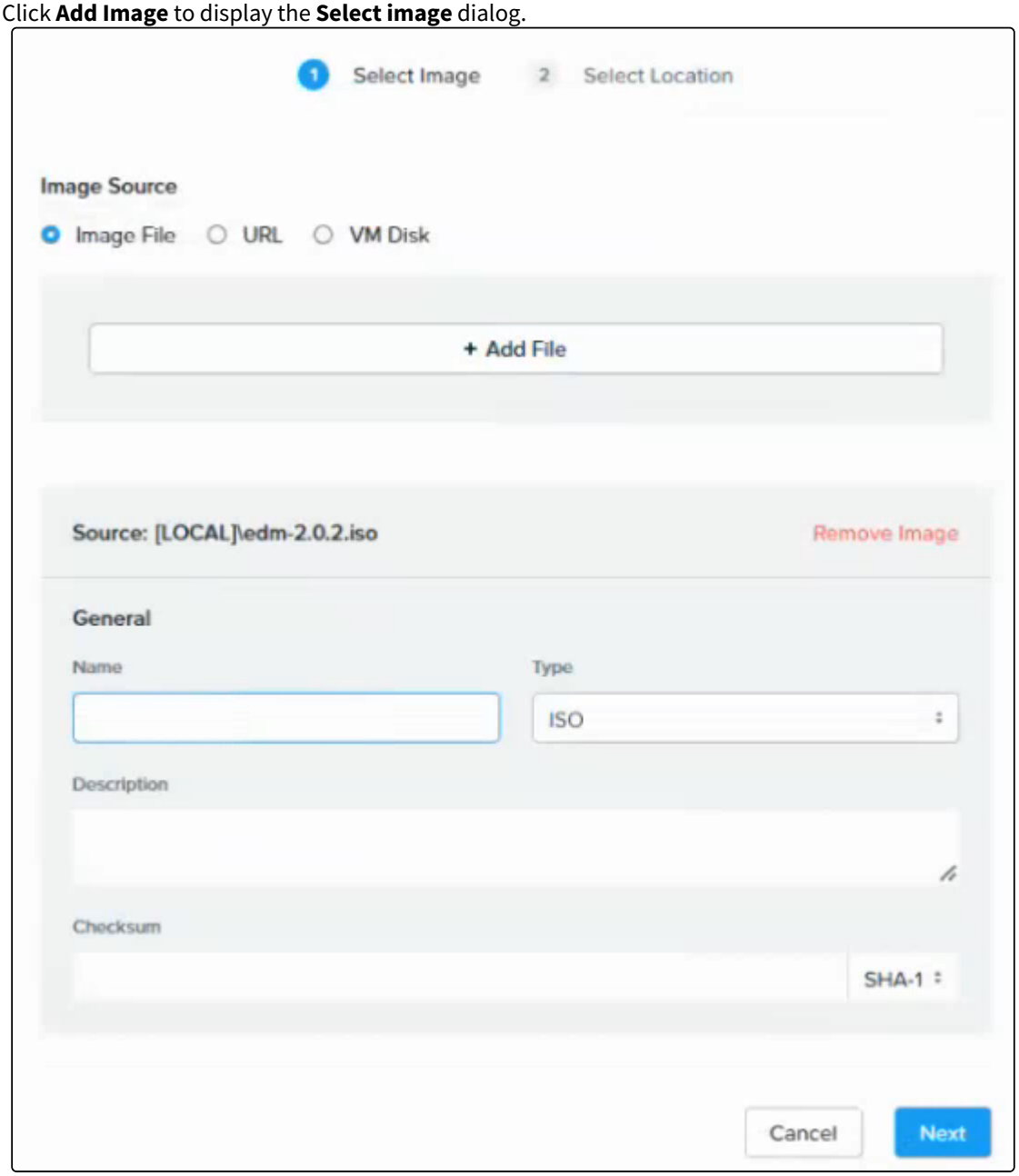
3. Log into the Prism Central portal and select **Infrastructure** in the top-left menu.



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

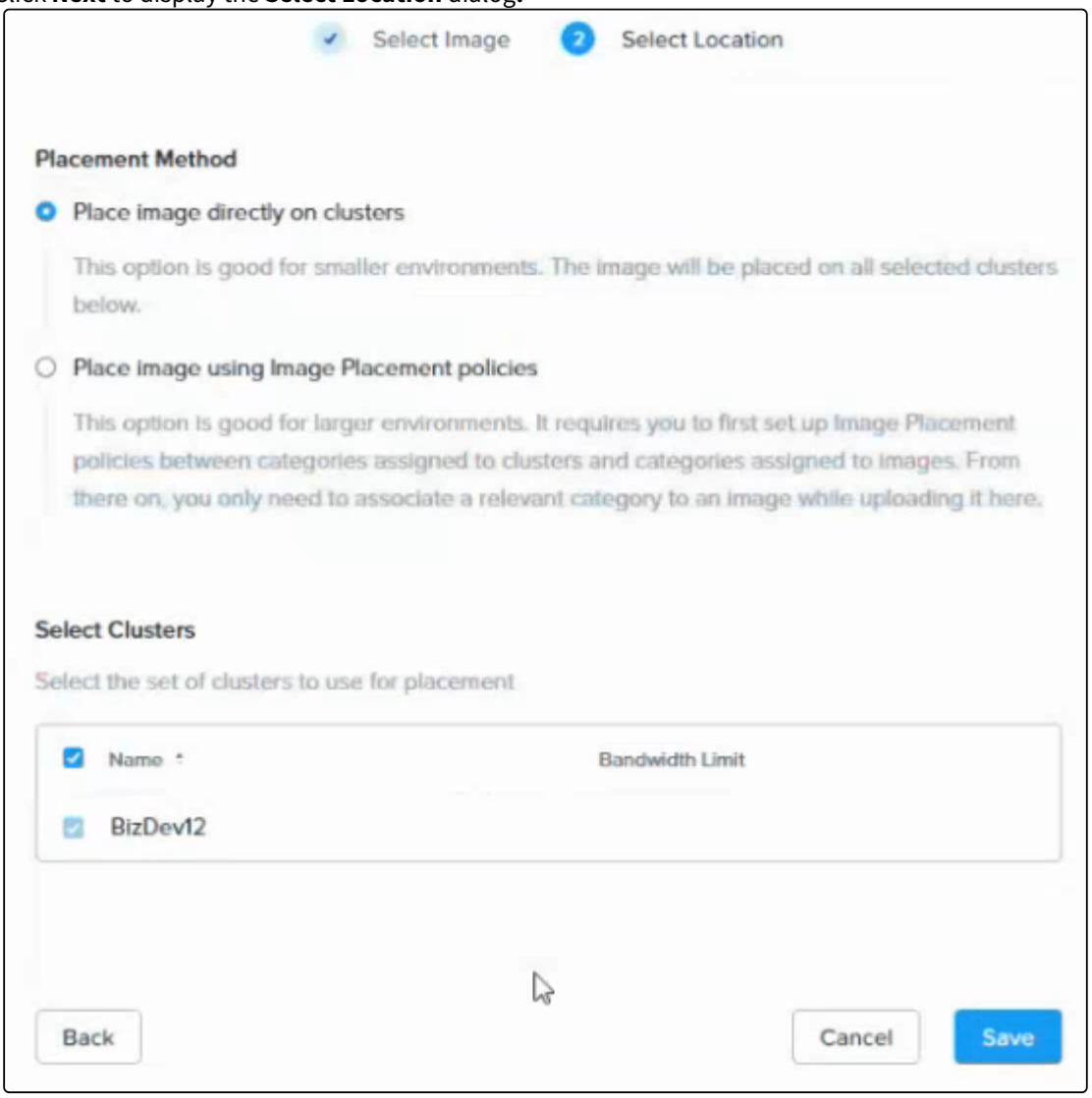


5. Click **Add Image** to display the **Select image** dialog.



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.



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

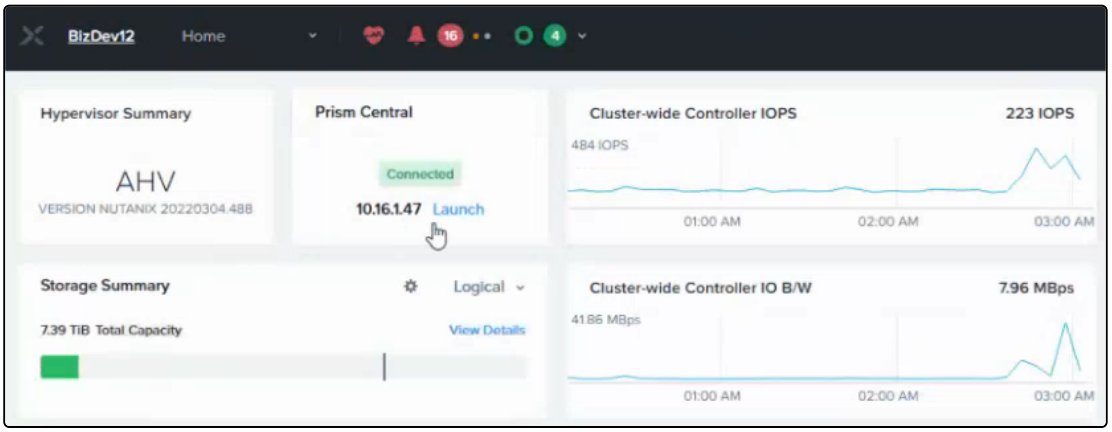
Importing the ISO image to Nutanix Prism Central

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

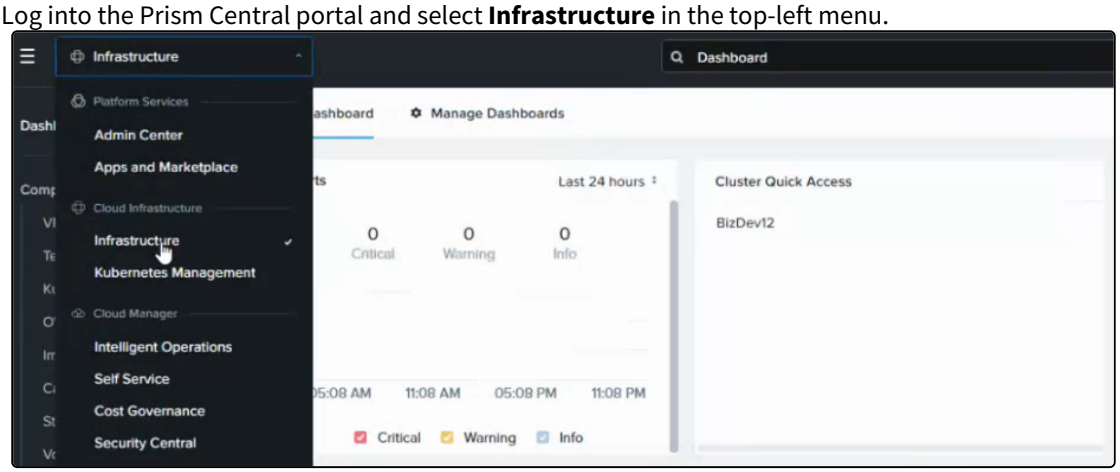
To import the Entrust Cryptographic Security Platform image from Nutanix Prism Element to Nutanix Prism Central

1. Log into your Nutanix Prism element web portal.

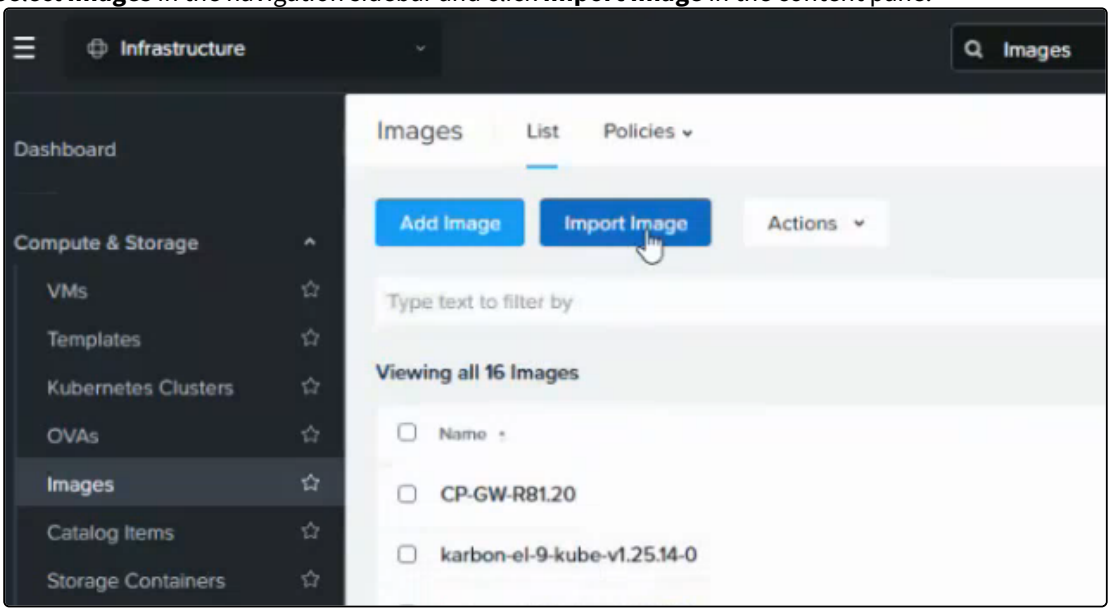
2. Click **Launch** under **Prism Central.**



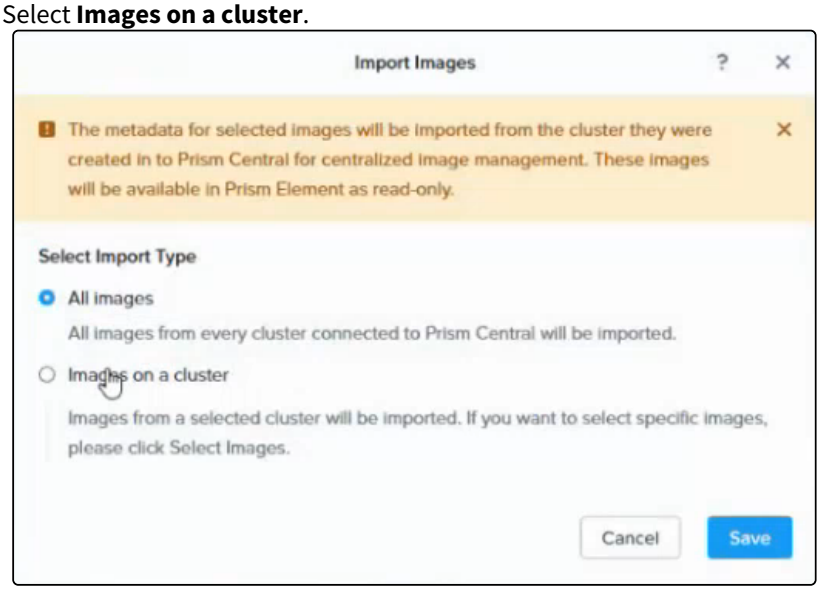
3. Log into the Prism Central portal and select **Infrastructure** in the top-left menu.



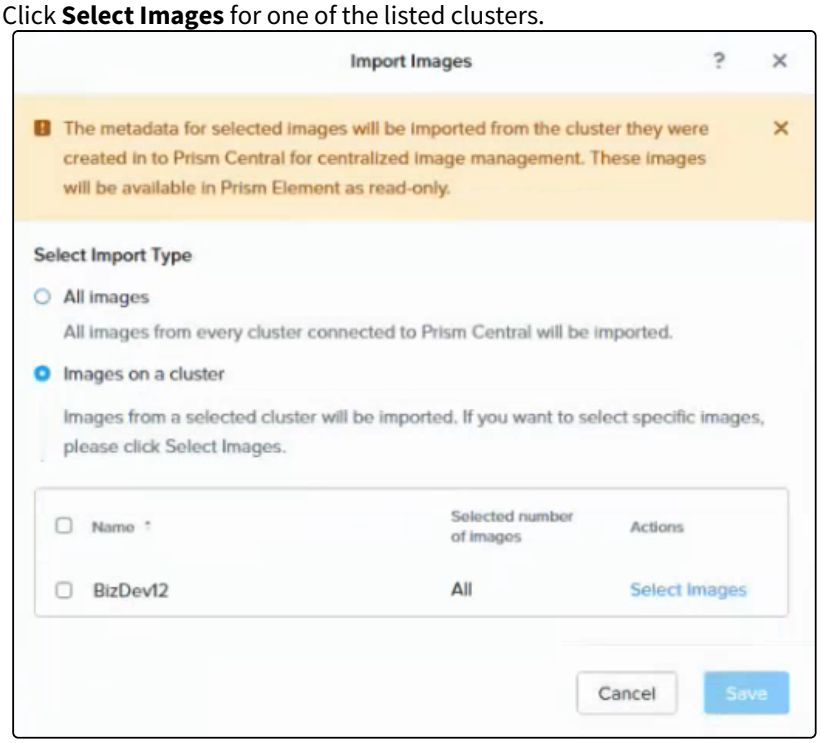
4. Select **Images** in the navigation sidebar and click **Import Image** in the content pane.



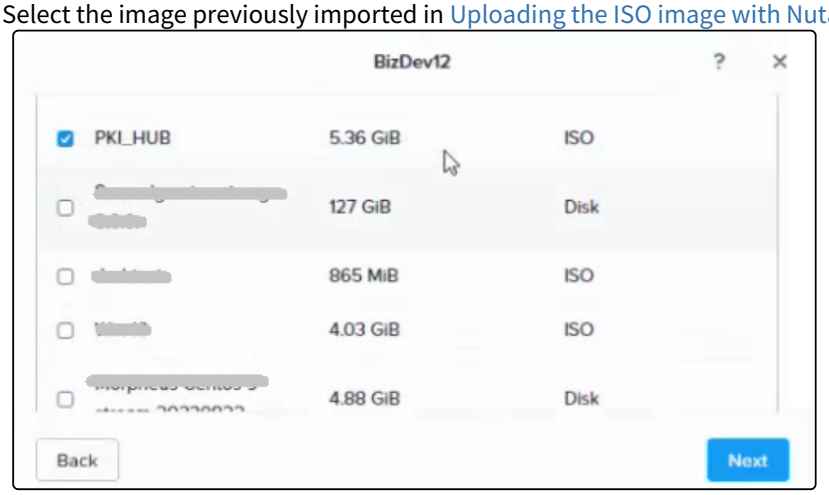
5. Select **Images on a cluster**.



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



7. Select the image previously imported in Uploading the ISO image with Nutanix Prism Element.



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

Creating a virtual machine on Nutanix

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

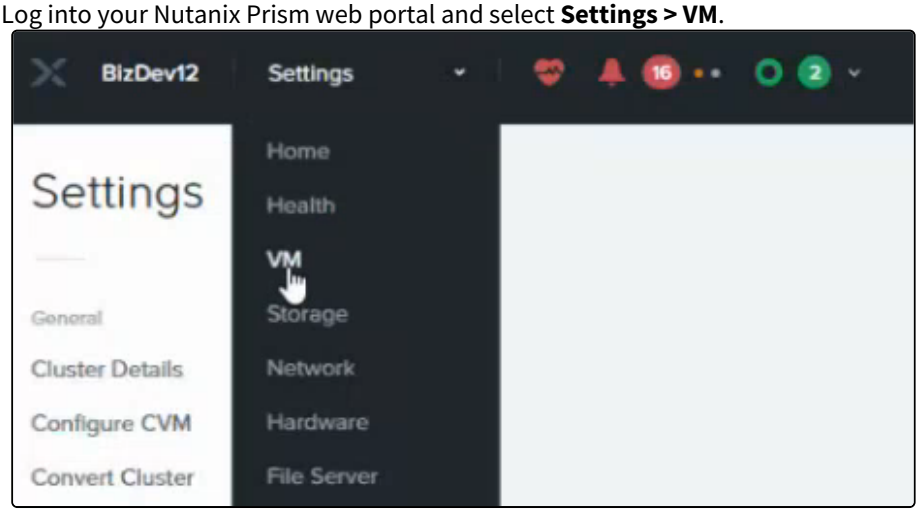
- Creating a virtual machine with Nutanix Prism Element
- Creating a cluster with Nutanix Prism Central

Creating a virtual machine with Nutanix Prism Element

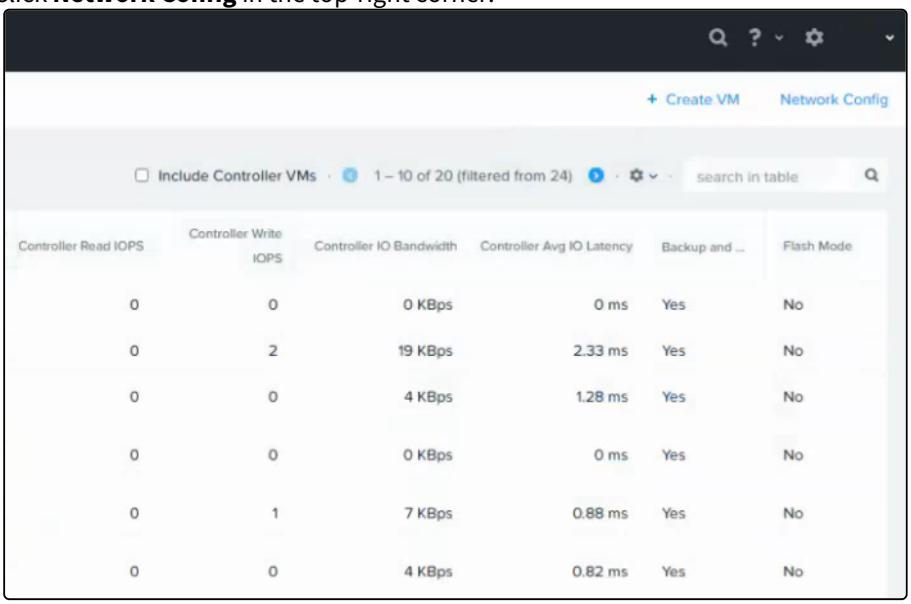
Follow the steps below to deploy the Cryptographic Security Platform image as a virtual image with the Nutanix Prism Element portal.

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

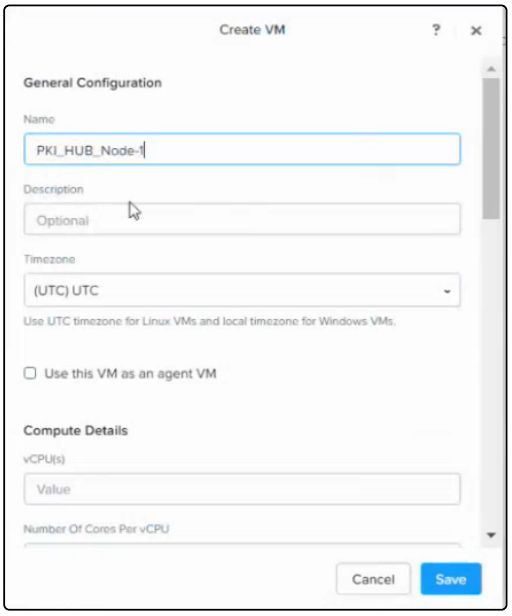
1. Log into your Nutanix Prism web portal and select **Settings > VM**.



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

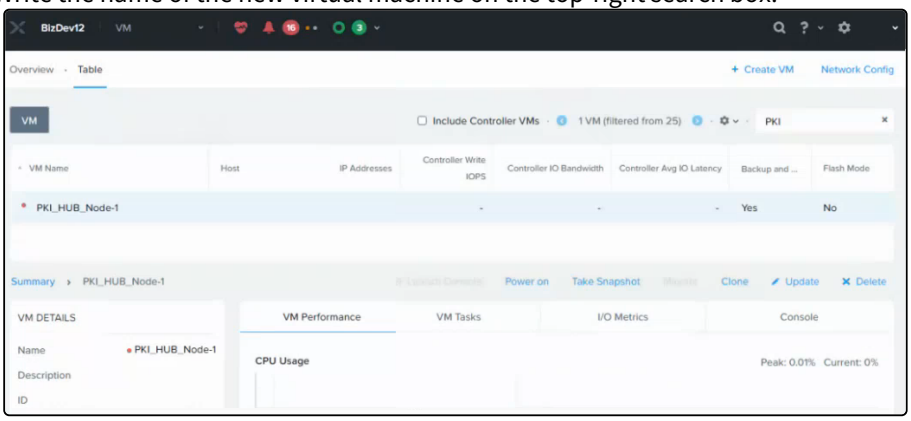


3. Create a new network or configure an existing one to meet the Network requirements.
4. Click **+ Create VM** in the top-right corner.
5. Configure the following settings in the **Create VM** dialog.
    - General Configuration
    - Compute Details
    - Boot Configuration
    - Disks
    - Network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



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

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



8. Select the new virtual machine on the content pane and click **Power On** in the bottom menu.
9. Click **Launch Console** in the bottom menu and wait while Cryptographic Security Platform starts.
10. Log in with the `sysadmin` username and the `changeme` password.
11. 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 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**.

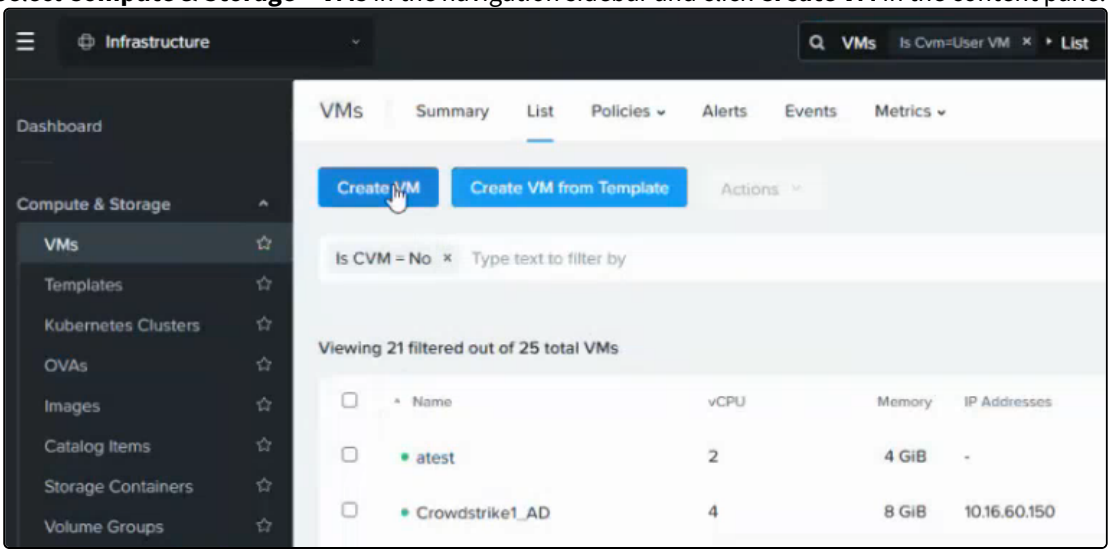
Click **+ Set Affinity** to select the host that will run the virtual machine.

Creating a cluster 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 ISO 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

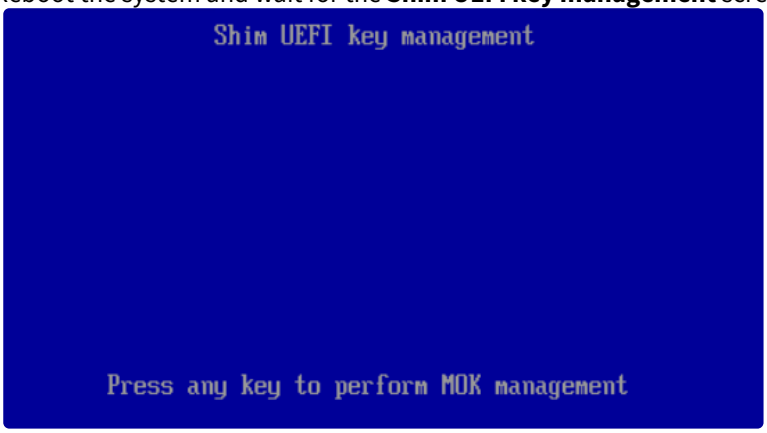
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

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

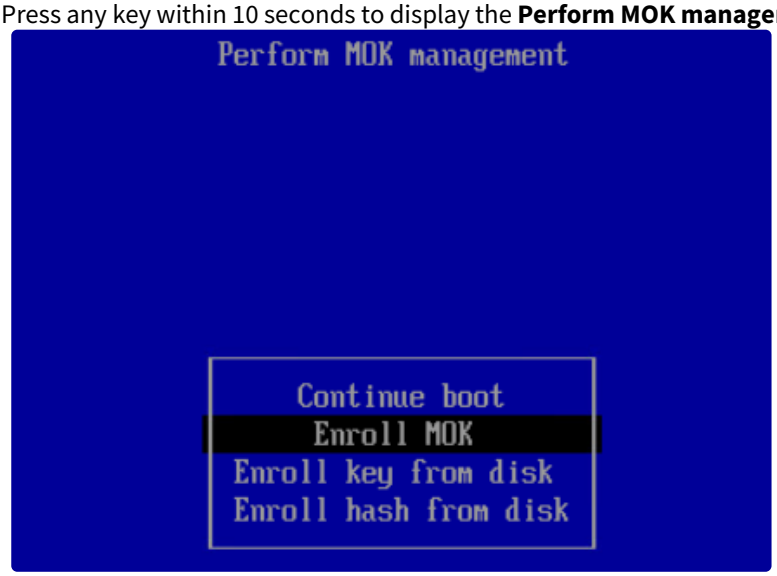
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

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

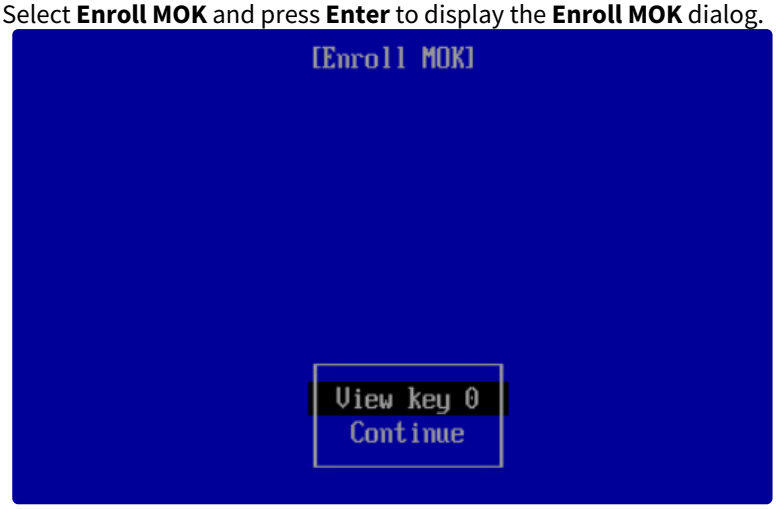
6. Reboot the system and wait for the **Shim UEFI key management** screen.



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



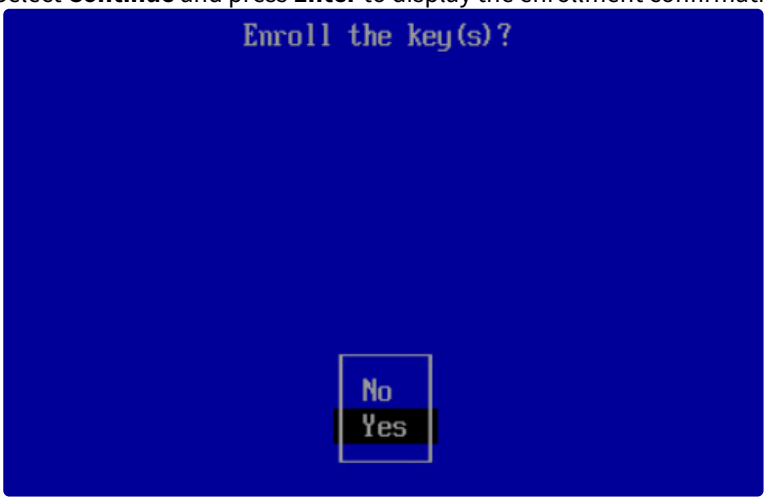
8. Select **Enroll MOK** and press **Enter** to display the **Enroll MOK** dialog.



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

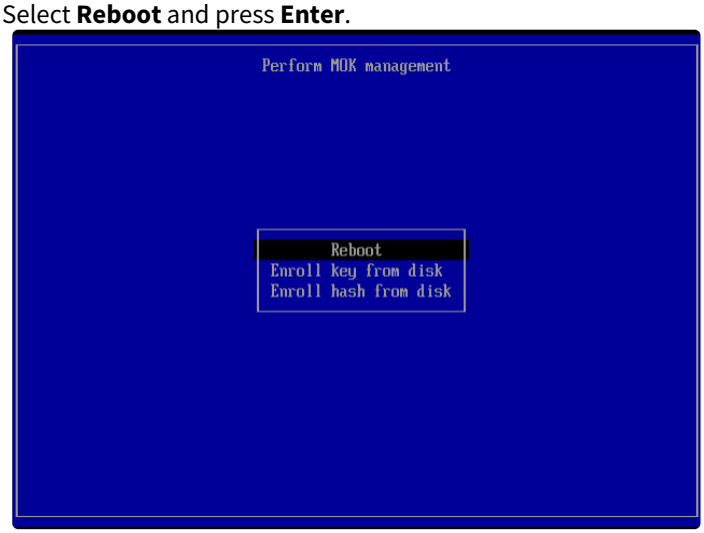


10. Check that the serial number is `0xe9d471cfb4fe136c`.
11. Check that the SHA1 fingerprint is `e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7`.
12. Press ESC to return to the **Enroll MOK** dialog.
13. Select **Continue** and press **Enter** to display the enrollment confirmation dialog.



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 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

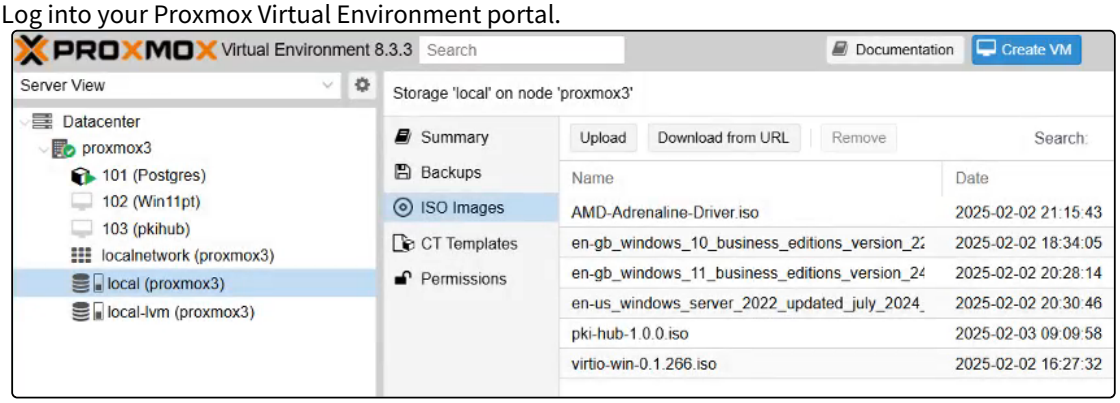
1. Download the ISO image, as explained in Downloading the installation files.
2. Follow the below steps.
    - Creating an virtual machine on Proxmox
    - Configuring the boot mode on Promox
    - Logging into Cryptographic Security Platform on Proxmox
3. Configure the image installation as explained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

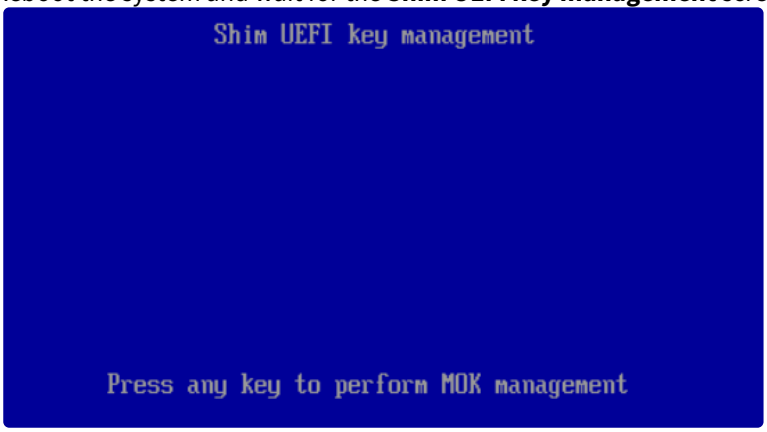
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

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

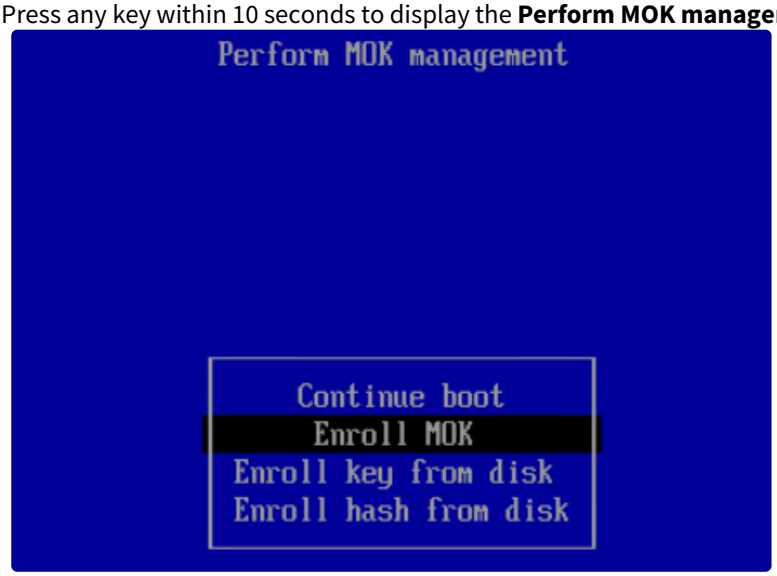
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

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

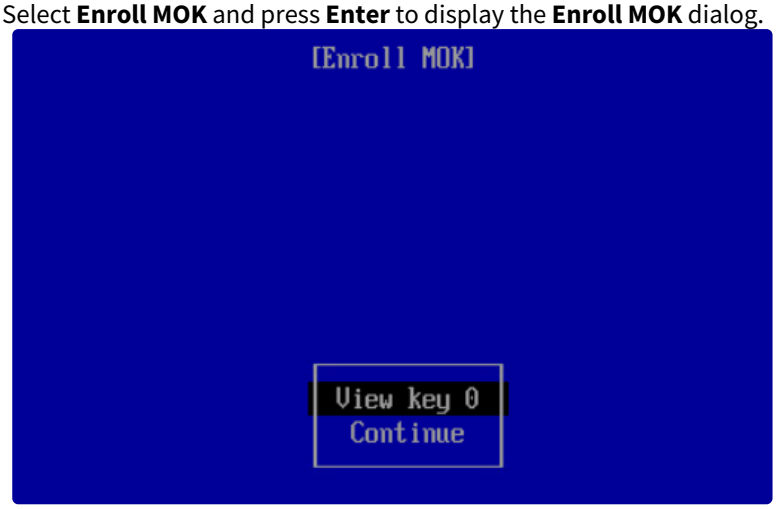
6. Reboot the system and wait for the **Shim UEFI key management** screen.



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



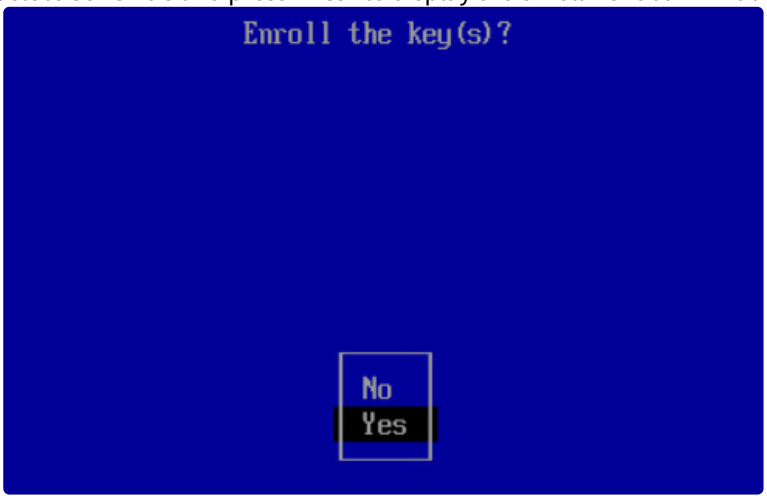
8. Select **Enroll MOK** and press **Enter** to display the **Enroll MOK** dialog.



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

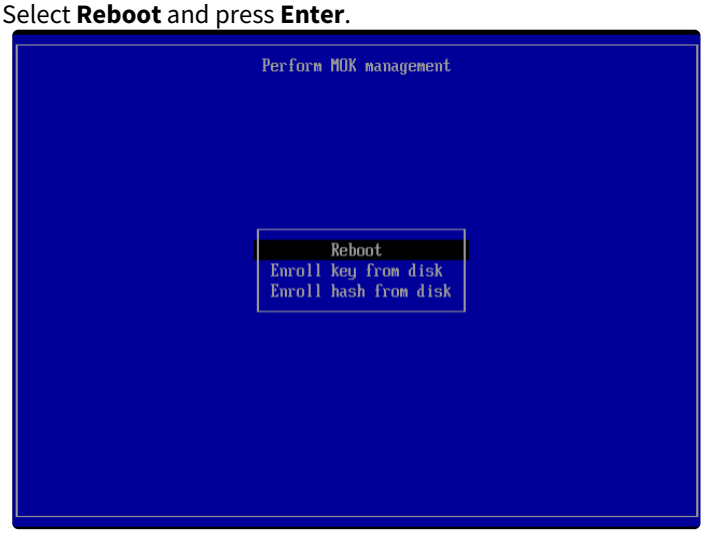


10. Check that the serial number is `0xe9d471cfb4fe136c`.
11. Check that the SHA1 fingerprint is `e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7`.
12. Press ESC to return to the **Enroll MOK** dialog.
13. Select **Continue** and press **Enter** to display the enrollment confirmation dialog.



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 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 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 ISO image installation.

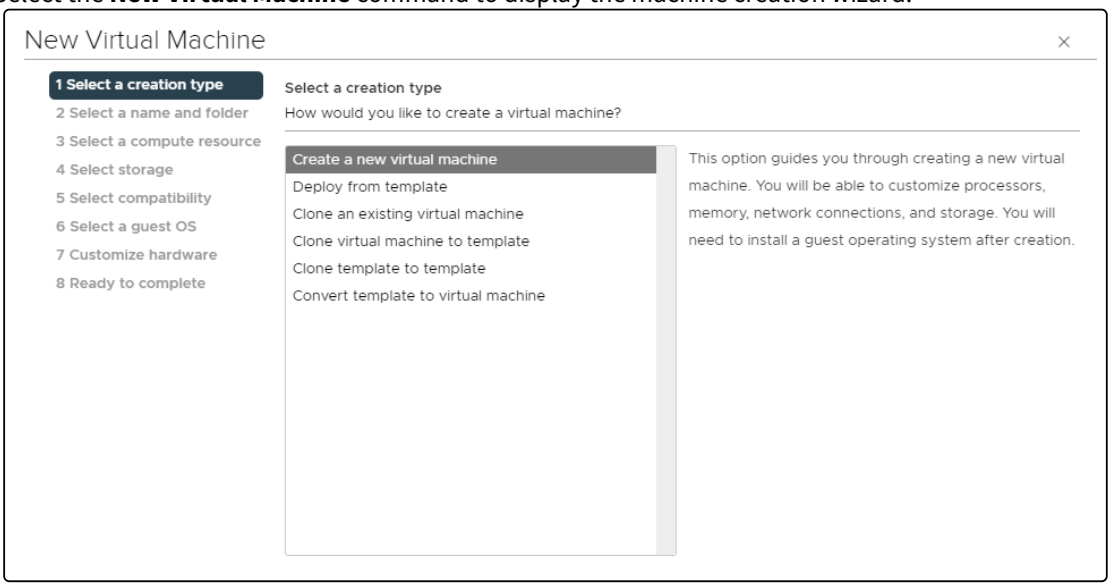
Creating a virtual machine on VMware vSphere

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 in to 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.
   - 1. Select a creation type
   - 2. Select a name and folder
   - 3. Select a compute resource
   - 4. Select storage
   - 5. Select compatibility
   - 6. Select a guest OS
   - 7. Customize hardware
   - 8. Ready to complete

1. Select a creation type

Configure the following settings.

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

2. 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.

3. Select a compute resource

Configure the following settings.

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

4. 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.

5. Select compatibility

Configure the following settings.

Field	Value
Compatible with	Select **ESXi 6.7 and later**.

6. Select a guest OS

Configure the following settings.

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

7. Customize hardware

Configure the following steps.

- Virtual Hardware
- VM Options

Virtual Hardware

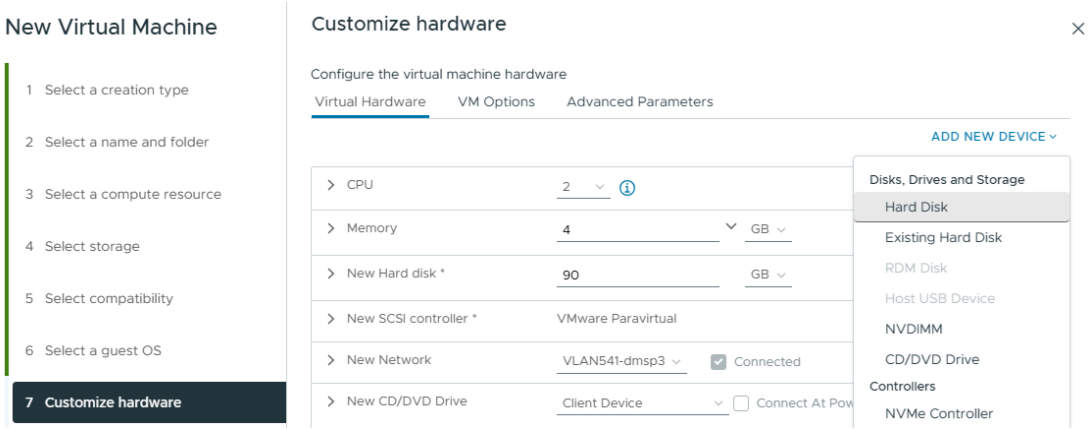
In the **Virtual Hardware** tab of the **Customize hardware** page, configure the main and the additional disks.

To configure the disks

1. In **CPU**, select the number of cores recommended in Machine requirements.
2. In **Memory**, select the RAM size recommended in Machine requirements.
3. In **New Hard disk:**

- Select at least 1 TiB for the main disk, as explained in Machine requirements.
- Set **Virtual Device Node** to **New SCSI controller**.

4. In **New SCSI controller**, set **Change Type** to **VMware Paravirtual**.
5. In **New CD/DVD Drive**:
   - Select the location of the ISO file.
   - Check the **Connect At Power On** box.
6. Click **ADD NEW DEVICE** and select **Hard disk** to add the additional disk.



7. In **New Hard disk 2:**
   - Assign at least 15 GiB for the additional disk, as recommended in Machine requirements.
   - Set **Disk Provisioning** to **Thick Provision Eager Zeroed**.
   - Set **Virtual Device Node** to **New SCSI controller**.

VM Options

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

- Boot Options
- VMWare Tools

Boot Options

Configure the following sections under this section.

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

See the next section Configuring the boot mode on VMware vSphere for how to configure the selected boot mode.

VMWare Tools

Configure the following sections under this section.

Field	Value	Description
Synchronize Time with Host > Synchronize at startup and resume (recommended)	Enabled	Synchronize guest time to the host at VM startup, power-on, resume from suspend, snapshot revert, or snapshot restore.
Synchronize Time with Host > Synchronize time periodically	Disabled	See the Configuring Time Synchronization Between Guest and Host Operating Systems section of the VMWare online documentation.

8. Ready to complete

Review the configured settings and click **Finish**.

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.

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

To enroll the ElRepo key

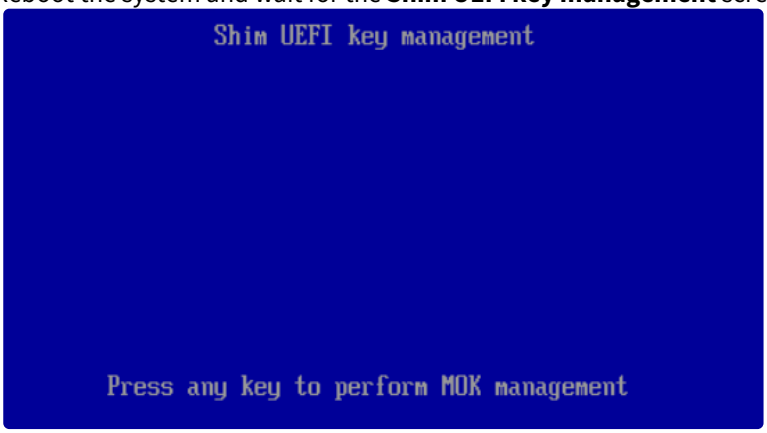
1. Run the following command to import the ELRepo key distributed with Cryptographic Security Platform.

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

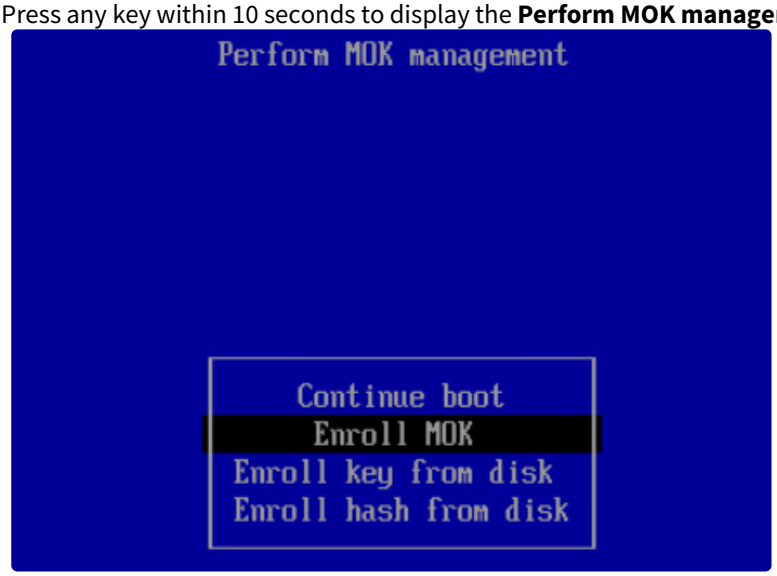
2. Type the password of the `sysadmin` user.
3. Type a password for the key.
4. Confirm the key password.
5. Log in to the local machine.

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

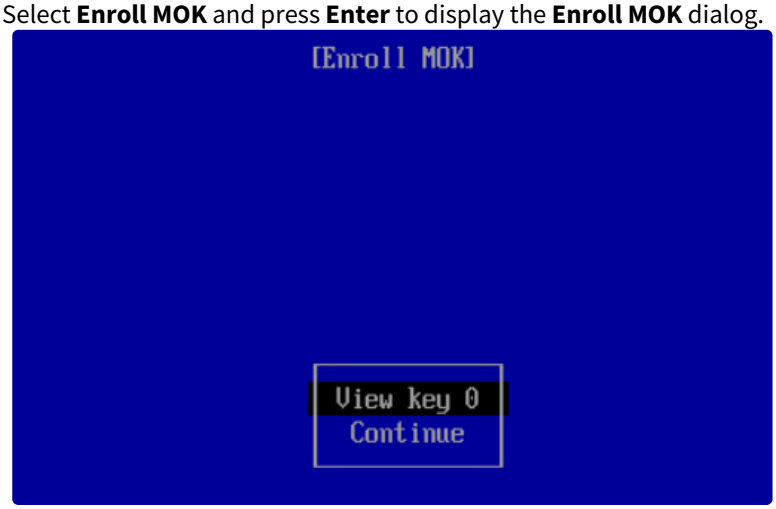
6. Reboot the system and wait for the **Shim UEFI key management** screen.



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



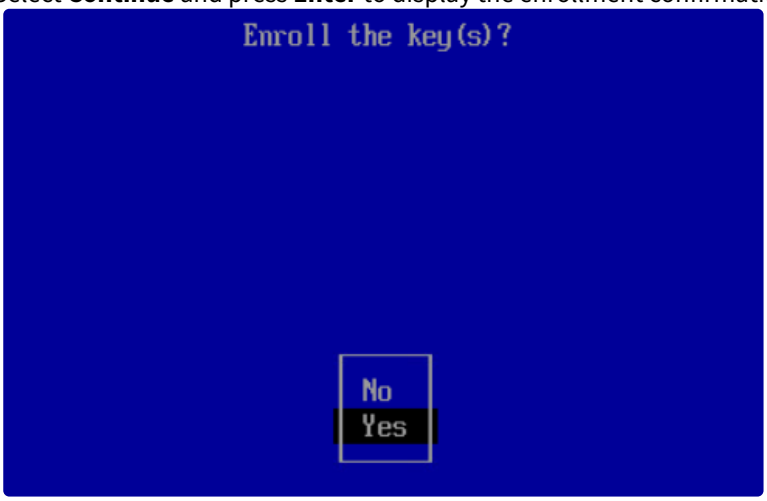
8. Select **Enroll MOK** and press **Enter** to display the **Enroll MOK** dialog.



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

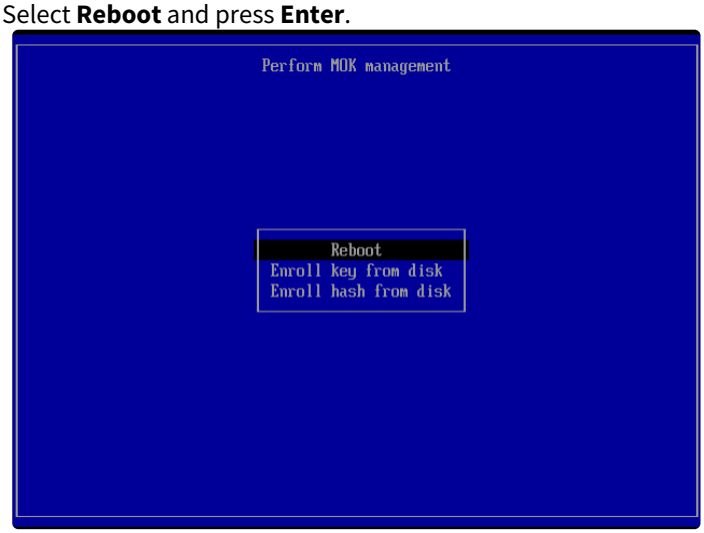


10. Check that the serial number is `0xe9d471cfb4fe136c`.
11. Check that the SHA1 fingerprint is `e1:21:a2:f6:07:2e:f2:94:de:20:0e:6b:5d:1b:49:c0:65:dc:e3:e7`.
12. Press ESC to return to the **Enroll MOK** dialog.
13. Select **Continue** and press **Enter** to display the enrollment confirmation dialog.



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 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 an ISO installation
- Checking the connection of an 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.

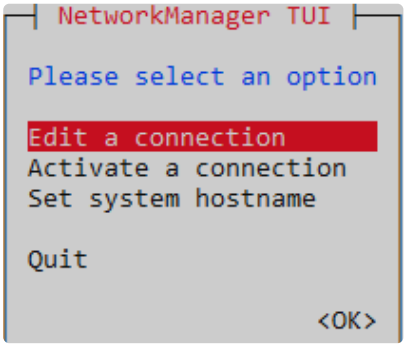
After running the clusterctl install or clusterctl node add commands you cannot change the IP address or hostname of a node.

To configure the connection of a Cryptographic Security Platform ISO installation

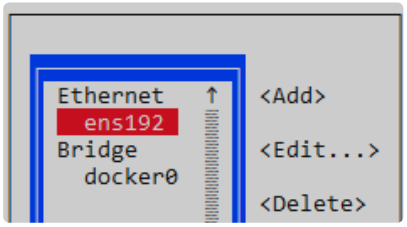
1. Log in to the machine locally as the `sysadmin` user.
2. Run the `nmtui` tool with `sudo` permissions.

```
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 **<OK>** and press **Enter**.
15. Select **<Back>** and press **Enter**.
16. Select **Quit** and press **Enter**.

Configuring the hostname of an ISO installation

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

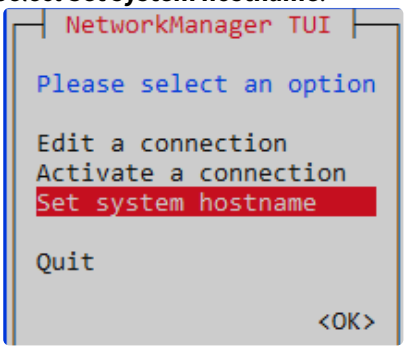
> After running the clusterctl install or clusterctl node add commands you cannot change the IP address or hostname of a node.

To configure the hostname

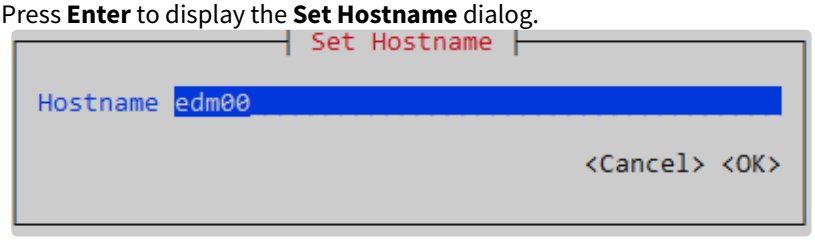
1. Log in to the Cryptographic Security Platform machine locally, as the `sysadmin` user.
2. Run the `nmtui` tool with `sudo` permissions.

```
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. Exit the session.

```
exit
```

11. Log in again.
12. Restart the `snmp` service to make the changes effective.

```
sudo systemctl restart snmpd
```

Checking the connection of an ISO installation

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

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

Check the state is `connected` for each connection.

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

```
ping <hostname>
```

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

Installing the RAW image on AWS

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

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

To install and configure the Cryptographic Security Platform image in AWS

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

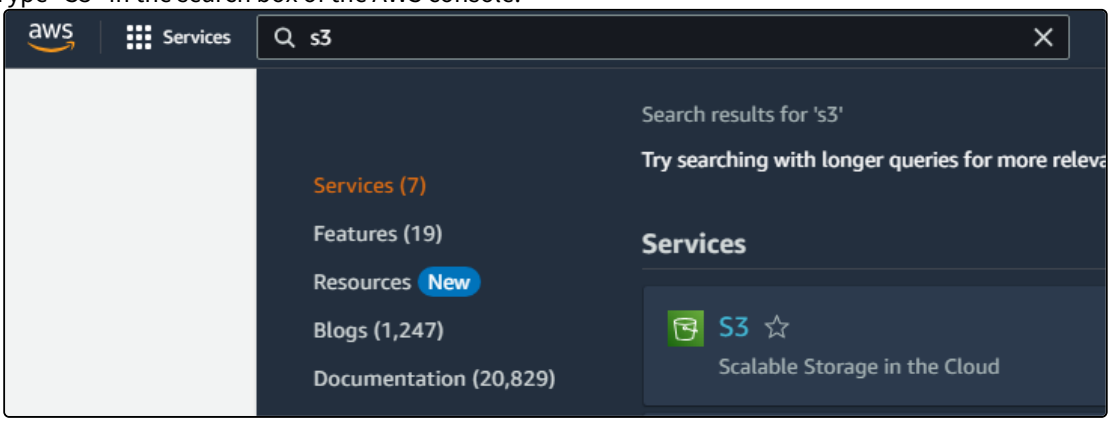
- Creating an AMI from the snapshot
- Creating the EC2 instance
- Opening a session into AWS
- Configuring the hostname on AWS

Creating an S3 bucket

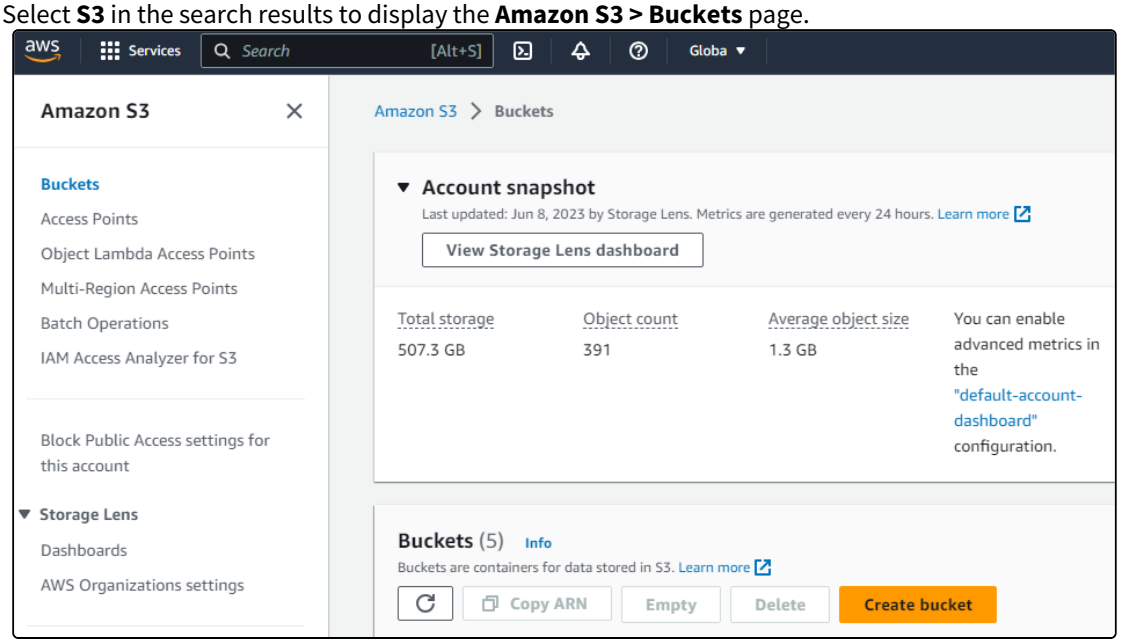
If you don't have an S3 bucket, create a new one as explained below.

To create an S3 bucket

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



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



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

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

6. For the other S3 settings, you can leave the default values.

- Object Ownership
- Block Public Access settings for this bucket
- Bucket Versioning
- Default encryption
- Advanced settings

7. Click **Create bucket**.

Uploading the RAW image

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

To upload the RAW image

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

Configuring the IAM policy

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

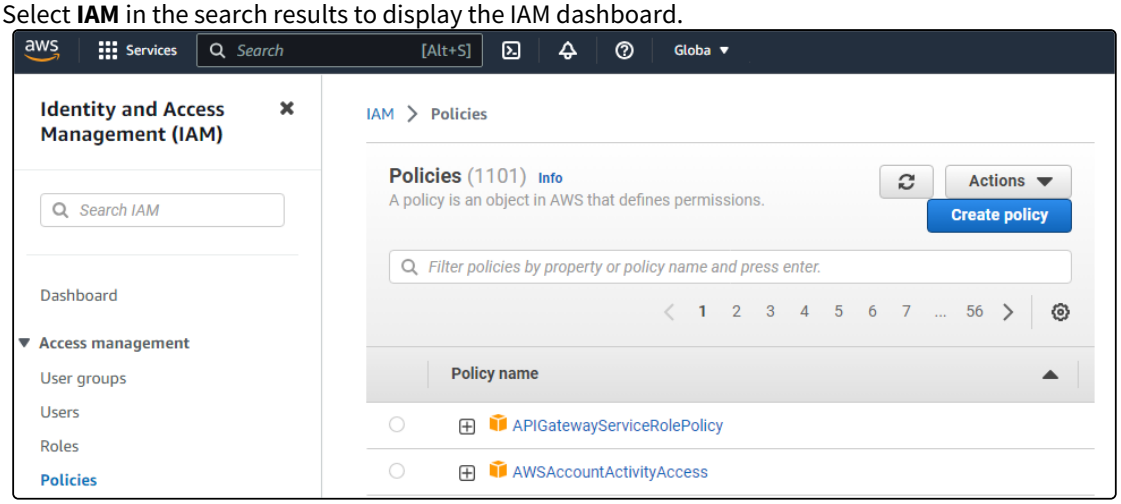
- Creating a new IAM policy
- Updating an existing IAM policy

Creating a new IAM policy

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

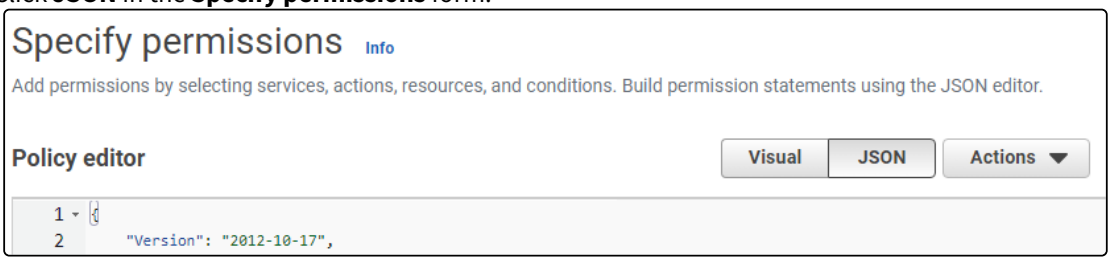
To create an IAM policy

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



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

5. Click **JSON** in the **Specify permissions** form.



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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::$S3_BUCKET_NAME",
                "arn:aws:s3:::$S3_BUCKET_NAME/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifySnapshotAttribute",
                "ec2:CopySnapshot",
                "ec2:RegisterImage",
                "ec2:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

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

Updating an existing IAM policy

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

To update an IAM policy

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

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



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

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

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

Creating an IAM role

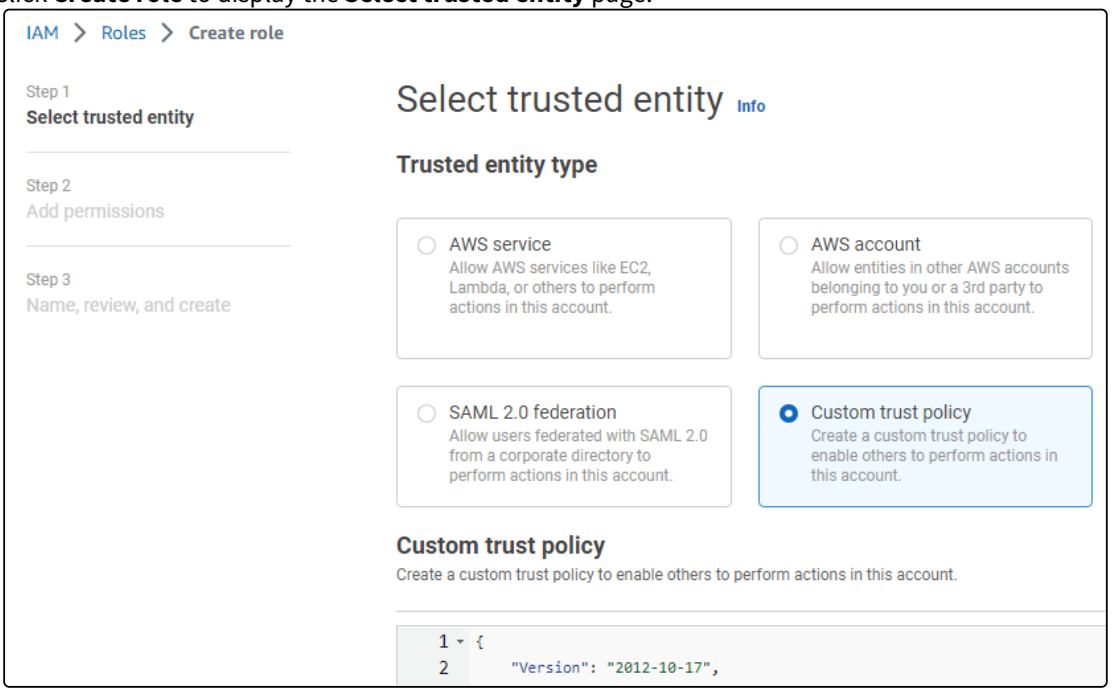
Create an IAM (Identity and Access Management) role for the policy described in Configuring the IAM policy.

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

To create an IAM role

1. Type "IAM" in the search box.
2. Select IAM in the search results to display the IAM dashboard.
3. Select **Access management> Roles** in the navigation sidebar.

4. Click **Create role** to display the **Select trusted entity** page.



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:

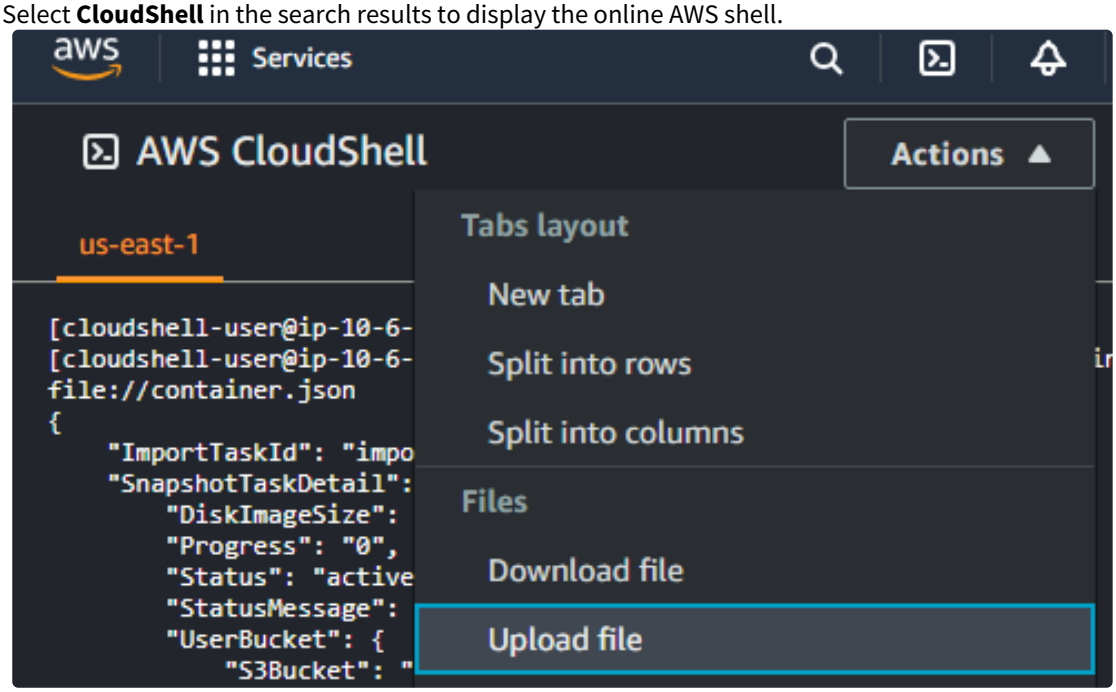
https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html

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-1.3.0_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-1.3.0_2025-01-06-10_38_16.raw"
                }
            },
            "Tags": []
        }
    ]
}
```

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

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

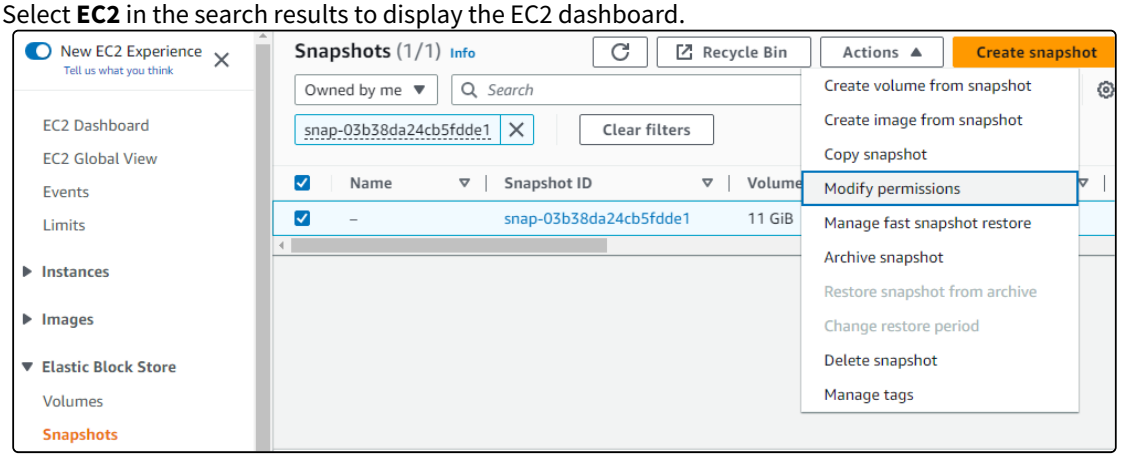
Creating an AMI from the snapshot

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

To create the AMI

1. Type "EC2" in the search box.

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



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

Image settings

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

Block device mappings

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

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

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

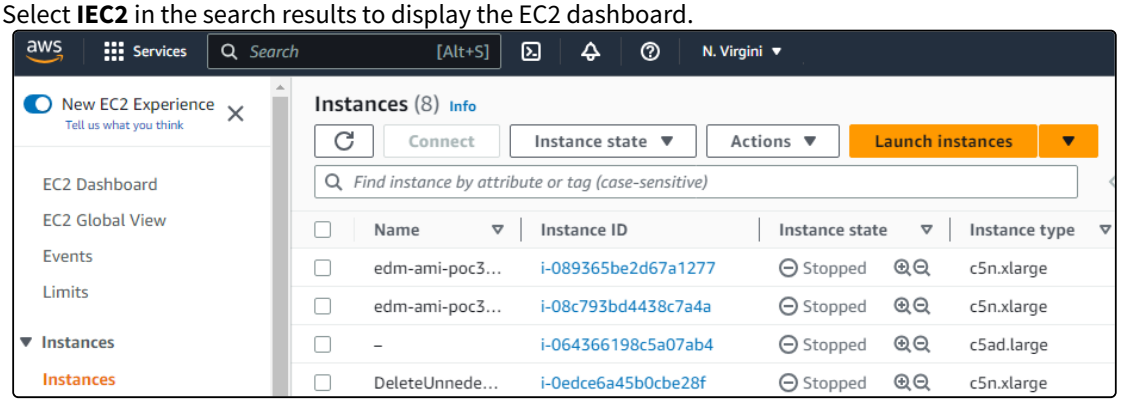
Creating the EC2 instance

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

To create the EC2 instance

1. Type "EC2" in the search box.

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



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

Name and tags > Name

Enter a name for the new EC2 instance.

Application and OS Images (Amazon Machine Image)

Select the machine described in Creating an AMI from the snapshot.

Instance type

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

Key pair (login)

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

Network settings > Firewall (security groups)

Select or create a security group with permission to open the ports described in Required open ports.

> 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.

ℹ 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.

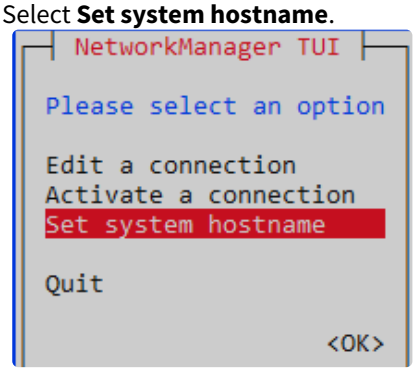
To configure the hostname

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

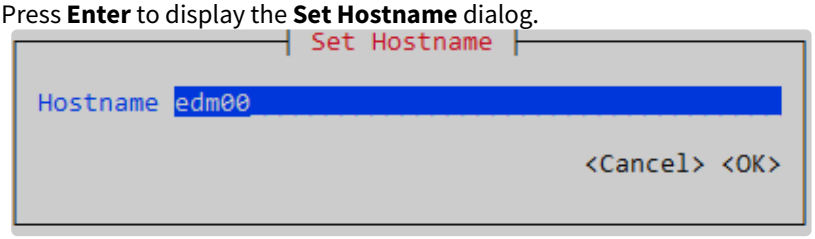
   ```
   sudo nmtui
   ```

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. Exit the session.

```
exit
```

11. Log in again.
12. Restart the `snmp` service to make the changes effective.

```
sudo systemctl restart snmpd
```

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

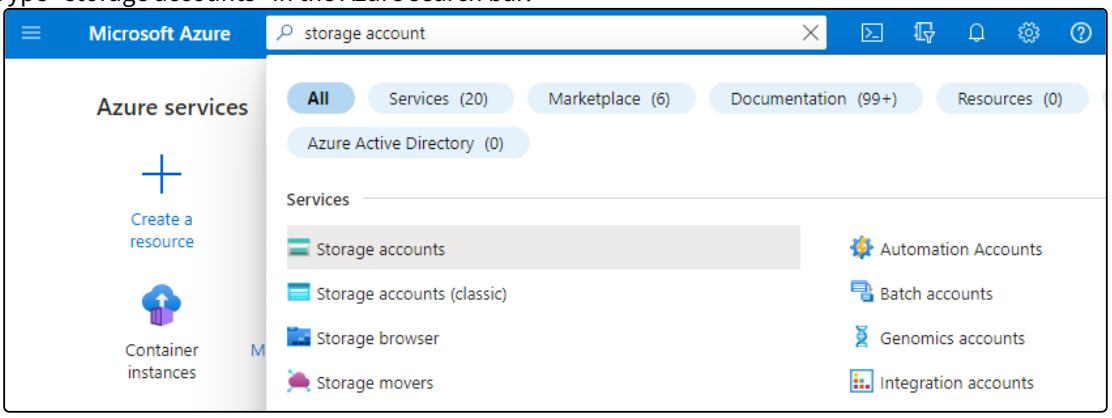
- Creating the Azure image
- Creating the Azure network rules
- Creating the SSH key for Azure
- Creating the Azure virtual machine
- Opening a session into Azure
- Configuring the hostname on Azure

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.

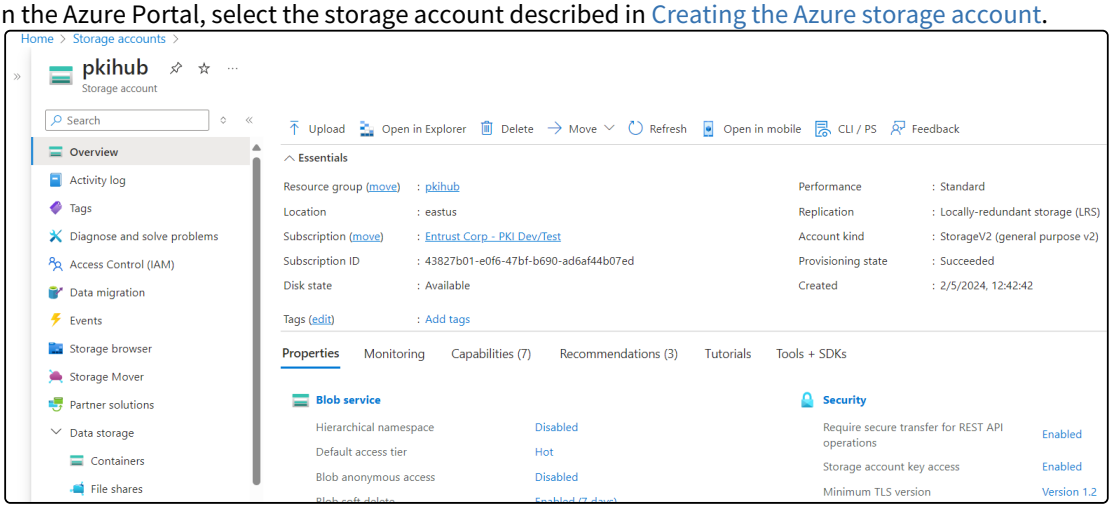
Uploading the VHD image file to Azure

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

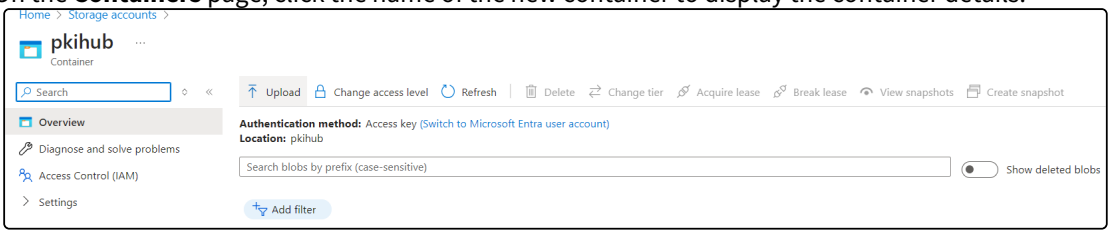
See Downloading the installation files for how to obtain this file.

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: `Standard_D8s_v3`, `Standard_D8s_v4`, `Standard_D8ds_v4`, `Standard_F8s_v2`.

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.

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

Inbound port rules

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

Setting	Value
Public inbound ports	Select **None**.

Licensing type

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

Setting	Value
License type	Select **Other**.

Disk

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

To configure the primary and secondary disks

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

OS disk

Set the following configuration for the primary disk.

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

Select a disk size

Set the following configuration for the secondary disk.

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

Networking

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

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

Advanced

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

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

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

Creating the Azure virtual machine with Azure CLI

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

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

See below for a description of each parameter.

- GROUP
- LOCATION
- VM
- IMAGE

- SIZE
- DISK_SIZE
- EXTRA_DISK_SIZE
- SSH_KEY
- NSG
- CUSTOM_DATA

⚠ 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.

ℹ 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.

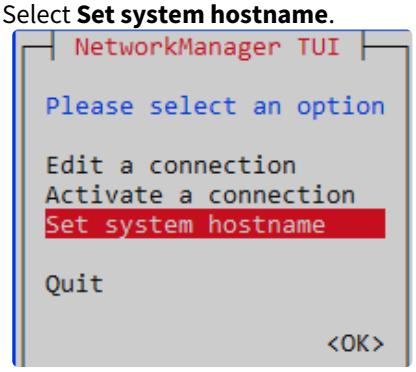
✖ After running the clusterctl install or clusterctl node add commands you cannot change the IP address or hostname of a node.

To configure the hostname

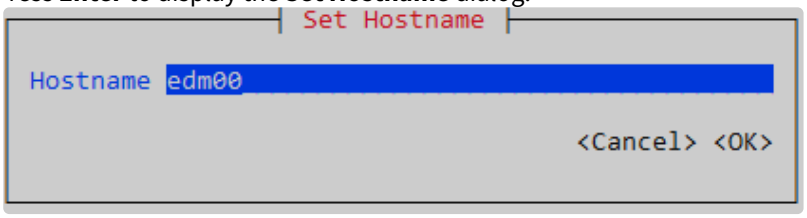
1. Log in to the Cryptographic Security Platform machine locally, as the `sysadmin` user.
2. Run the `nmtui` tool with `sudo` permissions.

```
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. Exit the session.

```
exit
```

11. Log in again.
12. Restart the `snmp` service to make the changes effective.

```
sudo systemctl restart snmpd
```

Installing the cluster

Run the clusterctl install command for installing Cryptographic Security Platform cluster. 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.

Setting	demo-mode	prod-mode
Requirements	Does not need the disk performance requirements described in Machine requirements. Specifically, fsync latency is not an issue in this mode.	All the Requirements.
Supported number of nodes	One	One or more. See Required number of nodes for details.
Supported operations	You cannot perform the operations described in Joining nodes, Backing up the state, Recovering from disaster, or Restoring the state.	All
Supported updates	You cannot upgrade to a newer version or migrate to a prod-mode 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). For example:

```
$ sudo clusterctl install --mode demo-mode --db-host db.example.com --db-port 5432 --
db-name clusterdb --db-username admin
Installing  done ╢▌▌▌
```

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. For example:

```
$ sudo clusterctl install --db-host db.example.com --db-port 5432 --db-name
clusterdb --db-username admin
Installing  done ╢▌▌▌
```

- 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
- ECDSA curve NIST P-384
- ECDSA curve NIST P-521

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.

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.

Selecting the keyboard keymap

The default keyboard keymap for Cryptographic Security Platform Installations is `us`. See below for selecting another one.

> Keymaps are configurations that define how keyboard keys correspond to specific actions or characters.

To select the keyboard keymap

1. Run the following command to list the available keyboard keymaps.

```
localectl list-keymaps
```

2. Run the following command to set the `<keymap>` keyboard keymap.

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

For example:

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

Selecting the operating system timezone

The default timezone for Cryptographic Security Platform Installations is UTC. See below for selecting another one.

To select the operating system timezone

1. Run the following command to list the available time zones.

```
timedatectl list-timezones
```

2. 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 the cluster, 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
```

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

Manually 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
- Creating the kmdata folder
- Creating the kmdata.tar file
- Integrating an nShield Trusted Verification Device

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

Selecting the platform for creating the Entrust nShield Security World

You can create the Entrust nShield Security World on the machine running Cryptographic Security Platform, 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:

1. Copy the file into the Security World `kmdata` folder that will be imported later as part of the solution 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
	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. Ensure the Cryptographic Security Platform node is registered on the HSM as a privileges client.
2. Run the client registration wizard as explained in https://nshielddocs.entrust.com/security-world-docs/v12.80/connect-ug-nix/configure.html#ConfigureConnectClient
3. When prompted **Please enter your client IP address**, type the node IP address and click **Yes**.
4. When prompted **Do you want to save the IP in the config?** click **Yes**.
5. When prompted **Please choose the client permissions** click **Privileged**.
6. When prompted **Do you want secure authentication enabled on this client?** click **No**.

Creating the kmdata folder

Create a `kmdata` folder with the `local` and `config` subdirectories. – for example:

```
mkdir -p kmdata/{local,config}
```

In this folder, add the following files.

- cardlist
- world
- config
- card(s)
- cknfastrc
- module

⚠ Do not add other files than those listed below.

cardlist

Copy this file from the Remote File System (RFS) or another existing HSM client.

Source path (Windows example)	Destination path
C:\ProgramData\nCipher\Key Management Data\config\config	kmdata/config/cardlist

Edit this file and ensure it contains either:

- The serial numbers of the Operator Card Set (OCS) cards for authenticating on the HSM
- An asterisk (*) value, meaning that cards with any serial number will be supported.

ℹ When copied from the Remote File System (RFS), this file already includes the correct values.

Save the file if modified.

world

Copy this file from the Remote File System (RFS) or another existing HSM client.

Source path (Windows example)	Destination path
C:\ProgramData\nCipher\Key Management Data\local	kmdata/local

config

Copy this file from the Remote File System (RFS) or another existing HSM client.

Source path (Windows example)	Destination path
C:\ProgramData\nCipher\Key Management Data\config\config	kmdata/config/config

Edit the copied file and ensure the `[nethsm_imports]` section includes the following content for each HSM.

```
local_module=0
remote_ip=<ip>
remote_port=9004
remote_esn=<ens>
keyhash=0000000000000000000000000000000000000000
privileged=1
privileged_use_high_port=0
ntoken_esn=
```

See below for a description of each parameter.

Parameter	Value
<ip>	The IP address of the HSM
<esn>	The Electronic Serial Number (ESN) unique identifier of the HSM

When deploying multiple HSMs, use five dashes ("-----") to separate each HSM configuration – for example:

```
local_module=0
remote_ip=<ip>
remote_port=9004
remote_esn=<esn>
keyhash=0000000000000000000000000000000000000000
privileged=1
privileged_use_high_port=0
ntoken_esn=
-----
local_module=0
remote_ip=<ip>
remote_port=9004
remote_esn=<esn>
```

```
keyhash=0000000000000000000000000000000000000000
privileged=1
privileged_use_high_port=0
ntoken_esn=
```

Save the changes.

card(s)

Copy these files from the Remote File System (RFS) or another existing HSM client.

Source path (Windows example)	Destination path
C:\ProgramData\nCipher\Key Management Data\config\card_<hash>	kmdata/config/card_<hash>_<n>
C:\ProgramData\nCipher\Key Management Data\config\cards_<hash>	kmdata/config/cards_<hash>

Where:

- `<n>` is the number of cards in the Operator Card Set (OCS).
- `<hash>` is the hash of the OCS token.

Run the following command to query for these files.

```
nfkminfo -c
```

In the command output, check the number of card files and token hashes. For example:

```
Cardset list - 1 cardsets: (P)ersistent/(N)ot, (R)emoteab/e/(L)oca/-only
Operator logical token hash                k/n   timeout name
67Sadb78b8c0dcbda9eabdca2d164393db69ca88   1/1   none-PR OCS
```

According to this output, the HSM configuration includes the following files:

```
card_67Sadb78b8c0dcbda9eabdca2d164393db69ca88_1
```

```
cards_67Sadb78b8c0dcbda9eabdca2d164393db69ca88
```

An OCS using two cards would include the following files:

```
card_67Sadb78b8c0dcbda9eabdca2d164393db69ca88_1
```

```
card_67Sadb78b8c0dcbda9eabdca2d164393db69ca88_2
```

```
cards_67Sadb78b8c0dcbda9eabdca2d164393db69ca88
```

cknfastrc

When using multiple HSMs, create the following file.

```
kmdata/cknfastrc
```

Edit this file and add the following line:

```
CKNFAST_LOADSHARING=1
```

Save the changes.

module

For each deployed HSM, copy this file from the Remote File System (RFS) or another existing HSM client.

Source path (Windows example)	Destination path
C:\ProgramData\nCipher\Key Management Data\local\module_<esn>_D947	kmdata/local/module_<esn>_D947
C:\ProgramData\nCipher\Key Management Data\local\module_<esn>_D947_<hash>	kmdata/local/module_<esn>_D947_<hash>

Where:

- `<esn>` The Electronic Serial Number (ESN) is the unique identifier of the HSM. This value always ends with the D947 sequence.
- `<hash>` is a Security World identifier hash.

For example:

```
kmdata/local/module_ECOA-33E0-D947
kmdata/local/module_ECOA-33E0-D947_d86ccdc604f3udF7b0duuf7aafdf8afb60ae6baa
```

Creating the kmdata.tar file

To create the `kmdata.tar file`, run the following command on a PowerShell prompt.

```
tar -cvf kmdata.tar -C <kmdata_dir> kmdata
```

Where `<kmdata_dir>` is the path of the folder described in Creating the kmdata folder. For example:

```
tar -cvf kmdata.tar -C c:\temp\ kmdata
a kmdata
a kmdata/cknfastrc
a kmdata/config
a kmdata/local
a kmdata/local/cards_675adb781P3c0dcbd49eabdca2d101393db69ca88
a kmdata/local/card_675adb713b8cedcbd49eabdca2d1641393db69ca88_1
a kmdata/local/module_ECOA-33E0-D947
a kmdata/local/module_ECOA-33E0-D947_d86ccdc604f3udF7b0duuf7aafdf8afb60ae6baa
a kmdata/local/world
a kmdata/config/cardlist
a kmdata/config/config
```

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.

Configuring SNMP Authentication for MIB information access

Cryptographic Security Platform exposes the following Management Information Bases (MIBs) to SNMP (Simple Network Management Protocol) managers.

MIB object identifier	MIB object description	MIB object path
SNMPv2-MIB::system	System information (e.g., uptime)	.1.3.6.1.3.1.1
UCD-SNMP-MIB::systemStats	CPU statistics	.1.3.6.1.4.1.3021.11
UCD-SNMP-MIB::memory	Memory usage	.1.3.6.1.4.1.3021.4
UCD-SNMP-MIB::laTable	Load averages	.1.3.6.1.4.1.3021.10
HOST-RESOURCES-MIB::hrFSTable	File system table	.1.3.6.1.3.1.35.3.8
HOST-RESOURCES-MIB::hrSystem	Host system info	.1.3.6.1.3.1.35.1
IF-MIB::ifTable	Network interface table	.1.3.6.1.3.1.3.2

For an SNMP manager to consume this information, you must enable at least one of the following SNMP authentication methods.

- Enabling SNMP access
- Configuring SNMPv2c authentication
- Configuring SNMPv3 authentication

⚠ As explained in Required ports for incoming traffic, the SNMP port must be open to incoming traffic.

Enabling SNMP access

To enable access to the SNMP service, run the following command on each Cryptographic Security Platform node.

```
sudo systemctl enable --now snmpd
```

Configuring SNMPv2c authentication

Configuring SNMPv2c authentication requires performing the following steps on each Cryptographic Security Platform node.

To configure SNMPv2c authentication on a node

1. Run the following command to edit the SNMP configuration file.

   ```
   sudo vi /etc/snmp/snmpd.conf
   ```

2. Find the following line.

   ```
   # rocommunity <PASSWORD> default -V systemonly
   ```

3. Remove # and change `<PASSWORD>` with a secure password – for example:

   ```
   rocommunity MySecret default -V systemonly
   ```

4. Save the file changes.
5. Run the following command to restart the `snmpd` service.

   ```
   sudo systemctl restart snmpd
   ```

Configuring SNMPv3 authentication

Configuring SNMPv3 authentication requires performing the following steps on each Cryptographic Security Platform node.

To configure SNMPv3 authentication on a node

1. Stop the `snmpd` service.

```
sudo systemctl stop snmpd
```

2. Create a user.

```
sudo net-snmp-create-v3-user -a SHA -x AES -ro
```

3. When prompted, enter a name and password for the new user.
4. Run the following command to edit the SNMP configuration file.

```
sudo vi /etc/snmp/snmpd.conf
```

5. Find a line with the "rouser <username>" content. For example, if the new user's name is "snmpuser", find the following line.

```
rouser snmpuser
```

6. Append "priv -V systemonly" to the line, for example:

```
rouser snmpuser priv -V systemonly
```

7. Save the file changes.
8. Restart the `snmpd` service.

```
sudo systemctl start snmpd
```

Replacing the initial password for the Management Console admin

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

> ⚠ This `admin` user of the Management is not to be confused with the `sysadmin` user for shell command operations.

To replace the initial password for the Management Console admin

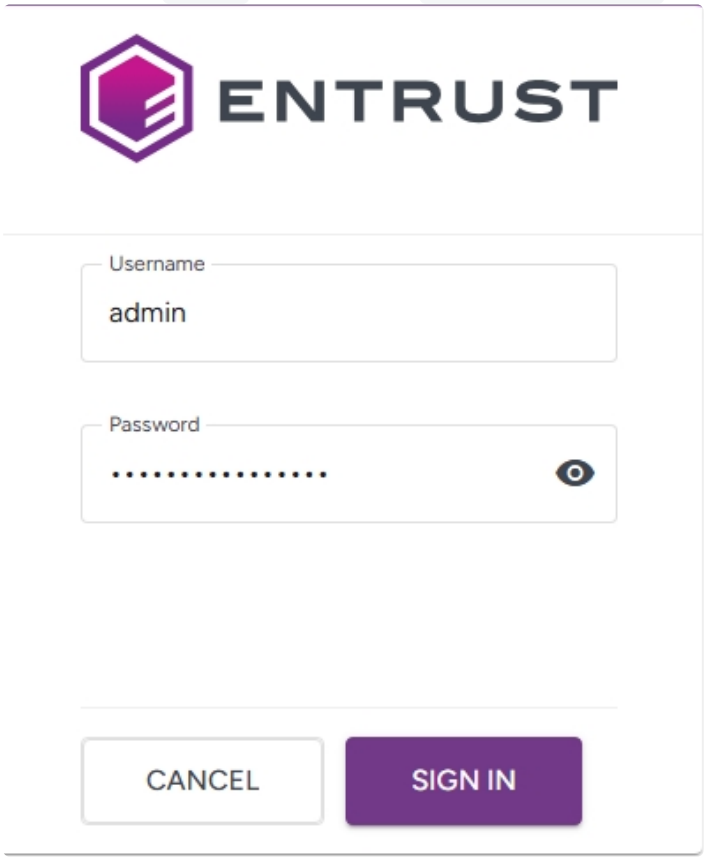
1. Open the following URL in a Web browser.

```
https://<machine>:8443/management-console
```

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

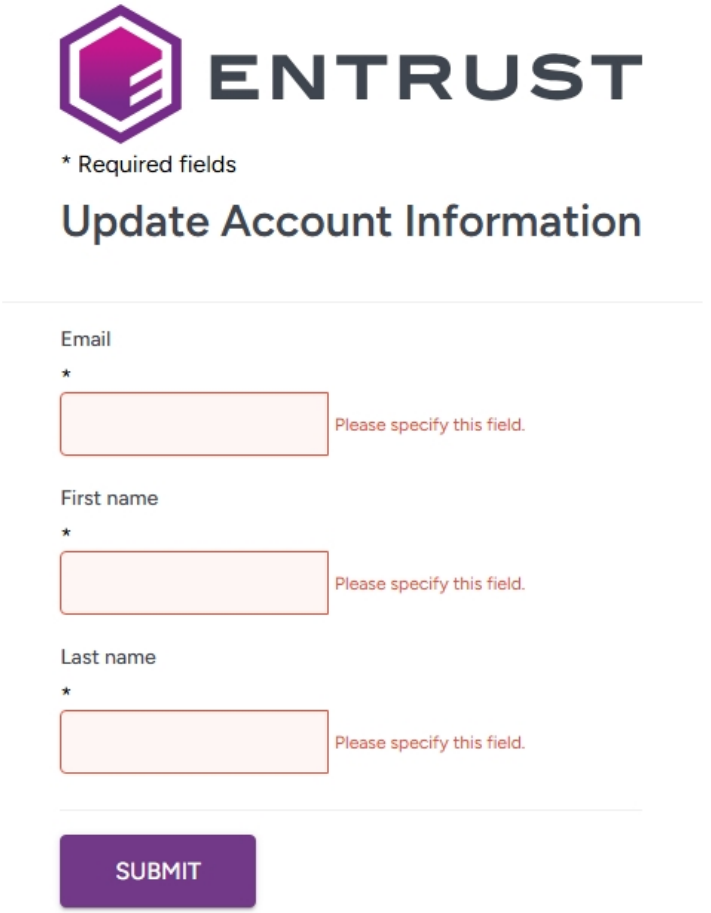
> ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in with the `admin` username and `Changeme123456@#` 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 with the default Authentication settings.

4. Complete your account information



5. Click **Submit**,

Setting 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

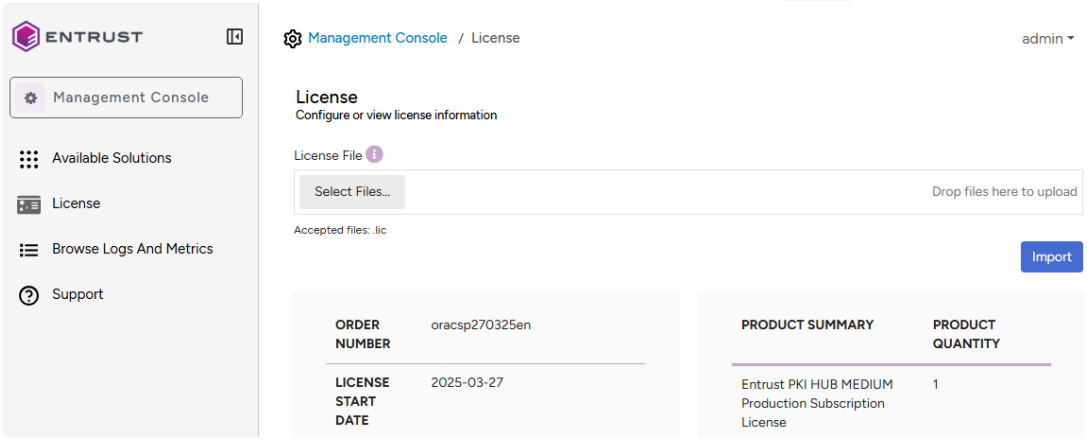
1. Open the following URL in a Web browser.

```
https://<machine>:8443/management-console
```

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

> ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as 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.
6. Click **Import**.

6 Managing identities

After Replacing the initial password for the Management Console admin and Setting the license, you can manage user identities as explained below.

- Roles
- Users
- Sessions
- Events
- Settings
- Authentication
- Identity providers
- User federation

> Management Console users are not to be confused with operating system users with permissions on the operations described in Command reference.

Roles

See below for managing user roles.

- Creating roles
- Browsing and updating roles
- Role reference

> See User registration for how to manage the list of default roles.

Creating roles

Cryptographic Security Platform provides a predefined set of roles for most of use cases. However, you can also create new roles as explained in this section.

To manage roles

1. Open the following URL in a Web browser.

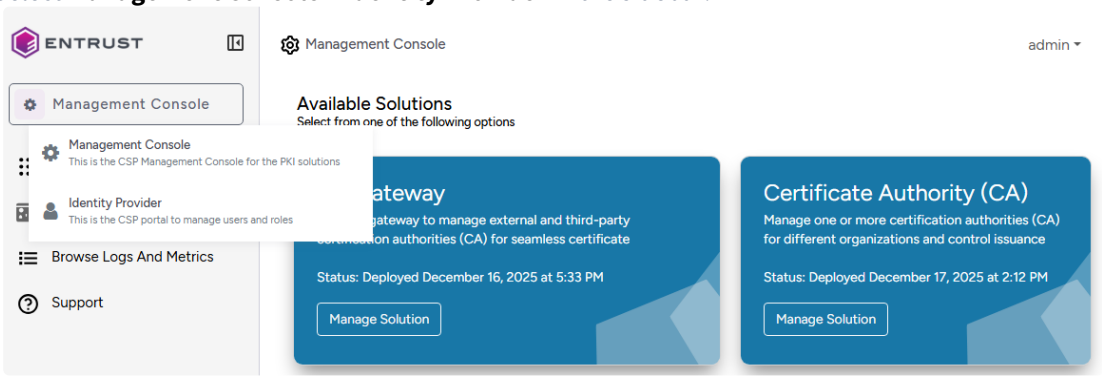
   ```
   https://<machine>:8443/management-console
   ```

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

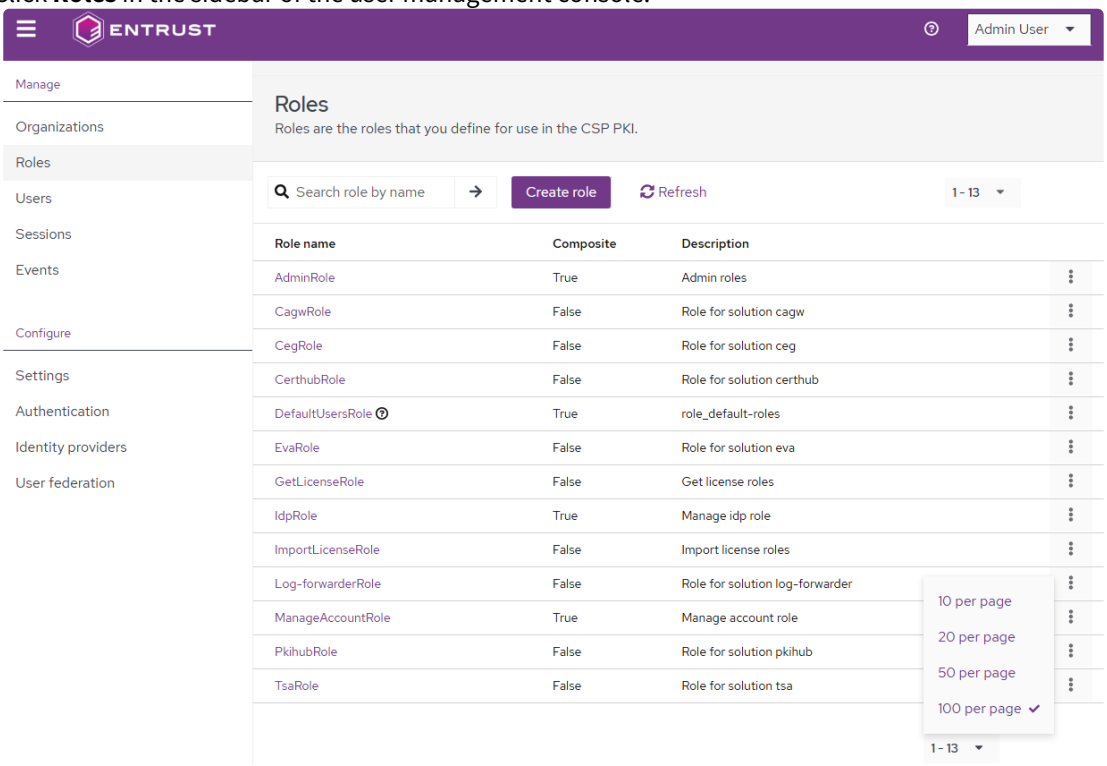
   > This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a user with a role granting user management permissions – for example, the initial `admin` administrator user.

3. Select **Management Console > Identity Provider** in the sidebar.

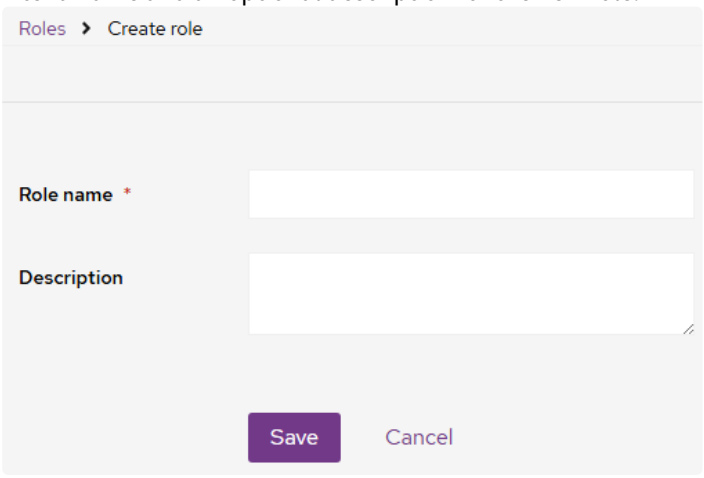


4. Click **Roles** in the sidebar of the user management console.



5. Click **Create role.**

6. Enter a name and an optional description for the new role.



7. Click **Save**.
8. Configure the following settings.
    - Associated roles
    - Attributes
    - Users in role
    - Admin events

Associated roles

The list of inherited and associated roles.

- Uncheck the **Hide inherited roles** box to display the inherited roles.
- Click **Assign role** and select a role to associate it.
- Select an associated role and click **Unassign** to remove an associated role.

The **Inherited** column displays `True` for inherited roles and `False` for the associated ones.

> ⚠ Role users will be granted the permissions of all inherited and associated roles.

Attributes

Key-pair values to store permission information.

> ⚠ Do not modify the existing attribute configuration of a role. Use associated roles instead to modify the permissions granted to user roles.

Users in role

The list of users to whom the role has been granted.

Admin events

A log record of the events performed by the role users in the administration console.

Browsing and updating roles

See below for browsing and optionally updating user roles.

To manage and update roles

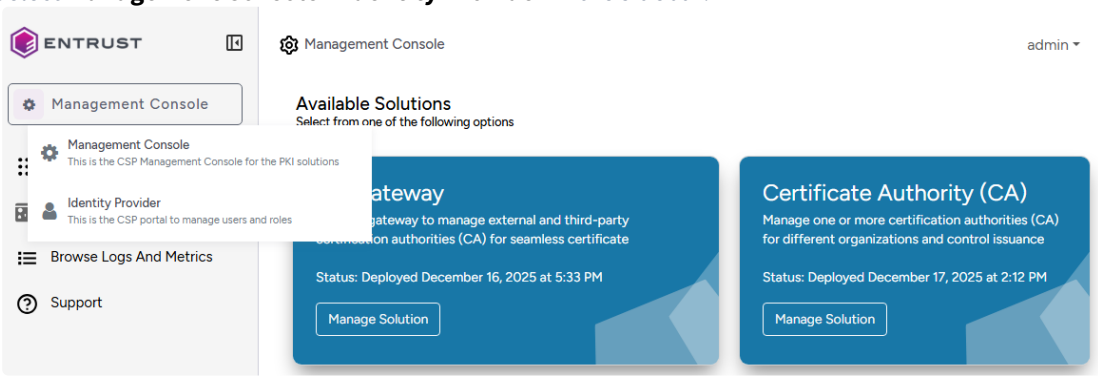
1. Open the following URL in a Web browser.

   ```
   https://<machine>:8443/management-console
   ```

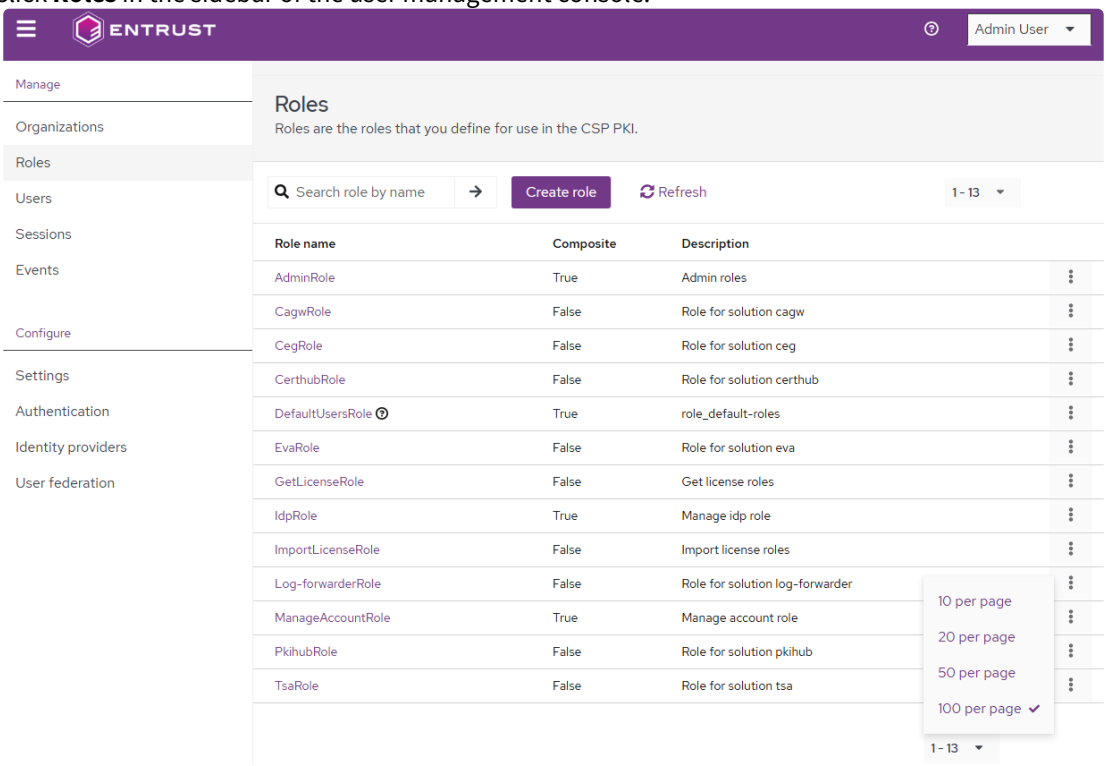
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a user with a role granting user management permissions – for example, the initial `admin` administrator user.
3. Select **Management Console > Identity Provider** in the sidebar.



4. Click **Roles** in the sidebar of the user management console.



5. Browse the list of existing User roles (use the bottom-left selector to display more roles).
   - Roles with the **Composite** column set to `True` are sets of roles.
   - Roles with the **Composite** column set to `False` are single roles.
6. Browse or update the following role details.
   - Details
   - Associated roles
   - Attributes
   - Users in role
   - Admin events

Details

The name and description of the role.

Associated roles

The list of inherited and associated roles.

- Uncheck the **Hide inherited roles** box to display the inherited roles.
- Click **Assign role** and select a role to associate it.
- Select an associated role and click **Unassign** to remove an associated role.

The **Inherited** column displays `True` for inherited roles and `False` for the associated ones.

⚠ Role users will be granted the permissions of all inherited and associated roles.

Attributes

Key-pair values to store permission information.

> ⚠ Do not modify the existing attribute configuration of a role. Use associated roles instead to modify the permissions granted to user roles.

Users in role

The list of users to whom the role has been granted.

Admin events

A log record of the events performed by the role users in the administration console.

Role reference

See below for a reference of the default Cryptography Security Manager roles.

- User roles
- Client roles

User roles

The following default roles grant permissions on Cryptography Security Manager configuration and solutions.

- AdminRole
- CagwRole
- CegRole
- CertHubRole
- DefaultUsersRole
- EvaRole
- GetLicenseRole
- ImportLicenseRole
- Log-forwarderRole
- ManageAccountRole
- offline_access
- PkihubRole
- TsaRole

AdminRole

Users with this role have permissions on all the identity manager and management console operations.

- Identity Manager permissions
- Management Console permissions

Identity Manager permissions

See below for the permissions granted to users with this role on the Identity Manager console.

Operation	View	Manage
Roles	✓	✓
Users	✓	✓
Sessions	✓	✓
Events	✓	✓
Settings	✓	✓
Authentication	✓	✓
Identity providers	✓	✓
User federation	✓	✓

Management Console permissions

See below for the permissions granted to users with this role on the Management Console.

Scope	View	Manage
Managing CA Gateway	✓	✓
Managing Certificate Authority	✓	✓
Managing Certificate Enrollment Gateway	✓	✓
Managing Certificate Manager	✓	✓
Managing Timestamping Authority	✓	✓
Managing Validation Authority	✓	✓
Managing Log Forwarder	✓	✓
Setting the license	✓	✓
Browsing logs with Grafana	✓	✓

CagwRole

See below for the permissions granted to users with this role.

- Identity Manager permissions
- Management Console permissions

Identity Manager permissions

See below for the permissions granted to users with this role on the Identity Manager console.

Scope	View	Manage
Roles	✓	✗
Users	✓	✗
Sessions	✗	✗
Events	✗	✗
Settings	✓	✗
Authentication	✗	✗
Identity providers	✗	✗
User federation	✓	✗

Management Console permissions

See below for the permissions granted to users with this role on the Management Console.

Scope	View	Manage
Managing CA Gateway	✓	✓
Managing Certificate Authority	✗	✗
Managing Certificate Enrollment Gateway	✗	✗
Managing Certificate Manager	✗	✗
Managing Timestamping Authority	✗	✗

Scope	View	Manage
Managing Validation Authority	✗	✗
Managing Log Forwarder	✗	✗
Setting the license	✓	✗
Browsing logs with Grafana	✓	✓

CegRole

See below for the permissions granted to users with this role.

- Identity Manager permissions
- Management Console permissions

Identity Manager permissions

See below for the permissions granted to users with this role on the Identity Manager console.

Operation	View	Manage
Roles	✓	✗
Users	✓	✗
Sessions	✗	✗
Events	✗	✗
Settings	✓	✗
Authentication	✗	✗
Identity providers	✗	✗
User federation	✓	✗

Management Console permissions

See below for the permissions granted to users with this role on the Management Console.

Scope	View	Manage
Managing CA Gateway	✗	✗
Managing Certificate Authority	✗	✗
Managing Certificate Enrollment Gateway	✓	✓
Managing Certificate Manager	✗	✗
Managing Timestamping Authority	✗	✗
Managing Validation Authority	✗	✗
Managing Log Forwarder	✗	✗
Setting the license	✓	✗
Browsing logs with Grafana	✓	✓

CertHubRole

See below for the permissions granted to users with this role.

- Identity Manager permissions
- Management Console permissions

Identity Manager permissions

See below for the permissions granted to users with this role on the Identity Manager console.

Operation	View	Manage
Roles	✓	✗
Users	✓	✗
Sessions	✗	✗
Events	✗	✗
Settings	✓	✗

Operation	View	Manage
Authentication	✗	✗
Identity providers	✗	✗
User federation	✓	✗

Management Console permissions

See below for the permissions granted to users with this role on the Management Console.

Scope	View	Manage
Managing CA Gateway	✗	✗
Managing Certificate Authority	✗	✗
Managing Certificate Enrollment Gateway	✗	✗
Managing Certificate Manager	✓	✓
Managing Timestamping Authority	✗	✗
Managing Validation Authority	✗	✗
Managing Log Forwarder	✗	✗
Setting the license	✓	✗
Browsing logs with Grafana	✓	✓

DefaultUsersRole

Click this role to display the list of roles automatically assigned to new users. As explained in User registration, you can add or remove roles to this list.

EvaRole

See below for the permissions granted to users with this role.

- Identity Manager permissions
- Management Console permissions

Identity Manager permissions

See below for the permissions granted to users with this role on the Identity Manager console.

Operation	View	Manage
Roles	✓	✗
Users	✓	✗
Sessions	✗	✗
Events	✗	✗
Settings	✓	✗
Authentication	✗	✗
Identity providers	✗	✗
User federation	✓	✗

Management Console permissions

See below for the permissions granted to users with this role on the Management Console.

Scope	View	Manage
Managing CA Gateway	✗	✗
Managing Certificate Authority	✗	✗
Managing Certificate Enrollment Gateway	✗	✗
Managing Certificate Manager	✗	✗
Managing Timestamping Authority	✗	✗
Managing Validation Authority	✓	✓
Managing Log Forwarder	✗	✗

Scope	View	Manage
Setting the license	✓	✗
Browsing logs with Grafana	✓	✓

GetLicenseRole

See below for the permissions granted to users with this role.

- Identity Manager permissions
- Management Console permissions

Identity Manager permissions

See below for the permissions granted to users with this role on the Identity Manager console.

Operation	View	Manage
Roles	✓	✗
Users	✓	✗
Sessions	✗	✗
Events	✗	✗
Settings	✓	✗
Authentication	✗	✗
Identity providers	✗	✗
User federation	✓	✗

Management Console permissions

See below for the permissions granted to users with this role on the Management Console.

Scope	View	Manage
Managing CA Gateway	✗	✗
Managing Certificate Authority	✗	✗

Scope	View	Manage
Managing Certificate Enrollment Gateway	✗	✗
Managing Certificate Manager	✗	✗
Managing Timestamping Authority	✗	✗
Managing Validation Authority	✗	✗
Managing Log Forwarder	✗	✗
Setting the license	✓	✗
Browsing logs with Grafana	✓	✓

ImportLicenseRole

See below for the permissions granted to users with this role.

- Identity Manager permissions
- Management Console permissions

Identity Manager permissions

See below for the permissions granted to users with this role on the Identity Manager console.

Operation	View	Manage
Roles	✓	✗
Users	✓	✗
Sessions	✗	✗
Events	✗	✗
Settings	✓	✗
Authentication	✗	✗
Identity providers	✗	✗

Operation	View	Manage
User federation	✓	✗

Management Console permissions

See below for the permissions granted to users with this role on the Management Console.

Scope	View	Manage
Managing CA Gateway	✗	✗
Managing Certificate Authority	✗	✗
Managing Certificate Enrollment Gateway	✗	✗
Managing Certificate Manager	✗	✗
Managing Timestamping Authority	✗	✗
Managing Validation Authority	✗	✗
Managing Log Forwarder	✗	✗
Setting the license	✓	✓
Browsing logs with Grafana	✓	✓

Log-forwarderRole

See below for the permissions granted to users with this role.

- Identity Manager permissions
- Management Console permissions

Identity Manager permissions

See below for the permissions granted to users with this role on the Identity Manager console.

Operation	View	Manage
Roles	✓	✗
Users	✓	✗

Operation	View	Manage
Sessions	✗	✗
Events	✗	✗
Settings	✓	✗
Authentication	✗	✗
Identity providers	✗	✗
User federation	✓	✗

Management Console permissions

See below for the permissions granted to users with this role on the Management Console.

Scope	View	Manage
Managing CA Gateway	✗	✗
Managing Certificate Authority	✗	✗
Managing Certificate Enrollment Gateway	✗	✗
Managing Certificate Manager	✗	✗
Managing Timestamping Authority	✗	✗
Managing Validation Authority	✗	✗
Managing Log Forwarder	✓	✓
Setting the license	✓	✗
Browsing logs with Grafana	✓	✓

ManageAccountRole

See below for the permissions granted to users with this role.

- Identity Manager permissions

- Management Console permissions

Identity Manager permissions

See below for the permissions granted to users with this role on the Identity Manager console.

Operation	View	Manage
Roles	✓	✗
Users	✓	✗
Sessions	✗	✗
Events	✗	✗
Settings	✓	✗
Authentication	✗	✗
Identity providers	✗	✗
User federation	✓	✗

Management Console permissions

See below for the permissions granted to users with this role on the Management Console.

Scope	View	Manage
Managing CA Gateway	✗	✗
Managing Certificate Authority	✗	✗
Managing Certificate Enrollment Gateway	✗	✗
Managing Certificate Manager	✗	✗
Managing Timestamping Authority	✗	✗
Managing Validation Authority	✗	✗
Managing Log Forwarder	✗	✗

Scope	View	Manage
Setting the license	✗	✓
Browsing logs with Grafana	✓	✓

offline_access

Internal role for supporting offline tokens.

> ⚠ Do not modify this role, remove this role, or assign this role to users.

PkihubRole

See below for the permissions granted to users with this role.

- Identity Manager permissions
- Management Console permissions

Identity Manager permissions

See below for the permissions granted to users with this role on the Identity Manager console.

Operation	View	Manage
Roles	✓	✗
Users	✓	✗
Sessions	✗	✗
Events	✗	✗
Settings	✓	✗
Authentication	✗	✗
Identity providers	✗	✗
User federation	✓	✗

Management Console permissions

See below for the permissions granted to users with this role on the Management Console.

Scope	View	Manage
Managing CA Gateway	✗	✗
Managing Certificate Authority	✓	✓
Managing Certificate Enrollment Gateway	✗	✗
Managing Certificate Manager	✗	✗
Managing Timestamping Authority	✗	✗
Managing Validation Authority	✗	✗
Managing Log Forwarder	✗	✗
Setting the license	✓	✗
Browsing logs with Grafana	✓	✓

TsaRole

See below for the permissions granted to users with this role.

- Identity Manager permissions
- Management Console permissions

Identity Manager permissions

See below for the permissions granted to users with this role on the Identity Manager console.

Setting	View	Manage
Roles	✓	✗
Users	✓	✗
Sessions	✗	✗
Events	✗	✗
Settings	✓	✗

Setting	View	Manage
Authentication	✗	✗
Identity Providers	✗	✗
User federation	✓	✗

Management Console permissions

See below for the permissions granted to users with this role on the Management Console.

Scope	View	Manage
Managing CA Gateway	✗	✗
Managing Certificate Authority	✗	✗
Managing Certificate Enrollment Gateway	✗	✗
Managing Certificate Manager	✗	✗
Managing Timestamping Authority	✓	✓
Managing Validation Authority	✗	✗
Managing Log Forwarder	✗	✗
Setting the license	✓	✗
Browsing logs with Grafana	✓	✓

Client roles

See below for the low-level client roles.

- Permissions for managing your account
- Permissions for managing other accounts

> Unlike user roles, low-level roles cannot be added or modified.

Permissions for managing your account

The following client roles grant permissions on the user's personal account.

Role	Permissions
delete-account	Delete the personal account
manage-account-links	Link or unlink identity providers (IdPs) to the personal account
manage-account	Manage the personal account
manage-consent	Review, grant, or revoke consent for an application to access personal data
read-token	Read the personal access token
view-applications	View the applications linked to the personal account
view-consent	View the consents granted for an application to access personal data
view-profile	View personal profile information

Permissions for managing other accounts

The following client roles grant permissions on other user accounts.

Role	Permissions
create-client	Create clients
impersonation	Log in as that user without knowing their password (typically for troubleshooting or support purposes)
manage-authorization	Manage user authorization settings
manage-clients	Manage client application settings such as protocols, credentials, or roles.
manage-events	Manage event settings such as listeners, types, or retention policies
manage-identity-providers	Add, configure, and remove identity providers (IdPs)

Users

See below for managing users.

- Registering users with the built-in identity provider
- Registering users with external identity providers
- Browsing and updating users
- Deleting or disabling users

> Management Console users are not to be confused with operating system users with permissions on the operations described in Command reference.

Registering users with the built-in identity provider

See below for registering users with the Cryptographic Security Platform built-in identity provider.

> Management Console users are not to be confused with operating system users with permissions on the operations described in Command reference.

To create a user

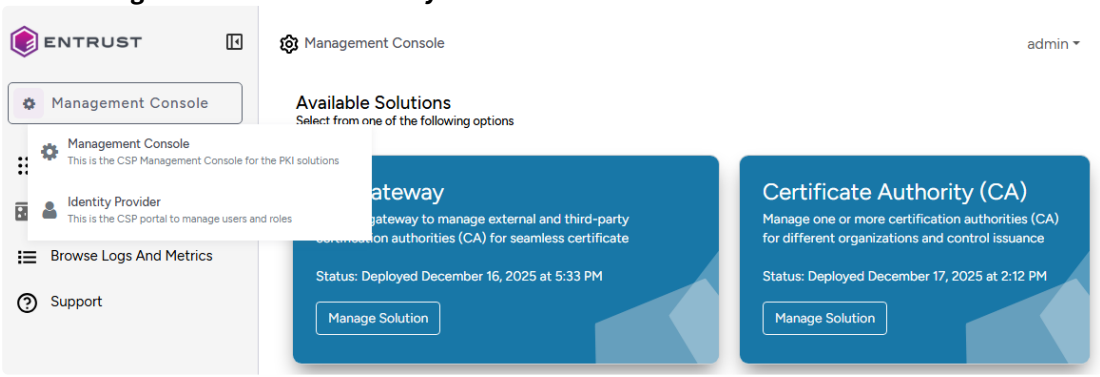
1. Open the following URL in a Web browser.

   ```
   https://<machine>:8443/management-console
   ```

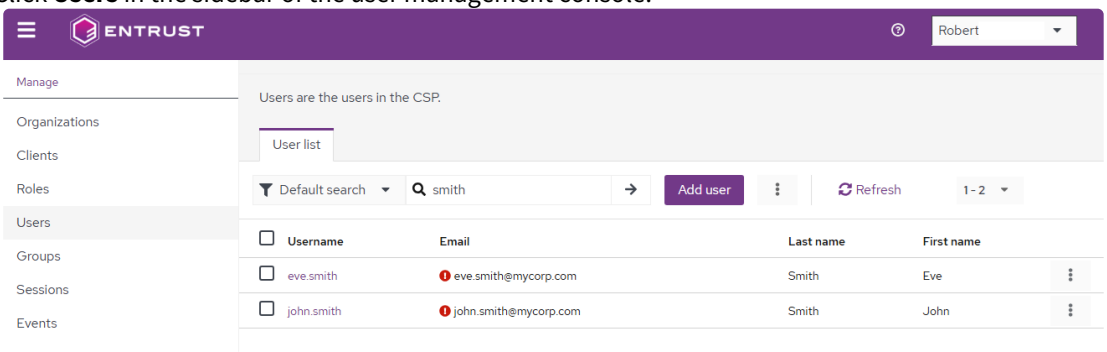
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a user with a role granting user management permissions – for example, the initial `admin` administrator user.
3. Select **Management Console > Identity Provider** in the sidebar.



4. Click **Users** in the sidebar of the user management console.

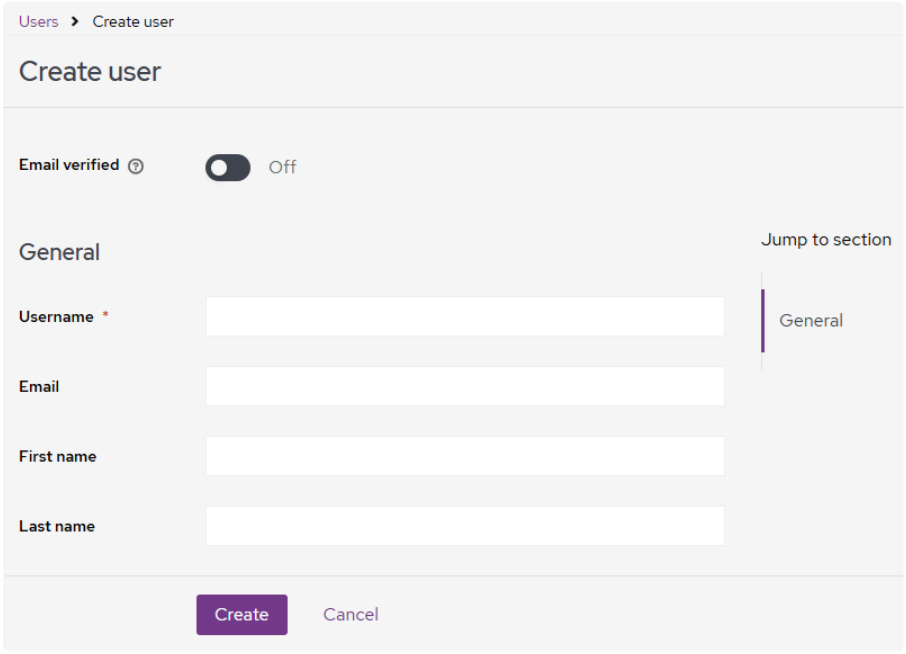


5. Click **Add user.**
6. Fill in the values of the following forms.
    - General
    - Details
    - Credentials
    - Role mapping
    - Organizations
    - Consents
    - Identity provider links

General

The user's general settings.

Field	Value
Email verified	**On** if the user's email has been verified, **Off** otherwise
Username	The user's login name
Email	The user's email
First name	The user's first name
Last name	The user's last name
Groups	The groups the user belongs to. Click **Join Groups** to add the user to user groups



Click **Create to continue with** user creation.

Details

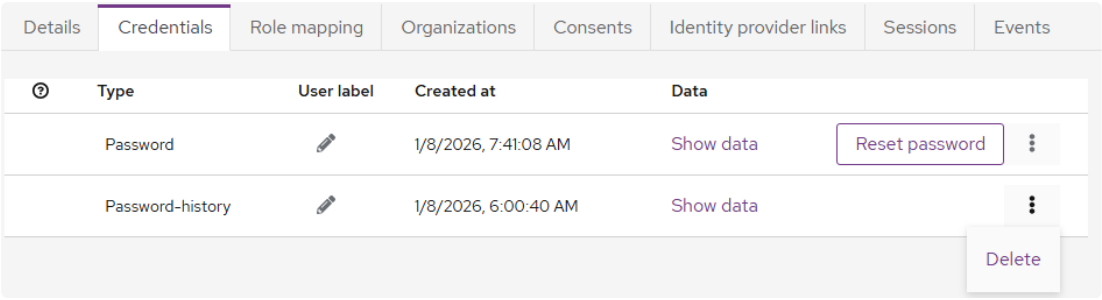
The user's main details.

Field	Value
ID	The user's internal identifier generated by Cryptographic Security Platform
Created at	The user's creation date
Email verified	**On** if the user's email has been verified, **Off** otherwise
Username	The user's login name
Email	The user's email
First name	The user's first name
Last name	The user's last name
Temporary locked	**On** if the user has been locked after multiple failed login attempts; **Off** otherwise .

Credentials

The user's login credentials.

- Click **Set password** to set the user login password
- Click **Credential Reset** to force a password change.
- Click the three horizontal dots for **Password** and select **Delete** to remove the password.
- Click the three horizontal dots for **Password-history** and select **Delete** to remove the password history.



See Authentication for details on the password policy requirements.

Role mapping

The list of Roles the user belongs to.

- Uncheck Hide inherited roles to display the roles inherited by the roles currently assigned to the user.
- Click **Assign Role** to grant a role to the user.
- Select a role and click **Unassign** to unassign.

Organizations

The organizations the user belongs to.

Consents

The consents granted by client applications, if any.

Identity provider links

The third-party identity providers allowing the user to authenticate in the administration console.

Registering users with external identity providers

See below for registering Cryptographic Security Platform users with external identity providers.

> Management Console users are not to be confused with operating system users with permissions on the operations described in Command reference.

To register users with external identity providers

1. Register one of the external identity providers described in Identity providers
2. Log out of the User Management Console.
3. Log in to the User Management Console using the new identity provider as the authentication mode.
4. Browse and update the certificate details as explained in Browsing and updating users.

Browsing and updating users

See below for how to browse and optionally update existing users.

To browse and create users

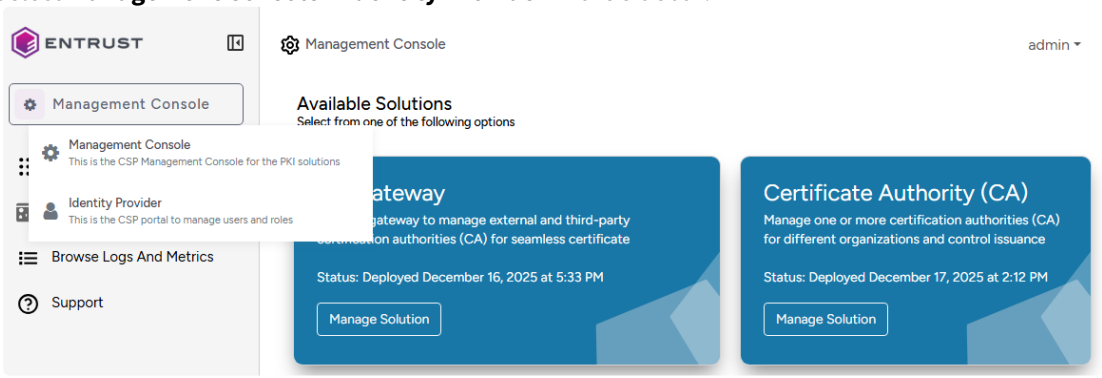
1. Open the following URL in a Web browser.

   ```
   https://<machine>:8443/management-console
   ```

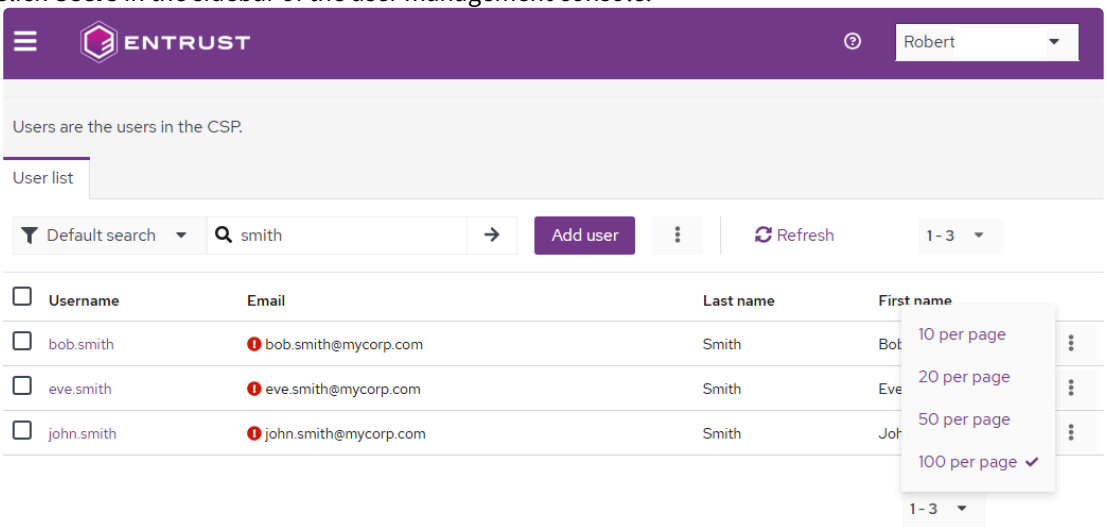
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a user with a role granting user management permissions – for example, the initial `admin` administrator user.
3. Select **Management Console > Identity Provider** in the sidebar.

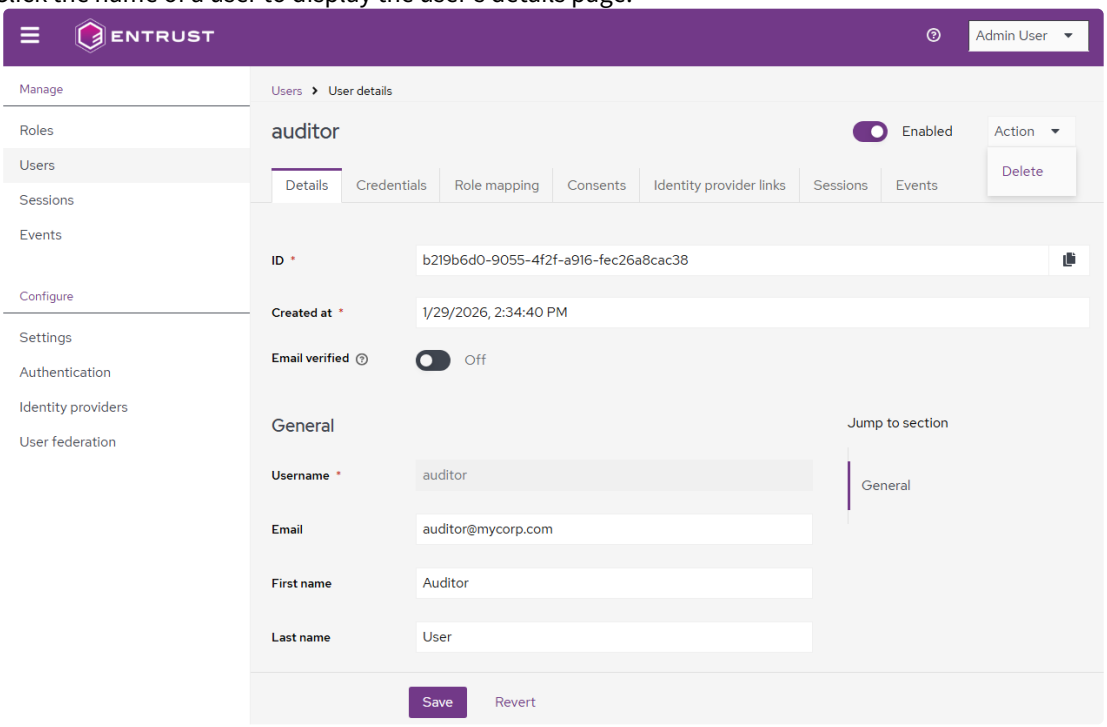


4. Click **Users** in the sidebar of the user management console.



5. Use the search options to filter users and select the number of users per page.

6. Click the name of a user to display the user's details page.

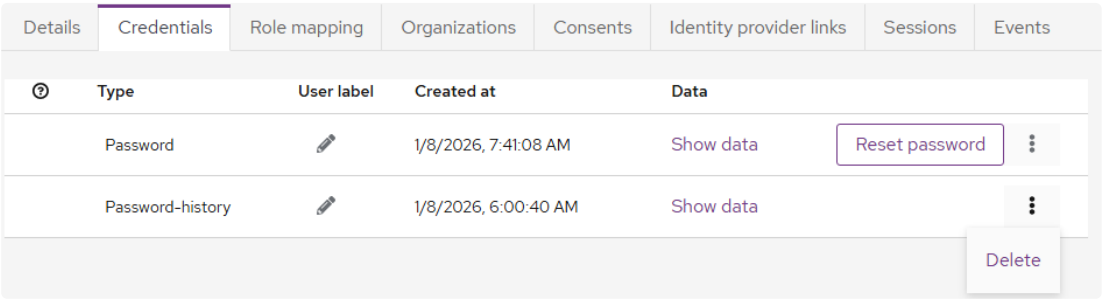


7. Browse or update the following user settings.
   - Credentials
   - Role mapping
   - Organizations
   - Consents
   - Identity provider links
   - Sessions
   - Events

Credentials

The user's login credentials.

- Click **Set password** to set the user login password
- Click **Credential Reset** to force a password change.
- Click the three horizontal dots for **Password** and select **Delete** to remove the password.
- Click the three horizontal dots for **Password-history** and select **Delete** to remove the password history.



See Authentication for details on the password policy requirements.

Role mapping

The list of Roles the user belongs to.

- Uncheck Hide inherited roles to display the roles inherited by the roles currently assigned to the user.
- Click **Assign Role** to grant a role to the user.
- Select a role and click **Unassign** to unassign.

Organizations

The organizations the user belongs to.

Consents

The consents granted by client applications, if any.

Identity provider links

The third-party identity providers allowing the user to authenticate in the administration console.

Sessions

A log record of the console sessions started by the user. See Sessions for a description of each field.

Events

A log record of the user and administrative events triggered by the user.

- Select the **User events** tab to display the details described in User events.
- Select the **Admin events** tab to display the details described in Admin events.

Deleting or disabling users

See below for deleting or disabling users.

Before deleting or disabling the initial `admin` user, ensure that you create a new user with the AdminRole role; otherwise, you will lose access to the system.

To delete or disable a user

1. Open the following URL in a Web browser.

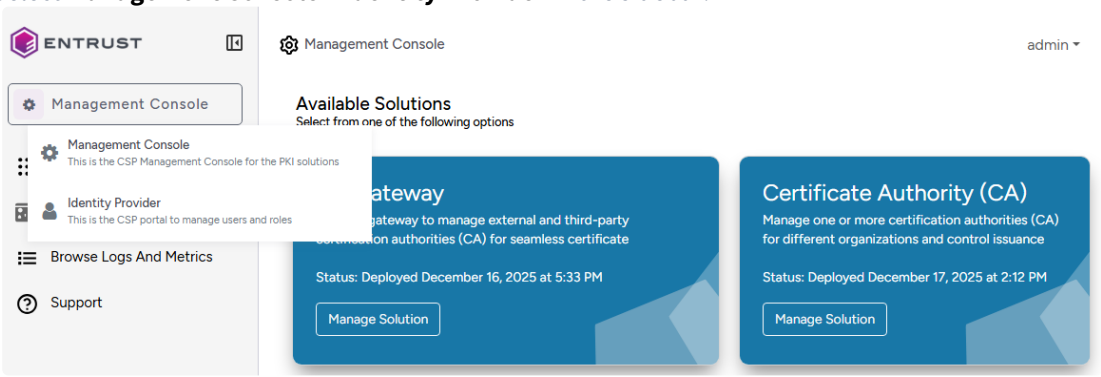
   ```
   https://<machine>:8443/management-console
   ```

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

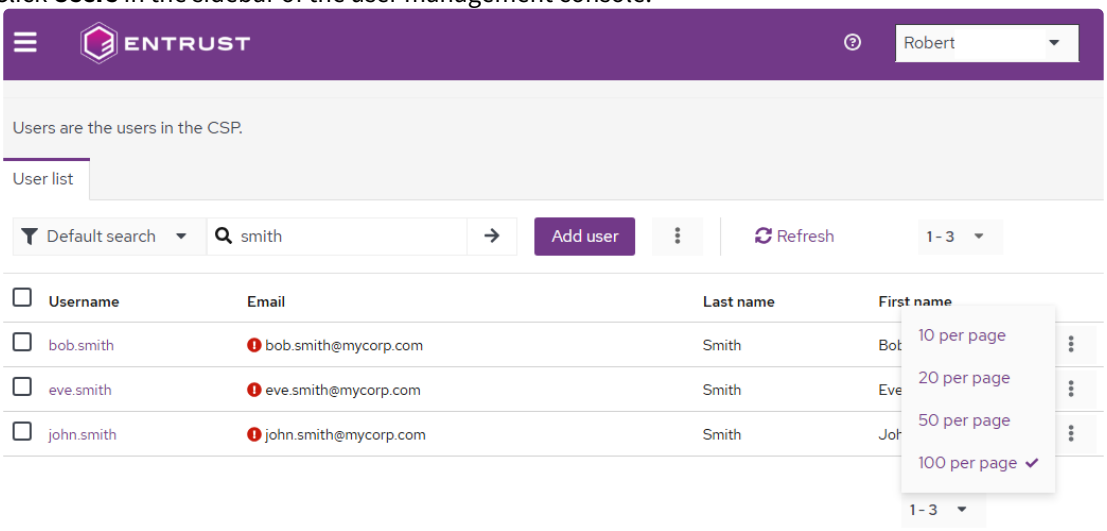
   This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a user with a role granting user management permissions – for example, the initial `admin` administrator user.

3. Select **Management Console > Identity Provider** in the sidebar.

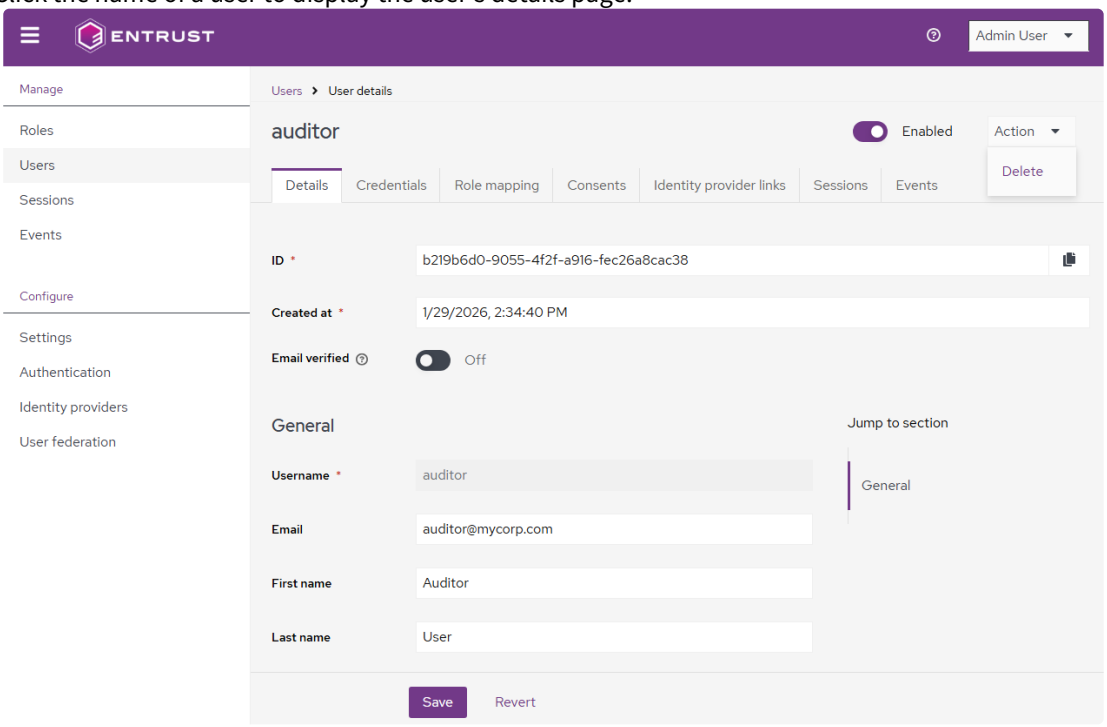


4. Click **Users** in the sidebar of the user management console.



5. Use the search options to filter users and select the number of users per page.

6. Click the name of a user to display the user's details page.



7. In the user's details page:
   - Turn off the **Enabled** toggle switch to disable the user.
   - Select **Action > Delete** to permanently remove the user.

Sessions

See below for browsing session logs.

To browse session logs

1. Open the following URL in a Web browser.

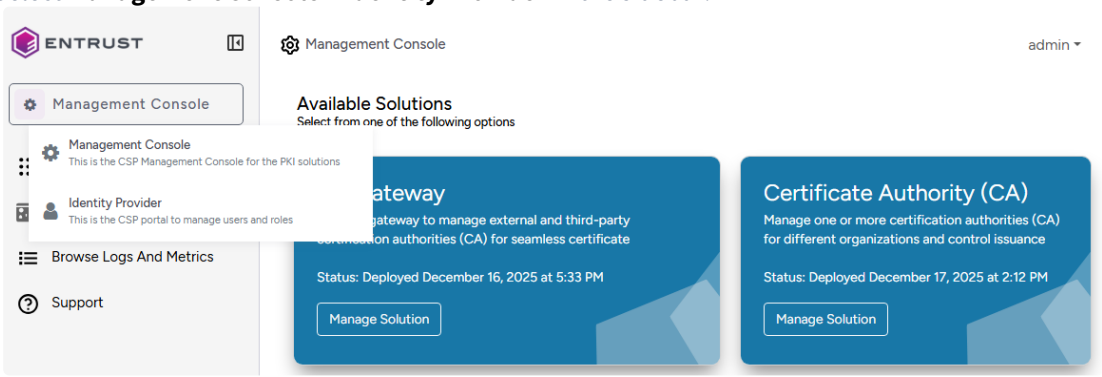
   ```
   https://<machine>:8443/management-console
   ```

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

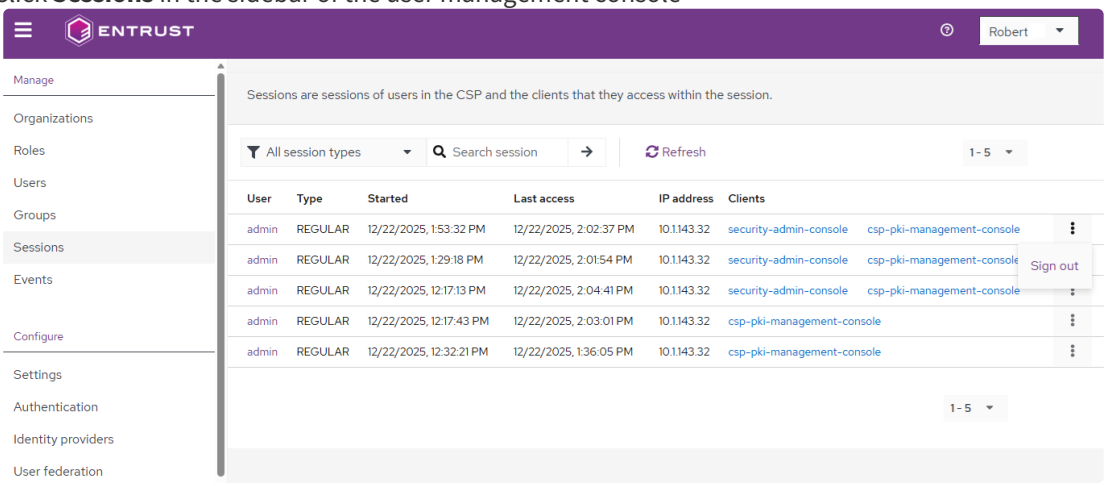
   > ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a user with a role granting user management permissions.

3. Select **Management Console > Identity Provider** in the sidebar.



4. Click **Sessions** in the sidebar of the user management console



5. Browse the following settings for each user session.
   - User
   - Type
   - Started
   - Last access
   - IP address
   - Client
6. Click the three dots for a session and select **Sign out** to terminate it.

User

The user login name.

Type

The session type.

Type	Description
REGULAR	The sessions was created using a standard access token

Type	Description
OFFLINE	The session is tied to an offline token

Started

The session start date and time.

Last access

The time and date of the last user activity during the session.

IP address

The IP address of the console.

Client

The client application that accessed the console.

Events

See below for browsing user session log records.

> See the Events section under Settings to manage event recording.

To browse session log records

1. Open the following URL in a Web browser.

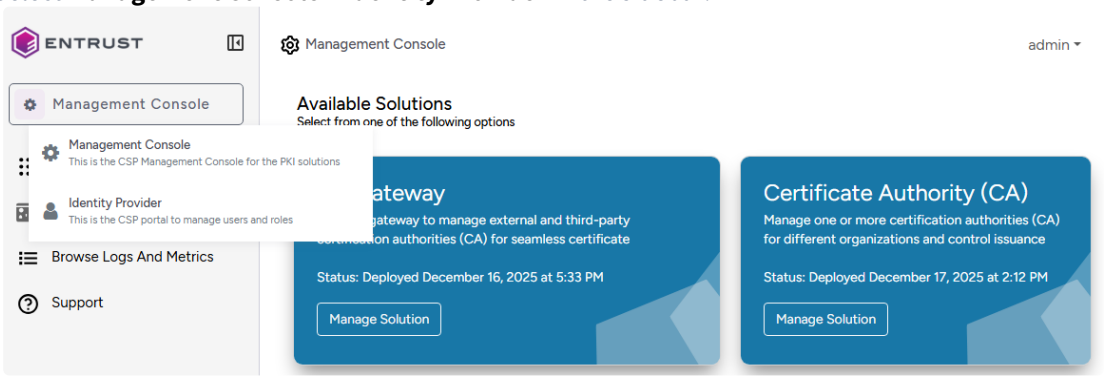
   ```
   https://<machine>:8443/management-console
   ```

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

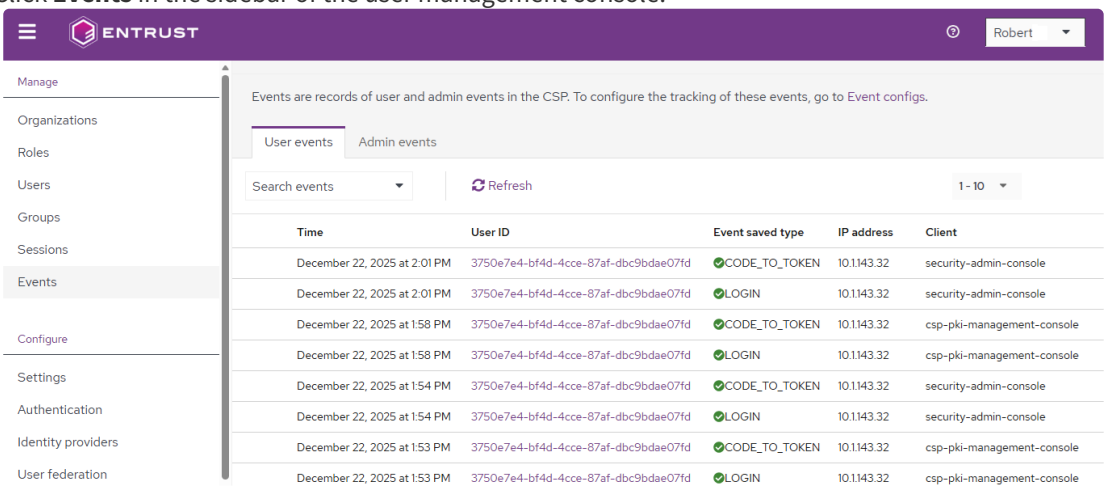
   > This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a user with a role granting user management permissions.

3. Select **Management Console > Identity Provider** in the sidebar.



4. Click **Events** in the sidebar of the user management console.



5. Browse the following event types.
   - User events
   - Admin events

User events

Select the **User events** tab to display the following details for each user event.

- Time
- User ID
- Event saved type
- IP address
- Client

Time

The timestamp when the event occurred.

User ID

The Cryptographic Security Platform internal identifier of the user associated with the event.

Event saved type

The type of saved event. See the table below for examples.

Type	Event
LOGIN	User login
REGISTER	User registration
UPDATE_PROFILE	Profile update
REMOVE_ROLE	Role removed from user or group

Each event is prefixed with ✅ on success and ❌ on error.

IP address

The IP address from which the event originated.

Client

The client application involved in the event.

Admin events

Select the **Admin events** tab to display the following details for each administrative event triggered by users.

- Time
- Resource path
- Resource type
- Operation type
- User

Select three horizontal dots for an administrative event and select:

- **Auth** to display the user authorization details.
- **Representation** to display the internal event representation.

> ℹ See the Events section under Settings to enable or disable the internal representation display.

Time

The timestamp when the event occurred.

Resource path

The path of the Cryptographic Security Platform resource affected by the administrative action, such as a client, user, or realm.

Resource type

The type of resource that was changed. See the table below for examples.

Type	Resource
GROUP	User group
USER	User
REALM_ROLE	Role
GROUP_MEMBERSHIP	User assignment to a group
REALM_ROLE_MAPPING	Role assignment to a user or group
ORGANIZATION_MEMBERSHIP	User assignment to an organization

Operation type

The type of operation on the resource. See the table below for examples:

Type	Operation
CREATE	Create resource
UPDATE	Modify resource
DELETE	Remove resource

User

The Cryptographic Security Platform internal identifier of the administrator responsible for the event.

Settings

See below for managing user management settings.

To manage settings

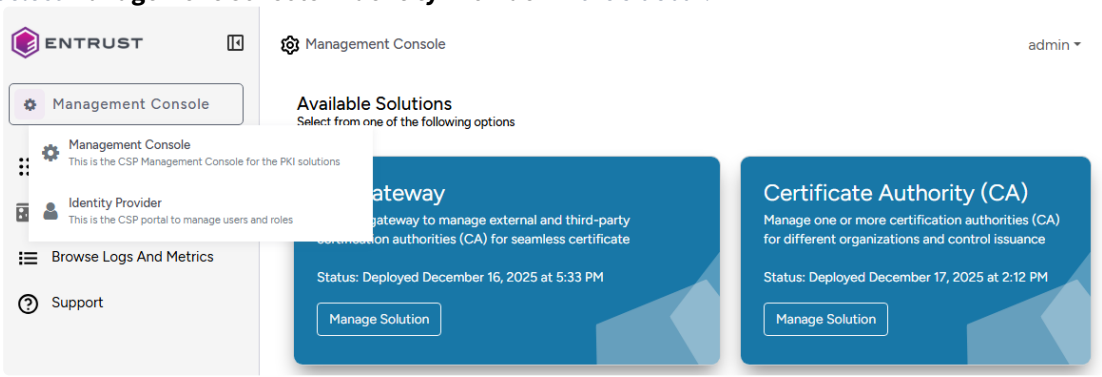
1. Open the following URL in a Web browser.

```
https://<machine>:8443/management-console
```

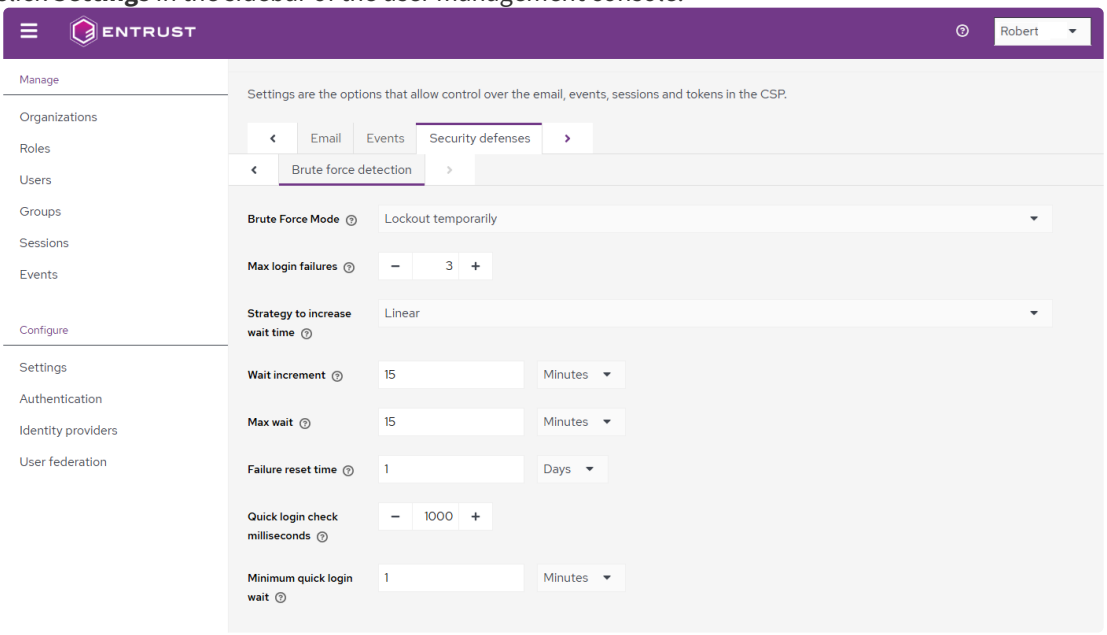
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

> ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a user with a role granting user management permissions.
3. Select **Management Console > Identity Provider** in the sidebar.



4. Click **Settings** in the sidebar of the user management console.



5. Browse or update the following settings.
   - Events
   - Security defenses
   - User registration

Events

Configure event recording.

- Event listeners
- User events settings
- Admin events settings

Event listeners

Select the components that will process and react to events generated by the system. Such as:

- User login or logout
- Registration
- Password reset
- Admin actions – for example: role assignment

User events settings

Configure the user events recording.

Field	Value
Save events	Enable this setting to continue recording user events; disable it to stop recording.
Expiration	Select the retention period for the user events logs.

Click:

- **Save** to save the updated settings
- **Clear user events** to clear the recorded user events
- **Add saved types** to add types of user events
- **Remove** to remove the selected user event type

Admin events settings

Configure the administrative events recording.

Field	Value
Save events	Enable this setting to continue recording administrative events; disable it to stop recording.
Include representation	Enable this setting to display the internal representation of each event; disable it to hide it.
Expiration	Select the retention period for the administrative event logs.

Click:

- **Save** to save the updated settings
- **Clear user events** to clear the recorded user events

Security defenses

Configure the protection against brute force login attacks.

- Brute force mode
- Max login failures

- Maximum temporary lockouts
- Strategy to increase wait time
- Wait Increment
- Max wait
- Failure Reset Time
- Quick login check milliseconds
- Minimum quick login wait

Brute force mode

The action to be performed when the maximum number of failed logins is exceeded.

Mode	Description	Default
Disabled	Turn off brute force protection (not recommended)	
Lockout Permanently	Permanently locks the user account after reaching Max Login Failures	✓
Lockout Temporarily	Locks the user account for a defined period after reaching Max Login Failures	
Lockout Permanently After Temporary Lockout	First, apply temporary lockouts after failed attempts. If the user exceeds Maximum temporary lockouts, permanently lock the account	

Max login failures

The maximum number of failed login attempts allowed before triggering the brute force defense.

Default value: 3

Maximum temporary lockouts

The maximum number of temporary lockouts a user can experience before a permanent lockout (when Brute Force Mode is **Lockout Permanently After Temporary Lockout**).

Default value: 1

Strategy to increase wait time

The added waiting time after repeated failures.

Option	Description	Default
Linear	Wait time increases by a fixed amount each time	✓
Multiple	Wait time grows exponentially with each failure	

Wait Increment

The base time added to the wait period after each failure.

Default value: 15 minutes

Max wait

The maximum wait time allowed between login attempts.

Default value: 15 minutes

Failure Reset Time

The time window after which the failure count resets if no new failures occur.

Default value: 1 day

Quick login check milliseconds

The time frame to detect rapid consecutive login attempts (in milliseconds). For example, if set to 1000, multiple attempts within a 1-second period are flagged as suspicious.

Default value: 1000 milliseconds

Minimum quick login wait

The minimum enforced wait time when detecting quick login attempts. For example, if set to 10 seconds, the user must wait at least 10 seconds before retrying after a rapid attempt.

Default value: 1 minute

User registration

Manage the list of default user roles, that is, the roles automatically assigned to new users. Click:

- **Hide inherited** roles to display the roles that the default roles inherit from.
- **Assign role** to add new default roles. See:
  - Role reference for the list of default roles
  - Creating roles for how to create new roles.
- **Unassign** to remove a role from the list of default roles.

Authentication

Configure the password authentication settings.

To password authentication settings.

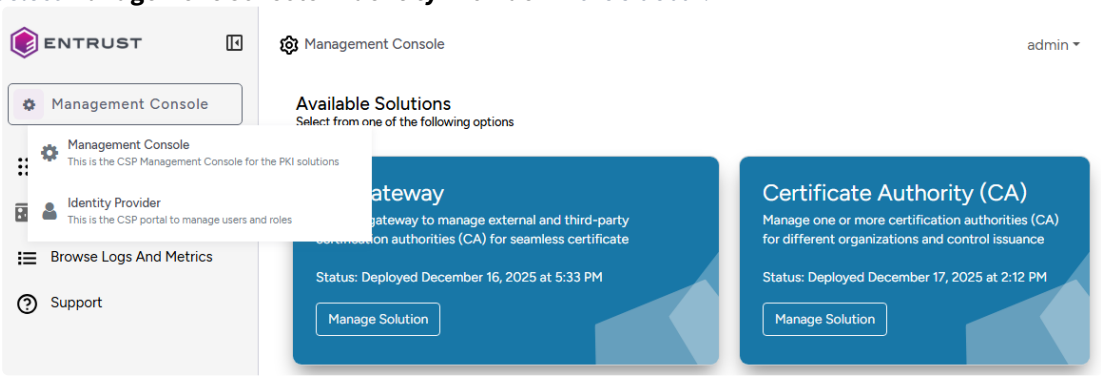
1. Open the following URL in a Web browser.

   ```
   https://<machine>:8443/management-console
   ```

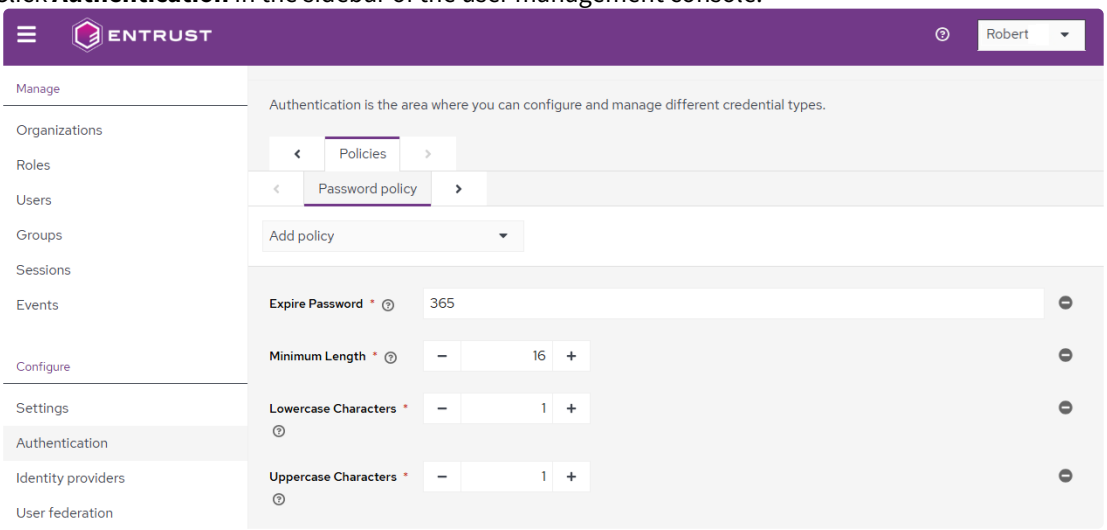
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

> ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a user with a role granting user management permissions – for example, the initial `admin` administrator user.
3. Select **Management Console > Identity Provider** in the sidebar.



4. Click **Authentication** in the sidebar of the user management console.



5. Configure the following password authentication settings.
   - Expire Password
   - Minimum Length
   - Lowercase Characters
   - Uppercase Characters
   - Not Contains Username
   - Special Characters
   - Not Recently Used
   - Maximum Authentication Age
   - Not Username
   - Not Email
   - Digits
6. Click **Save**.

Expire Password

The maximum age in days of a password.

Default value: 365

Minimum Length

The minimum number of characters required in the password.

Default value: 16

Lowercase Characters

The minimum number of lowercase letters required.

Default value: 1

Uppercase Characters

The minimum number of uppercase letters required.

Default value: 1

Not Contains Username

Whether the password can contain the username.

Option	Description	Default
On	user passwords cannot contain the username	✓
Off	User passwords can contain the username	

Special Characters

The Minimum number of required special characters, such as:

```
!@#$%
```

Default value: 1

Not Recently Used

The number of previous passwords used to prevent the reuse of recent passwords.

> See Browsing and updating users for removing the password history of a user.

Default value: 8

Maximum Authentication Age

The maximum time since the last authentication before requiring re-login.

Default value: 365

Not Username

Whether the password can match the username.

Option	Description	Default
On	The password cannot be exactly the same as the username	✓
Off	The password value can match the username	

Not Email

Whether the password can match the user's email address.

Option	Description	Default
On	The password value cannot be exactly the same as the user's email address	✓
Off	The password value can match the user's email address	

Digits

The minimum number of numeric digits required.

Default value: 1

Identity providers

See below for integrating the Cryptographic Security Platform with external OpenID or Entrust IDaaS identity providers.

To integrate an external identity provider

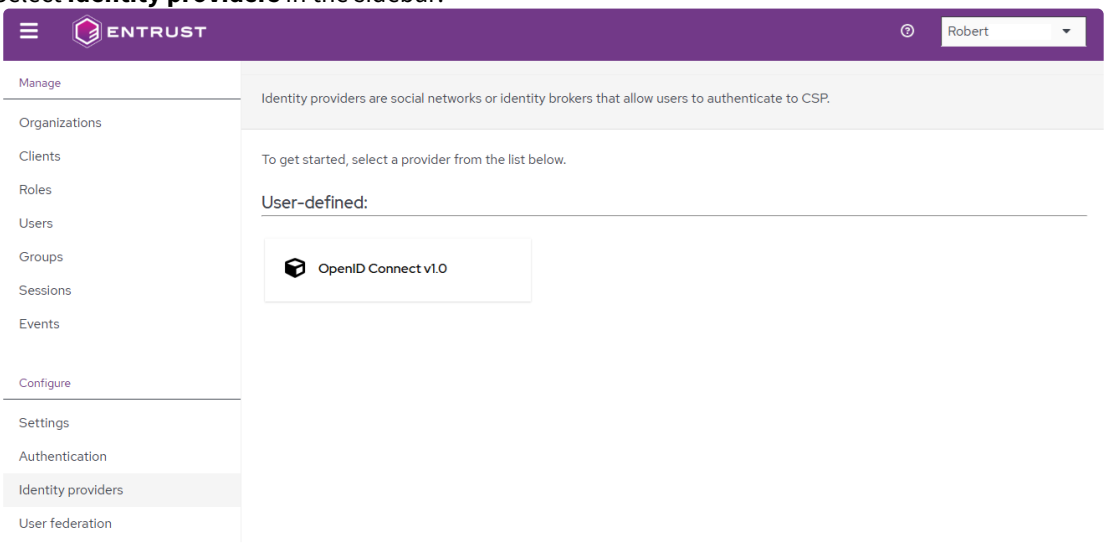
1. Open the following URL in a Web browser.

   ```
   https://<machine>:8443/management-console
   ```

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

   ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a user belonging to a role with identity provider management permissions – for example, the initial `admin` administrator user.
3. Select **Identity providers** in the sidebar.



4. Click **OpenID Connect v10**.
5. Configure the following settings.
    - Redirect URI
    - Alias
    - Display name
    - Display order
    - Use discovery endpoint
    - Authorization URL
    - Token URL
    - Logout URL
    - User Info URL
    - Token Introspection URL
    - Issuer
    - Validate Signatures
    - Use PKCE
    - Client authentication
    - Client ID
    - Client Secret
    - Client assertion signature algorithm
    - Client assertion audience
    - Add X.509 Headers to the JWT

Redirect URI

The callback URL where the external IdP instance will send the authentication response after the user logs in. This URI must match the one registered in the external IdP, and usually looks like:

```
https://<csp>:8443/identity/realms/end-users/broker/oidc/endpoint
```

Where `<csp>` is the domain or IP address of the Cryptographic Security Platform deployment.

Alias

A unique identifier for this identity provider configuration in Cryptographic Security Platform.

Display name

The name shown to users on the login page for this identity provider – for example:

```
Login with external identity provider
```

Display order

The position of this identity provider button on the login screen. Where:

- Lower numbers appear first.
- 1 is the top of the list.

Use discovery endpoint

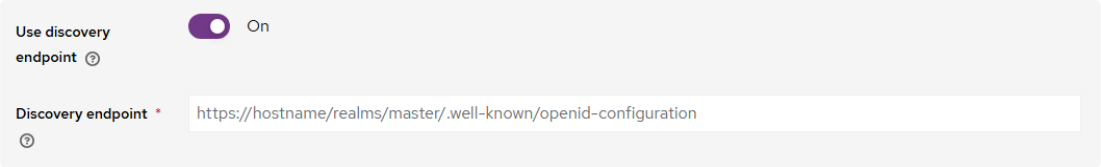
The status of the OpenID Connect discovery endpoint.

- Enabling the discovery endpoint
- Disabling the discovery endpoint

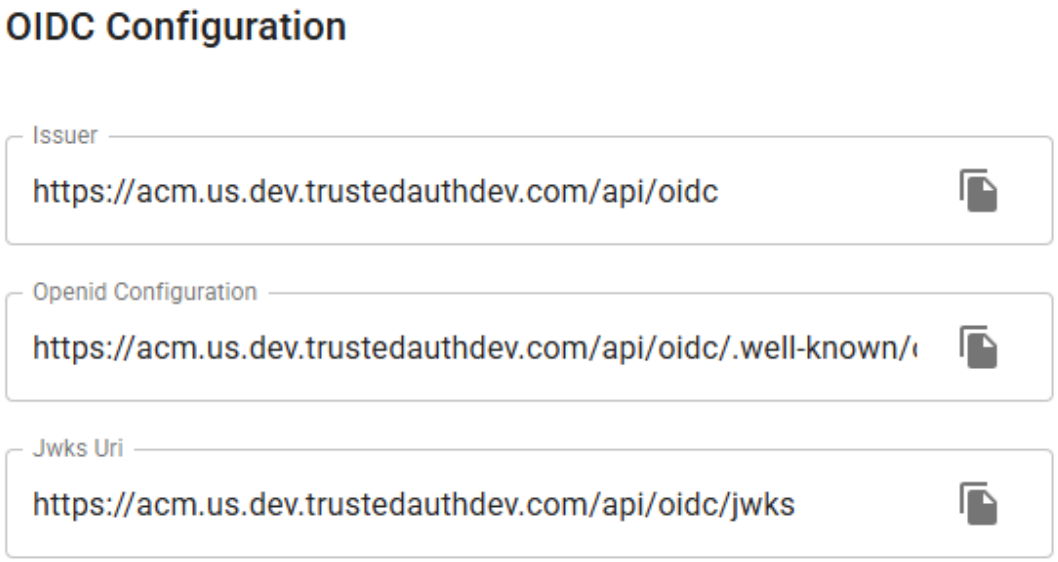
> With the discovery endpoint, clients and applications can automatically obtain configuration details about an identity provider without manual setup.

Enabling the discovery endpoint

If your identity provider supports discovery, enable the **Use discovery endpoint** setting and paste the base URL to the provider's OIDC discovery document in the **Discovery endpoint** field.



Specifically, to use Entrust IDaaS as an identity provider, paste the **OpenID Configuration** under the **OIDC Configuration** section.



Disabling the discovery endpoint

Disable the **Use discovery endpoint** setting in any of the following cases:

- The provider does not support discovery
- You want to override endpoints manually.

Authorization URL

The URL where the browser is redirected to start the OIDC authorization flow.

> Click **Show metadata** to display this advanced setting.

Token URL

The back-channel endpoint to exchange an authorization code for tokens, such as:

- ID token
- access token
- refresh token

> Click **Show metadata** to display this advanced setting.

Logout URL

The endpoint for RP-initiated logout at the provider. When users log out of your realm, Cryptographic Security Platform can ask the provider to end the session too.

Click **Show metadata** to display this advanced setting.

User Info URL

The endpoint Cryptographic Security Platform calls with the user's access token to retrieve profile claims, such as:

- email
- given_name
- family_name

Click **Show metadata** to display this advanced setting.

Token Introspection URL

The endpoint to validate or obtain metadata about an access token, such as:

- activation status
- scopes
- expiry

Click **Show metadata** to display this advanced setting.

Issuer

The exact issuer identifier of the provider, as the exact `iss` value of the incoming tokens.

Click **Show metadata** to display this advanced setting.

Validate Signatures

The token signature validation.

Option	Validation	Default
On	Validate the token signature against the provider's public keys	
Off	None	✓

Click **Show metadata** to display this advanced setting.

Use PKCE

The protection against code interception during the authorization flow.

Option	Protection	Default
On	Use Proof Key for Code Exchange (PKCE)	
Off	None	✓

Click **Show metadata** to display this advanced setting.

Client authentication

The method for Cryptographic Security Platform to authenticate in the provider's token endpoint.

Method	Authentication method
Client secret sent in the request body	Send the `client_id` and `client_secret` values in the POST body when calling the token endpoint
Client secret sent as HTTP Basic authentication	Send the `client_id` and `client_secret` values in the Authorization header using HTTP Basic
Client secret sent as HTTP Basic authentication without URL encoding (deprecated)	Deprecated because it can cause interoperability and security issues
JWT signed with client secret	JWT assertion signed with an HMAC-based client secret
JWT signed with private key	A JWT assertion signed with a private key (recommended)

Client ID

The client identifier registered on the external provider.

Client Secret

The client secret registered with the external identity provider.

Client assertion signature algorithm

The algorithm to sign the JWT client assertion when **Client authentication** is **JWT signed with private key**.

- ES256
- ES384
- ES512
- EdDSA

- HS256
- HS384
- HS512
- PS256
- PS384
- PS512
- RS256
- RS384
- RS512

⚠ The provider must accept the chosen algorithm, and your client must have a matching private key (with a corresponding public key certificate registered at the provider).

Client assertion audience

The audience of the JWT client assertion Cryptographic Security Platform sends the provider's token endpoint when **Client authentication** is **JWT signed with private key**,

The audience claim tells the provider who the token is intended for and is usually the Token URL of the provider – for example:

```
https://idp.example.com/realms/idp/protocol/openid-connect/token
```

Add X.509 Headers to the JWT

The X.509 header Cryptographic Security Platform adds to the signed JWT when **Client authentication** is **JWT signed with private key.**

Option	Header	Default
On	The certificate chain of the user's private key	
Off	None	✓

User federation

See below for federating an external LDAP user repository.

To federate an external LDAP user repository

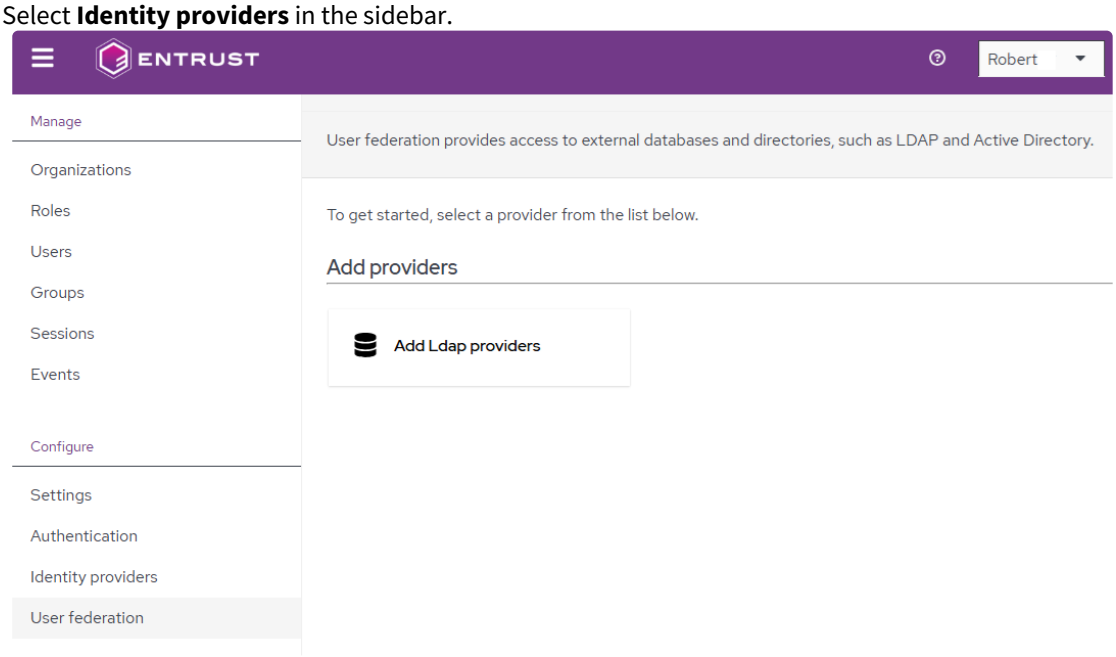
1. Open the following URL in a Web browser.

   ```
   https://<machine>:8443/management-console
   ```

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

> ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a user belonging to a role with identity provider management permissions – for example, the initial `admin` administrator user.
3. Select **Identity providers** in the sidebar.



4. Click **Add LDAP providers**.
5. Configure the following options.
    - General options
    - Connection and authentication settings
    - LDAP searching and updating
    - Synchronization settings
    - Kerberos integration
    - Cache settings (LDAP)
    - Advanced settings

General options

Configure the following settings.

- UI display name
- Vendor

UI display name

The LDAP server name in the Management Console

Vendor

The manufacturer of the LDAP server.

Vendor	Description
Active Directory	Microsoft Active Directory
Red Hat Directory Server	Red Hat Directory Server
Tivoli	IBM Tivoli Directory Server
Novell eDirectory	NetIQ eDirectory
Other	Generic LDAP configuration

Connection and authentication settings

Configure the following settings.

- Connection URL
- Enable StartTLS
- Use Truststore SPI
- Connection pooling
- Connection timeout
- Bind type
- Bind DN
- Bind credentials

When completing this configuration, click:

- **Test the connection** to check the connection settings.
- **Test authentication** to check the authentication settings.

Connection URL

The URL of the LDAP server – for example:

```
ldap://ldap.example.com:389
```

Enable StartTLS

Whether to enable StartTLS.

Option	Description
On	Enable StartTLS so that plain LDAP connections are updated to secure ones
Off	Disable StartTLS

Use Truststore SPI

The truststore for SSL/TLS certificate validation.

Option	Truststore
Always	The internal truststore
Always	A JVM truststore

Connection pooling

Whether to reuse LDAP connections.

Option	Description
On	Reuse LDAP connections instead of creating a new one for each request. This option creates a new connection for each request.
Off	Create a new connection for each request.

Connection timeout

The maximum waiting time (in milliseconds) to establish a connection to LDAP.

Bind type

The mechanism for authenticating on the LDAP server.

Option	Mechanism
Simple	DN (Distinguished Name) and password for authentication
SASL	SASL mechanisms (more secure)

Bind DN

The account to connect and perform operations in the LDAP server – for example:

```
cn=admin,dc=example,dc=com
```

⚠ The selected account must have sufficient privileges to read user attributes and to write changes (if synchronization is enabled).

Bind credentials

The password for the **Bind DN** account.

> ⚠ Store this password securely and periodically rotate it.

LDAP searching and updating

Configure the following settings

- Edit mode
- Users DN
- Relative user creation DN
- Username LDAP attribute
- RDN LDAP attribute
- UUID LDAP attribute
- User object classes
- User LDAP filter
- Search scope
- Read timeout
- Pagination
- Referral

Edit mode

The edit permissions on the LDAP server.

Mode	Permissions
READ_ONLY	Read LDAP users without modifying them
WRITABLE	Update LDAP attributes such as passwords and profiles
UNSYNCED	Imports users without syncing changes back to the LDAP server

Users DN

The base DN (Distinguished Name) to search for users in the LDAP tree – for example:

```
ou=users,dc=example,dc=com
```

Relative user creation DN

The sub-DN under **Users DN** for creating users when **Edit mode** is **WRITABLE** – for example:

```
ou=newusers
```

Username LDAP attribute

The LDAP attribute Cryptographic Security Platform will use as username – for example:

- uid
- sAMAccountName (when **Vendor** is **Active Directory**)

⚠ This field value must match the attribute that uniquely identifies users in Cryptographic Security Platform.

RDN LDAP attribute

The attribute used as Relative Distinguished Name when creating LDAP entries – for example:

- uid
- cn

⚠ This value determines how new LDAP entries are named.

UUID LDAP attribute

An attribute to uniquely identify LDAP entries – for example:

- entryUUID
- objectGUID (when **Vendor** is **Active Directory**)

ℹ This value ensures a stable mapping with the LDAP server.

User object classes

The LDAP object classes assigned to user entries – for example:

- inetOrgPerson
- organizationalPerson

ℹ This value defines a compliance schema for new LDAP users.

User LDAP filter

Additional LDAP filter for searching users – for example:

```
(memberOf=cn=KeycloakUsers,ou=groups,dc=example,dc=com)
```

ℹ This value restricts the LDAP users visible in Cryptographic Security Platform appliance.

Search scope

The scope of user searches under **Users DN**.

Option	Scope
ONE_LEVEL	Only immediate children
SUBTREE	Entire subtree

Read timeout

The maximum waiting time (in milliseconds) for LDAP read operations.

Pagination

Whether to enable pagination.

Optoin	Description
On	Enable LDAP paged results. Select his option for large directories with size limits, such as the default 1000 entries of Active Directory.
Off	Do not enable LDAP paged results.

Referral

The LDAP referral handling mode.

Option	Mode
FOLLOW	Follow referrals to other LDAP servers
IGNORE	Ignore referrals

Synchronization settings

Configure the following settings.

- Import users
- Sync Registrations
- Batch size
- Periodic full sync
- Periodic changed users sync
- Remove invalid users during searches

Import users

Whether to import users.

Option	Description
On	Create a local copy of the LDAP user for faster access and additional features, such as roles and groups
Off	Users remain only in LDAP, and Cryptographic Security Platform must query LDAP every time.

Sync Registrations

Whether to synchronize registrations.

Option	Description
On	Users registered in Cryptographic Security Platform are also created in LDAP
Off	Users registered in Cryptographic Security Platform are not additionally created in LDAP

Batch size

The number of users processed per batch during synchronization.

⚠ Large batch sizes speed up synchronization but increase memory usage.

Periodic full sync

Whether to periodically perform full user synchronizations with the LDAP server.

Option	Description	Default
On	Sync all LDAP users with the periodicity (in seconds) entered in the **Full sync period** field. For example, enter 86400 for a daily synchronization.	
Off	Do not periodically sync all LDAP users.	✓

Periodic changed users sync

Whether to periodically perform updated user synchronizations with the LDAP server.

Option	Description	Default
On	Sync the updated LDAP servers with the periodicity (in seconds) entered in the **Changed users sync period** field. For example, enter 86400 for a daily synchronization.	
Off	Do not periodically sync updated LDAP users.	✓

Remove invalid users during searches

Whether syncs must remove Cryptographic Security Platform users that no longer exist in LDAP.

Option	Description	Default
On	Remove Cryptographic Security Platform users that no longer exist in LDAP (recommended for consistency)	✓
Off	Do not remove Cryptographic Security Platform users that no longer exist in LDAP	

Kerberos integration

Configure the following settings.

- Allow Kerberos authentication
- Use Kerberos for password authentication

Allow Kerberos authentication

Whether to use SPNEGO/Kerberos-based authentication for users coming from LDAP.

Option	Description	Default
On	Users can log in using Kerberos tickets – for example, using browser SSO in a Windows domain	
Off	Users cannot log in using Kerberos tickets	✓

Use Kerberos for password authentication

Whether to validate user passwords against Kerberos instead of LDAP.

Option	Description	Default
On	Validate user passwords with Kerberos authentication rather than a simple LDAP bind	

Option	Description	Default
Off	Do not validate user passwords with Kerberos	✓

Cache settings

Select the periodicity for clearing the cache of authentication or user data retrieved from external sources, such as LDAP or Kerberos.

Policy	Periodicity
DEFAULT	After a reasonable period, to improve performance
EVICT_DAILY	Once every day
EVICT_WEEKLY	Once every week
MAX_LIFESPAN	After the number of milliseconds entered in the **Max lifespan** field
NO_CACHE	Never

Advanced settings

Configure the following settings.

- Enable the LDAPv3 password modify extended operation
- Validate password policy
- Trust Email
- Connection trace

When completing this configuration, click **Query Supported Extensions** to diagnose which LDAPv3 extended operations your LDAP server supports.

Enable the LDAPv3 password modify extended operation

The mechanism for updating passwords.

Option	Mechanism	Default
On	LDAPv3 Password Modify Extended Operation	
Off	Basic attribute update.	✓

Validate password policy

The password complexity check performed when setting or updating a password.

Option	Complecity check	Default
On	The password meets the requirements configured in Authentication	
Off	None	✅

Trust Email

The Cryptographic Security Platform trust on the email attribute from LDAP.

Option	Trust	Default
On	Mark LDAP-provided email addresses as verified	
Off	NOne	✅

Connection trace

The log level for LDAP operations.

Option	Log level	Default
On	Detailed (recommended for debugging and troubleshooting)	
Off	None (recommended for production)	✅

7 Managing CA Gateway

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

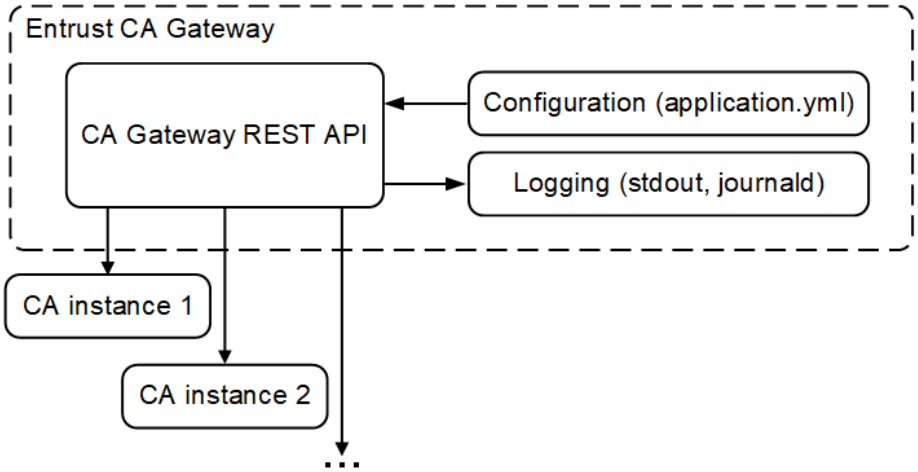
- CA Gateway architecture
- Obtaining the Gateway server certificate
- Integrating Certificate Authorities with CA Gateway
- Configuring and deploying CA Gateway
- Issuing public trust certificates with CA Gateway
- Administrating CA Gateway
- CA Gateway endpoints
- CA Capabilities reference

See Browsing logs with Grafana for how to browse Certificate Authority logs.

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

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

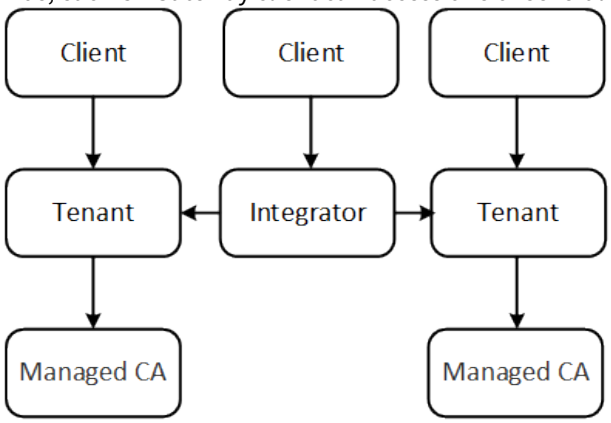
CA-specific plugins communicate with the underlying CAs through mutually authenticated TLS.

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 DigiCert CA
- Integrating a Microsoft CA
- Integrating an ECS CA
- Integrating an EJBCA CA
- Integrating an Entrust CA
- Integrating a Sectigo CA

Integrating a DigiCert CA

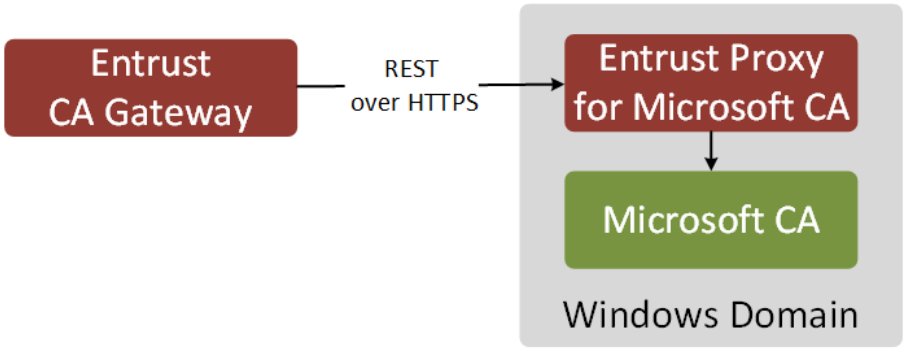
DigiCert CAs do not require preliminary integration steps. See Configuring and deploying CA Gateway for instructions on:

- Selecting and configuring the com.DigiCert connector.
- Add a certificate profile with the DigiCert CA Profile Properties.

See Digicert CA capabilities for a complete description of the operations supported by these CAs.

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.

- Adding Microsoft Management Console snap-ins
- Enabling supply in the request

- Configuring Request Handling in the Microsoft CA
- Enabling SAN attributes in the enrollment request
- Installing the Entrust Proxy for Microsoft CA
- Creating RA agents
- Issuing the SSL certificates
- Generating a client keystore for Entrust Proxy for Microsoft CA
- Generating a truststore for CA Gateway
- Generating the server keystore of the Entrust Proxy for Microsoft CA
- Running the Entrust Proxy for Microsoft CA

See Microsoft CA capabilities for a complete description of the operations supported by these CAs.

Only Microsoft Enterprise CA is supported; standalone CA is not supported.

Adding Microsoft Management Console snap-ins

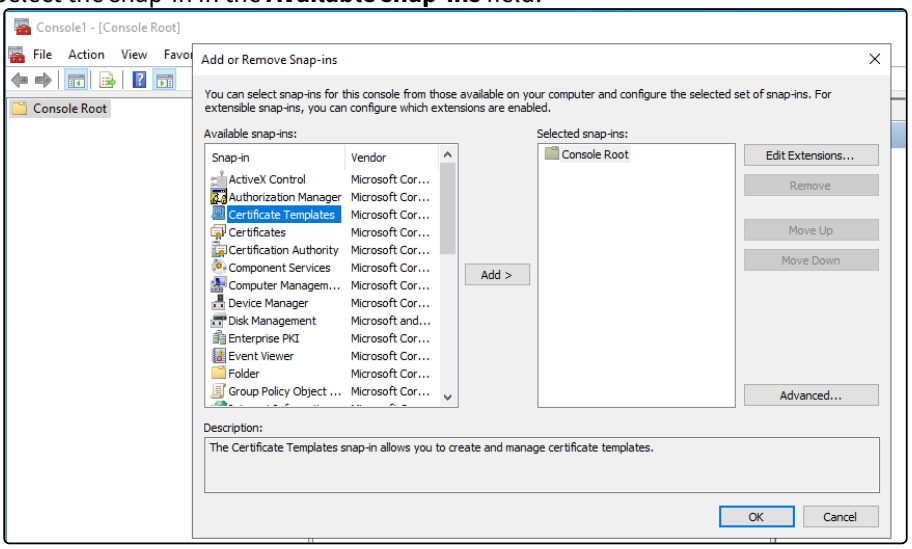
Run the Microsoft Management Console and add the following snap-ins.

- 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.



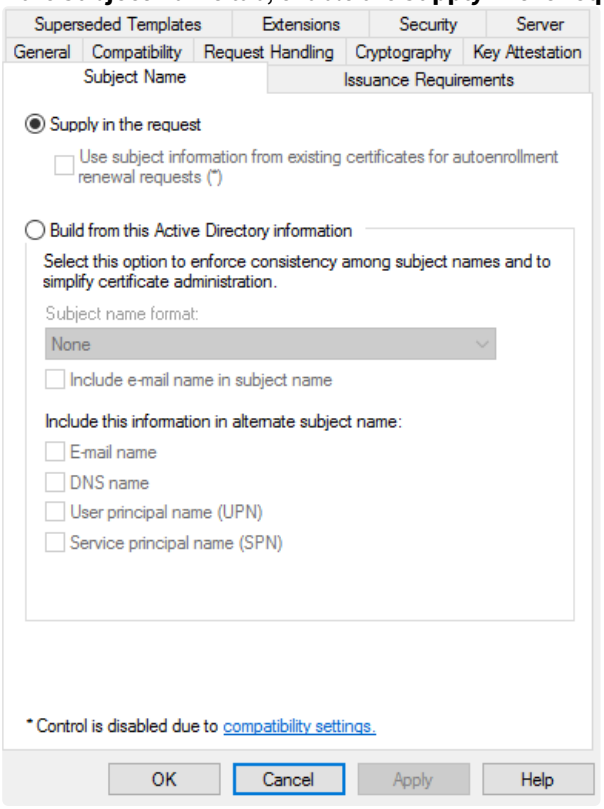
6. Click **Add** to include the snap-in in the **Selected snap-ins** field.
7. Click **OK.**

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.



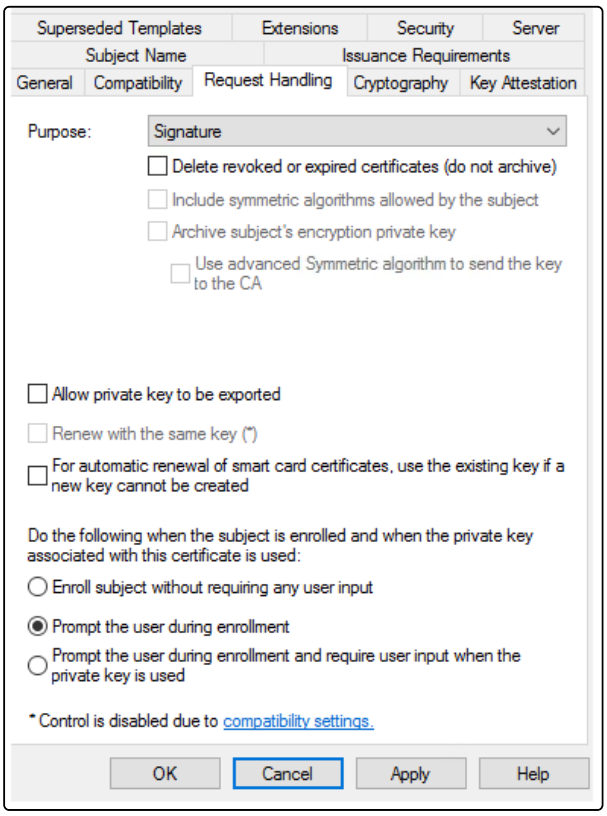
Configuring Request Handling in the Microsoft CA

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	

Parameter	Value
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.



Enabling SAN attributes in the enrollment request

Microsoft CA can be configured to allow Subject Alternative Name (SAN) values in enrollment requests and include them in the issued certificates.

- Security risks of allowing SAN fields in enrollment requests
- Enabling the Config_CA_Accept_Request_Attributes_SAN flag

⚠ If you don't enable this feature, you will lose the capability to extend the SAN attributes of the issued certificates with SAN from the certificate request.

Security risks of allowing SAN fields in enrollment requests

Allowing Subject Alternative Name (SAN) fields in enrollment requests creates a serious security risk. Once enabled, any certificate template may accept alternate names regardless of how the template defines the subject. An attacker could exploit this to obtain a certificate with an alternate name and impersonate another user.

For this reason, the CA must limit enrollment permissions to only trusted accounts. Specifically, the security model described in Installing the Entrust Proxy for Microsoft CA focuses on allowing only the Proxy Admin to have enrollment permission.

Enabling the Config_CA_Accept_Request_Attributes_SAN flag

If you want Microsoft CA to accept Subject Alternative Name (SAN) fields in enrollment requests, enable the following flag.

```
Config_CA_Accept_Request_Attributes_SAN
```

To enable Config_CA_Accept_Request_Attributes_SAN flag

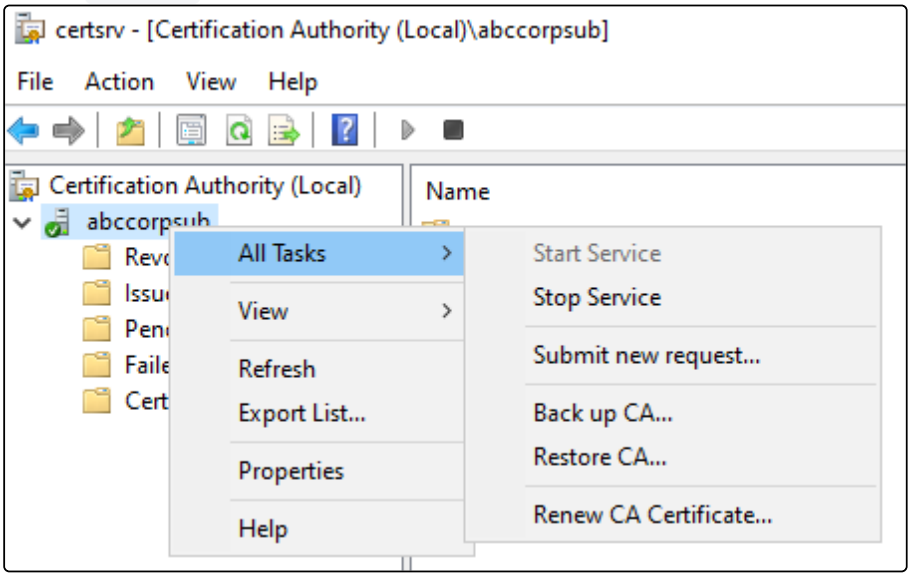
1. Log in to the Windows machine hosting the Microsoft CA server.
2. Run the `regedit` command to open the Registry Editor.
3. Select the following registry key (`<CA_CN>` is the Common Name of the Microsoft CA).

   ```
   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.

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
- Creating a Proxy Admin account
- Configuring the Windows domain account
- Adding the Windows domain account to the logon as a service policy
- Installing Java
- Downloading the Entrust Proxy for Microsoft CA installer
- Configuring logs
- Running the Entrust Proxy for Microsoft CA installer
- Uninstalling 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.

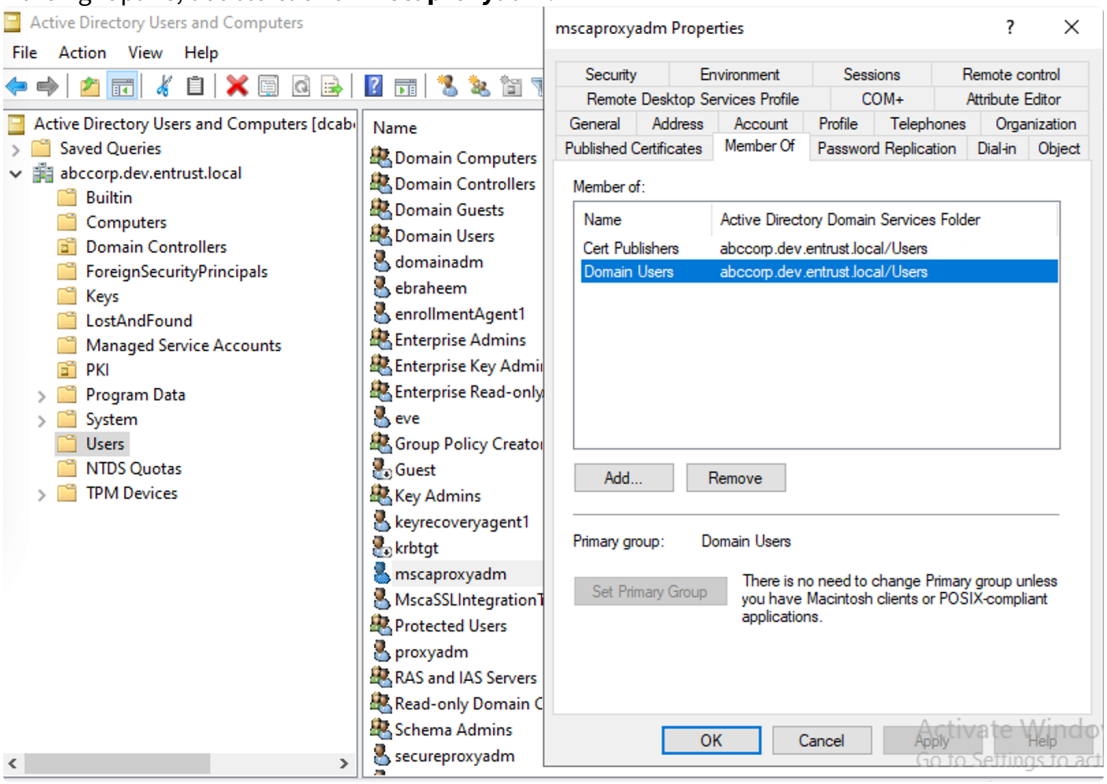
Creating a Proxy Admin account

Create a **Proxy Admin** user belonging to the **Cert Publishers** and **Domain User** groups.

To create a proxy admin user

1. Press **Win + R** to open the **Run** dialog.
2. Type `dsa.msc` and press Enter.
3. Select **Users** under the Windows domain

4. In the right pane, double-click on **mscaproxyadm**.



5. Create a **Proxy Admin** user
6. Add the users only to the **Cert Publishers** and **Domain User** groups.

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 domain user	Automatic (Delayed Start)	✓	✗

In either case, enable only the following user permissions.

- Issue and Manage Certificates
- Request Certificates
- Read

Adding the Windows domain account to the logon as a service policy

Add the new Windows account to the **Logon as a service** policy.

To add the Windows domain account to the logon as a service policy

1. Press **Windows + R** to open the **Run** window.

2. Type `secpol.msc` and press Enter.
3. In the **Local Security Policy** window, navigate to **Local Policies > User Rights Assignment**.
4. In the right pane, double-click on **Log on as a service**.
5. Click **Add User or Group**,
6. Select the account created in the previous section, Creating a Proxy Admin account
7. .
8. Click **OK**,
9. Click **Apply**.

Installing Java

Install Java on the machine that will host the Entrust Proxy for Microsoft.

To install Java

1. Log in using the account created in the previous section, Creating a Proxy Admin account.
2. Install one of the following LTS (Long Term Support) Java distributions.
   - Oracle Java x86_64 version 17
   - OpenJDK 17
   - AdoptOpenJDK 17
3. Set the `JAVA_HOME` environment to the Java installation path.
4. Extend the value of the `PATH` environment variable to:

```
%JAVA_HOME%\bin
```

5. Run the following command to check the Java version and architecture details.

```
java -XshowSettings:properties -version
```

Downloading the Entrust Proxy for Microsoft CA installer

Download and extract the Entrust Proxy for Microsoft CA installer files.

To download the Entrust Proxy for Microsoft CA installer

1. Log in trustedcare.entrust.com
2. Go to **PRODUCTS > Cryptographic Security Platform**
3. Select the latest version.
4. Click the download link of the Entrust Proxy for Microsoft CA.
5. Unzip the compressed file contents to your selected installation directory on the Windows machine – for example, in `c:\mscaproxy`

> ⚠ Installing into `c:\Program Files` may not be functional due to Windows privilege enforcement.

Configuring logs

Optionally, edit the configuration files to modify the default log recording settings.

Configuration file	Parameter	Value
MSCAProxy.xml	logpath	The folder where to save logs.
config\application.yml	com.entrust.mscaproxy	The supported log levels. Supported values in increasing severity are `TRACE`, `DEBUG`, `INFO`, `WARN`, `ERROR`, `FATAL` and `OFF.`

> If you edit these pages after starting Entrust Proxy for Microsoft, run the `MSCAProxy.exe restart` command to restart it.

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

See below for running the Entrust Proxy for Microsoft CA installer and registering the Entrust Proxy for Microsoft CA as a Windows service.

To run the Entrust Proxy for Microsoft CA installer

1. Log in to a Windows machine as the Proxy Admin user (created in section Creating a Proxy Admin account).
2. Run the following command.

   ```
   MSCAProxy.exe install /p
   ```

3. When prompted, type the `<domainName>` domain name and the `<proxyAdminUserName>` Proxy Admin username. Supported formats are:
   - User Principal Name (UPN) – for example: `<domainName>@<proxyAdminUserName>`
   - The Down-Level Logon Name – for example: `<domainName>\<proxyAdminUserName>`
4. Type the password of the Proxy Admin user.
5. Type "y" to allow the log-on as a service.

   > The installer does not wait for you to press the **Enter** key.

Uninstalling the Entrust Proxy for Microsoft CA

Run the following command as an administrator in case you want to uninstall the Entrust Proxy for Microsoft CA.

```
MSCAProxy.exe uninstall
```

Creating RA agents

Create RA recovery and enrollment agents as explained below.

- Creating the CA enrollment agents
- Creating the RA recovery agents
- Creating RA enrollment agents

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

> 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**.

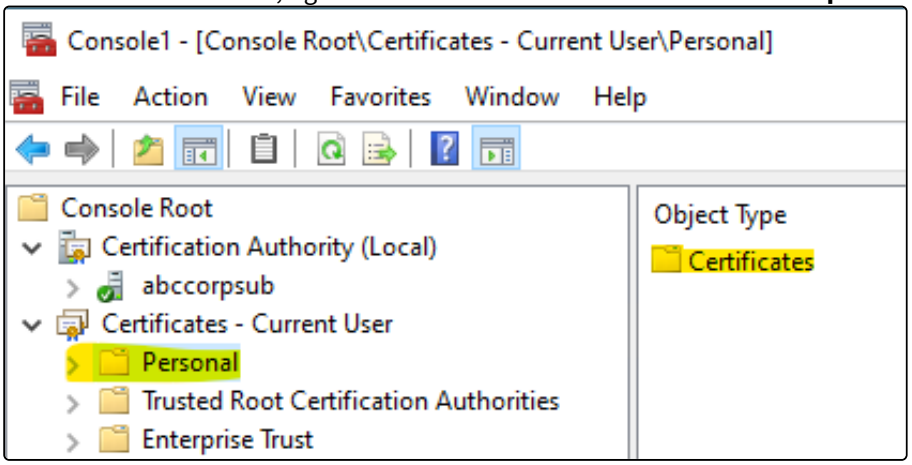
Creating an enrollment certificate for the CA Administrator

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 in to 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 **All 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 users and user groups.

Permission	Authenticated user	Proxy Admin
Full Control		
Read	✓	✓
Write		
Enroll		✓
Autoenroll		

Creating RA enrollment agents

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 users and user groups.

Permission	Authenticated user	Proxy Admin
Full Control		
Read	✓	✓
Write		
Enroll		✓
Autoenroll		

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 Entrust Proxy for Microsoft CA

Generate a keystore containing:

- The private key of Entrust Proxy for Microsoft CA for client authentication.
- The key's certificate.
- The certificate's chain.

See below the required steps.

- Creating a client authentication template for Microsoft CA
- Certifying a client key pair for Entrust Proxy for Microsoft CA
- Importing a key pair and a certificate in the client keystore for Entrust Proxy for Microsoft CA
- Deleting temporary files of the client keystore Entrust Proxy for Microsoft CA

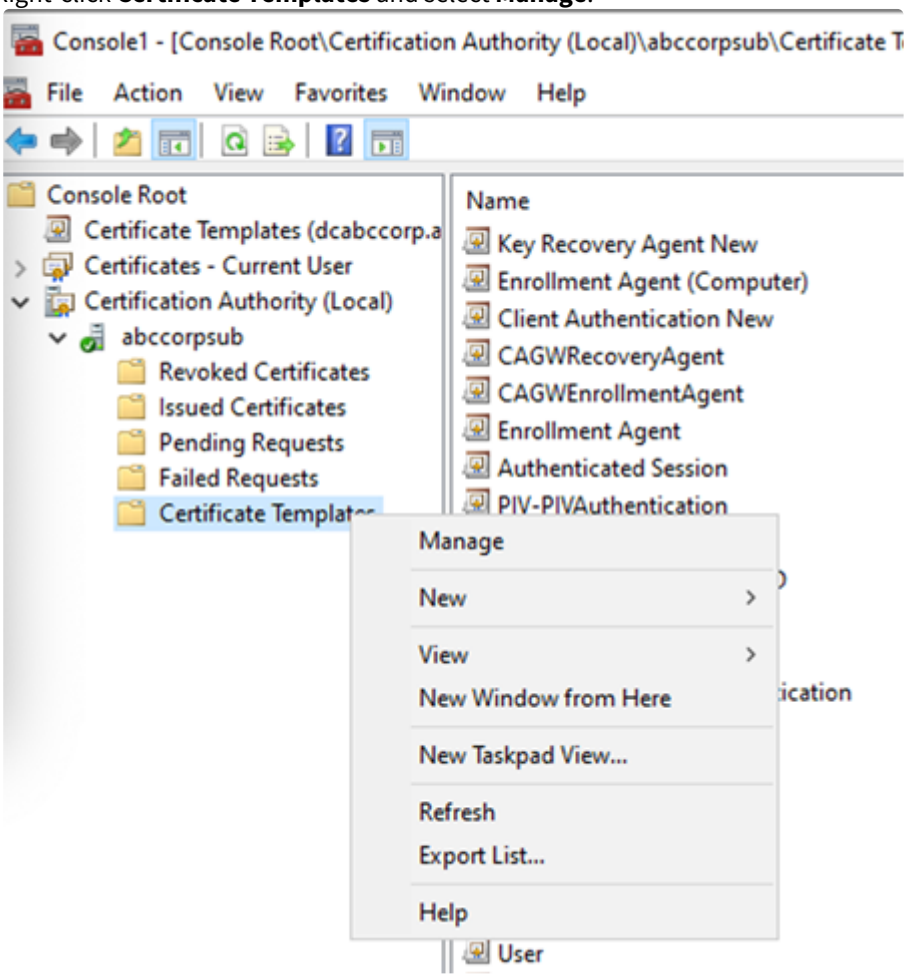
When configuring CA Gateway, you will later assign the path of this file to the Client Certificate Keystore File setting.

Creating a client authentication template for Microsoft CA

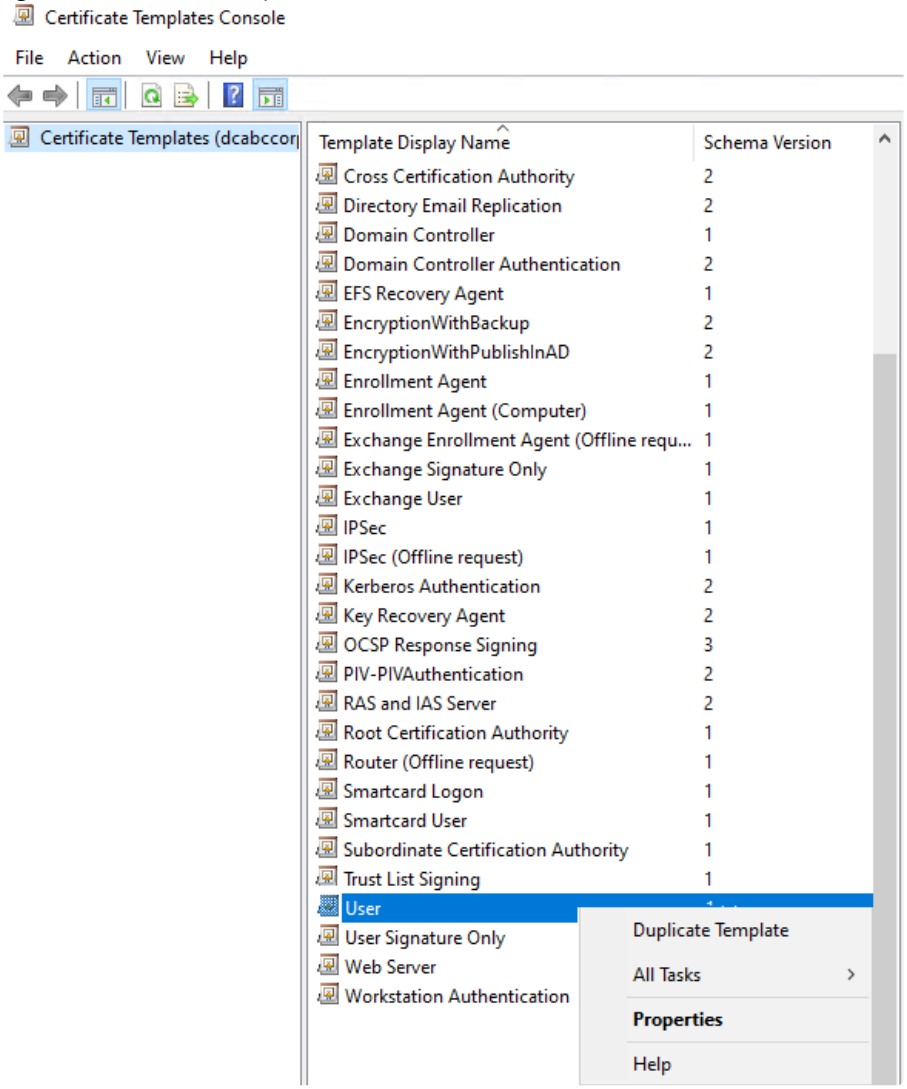
Create an authentication template for generating the client keystore. For example, you can copy an existing template and configure it as explained below.

To create a client authentication template for Microsoft CA

1. Log in to the Microsoft CA server machine.
2. Press **Win + R** to open the **Run** dialog.
3. Type "mmc" and press Enter to open the Microsoft Management Console.
4. Go to **Certificate Authority**.
5. Right-click **Certificate Templates** and select **Manage**.



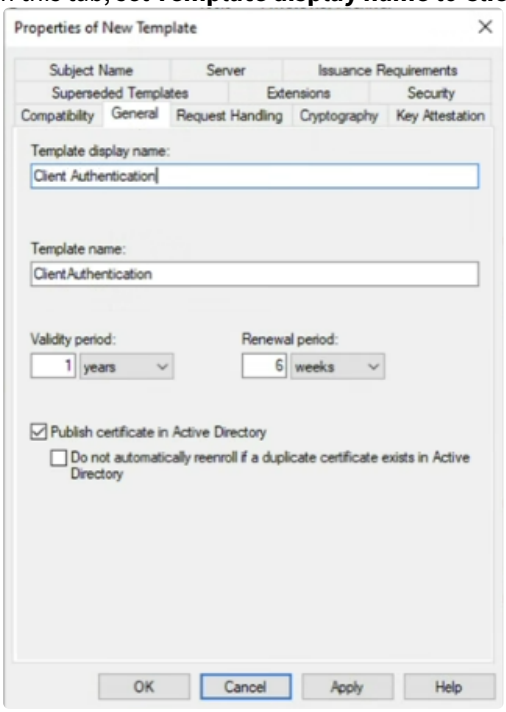
6. Right-click the **User** template and select **Duplicate Template**.



7. In the template properties dialog, configure the settings described below.
    - General
    - Security
    - Subject Name
    - Extensions
8. Click **OK** to close the dialog.
9. Go to **Certificate Authority.**
10. Right-click **Certificate Templates** and select **New >Certificate Template to Issue**.
11. Select **Client Authentication** from the list.

General

In this tab, set **Template display name** to **Client Authentication**.



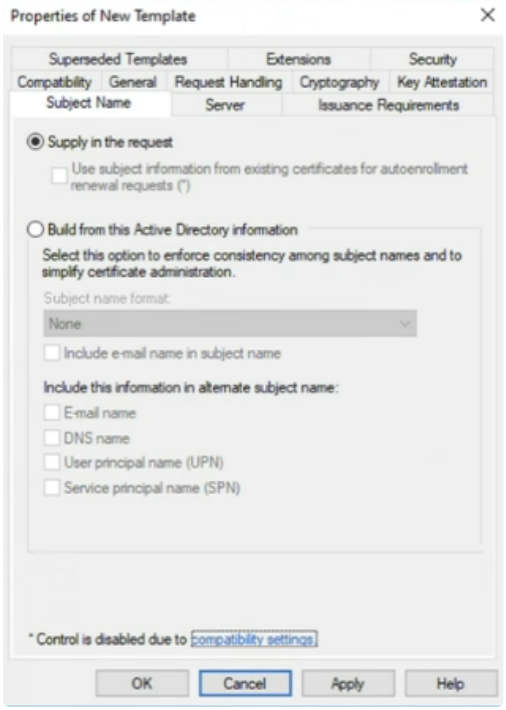
Security

In this tab:

- Grant necessary permissions to a user group – for example, click **Read**, **Write**, **Enroll** for the **Domain Admins** group.
- Deselect the **Write** and **Enroll** permissions from the **Authenticated Users** group.
- Remove unnecessary groups.

Subject Name

In this tab, enable the **Supply in request** radio button.



Click **OK** to close the warning pop-up message.

Extensions

In this tab**,** edit **Application Policies** and remove:

- Encrypting File System
- Secure Email

Certifying a client key pair for Entrust Proxy for Microsoft CA

In a temporary directory under the Microsoft Proxy Server, run the following commands to generate and certify a key pair.

Generate a key pair and keystore

```
keytool -genkey -noprompt -alias <alias> -dname <dname> -keyalg <keyalg> -keysize
<keysize> -keystore <keystore> -storepass <storepass> -keypass <keypass>
```

Generate a Certificate Signing Request (CSR)

```
keytool -certreq -alias <alias> -file <file> -keystore <keystore> -storepass
<storepass>
```

Submit CSR to Microsoft CA and get certificate chain

```
certreq.exe -f -attrib "<atrib>" -config "<host>\<CA>" <file> CertChainFileOut
<CertChainFileOut>
```

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
<alias>	A label for the new keystore
<attrib>	The name of the template described in Creating a client authentication template for Microsoft CA.
<ca>	The CA name assigned to the Microsoft CA in CA Gateway.
<dname>	The distinguished name of the key pair holder
<file>	The path of the generated certificate request
<host>	The Microsoft CA's hostname
<keyalg>	The algorithm for generating the key pair
<keypass>	The password for protecting the key pair withing the keystore
<keysize>	The size of the generating keys
<keystore>	The path of the generated keystore
<storepass>	The password for protecting the keystore

For example:

Generate a key pair and keystore

```
keytool -genkey -noprompt -alias mscaproxyclient -dname "cn=mscaproxy client" -keyalg
RSA -keysize 2048 -keystore mscaproxyclient.jks -storepass ***** -keypass *****
```

Generate a Certificate Signing Request (CSR)

```
keytool -certreq -alias mscaproxyclient -file mscaproxyclient.csr -keystore
mscaproxyclient.jks -storepass *****
```

Submit CSR to Microsoft CA and get certificate chain

```
certreq.exe -f -attrib "CertificateTemplate:ClientAuthentication" -config
"<HOST>\<CA>" mscaproxyclient.csr CertChainFileOut mscaproxyclient.p7b
```

Importing a key pair and a certificate in the client keystore for Entrust Proxy for Microsoft CA

Import into a keystore the certificate and the keys generated when Certifying a client key pair for Entrust Proxy for Microsoft CA.

```
keytool -import -noprompt -alias <alias> -file <file> -keystore <keystore> -storepass
<storepass>
```

Import the keys and the certificate into the keystore.

Option	Value
<alias>	The keystore `<alias>` selected when Certifying a client key pair for Entrust Proxy for Microsoft CA
<file>	The `<CertChainFileOut>` file path of the certificate chain obtained when Certifying a client key pair for Entrust Proxy for Microsoft CA
<keystore>	The `<keystore>` file path of the keystore generated when Certifying a client key pair for Entrust Proxy for Microsoft CA
<storepass>	The <storepass> keystore password selected when Certifying a client key pair for Entrust Proxy for Microsoft CA

```
keytool -import -noprompt -alias mscaproxyclient -file mscaproxyclient.p7b -keystore
mscaproxyclient.jks -storepass *****
```

Deleting temporary files of the client keystore Entrust Proxy for Microsoft CA

Delete the temporary files created in the previous sections. For example:

```
del mscaproxyclient.csr
```

```
del mscaproxyclient.p7b
```

Generating a truststore for CA Gateway

- Creating the SSL directory
- Importing the CA certificates

You need a truststore containing the CA chain for validating the Entrust Proxy for Microsoft CA's connection during tls handshake. This is a chain of CA certs which has issued the server certificate of Entrust Proxy for Microsoft CA.

> ⚠ The following instructions create a Java KeyStore (JKS) with the Java `keytool` command line utility. Consider using a more secure PKCS#12 type instead.

Creating the SSL directory

Create an SSL directory under the Entrust Proxy for Microsoft CA installation. For example:

```
c:\mscaproxy\ssl
```

Importing the CA certificates

In the SSL directory, run the following command to include the certificate of the root CA and all the intermediate CAs. See below for a description of each parameter.

```
keytool -import -noprompt -alias <alias> -file <file> -keystore <keystore> -storepass
<storepass>
```

See below for a description of each parameter.

Option	Value
<alias>	The alias of the CA in CA Gateway
<file>	The path of the CA certificate file
<keystore>	The path of the truststore file
`<storepass>`	The password of the trustore

For example:

```
keytool -import -noprompt -alias myca -file myca.crt -keystore truststore.jks
-storepass ****
```

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 Entrust Proxy for Microsoft CA

⚠ 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 Entrust Proxy for Microsoft CA

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 start, stop, and restart 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 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 ECS CA capabilities 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 EJBCA CA

This section explains how to configure CA Gateway for integrating Enterprise Java Beans Certificate Authorities (EJBCAs).

- Configuring and issuing the EJBCA client certificate
- Configuring client EJBCA authorization
- Enabling EJBCA API protocols
- Configuring SANs in EJBCA certificates
- Verifying the EJBCA server SSL certificate
- Enabling EJBCA dynamic profile generation

See the EJBCA capabilities for a complete description of the operations supported by these CAs.

Configuring and issuing the EJBCA client certificate

CA Gateway requires a client authentication certificate to authenticate in the EJBCA's APIs.

- Creating an EJBCA certificate profile
- Creating an EJBCA entity profile

- Issuing the EJBCA client certificate
- Downloading the EJBCA certificate chain

> See https://docs.keyfactor.com/how-to/latest/quick-start-issue-client-authentication-certificat for a more detailed description of the operations below.

Creating an EJBCA certificate profile

If no certificate profile exists for the client certificate, create one as explained below.

To create a certificate profile for the client certificate

1. Log in to the EJBCA administration GUI.
2. Navigate to **CA Functions > Certificate Profiles**.
3. Create a new profile or clone an existing one.
4. Assign the following settings to the profile.
    - Validity or end date of the certificate
    - Type
    - Available Key Algorithms
    - Key Usage
    - Extended Key Usage
5. Click **Save**.

Validity or end date of the certificate

Select an appropriate period, for example: **1y**.

Type

Select **End Entity**.

Available Key Algorithms

Select RSA algorithms with 2048 bits or higher.

Key Usage

Select **Digital Signature**.

Extended Key Usage

Select **Client Authentication** (TLS Web Client Authentication)

Creating an EJBCA entity profile

If no end-entity profile exists for the client certificate, create one as explained below.

To create an end entity profile for the client certificate

1. Log in to the EJBCA administration GUI.
2. Navigate to **RA Functions > End Entity Profiles.**
3. Create a new profile or clone an existing one.
4. Assign the following settings to the profile.
    - Available CAs
    - Available Certificate Profiles
    - Subject DN Attributes
    - Default Certificate Profile

5. Click **Save**.

Available CAs

Select **ManagementCA**.

Available Certificate Profiles

Select the certificate profile described in Creating an EJBCA certificate profile.

Subject DN Attributes

Select the required Distinguished Name (DN) attributes.

> ⚠ You must enter at least the `CN` attribute value.

Default Certificate Profile

Select the certificate profile described in Creating an EJBCA certificate profile.

Issuing the EJBCA client certificate

Issue the client authentication certificate for CA Gateway to authenticate in the EJBCA's APIs.

To issue the client authentication certificate

1. Log in to the EJBCA administration GUI.
2. Navigate to **Enroll > Make New Request.**
3. Assign the following settings to the new certificate request.
   - Certificate Type
   - CA
   - Available Key Algorithms
   - Subject DN
4. Select the **PKCS#12** certificate format.
5. Set a password for the PKCS#12 file.
6. Click **Download PKCS#12**.
7. When configuring the EJBCA properties, provide the path and password of this PKCS#12 file.

Certificate Type

Select the profile described in Creating an EJBCA entity profile.

CA

Select **ManagementCA**.

Available Key Algorithms

Select RSA algorithms with 2048 bits or higher.

Subject DN

The Distinguished Name (DN) for the administrator – for example:

```
CN=CAGW Admin,O=Your Organization
```

Downloading the EJBCA certificate chain

Download a trust store containing the CA certificate chain of the client authentication certificate.

To issue the client authentication certificate

1. Log in to the EJBCA administration GUI.
2. Navigate to **CA Certificates and CRLs.**
3. In the **Certificate chain** column of the **ManagementCA** row, select **JKS**.
4. Click **Download**.

> When configuring the EJBCA Profile Properties, you must provide the path to the downloaded trust store file.

Configuring client EJBCA authorization

Grant permissions to the holder of the EJBCA client authorization certificate.

To configure client authorization

1. Log in to the EJBCA administration GUI.
2. Navigate to **System Functions > Roles and Access Rules**.
3. Click **Add** to create a new one.
4. Configure the following role settings.
   - Members
   - Access Rules

Members

Click **Members** and configure the following properties.

Settings	Value
Match with	Select either **X.509 Certificate Serial Number** or **X.509: CN, Common name**.
Match value	Enter the serial number or Common Name (CN) of the certificate described in Issuing the EJBCA client certificate.
CA	Select **ManagementCA** – that is, the same CA that issued the certificate described Issuing the EJBCA client certificate.

Access Rules

Click **Access Rules** and configure the following properties.

Settings	Value
Authorized CAs	Select only the certificate authorities to which role holders should have access. Do not select the ManagementCA authority.

Settings	Value
End Entity Profiles	Select only the end entity profiles that should be available. Ensure that each end-entity profile has certificate profiles and CAs configured.

Enabling EJBCA API protocols

Enable the required protocols for CA Gateway to consume the EJBCA's APIs.

To enable EJBCA API protocols

1. Log in to the EJBCA Administrator GUI.
2. Navigate to **System Configuration > Protocol Configuration > Enabled or disable protocol access**.
3. Enable the following protocols:
    - REST Certificate Management
    - REST Certificate Management V2
    - Web Service
4. Click **Save**.

Configuring SANs in EJBCA certificates

Follow the steps below if you need to support Subject Alternative Names (SANs) in issued certificates.

To configure Subject Alternative Names

1. Log in to the EJBCA administration GUI.
2. Navigate to **RA Functions** > **End Entity Profiles**
3. Select the End Entity Profile you want to configure
4. In the **Subject Alternative Name** section, add the SAN types you wish to support – for example:
    - DNS Name
    - IP Address
    - RFC 822 Name (Email)
    - URI
    - UPN (User Principal Name)
5. Configure the **Required**, **Modifiable**, and **Validation** fields for each type.
6. Click **Save.**

Verifying the EJBCA server SSL certificate

Check that the EJBCA server SSL certificate is properly configured. That is:

- Can be validated using the trust store described in Downloading the EJBCA certificate chain.
- Includes the EJBCA server hostname in the Common Name (CN) or SAN (Subject Alternative Names) fields.

Enabling EJBCA dynamic profile generation

When Enable CA Profile Sync parameter is set to `true`, CA Gateway synchronizes EJBCA profiles as explained below.

1. CA Gateway queries EJBCA certificate authorities for End Entity Profiles and Certificate Profiles.
2. CA Gateway combines each End Entity Profile with its corresponding Certificate Profiles.

> Each generated profile is defined by a combination of an End Entity Profile identifier and a Certificate Profile identifier.

3. CA Gateway checks its configuration for profiles where the End Entity Profile and Certificate Profile values match the identifiers of an EJBCA-generated profile.
    - If a profile exists, CA Gateway uses the EJBCA-generated profile to complete only the missing profile settings. As manually set values always take precedence.
    - If the profile does not exist, CA Gateway uses the EJBCA-generated profile to create a new profile.
4. On certificate enrollment, requested properties also take precedence over EJBCA profile settings.

Integrating an Entrust CA

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
- Enabling Entrust Certificate Authority dynamic profile generation

See the Entrust CA capabilities 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 that CA Gateway will use to connect and perform operations with Entrust Certificate Authority.

> Skip this section if you are using Post-Quantum Cryptography (PQC) algorithms: ML-DSA algorithms for signing/verification and ML-KEM algorithms for encryption/decryption. For PQC algorithms, the CA includes a predefined **Admin Services User Management (3-key-pair)** (ent_as_ums_3kp) certificate type that you can use for the administrator profile. This certificate type contains three certificate definitions: Encryption, Verification, and TlsVerification. The TlsVerification certificate definition policy should use an RSA-4096 algorithm for TLS client authentication.

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 Administration for the CA.
    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 Administration for the CA.
    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

To connect and perform operations with an Entrust Certificate Authority, 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.

Permission category	Permissions
Searchbases	• View • Administer at least one searchbase.
Security Policy	• View Security Policy • Export Certificate Specification • Export User Templates • Force CRLs • View User Policy
User Templates	Administer at least one template
User - General	• View • Add • Reactivate • Deactivate/Remove • Change DN • Modify properties • Revoke certificates • Update key pairs • Set for key recovery • Cancel key recovery • Modify key update options • View activation code • Reissue activation code
User - Advanced	• Change user's role • Perform PKIX requests • Create user profile

Refer to the Entrust Certificate Authority Administration documentation for more details on role configuration.

To create a new role for the administrator profile

1. Log in to Entrust Certificate Authority Administration for the Entrust Certificate Authority.
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 Administration 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	If you are using RSA or EC algorithms for user certificates, select **CAGW Admin** (the certificate type described in Creating a certificate type for the administrator profile). If you are using Post-Quantum Cryptography (PQC) algorithms – ML-DSA algorithms for signing/verification and ML-KEM for encryption/decryption – select **Admin Services User Management (3-key-pair)**. This certificate type contains three certificate definitions: Encryption, Verification, and TlsVerification. The TlsVerification certificate definition policy should use an RSA-4096 algorithm for TLS client authentication.

Key Update Options

Under this tab, enable the **Use default key update policy** option.

Creating the administrator profile

For connecting and performing 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 **3** 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).

Enabling Entrust Certificate Authority dynamic profile generation

When Enable CA Profile Sync parameter is set to `true` , CA Gateway synchronizes Entrust Certificate Authority profiles as explained below.

1. 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.
2. CA Gateway suppresses niche certificate types relating to ePassport applications and legacy software. To expose these types, enable `include-niche-cert-types` under com.entrust.SecurityManager.

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

See the Sectigo CA capabilities for a complete description of the operations supported by these CAs.

Setting Sectigo permissions for API login

You need a Sectigo user with the following minimum privileges.

- SSL certificate privileges
- Domain validation



See com.SectigoCA 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.SectigoCA 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.SectigoCA 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.SectigoCA, 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.SectigoCA 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 the following URL in a Web browser.

```
https://<machine>:8443/management-console
```

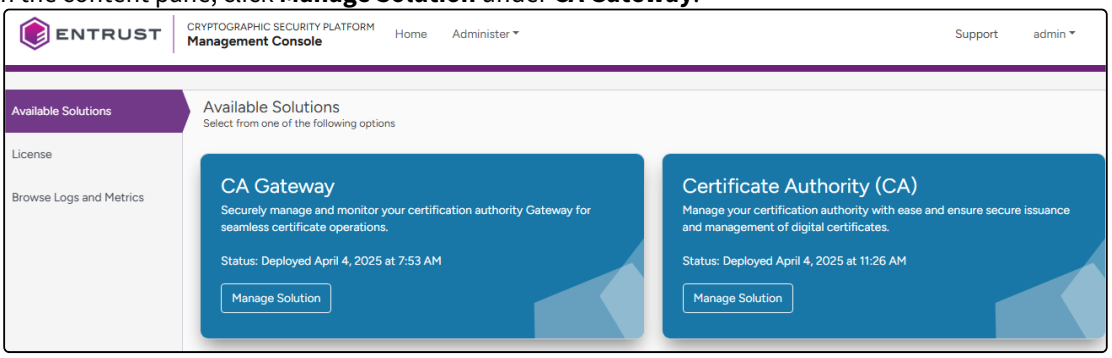
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

> ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

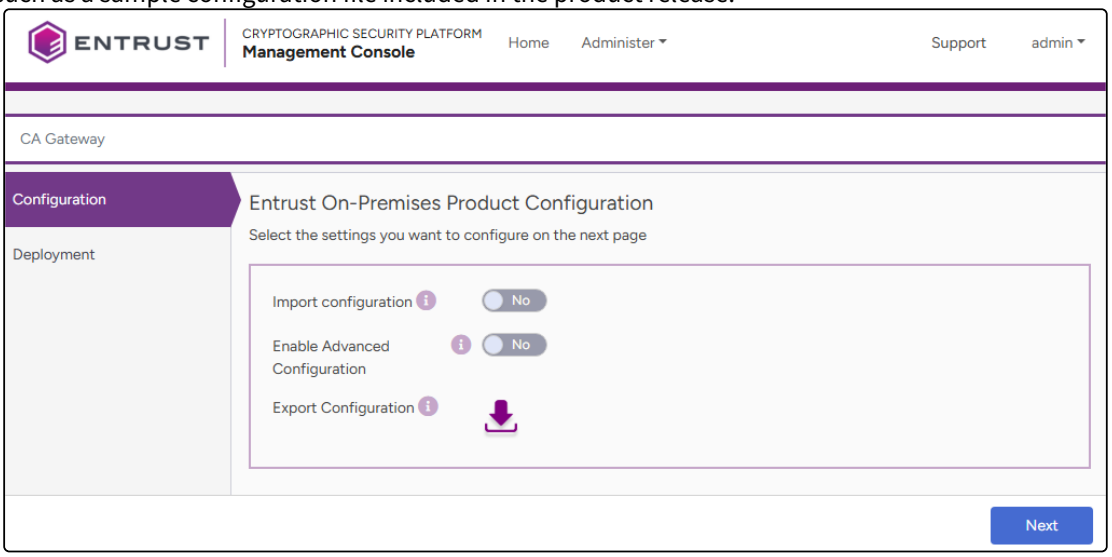
2. Log in to the Management Console as a user belonging to a role with CA Gateway management permissions – for example, the initial `admin` administrator user.

> See Managing identities for how to manage users and roles.

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



1. Activate the **Import configuration** toggle switch if you want to import configuration settings from a file, such as a sample configuration file included in the product release.



2. Click **Next.**
3. Configure the solution settings described in the following sections.
    - Logging
    - Server
    - Connector filters
    - Authorities
    - Profiles
    - Tenants
    - Clients
    - Cmpv2
    - TLS CRL-settings

1. Click **Validate** to validate the configured settings.
2. Correct any detected configuration error until the **Validate** option displays no warnings.
3. Optionally, click the **Download** button to export the current configuration. You can later import this configuration using the already mentioned **Import configuration** toggle switch.

4. Click **Submit** and wait while Cryptographic Security Platform uploads the configuration and any attached file, such as a P12 file with authentication credentials.
5. Click **Deploy**.

Logging

Set the following parameters in the **Logging** tab of the **Configuration** page.

Level

The level of detail for the root CA Gateway logger. In increasing severity.

Level	Description
TRACE	Captures the most detailed information
DEBUG	Provides diagnostic information, such as HTTP headers
INFO	Records general operational events that confirm the system is working as expected
WARN	Indicates a potential issue or unexpected situation that does not stop the application but may require attention
ERROR	Reports errors that prevent a specific operation from completing, but do not cause the entire application to stop
FATAL	Signals a severe failure that forces the application or a major subsystem to shut down
OFF	Disables all logging output

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
timeout-first-seconds	The timeout of the first DNS lookup attempt, in seconds.	3
timeout-second-seconds	Timeout of the second DNS lookup attempt, in seconds. Applicable if the first attempt results in an error.	7
timeout-dsquery-seconds	Timeout in seconds of the Delegation Signer (DS) query when querying DNSSEC support.	7

Mandatory: Yes.

issuer-string

The CAA issuer name, as expected in the DNS resource record. Real-world examples include:

- entrust.net
- pki.goog

The name is owned and defined by the issuer and registered in DNS for any CA to check.

Mandatory: Yes

log-server.<i>.<setting>

The settings of each log server CA Gateway must contact to request the signed CT response. Therefore, you must define at least one server, with `<i>` starting a 0.

<setting>	Value
name	A friendly name for the log server. For example: "Google Log Server".

<setting>	Value
url	The URL of the log server
google	True if the SCTs produced by this log server are Google Chrome compatible.
public-key	The public key of the log server, as a Base64 DER-encoded public key. Log servers typically advertise their keys publicly.
tls-trust-anchor	The trust anchor for the CT Filter to perform the TLS handshake with the log server, as a Base64 DER-encoded certificate.

Mandatory: Yes.

com.entrust.CertificateEvents

Convenience filter to:

1. Read a certificate.
2. Extract data from the certificate.
3. Add the data to the response so that the caller does not have to immediately decode the certificate.

This filter does not require configuring properties.

com.entrust.CertTransparency

Filter to:

1. Collect a set of signed CT log server responses.
2. Ask the underlying CA if the certificates for public trust include these responses in an SCT List extension.

When selecting this filter, configure the following settings under `properties.`

- connection-timeout-millis
- ct-policy-json
- log-server.<i>.<setting>
- proxy-host-name
- proxy-port
- socket-timeout-millis

connection-timeout-millis

The connection timeout for the HTTP communication with the log server, in milliseconds.

Mandatory: No. This optional parameter defaults 5000 milliseconds.

ct-policy-json

The number of log server responses CA Gateway must wait for.

> 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 below for a description of each field.

- months-threshold
- threshold-equals
- google-min-responses
- non-google-min-responses
- insurance

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}
```

months-threshold

The applicability of the `sct-policy` 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.
- Specifying a high value ensures this policy applies to all certificates issued.

threshold-equals

The operator for comparing the months-threshold and the actual certificate lifetime.

Value	Operator
true	=
false	<=

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.

```
google-min-responses + non-google-min-responses
```

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:

- ","
- "="
- "+"
- "<"
- ">"
- "#"
- ";"

When configuring a DigiCert CA, refer to https://knowledge.digicert.com/general-information/digicert-trusted-root-authority-certificates for the DN of intermediate certificate issuers.

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.DigiCert	DigiCert Certificate Authority
com.EJBCA	EJBCA Certificate Authority
com.entrust.ECS	Entrust Certificate Services
com.entrust.MicrosoftCA	Microsoft Certification Authority
com.entrust.SecurityManager	Entrust Certificate Authority
com.SectigoCA	Sectigo CA

com.DigiCert

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

- DigiCert Services API URL
- API Key
- Organization ID
- Payment Method
- Proxy Hostname
- Proxy Port
- Proxy username
- Proxy password

DigiCert Services API URL

The base URL for the request ot the DigiCert services API. For example:

```
https://www.digicert.com/services/v2
```

Mandatory: Yes.

API Key

The API key for consuming the CA services.

Mandatory: Yes.

Organization ID

The identifier of your organization in the DigiCert services.

Mandatory: Yes.

Payment Method

The method for billing requests to the DigiCert services. Supported values are:

- balance
- profile

Mandatory: No. This value defaults to `balance`.

Proxy Hostname

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.

Proxy username

The username for authenticating in the CA server proxy.

Mandatory: Only when the proxy requires authentication.

Proxy password

The password for authenticating in the server proxy.

Mandatory: Only when the proxy requires authentication.

com.EJBCA

To integrate an EJBCA (Enterprise JavaBeans Certificate Authority), select this connector and configure the following settings.

- CA Name
- EJBCA Edition
- Base URL
- Admin PKCS#12 File Path
- Admin PKCS#12 Password
- Trust Store File Path
- Trust Store Password
- Trust Store Type

CA Name

The CA name – for example:

```
abc-issuing
```

Mandatory: Yes.

EJBCA Edition

The base URL of the EJBCA server.

Mandatory: Yes.

Base URL

The base URL of the EJBCA server.

Mandatory: Yes.

Admin PKCS#12 File Path

Click **Choose File** to import the PKCS #12 file described in Issuing the EJBCA client certificate.

Mandatory: Yes.

Admin PKCS#12 Password

The password of the PKCS #12 file described in Issuing the EJBCA client certificate.

Mandatory: Yes.

Trust Store File Path

Click **Choose File** to import the file described in Downloading the EJBCA certificate chain.

Mandatory: Yes.

Trust Store Password

The password of the file described in Downloading the EJBCA certificate chain. Leave empty if the file is not password-protected.

Mandatory: No. This optional value defaults to no password.

Trust Store Type

The type of the file described in Downloading the EJBCA certificate chain. Supported values are:

- JKS
- PKCS12

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

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 CA services.

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
```

> 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.

> 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.

> 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 CA services.

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
```

> 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
```

> You must statically configure this setting because the ECS public API does not yet allow querying certificates from the CA.

Mandatory: Yes.

client-id-domains

The client identifier defined in ECS for all domain operations sent to the ECS API.

> You must statically configure this setting because the ECS public API does not yet allow querying certificates from the CA.

Mandatory: No. This optional parameter defaults to 1.

ecs-url

Set this parameter to:

```
https://api.entrust.net/enterprise/v2
```

Mandatory: Yes.

enrollment-agent-p12

The SSL PKCS#12, as a file path or a Base64 encoding.

Mandatory: Yes.

enrollment-agent-p12-password

The password of the SSL PKCS#12.

Mandatory: Yes.

proxy-host-name

The hostname of the proxy for accessing the ECS CA server.

Mandatory: Only when traffic to the ECS CA server passes through a proxy.

proxy-password

The password for authenticating in the proxy server.

Mandatory: Only when the proxy requires authentication.

proxy-port

The port for accessing the proxy server.

Mandatory: Only when traffic to the ECS CA server passes through a proxy.

proxy-username

The username for authenticating in the proxy server.

Mandatory: Only when the proxy requires authentication.

rdn-corrections.<i>.rep

A distinguished name (DN) attribute you want to rename using the rdn-corrections.<i>.rep-with parameter.

Specifically, some Entrust Certificate Services profiles may include legacy attribute names in the subject of the issued certificates. However, these attribute names may not be compatible with the industry-standard names used by some client applications.

Entrust Certificate Services legacy attribute name	Industry-accepted attribute name
jurisdictionOfIncorporationStateOrProvinceName	jurisdictionStateOrProv
jurisdictionOfIncorporationCountryName	jurisdictionCountryName

In this case, add the following lines to the CA Gateway configuration.

```
rdn-corrections.0.rep: jurisdictionCountryName
rdn-corrections.0.rep-with: jurisdictionOfIncorporationCountryName
rdn-corrections.1.rep: jurisdictionStateOrProvinceName
rdn-corrections.1.rep-with: jurisdictionOfIncorporationStateOrProvinceName
```

Before sending certificate renewal requests to Entrust Certificate Services, CA Gateway will apply this configuration and replace industry-compliant subject attributes with legacy ones.

Example of subject name with industry-compliant attribute names

```
CN=test.com, serialNumber=705421, businessCategory=Private Organization, O=Entrust
Corporation, jurisdictionStateOrProv=Delaware, jurisdictionCountryName=US,
L=Shakopee, ST=Minnesota
```

Example of subject name with Entrust Certificate Services legacy attribute names

```
CN=test.com, serialNumber=705421, businessCategory=Private Organization, O=Entrust
Corporation,  jurisdictionOfIncorporationStateOrProvinceName=Delaware,
jurisdictionOfIncorporationCountryName=US, L=Shakopee, ST=Minnesota
```

Mandatory: Only when renewing certificates with Entrust Certificate Services.

rdn-corrections.<i>.rep-with

A new name for the distinguished name (DN) attribute you selected with the rdn-corrections.<i>.rep parameter.

Mandatory: Only when renewing certificates with Entrust Certificate Services.

user-name

The API username for consuming the ECS CA services. See the CA Gateway guide for how to obtain this username.

Mandatory: Yes.

com.entrust.MicrosoftCA

To integrate a Microsoft certificate authority, select this connector and configure the following settings.

- CA Proxy URL
- CA Host
- CA Name
- LDAP Port
- LDAPS Port
- LDAP Host
- Key Recovery Agent PKCS#12
- Key Recovery Agent PKCS#12 Password
- Client Certificate Key Alias
- Client Certificate Keystore Type
- Client Certificate Keystore File
- Client Certificate Keystore Password
- SSL Truststore Type

- SSL Truststore File
- SSL Truststore Password
- Additional Microsoft CA Properties

CA Proxy URL

The URL of the Entrust Proxy for Microsoft CA, in the following format:

```
https://<server>:8443/MSCAProxy
```

Mandatory: Yes.

CA Host

The CA hostname, as either:

- An IP
- A hostname
- A FQDN

As long as it resolves from the DNS.

Mandatory: Yes.

CA Name

The CA name – for example:

```
abc-issuing
```

Mandatory: Yes.

LDAP Port

The port number for LDAP connections with Microsoft Active Directory (for LDAPS connections, configure LDAPS Port instead).

> The port is anonymously bound. The Microsoft CA proxy connects to Active Directory to get certificate template information.

This value is typically 389, the well-known port for LDAP.

Mandatory: When not configuring LDAPS Port.

LDAPS Port

The port number for LDAPS connections with Microsoft Active Directory (for LDAP connections, configure LDAP Port instead).

> 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 `JKS`	✓
ssl-trust-store	The path of the CA Gateway trust store	✓
ssl-trust-store-password	The password of the CA Gateway trust store	✓
ssl-trust-store-type	The type of CA Gateway trust store. Supported values are `JKS` and `PKCS12`	✓

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
- oid.<oidName>

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.



This value is typically 389, the well-known port for LDAP.

Mandatory: When using an LDAP connection.



Configure either **LDAP Port** or **LDAPS Port**, but not both.

LDAPS Port

The port number for LDAPS connections with Entrust Certificate Authority.

> This value is typically 636, the well-known port for LDAPS.

Mandatory: When using an LDAPS connection.

> Configure either **LDAP Port** or **LDAPS Port**, but not both.

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

Click **Select Files** to import the administrator's Entrust Profile File (EPF) for connecting to Entrust Certificate Authority.

> See Creating the administrator profile for how to create 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 `optionalCertificateRequestDetails.validityPeriod` value.
false	Set by the CA.



As explained in RFC2459, the `PrivateKeyUsagePeriod` extension "allows the certificate issuer to specify a different validity period for the private key than the certificate".

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

Enable CA Profile Sync

`true` to enable profile synchronization with Entrust Certificate Authority, `false` otherwise. When set to `true`, CA Gateway:

- Mirrors any eligible certificate types and definitions defined in Entrust Certificate Authority as basic CA Gateway certificate profiles without the need to define them in the CA Gateway configuration explicitly.
- Suppresses niche certificate types relating to ePassport applications and legacy software. To expose these types, enable the **Enable niche certificate types** parameter setting of the com.entrust.SecurityManager connector.

Mandatory: No.

oid.<oidName>

Click **+ Security Manager Properties** to add attributes with the `oid.<oidName>` key name. Such properties allow CA Gateway clients to request non-standard Subject DN attributes. For example:

Key name	Value
oid.jurisdictionOfIncorporationLocalityName	1.3.6.1.4.1.311.60.2.1.1

Security Manager also requires configuring the OIDs in the CA configuration:

1. Edit the `manager/entrust.ini` file.
2. Add entries for each OID under both the `[OIDTable]` and `[X500AttrSyntax]` sections.

For example:

```
[OIDTable]
jurisdictionOfIncorporationLocalityName=1.3.6.1.4.1.311.60.2.1.1

[X500AttrSyntax]
```

```
jurisdictionOfIncorporationLocalityName=caseIgnoreStringSyntax
```

See the Entrust CA Operations Guide for further detail.

Mandatory: No.

com.SectigoCA

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

- Sectigo settings
- Authentication settings
- SSL settings
- Enrollment settings
- Proxy settings

See CA enrollments endpoint for considerations on renewing Sectigo-issued certificates.

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 Certificate Keystore File	The path of the client trust store described in Creating a Sectigo client key store
Client Certificate Keystore Password	The alias of the client key in the client trust store
Client Certificate Keystore Password	The password of the client trust store
Client Certificate Keystore Type	The type of client trust store. Supported values are `JKS` and `PKCS12`

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 Truststore Password	The password of the trust store
SSL Truststore Type	The type of CA Gateway trust store. Supported values are `JKS` and `PKCS12`

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 `enroll-max-attempts` 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.

> 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; `false` otherwise.

Certificate authority provider	Synchronization details
Entrust Certificate Authority	Enabling Entrust Certificate Authority dynamic profile generation
Sectigo CA	Sectigo CA profile properties
EJBCA	Enabling EJBCA dynamic profile generation

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
- DigiCert CA Profile Properties
- ECS Profile Properties
- EJBCA 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.

DigiCert CA Profile Properties

Under this section, add the following profile settings for each DigiCert authority.

- Product Identifier
- Domain Validation Method
- Verified Contact Email for Extended Validation (EV)
- Signature Hash Algorithm
- Order Validity (years)
- Certificate Validity (years)

Product Identifier

Enter the certificate types, also referred to as "DigiCert products", supported by the profile. List them as a comma-separated string of DigiCert identifiers.

```
["ssl_cloud_wildcard", "ssl_plus", "ssl_multi_domain"]
```

See the available values at:

https://dev.digicert.com/en/certcentral-apis/services-api/glossary.html#product-identifiers

Mandatory: Yes.

Domain Validation Method

The method to prove control over a domain when requesting an SSL/TLS certificate from a DigiCert CA. Supported values are the following.

Value	Description
`dns-cname-token`	CNAME DNS record validation
`http-token`	HTTP file validation
`http-token-dynamic`	Dynamic HTTP file validation
`dns-txt-token`	TXT DNS record validation

Mandatory: When the selected product requires a validation method.

Verified Contact Email for Extended Validation (EV)

The email address of the Verified Contact associated with the organization requesting an EV certificate.

Mandatory: Only for Extended Validation (EV) certificates.

Signature Hash Algorithm

The cryptographic algorithm for generating a hash of the signed data.

Supported values are:

- sha256
- sha384
- sha512

Mandatory: Yes.

Order Validity (years)

The number of years for which each certificate order remains active, allowing certificates to be issued, reissued, or renewed under the same order.

Mandatory: No. This optional value defaults to one year.

Certificate Validity (years)

The number of years for which each certificate is valid and trusted after issuance, as determined by the issuance date and expiration date.

Mandatory: Only applies to multi-year plans. When this optional value is omitted, the CA sets the validity period according to the CAB Forum baseline requirements.

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.

EJBCA Profile Properties

Under this section, add the following profile settings for each EJBCA certificate authority.

- Certificate Profile
- End Entity Profile
- Key Client Generated
- Key Recoverable
- EJBCA Requested Properties

Certificate Profile

The name of the certificate profile in EJBCA.

Mandatory: Yes.

> When Enable CA Profile Sync is set to `true`, this setting is automatically populated; however, manually configured values take precedence.

End Entity Profile

The name of the end-entity profile in EJBCA.

Mandatory: Yes.

When Enable CA Profile Sync is set to `true`, this setting is automatically populated; however, manually configured values take precedence.

Key Client Generated

The key generation mode.

Value	Key generation
✅	Generate the keys on the client side with a CSR
❌	Generate the keys on the server side, in a PKCS #12

When Enable CA Profile Sync is set to `true`, this setting is automatically populated; however, manually configured values take precedence.

Key Recoverable

The key recovery status.

Value	Key recovery
✅	Server-side-generated keys can be recovered
❌	Server-side-generated keys cannot be recovered

When Enable CA Profile Sync is set to `true`, this setting is automatically populated; however, manually configured values take precedence.

EJBCA Requested Properties

Add the following settings under this section.

Property Name	Description	Type	Required
username	The unique name of the end entity in EJBCA.	text	✅
password	The password for authenticating enrollment requests in EJBCA.	password	✅

Property Name	Description	Type	Required
key_algs	The key algorithm for server-side key generation. The selected value must be included in the **Available Key Algorithms** list described in Creating an EJBCA certificate profile.	text	✗

When Enable CA Profile Sync is set to `true`, this setting is automatically populated; however, manually configured values take precedence.

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"
```

```
}
```

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

To modify the value of these parameters using the Management Console:

1. Click **+ Sectigo CA Profile Properties**.
2. In the **Choose a key name** field, enter the parameter name without quotation marks. For example:
   - key_types
   - terms
3. In the **New Value** field, enter the parameter value enclosed in quotation marks.

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\"]}"
```

Each list must be enclosed in square brackets `[]`.

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 `key-types` list	As selected in the request
	Not included in the `key-types` list	Error
PKCS #12	—	The first in the `key-types` 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 comma-separated list of supported certificate validity periods (in days). . For example:

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

The list must be enclosed in square brackets `[]`.

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 `terms` list	As selected in the request
	Not included in the `terms` list	Error
	None	The first in the `term` list, if term list not available, uses default.
PKCS #12	—	The first in the `term` 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 Role Override
- 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 `managed-cas.profiles.directory-mode` value.

Mandatory: No. This optional parameter defaults to `true`.

LDAP directory mode

When the **LDAP entry creation mode** option is disabled, this setting controls whether Entrust Certificate Authority creates an LDAP entry for the user.

Value	Action
DO_OP_FAIL_IF_NOT_NEEDED	Perform the repository operation when needed, and fail if not needed.
DO_OP_SUCCEED_IF_NOT_NEEDED	Perform the repository operation when needed, and return success if not needed.
NO_OP	Omit the repository operation and do not check if the operation is needed.
NO_OP_FAIL_IF_NEEDED	Omit the repository operation, but fail if the operation is needed.

In the CA profile, certificate types as `vpn_nodir` include the following `master.certspec` advanced setting under `[Extension Definitions]`.

```
noUserInDirectory=1
```

Mandatory: Yes.

User Role

The Entrust Certificate Authority role for processing enrollment requests under the certificate profile (for example, "End User").

⚠ The administrator EPF for the Managed CA must have permission to administer this role.

Mandatory: No.

User Role Override

True to allow enrollment requests to specify a user role that overrides the default role of the profile; **False** otherwise.

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

User Type

The Entrust Certificate Authority user type to use when processing an enrollment request under the certificate profile. For example:

- Person
- Web Server

> ⚠ The administrator EPF for the Managed CA must have permission to administer this user type.

Mandatory: No. The user type is not required when the **LDAP entry creation mode** option is disabled.

Tenants

Set the following parameters in the **Tenants** tab of the **Configuration** page.

- Tenants
- Integrators

Tenants

For each tenant, set the following field values under **Tenants**.

Setting	Value	Mandatory
Name	A friendly name for the tenant.	✓
Unique-Id	A unique identifier for the tenant. When configuring integrators, you will specify this identifier to map an integrator to a tenant.	✓
Certificate Authority Id	The CA unique identifier in CA Gateway. Map each tenant to a different managed CA because errors will occur if you map multiple tenants to the same managed CA.	✓

Integrators

Set the following fields under **Integrators**.

Setting	Value	Mandatory
Name	A friendly name for the integrator	✓
Unique-Id	A unique identifier for the integrator. When creating certificates for clients, you can specify this integrator ID to map a client to an integrator.	✓
Tenant IDs	One or more of the tenant identifiers previously defined when configuring tenants. Map each integrator to a different tenant because errors will occur if you map multiple integrators to the same tenant.	✓

Clients

For each client, set the following field values in the **Clients** tab of the **Configuration** page.

- Subject DN
- Tenant ID
- Integrator ID
- Role

Subject DN

The subject DN of the client.

⚠ You must issue the client a digital certificate with this subject DN.

Mandatory: Yes.

Tenant ID

One of the tenant identifiers listed under Tenants

⊗ This value is mapped with the client and is mutually exclusive with Integrator ID.

Mandatory: Yes.

Integrator ID

The integrator identifier.

⊗ This value is mapped with the client and is mutually exclusive with Tenant ID.

Mandatory: Yes.

Role

One of the following roles.

Role identifier	Role main permissions	Granted by default
integrator	Access to multiple CAs. For example, as an organization providing services or capabilities to customers, such as Identity Management service providers like Microsoft Intune.	Default role for clients mapped to an integrator.
policy-constrained-tenant	View a single CA. For example, as a consumer of the services provided by the Integrator.	Default role for clients mapped to a tenant.

Role identifier	Role main permissions	Granted by default
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 `get` operations on any of them.	—
read-only-tenant	Access one CA and perform `get` operations.	—

See the following table for a more detailed description of the permissions assigned to each predefined role.

Permission	integrator	policy-override-tenant	policy- constrained- tenant	read-only-integrator	read-only-tenant
Access multiple CAs	✓	Single CA only	Single Entrust Certificate Authority only	✓	Single CA only
Request explicit extensions	✓	✓	✗	✗	✗
Request private key usage period	✓	✓	✗	✗	✗
External public keys (no CSR)	✓	✓	✗	✗	✗
Override Proof of Possession	✓	✓	✗	✗	✗
Request explicit validity dates	✓	✓	Can shorten the lifetime in CSR enrollments (relative to the CA policy).	✗	✗
CSR	✓	✓	✓	✗	✗
PKCS#12	✓	✓	✓	✗	✗

Permission	integrator	policy-override-tenant	policy- constrained- tenant	read-only-integrator	read-only-tenant
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

Mandatory: Yes.

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 CA 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 endpoint
- Ping endpoint
- Metrics endpoint

Checking the health of a CA

CA Gateway provides the Status endpoint endpoint to check the health of a Certificate Authority.

CA Gateway endpoints

CA Gateway provides the following endpoints.

Description	Endpoint
CA endpoints	`https://{host}:{port}/<server.servlet.context-path>/v1/certificate-authorities`
Documentation endpoint	`https://{host}:{port}/{server.servlet.context-path}/doc`
Health endpoint	`https://{host}:{port}/`

Description	Endpoint
	`{management.endpoints.web.base-path}/health`
Metrics endpoint	`https://{host}:{port}/{management.endpoints.web.base-path}/prometheus`
Ping endpoint	`https://{host}:{port}/{management.endpoints.web.base-path}/health/{group}/ping`
Properties endpoint	`https://{host}:{port}/{server.servlet.context-path}/v1/certificate-authorities/{caId}/properties?fields={properties}`
Status endpoint	`https://{host}:{port}/{server.servlet.context-path}/v1/certificate-`

Description	Endpoint
	`authorities/{caId}/status`
Swagger endpoint	`https://{host}:{port}/{server.servlet.context-path}/swagger-ui`
Version endpoint	`https://{host}:{port}/{server.servlet.context-path}/v1`

CA endpoints

The following endpoints support certificate and CA management operations.

Description	Endpoint
CA actions endpoint	`https://{host}:{port}/<server.servlet.context-path>/v1/certificate-authorities/{caId}/certificates/{sn}/actions`
CA certificate events endpoint	`https://{host}:{port}/<server.servlet.context-path>/`

Description	Endpoint
	`v1/certificate-authorities/{caId}/certificate-events`
CA domains actions endpoint	`https://{host}:{port}/<server.servlet.context-path>/v1/certificate-authorities/{caId}/domains/{domain}/actions`
CA domains endpoint	`https://{host}:{port}/<server.servlet.context-path>/v1/certificate-authorities/{caId}/domains`
CA enrollments endpoint	`https://{host}:{port}/<server.servlet.context-path>/v1/certificate-authorities/{caId}/enrollments`

Description	Endpoint
CA properties endpoint	`https://{host}:{port}/<server.servlet.context-path>/v1/certificate-authorities/{caId}/properties?fields={properties}`
CA status endpoint	`https://<HOST>:<CAGW_HOST_PORT>/<server.servlet.context-path>/v1/certificate-authorities/{caId}/status`

CA actions endpoint

The following endpoint returns the supported actions for a certificate.

```
https://{host}:{port}/<server.servlet.context-path>/v1/certificate-authorities/
{caId}/certificates/{sn}/actions
```

Where:

- `{caId}` is the Entrust Certificate Authority identifier
- `{sn}` is the serial number of the certificate

See below for CA-specific considerations on this endpoint.

- Renewing Sectigo CA certificates with the actions endpoint
- Revoking GlobalSign certificates with actions endpoint

Renewing Sectigo CA certificates with the actions endpoint

When using the action endpoint to renew a certificate issued by a Sectigo CA, the JSON request must include the `csr` property inside the `properties` field. For example:

```
{
  "action": {
    "comment": "Test",
    "properties": {
      "csr":
"MIIC1TCCAb0CAQAwIzEhMB8GA1UEAwwYbWF3aWEudGVzdC5zZWN0aWdvLnJlbmV3MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAt/
hiyBuXWjhsnhIrr32Xnv9fUwrUKru4UjuNEtmqtOftfNkUMnBmwKFZ1DxHeuatzeVYXPCXoWAfteU2g4JibAC
MJAEDMARd338XiOVDRZW2e/VOs49wZJN9q7f+IFVw5B3x4qCDSE7zjsohgP3/
ISvMyHkjs9h4sYw+Bn9+VBk1yA+S3IrWigbMA5ILod2y+MKZ6F2kdcgKl6ytFzDFV9n3TgzpJKVaQvgH696b6
+4cqZMlOn+2ScuQDJ+blZixpqrsnT9ag4It2RPtpu+IX/
DW5LvHFfGE5RPyD+GI1Ohi6B8iUxm6wfpcGwzkxsy8F5lZAD5FKUvKk94M4+yaAwIDAQABoG0wawYJKoZIhvc
NAQkOMV4wXDAJBgNVHRMEAjAAMAsGA1UdDwQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw
IwYDVR0RBBwwGoIYbWF3aWEudGVzdC5zZWN0aWdvLnJlbmV3MA0GCSqGSIb3DQEBCwUAA4IBAQAK7YbCBrqnN
fhJsNQbdTa68bt8UTqbPL/2PsapsKPOkPugggN5dP0D5glzRG/tiBhsNNxjEPW+TKyX7g8j5ACHCt5r/
cSy3zKkj9Z2TJCjOyt+wC1GYqDLse7vHqb+102920GwqY/dRYq/uswuP4ZTo/
TpVIEbwhXZzWVfaAC40F8O9Wb8S8UCyuv2hV+NW9gE9bTEC1sNr1XU9+5TxikRbHda2SPqR+pK2/
yfdMQ970e82jfHisvBJWKHBnbvd3yrRVEcKJOkQ1yuuR2/
kzPdfB3DG5xkDIcNodvDznKEMHLv5bR8f+kzlz4poYggZa2Kw617pUgB5GGP2AiWiHn/"
    },
    "type": "RenewAction"
  }
}
```

Revoking GlobalSign certificates with actions endpoint

When using the actions endpoint to revoke a certificate issued by a GlobalSign CA, the `action.reason` parameter is:

- Required by the CA gateway API.
- Ignored by the GlobalSign MSSL (Managed SSL) API, which does not support specifying a revocation reason.

Therefore, this value must be included in the requests, although it will not be evaluated. For example:

```
{
  "action": {
    "comment": "revoke",
    "succeedIfAlreadyInRequestedState": true,
    "type": "RevokeAction",
    "reason": "unspecified"
  }
}
```

CA certificate events endpoint

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

```
https://{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.

> The endpoint retrieves 0 events for days without events.

nextPageIndex

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

> 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 `nextPageIndex` till today
false	All events have been collected, so the caller can stop invoking the endpoint

CA domains actions endpoint

The following endpoint supports domain-related actions.

```
https://{host}:{port}/<server.servlet.context-path>/v1/certificate-authorities/
{caId}/domains/{domain}/actions
```

Where:

- `{caId}` is the Certificate Authority identifier. See below for CA-specific considerations on this endpoint.
- `{domain}` is the identifier of a domain added with the CA domains endpoint.

For example:

```
{
  "action": {
    "properties": {
```

```
      "tagLocation": "store.example.com,example.com"
    },
    "type": "ReverifyDomainAction",
    "verificationMethod": "dns"
  }
}
```

See below for a description of each parameter.

- action.type
- action.verificationMethod
- action.properties.tagLocation

action.type

The identifier of the domain action. See below for the values supported by this parameter.

Value	Action
ReverifyDomainAction	Verify a previously validated domain because the prior validation expired, failed, or must be refreshed to meet CA/Browser Forum or GlobalSign requirements.

action.verificationMethod

The identifier of the domain verification method. See below for the values supported by this parameter.

Value	Verification
dns	DNS-based domain verification, GlobalSign requires a unique Domain Validation Code (DVC) in a DNS TXT record to confirm domain control.
webServer	HTTP-based verification, also called file-based domain verification. GlobalSign requires a Domain Validation Code (DVC) on the web server to confirm domain control.

action.properties.tagLocation

The location of the domain validation control number.

> When providing multiple values, separate them with commas.

See below for sample values when `verificationMethod` is `dns`.

Value	Validated FQDN
`a.b.c.example.com,b.c.example.com,c.example.com,example.com`	`a.b.c.example.com`

Value	Validated FQDN
`store.example.com,example.com`	`store.example.com`
`example.com`	`example.com`

See below for sample values when `verificationMethod` is `webServer`.

Value	Requested domains
`https://example.com/.well-known/pki-validation/gsdv.txt`	`*.example.com` `example.com`
`https://example.com/.well-known/pki-validation/gsdv.txt,https://sub.example.com/.well-known/pki-validation/gsdv.txt`	`*.sub.example.com` `sub.example.com`
`https://example.com/.well-known/pki-validation/gsdv.txt,https://www.example.com/.well-known/pki-validation/gsdv.txt`	`*.www.example.com` `sub.example.com`

CA domains endpoint

The following endpoint supports adding domains for EV (Extended Validation) profiles.

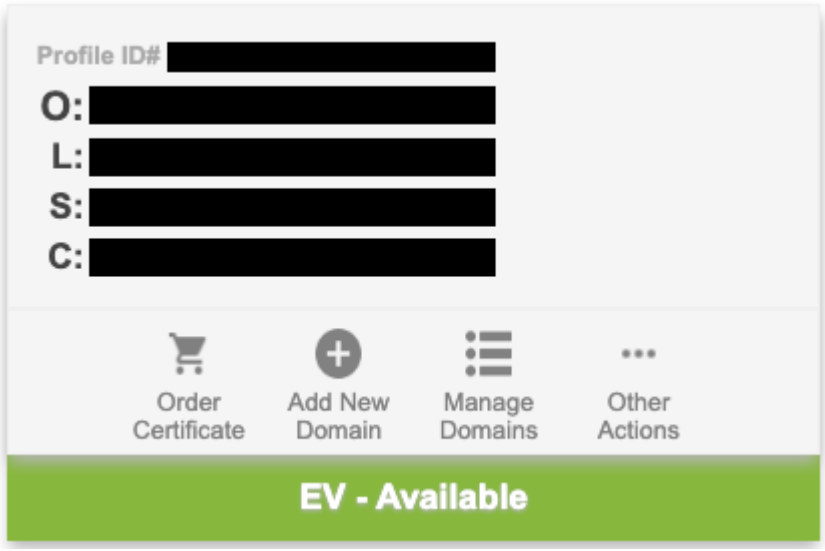
```
https://{host}:{port}/<server.servlet.context-path>/v1/certificate-authorities/{caId}/domains
```

Where `{caId}` is the Certificate Authority identifier. See below for CA-specific considerations on this endpoint.

- Adding GlobalSign domains

Adding GlobalSign domains

To check if a GlobalSign profile supports the domains endpoint, navigate to the profile information under **Managed SSL**.



When displayed, the **EV - Available** message indicates that the profile supports requests to add a domain – for example:

```
{
  "emailVerificationInfo": {
    "emailAddresses": [
      "fake@fake.com"
    ]
  },
  "name": "mydomain.com",
  "properties": {
    "vettingLevel": "EV"
  }
}
```

CA enrollments endpoint

The following endpoint allows enrolling and renewing certificates with the `{caId}` certificate authority.

```
https://{host}:{port}/<server.servlet.context-path>/v1/certificate-authorities/
{caId}/enrollments
```

See below for CA-specific considerations on this endpoint.

- Renewing GlobalSign certificates with the enrollments endpoint
- Renewing Sectigo CA certificates with the enrollments endpoint
- Requesting GlobalSign certificates with the enrollments endpoint

Renewing GlobalSign certificates with the enrollments endpoint

When using the enrollments endpoint to renew a certificate from a GlobalSign CA, the request body must contain one of the following values.

- properties.renewalOrderID
- properties.renewalOrderId
- properties.renewalSerialNumber

For example:

```
{
  "csr": "...",
  "includeCa": false,
  "optionalCertificateRequestDetails": {
    "subjectDn": "cn=grapefruitdesk.com,o=Test Company,c=CA",
    "useSANFromCSR": false,
    "validityPeriod": "P1Y0M0D"
  },
  "profileId": "profileA",
  "requiredFormat": {
    "format": "pem"
  },
  "properties": {
    "renewalOrderID": "mssl-order-id"
  }
}
```

Renewing Sectigo CA certificates with the enrollments endpoint

When using the enrollments endpoint to renew a certificate issued by a Sectigo CA, the JSON request must include the `RenewalSerialNumber` setting inside the `properties` field. For example:

```
{
  "csr":
"MIIC2zCCAcMCAQAwJjEkMCIGA1UEAwwbbWF3aWEudGVzdC5zZWN0aWdvLnJlbmV3LjA2MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6xeRXTqPSvmTVCtLi17pvGH2d5zQP2uiU5CR1r7ofGjJVumktr9MUf4DW
mAgaaumkmjn0xRMSew4viE99nONP7XfciJLBRKgjBBnwr0fLCCiGRVKLr3PiTQ/
N9J60gt8KkVYZ94Z1HmiGtXye6cZHX2ibnqfcW//
tN5ewUrzQTfLyIAiw0OqRPkt10M4xFrRtFv2d07bf6rlPS75VCjYdfUaerHf8aOmllFWzmciYaZkGM2/
Uds+rel+OeVT8gzBqAqvgxCRXf2On67acXV1x2gStaa+uJmk46EacLtL+b/
DHXigoNSqruchMUdHQfqnd8DtVVCjPy2nTBrHmBvl8wIDAQABoHAwbgYJKoZIhvcNAQkOMWEwXzAJBgNVHRME
AjAAMAsGA1UdDwQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwJgYDVR0RBB8wHYIbbWF3a
WEudGVzdC5zZWN0aWdvLnJlbmV3LjA2MA0GCSqGSIb3DQEBCwUAA4IBAQCdKzAHBavqRIDzVu1VSj0bI/
VjgOcF982p6/lPnFKfl+13fxslUN003kG/uuh4Zdxo/OOVMH6VSi+T4I06GuO/
7LoMg7oAxqN1FaBjK5VwlNAuro2uS54FGz+2ubYS8F+cTQXffMOuerNgVJXGFKaaHtrcoDynfp9PgyJg+I4zB
aPR/5E051Am2t5K+wQHtsO+ThoInnK5iwslE+SUnzCZwGwkf50Uf450/
pyjKnUKsjXpdfPSoTrkVEFTniNkM+FzFwjjhECp536EzWlLsX/C3d/
QGTndH4c4GN9qFGaybDmWZHHJHabj52/CeORJmkrI0REQi1ROFSGW8Zb66Dz9",
  "renewal": true,
  "properties": {
     "RenewalSerialNumber": "4c56db9f8f07af1e93c66a37e041ef8e"
```

```
  },
  "profileId": "profileA-local",
  "requiredFormat": {
    "format": "PEM"
  }
}
```

Requesting GlobalSign certificates with the enrollments endpoint

When using the enrollments endpoint to request a certificate from a GlobalSign CA, the `profileId` parameter must identify a GlobalSign MSSL (Managed SSL) profile. See below for the supported issuance modes.

Issuance mode	profileId
A PKCS #12 containing a certificate and key pair generated by the CA	The identifier of a profile that includes the **PV_INTRA_SKIP** or **PV_INTRA_SKIP_SHA2** product codes
A certificate for a client-generated key pair and CSR	The identifier of a profile that includes any other product codes

For example:

```
{
  "csr": "...",
  "includeCa": false,
  "optionalCertificateRequestDetails": {
    "subjectDn": "cn=grapefruitdesk.com,o=Test Company,c=CA",
    "useSANFromCSR": false,
    "validityPeriod": "P1Y0M0D"
  },
  "profileId": "profileA",
  "renewal": true,
  "requiredFormat": {
    "format": "pem"
  }
}
```

CA properties endpoint

The following endpoint returns property values on certificate authorities.

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

Where `{caId}` is the Entrust Certificate Authority 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 Entrust Certificate Authority 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"
      ]
    }
  }
}
```

CA status endpoint

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",
```

```
}
```

Documentation endpoint

The following endpoint provides documentation on using the CA Gateway API for certificate policy, certificate issuance, and certificate lifecycle management.

```
https://{host}:{port}/{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 endpoint

The following endpoint returns information on the CA Gateway server health.

```
https://{host}:{port}/{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.

Metrics endpoint

The following endpoint returns CA Gateway metrics in Prometheus-compliant format.

```
https://{host}:{port}/{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
```

Ping endpoint

The following endpoint returns the ping status of the CA Gateway server for a group.

```
https://{host}:{port}/{management.endpoints.web.base-path}/health/{group}/ping
```

Where:

- `{host}` is the hostname or IP address of the CA Gateway host server.
- `{post}` is the port of the CA Gateway service.
- `{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"}
```

Properties endpoint

The following endpoint returns property values on Entrust CAs.

```
https://{host}:{port}/{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 endpoint

The following endpoint returns the `UP` or `DOWN` status of a Certificate Authority.

```
https://{host}:{port}/{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 endpoint

The following endpoint povides 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}:84444/{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 tentant.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.

Version endpoint

The following endpoint returns version information on CA Gateway.

```
https://{host}:{port}/{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.

This endpoint is the main API entry point to invoke API capabilities.

CA Capabilities reference

The "Get CA Capabilities" endpoint of the CA Gateway API informs on the capabilities supported by each type of CA. The following sections give a complete reference of the returned values.

- Digicert CA capabilities
- ECS CA capabilities
- EJBCA capabilities
- Entrust CA capabilities
- Microsoft CA capabilities
- Sectigo CA capabilities

Digicert CA capabilities

See below for the capabilities supported by Digicert Certificate Authorities.

enrollments

See below for the enrollment-supported capabilities

Name	Description	Endpoint	Supported
EnrollmentByCSR	Process certificate signing requests	/v1/certificate-authorities/{caId}/enrollments	✅
X509CertificateResponse	Returns certificate in X509 form	/v1/certificate-authorities/{caId}/enrollments	✅
PKCS12Response	Return certificate and key in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	❌
SANInCSR	Process Subject Alternative Names (SANs) in CSR	/v1/certificate-authorities/{caId}/enrollments	✅
SANInRequest	Process Subject Alternative Names (SANs) in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✅
SubjectNameInRequest	Supply subject name parameters in request to construct a subject DN in the supplied order	/v1/certificate-authorities/{caId}/enrollments	✅
CAGeneratedKey	Generate the key and returned it to client in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	❌
KeyInRequest	Supports client-generated keys for enrollment in the enrollment request	/v1/certificate-authorities/{caId}/enrollments	❌

Name	Description	Endpoint	Supported
CAGeneratedKeyBackup	Supports key backup for CA generated keys	/v1/certificate-authorities/{caId}/enrollments	✗
ClientGeneratedKeyBackup	Supports key backup for client-generated keys	/v1/certificate-authorities/{caId}/enrollments	✗
ExtensionInCSR	Process extension request in CSR	/v1/certificate-authorities/{caId}/enrollments	✗
ExtensionInRequest	Process extension request in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✗
ValidateProofOfPossesion	Validates proof of possession if requested	/v1/certificate-authorities/{caId}/enrollments	✗
ValidityPeriodInRequest	Supports validity period in request	/v1/certificate-authorities/{caId}/enrollments	✓

certificates

See below for the certificate-supported capabilities

Name	Description	Endpoint	Supported
SearchBySerial	Lookup certificate by serial number	/v1/certificate-authorities/{caId}/certificates/{serial}	✓
CertificateAction	List supported actions on a certificate	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✓
CertificateRevocationReason	List supported revocation reasons for the certificate RevokeAction	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✓

certificate-events

See below for the certificate-event-supported capabilities

Name	Description	Endpoint	Supported
CertificateEvents	Support certificate events	/v1/certificate-authorities/{caId}/certificate-events	✓
MaxCertificateEventsPageSize	Return the maximum size of the certificate events Page	/v1/certificate-authorities/{caId}/certificate-events	✓

status

See below for the status-supported capabilities

Name	Description	Endpoint	Supported
CAStatus	Check whether the CA is up or down	/v1/certificate-authorities/{caId}/status	✗

ca-properties

See below for the CA property-supported capabilities

Name	Description	Endpoint	Supported
CAPropertiesRetrieval	Retrieve CA properties	/v1/certificate-authorities/{caId}/properties	✗

general

See below for the general capabilities

Name	Description	Endpoint	Supported
PermitsDefaultCA	Can operate as the default CA		✓
SupportsMultipleCAs	Supports multiple CA configurations		✓

ECS CA capabilities

See below for the capabilities supported by the Certificate Authorities of the Entrust Certificate Services.

- enrollments
- certificates
- certificate-events
- subjects
- domains
- status

- ca-properties

enrollments

See below for the enrollment-supported capabilities

Name	Description	Endpoint	Supported
EnrollmentByCSR	Process certificate signing requests	/v1/certificate-authorities/{caId}/enrollments	✓
X509CertificateResponse	Returns certificate in X509 form	/v1/certificate-authorities/{caId}/enrollments	✓
PKCS12Response	Return certificate and key in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	✓
SANInCSR	Process Subject Alternative Names (SANs) in CSR	/v1/certificate-authorities/{caId}/enrollments	✗
SANInRequest	Process Subject Alternative Names (SANs) in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✓
SubjectNameInRequest	Supply subject name parameters in request to construct a subject DN in the supplied order	/v1/certificate-authorities/{caId}/enrollments	✗
CAGeneratedKey	Generate the key and returned it to client in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	✓
KeyInRequest	Supports client-generated keys for enrollment in the enrollment request	/v1/certificate-authorities/{caId}/enrollments	✗
CAGeneratedKeyBackup	Supports key backup for CA generated keys	/v1/certificate-authorities/{caId}/enrollments	✗
ClientGeneratedKeyBackup	Supports key backup for client-generated keys	/v1/certificate-authorities/{caId}/enrollments	✗
ExtensionInCSR	Process extension request in CSR	/v1/certificate-authorities/{caId}/enrollments	✓
ExtensionInRequest	Process extension request in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✗

Name	Description	Endpoint	Supported
ValidateProofOfPossesion	Validates proof of possession if requested	/v1/certificate-authorities/{caId}/enrollments	✗
ValidityPeriodInRequest	Supports validity period in request	/v1/certificate-authorities/{caId}/enrollments	✗

certificates

See below for the certificate-supported capabilities

Name	Description	Endpoint	Supported
SearchBySerial	Lookup certificate by serial number	/v1/certificate-authorities/{caId}/certificates/{serial}	✓
CertificateAction	List supported actions on a certificate	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✓
CertificateRevocationReason	List supported revocation reasons for the certificate RevokeAction	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✓

certificate-events

See below for the certificate-event-supported capabilities

Name	Description	Endpoint	Supported
CertificateEvents	Support certificate events	/v1/certificate-authorities/{caId}/certificate-events	✓
MaxCertificateEventsPageSize	Return the maximum size of the certificate events Page	/v1/certificate-authorities/{caId}/certificate-events	✓

subjects

See below for the subject management-supported capabilities

Name	Description	Endpoint	Supported
SearchBySubject DN	Lookup certificates by subject DN	/v1/certificate-authorities/{caId}/subjects/{dn}	✅
SubjectDNAction	List supported actions on a subject DN	/v1/certificate-authorities/{caId}/subjects/{dn}/actions	✅

domains

See below for the domain-supported capabilities

Name	Description	Endpoint	Supported
Verification Method	List of supported verification methods	/v1/certificate-authorities/{caId}/domains/{domain}	dns, email, manual, unknown, webServer
Verification Status	Supported verification statuses	/v1/certificate-authorities/{caId}/domains/{domain}	APPROVED, CANCELLED, DECLINED, EXPIRED, EXPIRING, INITIAL_VERIFICATION
Filter	Supported filters for domain search	/v1/certificate-authorities/{caId}/domains	domainName, evEligible, evExpiry, ovEligible, ovExpiry, verificationMethod, verificationStatus

status

See below for the status-supported capabilities

Name	Description	Endpoint	Supported
CAStatus	Check whether the CA is up or down	/v1/certificate-authorities/{caId}/status	✅

ca-properties

See below for the CA property-supported capabilities

Name	Description	Endpoint	Supported
CAPropertiesRetrieval	Retrieve CA properties	/v1/certificate-authorities/{caId}/properties	❌

EJBCA capabilities

See below for the capabilities supported by EJB Certificate Authorities (EJBCAs).

- enrollments
- certificates
- certificate-events
- ca-events
- recoveries
- subjects
- status
- ca-properties

enrollments

See below for the enrollment-supported capabilities

Name	Description	Endpoint	Supported
EnrollmentByCSR	Process certificate signing requests	/v1/certificate-authorities/{caId}/enrollments	✓
X509CertificateResponse	Returns certificate in X509 form	/v1/certificate-authorities/{caId}/enrollments	✓
PKCS12Response	Return certificate and key in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	✓
SANInCSR	Process Subject Alternative Names (SANs) in CSR	/v1/certificate-authorities/{caId}/enrollments	✓
SANInRequest	Process Subject Alternative Names (SANs) in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✓
SubjectNameInRequest	Supply subject name parameters in request to construct a subject DN in the supplied order	/v1/certificate-authorities/{caId}/enrollments	✓
CAGeneratedKey	Generate the key and returned it to client in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	✓
KeyInRequest	Supports client-generated keys for enrollment in the enrollment request	/v1/certificate-authorities/{caId}/enrollments	✗
CAGeneratedKeyBackup	Supports key backup for CA generated keys	/v1/certificate-authorities/{caId}/enrollments	✓

Name	Description	Endpoint	Supported
ClientGeneratedKeyBackup	Supports key backup for client-generated keys	/v1/certificate-authorities/{caId}/enrollments	✗
ExtensionInCSR	Process extension request in CSR	/v1/certificate-authorities/{caId}/enrollments	✓
ExtensionInRequest	Process extension request in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✗
ValidateProofOfPossesion	Validates proof of possession if requested	/v1/certificate-authorities/{caId}/enrollments	✓
ValidityPeriodInRequest	Supports validity period in request	/v1/certificate-authorities/{caId}/enrollments	✓

certificates

See below for the certificate-supported capabilities

Name	Description	Endpoint	Supported
SearchBySerial	Lookup certificate by serial number	/v1/certificate-authorities/{caId}/certificates/{serial}	✓
CertificateAction	List supported actions on a certificate	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✓
CertificateRevocationReason	List supported revocation reasons for the certificate RevokeAction	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✓

certificate-events

See below for the certificate-event-supported capabilities

Name	Description	Endpoint	Supported
CertificateEvents	Support certificate events	/v1/certificate-authorities/{caId}/certificate-events	✓

Name	Description	Endpoint	Supported
MaxCertificateEventsPageSize	Return the maximum size of the certificate events Page	/v1/certificate-authorities/{caId}/certificate-events	✓

ca-events

See below for the event-supported capabilities

Name	Description	Endpoint	Supported
CAEvents	Support CA events	/v1/certificate-authorities/{caId}/ca-events	✗

recoveries

See below for the recovery-supported capabilities

Name	Description	Endpoint	Supported
Recover	Recover certificate by DN	/v1/certificate-authorities/{caId}/recoveries/{dn}	✓

subjects

See below for the subject management-supported capabilities

Name	Description	Endpoint	Supported
SearchBySubjectDN	Lookup certificates by subject DN	/v1/certificate-authorities/{caId}/subjects/{dn}	✓
SubjectDNAction	List supported actions on a subject DN	/v1/certificate-authorities/{caId}/subjects/{dn}/actions	✓

status

See below for the status-supported capabilities

Name	Description	Endpoint	Supported
CAStatus	Check whether the CA is up or down	/v1/certificate-authorities/{caId}/status	✓

ca-properties

See below for the CA property-supported capabilities

Name	Description	Endpoint	Supported
CAPropertiesRetrieval	Retrieve CA properties	/v1/certificate-authorities/{caId}/properties	✅

Entrust CA capabilities

See below for the capabilities supported by Entrust Certificate Authorities.

- enrollments
- certificates
- certificate-events
- subjects
- domains
- status
- ca-properties

enrollments

See below for the enrollment-supported capabilities

Name	Description	Endpoint	Supported
EnrollmentByCSR	Process certificate signing requests	/v1/certificate-authorities/{caId}/enrollments	✅
X509CertificateResponse	Returns certificate in X509 form	/v1/certificate-authorities/{caId}/enrollments	✅
PKCS12Response	Return certificate and key in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	✅
SANInCSR	Process Subject Alternative Names (SANs) in CSR	/v1/certificate-authorities/{caId}/enrollments	❌
SANInRequest	Process Subject Alternative Names (SANs) in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✅
SubjectNameInRequest	Supply subject name parameters in request to construct a subject DN in the supplied order	/v1/certificate-authorities/{caId}/enrollments	❌

Name	Description	Endpoint	Supported
CAGeneratedKey	Generate the key and returned it to client in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	✓
KeyInRequest	Supports client-generated keys for enrollment in the enrollment request	/v1/certificate-authorities/{caId}/enrollments	✗
CAGeneratedKeyBackup	Supports key backup for CA generated keys	/v1/certificate-authorities/{caId}/enrollments	✗
ClientGeneratedKeyBackup	Supports key backup for client-generated keys	/v1/certificate-authorities/{caId}/enrollments	✗
ExtensionInCSR	Process extension request in CSR	/v1/certificate-authorities/{caId}/enrollments	✓
ExtensionInRequest	Process extension request in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✗
ValidateProofOfPossesion	Validates proof of possession if requested	/v1/certificate-authorities/{caId}/enrollments	✗
ValidityPeriodInRequest	Supports validity period in request	/v1/certificate-authorities/{caId}/enrollments	✗

certificates

See below for the certificate-supported capabilities

Name	Description	Endpoint	Supported
SearchBySerial	Lookup certificate by serial number	/v1/certificate-authorities/{caId}/certificates/{serial}	✓
CertificateAction	List supported actions on a certificate	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✓
CertificateRevocationReason	List supported revocation reasons for the certificate RevokeAction	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✓

certificate-events

See below for the certificate-event-supported capabilities

Name	Description	Endpoint	Supported
CertificateEvents	Support certificate events	/v1/certificate-authorities/{caId}/certificate-events	✓
MaxCertificateEventsPageSize	Return the maximum size of the certificate events Page	/v1/certificate-authorities/{caId}/certificate-events	✓

subjects

See below for the subject management-supported capabilities

Name	Description	Endpoint	Supported
SearchBySubjectDN	Lookup certificates by subject DN	/v1/certificate-authorities/{caId}/subjects/{dn}	✓
SubjectDNAction	List supported actions on a subject DN	/v1/certificate-authorities/{caId}/subjects/{dn}/actions	✓

domains

See below for the domain-supported capabilities

Name	Description	Endpoint	Supported
Verification Method	List of supported verification methods	/v1/certificate-authorities/{caId}/domains/{domain}	dns, email, manual, unknown, webServer
Verification Status	Supported verification statuses	/v1/certificate-authorities/{caId}/domains/{domain}	APPROVED, CANCELLED, DECLINED, EXPIRED, EXPIRING, INITIAL_VERIFICATION
Filter	Supported filters for domain search	/v1/certificate-authorities/{caId}/domains	domainName, evEligible, evExpiry, ovEligible, ovExpiry, verificationMethod, verificationStatus

status

See below for the status-supported capabilities

Name	Description	Endpoint	Supported
CAStatus	Check whether the CA is up or down	/v1/certificate-authorities/{caId}/status	✅

ca-properties

See below for the CA property-supported capabilities

Name	Description	Endpoint	Supported
CAPropertiesRetrieval	Retrieve CA properties	/v1/certificate-authorities/{caId}/properties	❌

Microsoft CA capabilities

See below for the capabilities supported by Microsoft Certificate Authorities.

- enrollments
- certificates
- certificate-events
- recoveries
- subjects
- status
- ca-properties

enrollments

See below for the enrollment-supported capabilities

Name	Description	Endpoint	Supported
EnrollmentByCSR	Process certificate signing requests	/v1/certificate-authorities/{caId}/enrollments	✅
X509CertificateResponse	Returns certificate in X509 form	/v1/certificate-authorities/{caId}/enrollments	✅
PKCS12Response	Return certificate and key in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	✅
SANInCSR	Process Subject Alternative Names (SANs) in CSR	/v1/certificate-authorities/{caId}/enrollments	✅
SANInRequest	Process Subject Alternative Names (SANs) in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✅

Name	Description	Endpoint	Supported
SubjectNameInRequest	Supply subject name parameters in request to construct a subject DN in the supplied order	/v1/certificate-authorities/{caId}/enrollments	✗
CAGeneratedKey	Generate the key and returned it to client in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	✓
KeyInRequest	Supports client-generated keys for enrollment in the enrollment request	/v1/certificate-authorities/{caId}/enrollments	✓
CAGeneratedKeyBackup	Supports key backup for CA generated keys	/v1/certificate-authorities/{caId}/enrollments	✓
ClientGeneratedKeyBackup	Supports key backup for client-generated keys	/v1/certificate-authorities/{caId}/enrollments	✓
ExtensionInCSR	Process extension request in CSR	/v1/certificate-authorities/{caId}/enrollments	✓
ExtensionInRequest	Process extension request in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✗
ValidateProofOfPossesion	Validates proof of possession if requested	/v1/certificate-authorities/{caId}/enrollments	✗
ValidityPeriodInRequest	Supports validity period in request	/v1/certificate-authorities/{caId}/enrollments	✗

certificates

See below for the certificate-supported capabilities

Name	Description	Endpoint	Supported
SearchBySerial	Lookup certificate by serial number	/v1/certificate-authorities/{caId}/certificates/{serial}	✓
CertificateAction	List supported actions on a certificate	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✓

Name	Description	Endpoint	Supported
CertificateRevocationReason	List supported revocation reasons for the certificate RevokeAction	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✓

certificate-events

See below for the certificate-event-supported capabilities

Name	Description	Endpoint	Supported
CertificateEvents	Support certificate events	/v1/certificate-authorities/{caId}/certificate-events	✓
MaxCertificateEventsPageSize	Return the maximum size of the certificate events Page	/v1/certificate-authorities/{caId}/certificate-events	✓

recoveries

See below for the recovery-supported capabilities

Name	Description	Endpoint	Supported
Recover	Recover certificate by DN	/v1/certificate-authorities/{caId}/recoveries/{dn}	✓

subjects

See below for the subject management-supported capabilities

Name	Description	Endpoint	Supported
SearchBySubjectDN	Lookup certificates by subject DN	/v1/certificate-authorities/{caId}/subjects/{dn}	✓
SubjectDNAction	List supported actions on a subject DN	/v1/certificate-authorities/{caId}/subjects/{dn}/actions	✓

status

See below for the status-supported capabilities

Name	Description	Endpoint	Supported
CAStatus	Check whether the CA is up or down	/v1/certificate-authorities/{caId}/status	✗

ca-properties

See below for the CA property-supported capabilities

Name	Description	Endpoint	Supported
CAPropertiesRetrieval	Retrieve CA properties	/v1/certificate-authorities/{caId}/properties	✗

Sectigo CA capabilities

See below for the capabilities supported by Entrust Certificate Authorities.

- enrollments
- certificates
- ca-events
- recoveries
- subjects
- status
- ca-properties

enrollments

See below for the enrollment-supported capabilities

Name	Description	Endpoint	Supported
EnrollmentByCSR	Process certificate signing requests	/v1/certificate-authorities/{caId}/enrollments	✓
X509CertificateResponse	Returns certificate in X509 form	/v1/certificate-authorities/{caId}/enrollments	✓
PKCS12Response	Return certificate and key in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	✓
SANInCSR	Process Subject Alternative Names (SANs) in CSR	/v1/certificate-authorities/{caId}/enrollments	✓
SANInRequest	Process Subject Alternative Names (SANs) in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✓

Name	Description	Endpoint	Supported
SubjectNameInRequest	Supply subject name parameters in request to construct a subject DN in the supplied order	/v1/certificate-authorities/{caId}/enrollments	✓
CAGeneratedKey	Generate the key and returned it to client in PKCS#12 form	/v1/certificate-authorities/{caId}/enrollments	✓
KeyInRequest	Supports client-generated keys for enrollment in the enrollment request	/v1/certificate-authorities/{caId}/enrollments	✓
CAGeneratedKeyBackup	Supports key backup for CA generated keys	/v1/certificate-authorities/{caId}/enrollments	✓
ClientGeneratedKeyBackup	Supports key backup for client-generated keys	/v1/certificate-authorities/{caId}/enrollments	✓
ExtensionInCSR	Process extension request in CSR	/v1/certificate-authorities/{caId}/enrollments	✓
ExtensionInRequest	Process extension request in enrollment request	/v1/certificate-authorities/{caId}/enrollments	✓
ValidateProofOfPossesion	Validates proof of possession if requested	/v1/certificate-authorities/{caId}/enrollments	✓
ValidityPeriodInRequest	Supports validity period in request	/v1/certificate-authorities/{caId}/enrollments	✓

certificates

See below for the certificate-supported capabilities

Name	Description	Endpoint	Supported
SearchBySerial	Lookup certificate by serial number	/v1/certificate-authorities/{caId}/certificates/{serial}	✓
CertificateAction	List supported actions on a certificate	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✓

Name	Description	Endpoint	Supported
CertificateRevocationReason	List supported revocation reasons for the certificate RevokeAction	/v1/certificate-authorities/{caId}/certificates/{serial}/actions	✅

ca-events

See below for the event-supported capabilities

Name	Description	Endpoint	Supported
CAEvents	Support CA events	/v1/certificate-authorities/{caId}/ca-events	✅

recoveries

See below for the recovery-supported capabilities

Name	Description	Endpoint	Supported
Recover	Recover certificate by DN	/v1/certificate-authorities/{caId}/recoveries/{dn}	✅

subjects

See below for the subject management-supported capabilities

Name	Description	Endpoint	Supported
SearchBySubjectDN	Lookup certificates by subject DN	/v1/certificate-authorities/{caId}/subjects/{dn}	✅
SubjectDNAction	List supported actions on a subject DN	/v1/certificate-authorities/{caId}/subjects/{dn}/actions	✅

status

See below for the status-supported capabilities

Name	Description	Endpoint	Supported
CAStatus	Check whether the CA is up or down	/v1/certificate-authorities/{caId}/status	✅

ca-properties

See below for the CA property-supported capabilities

Name	Description	Endpoint	Supported
CAPropertiesRetrieval	Retrieve CA properties	/v1/certificate-authorities/{caId}/properties	✔

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 partition administrators
- Creating partitions
- Onboarding and adding partition administrators
- Using Certificate Authority
- 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>:8443/management-console
   ```

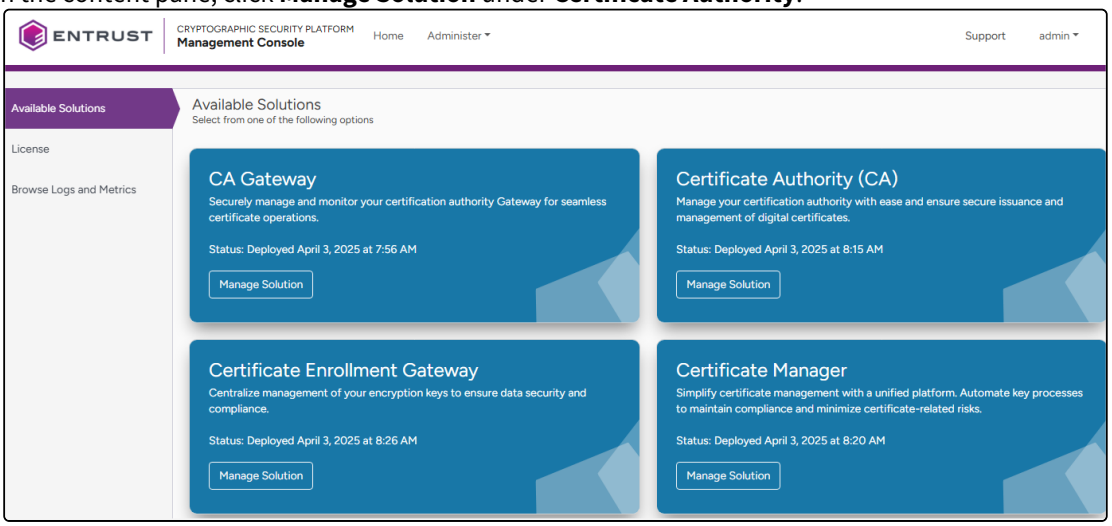
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

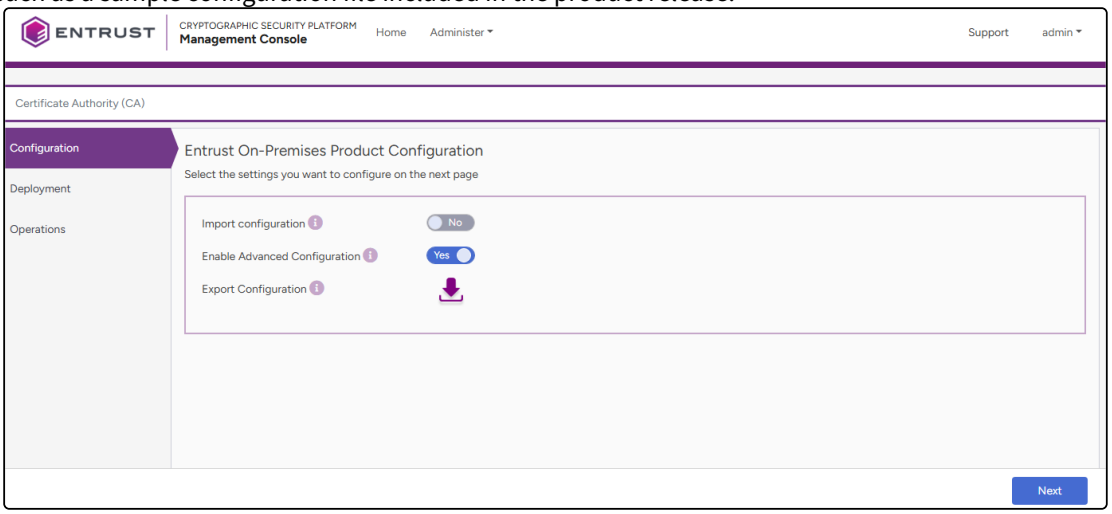
2. Log in to the Management Console as a user belonging to a role with permissions to manage Certificate Authorities – for example, the initial `admin` administrator user.

   > ℹ See Managing identities 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)

The databases for the cluster and the solutions can be hosted on the same DBMS. However, do not merge tables from different solutions into a single database. Both the cluster and each solution require their own dedicated 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
- The nShield kmdata tar file

> ⛔ 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 Administrating 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: When selecting **nShield** in **Vendor**.

The nShield kmdata tar file

Click **Choose File** to import the file described in Creating the kmdata.tar file.

Mandatory: When selecting **nShield** in **Vendor**.

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 partition administrators

To create an administrator with permissions on a Certificate Authority partition, follow the steps described in Users to create a user with the PkihubRole role.

Creating partitions

Create at least a partition for your certificate authorities and certificates.

> A partition is a dedicated and secure environment for a customer to manage and run a PKI. Each partition ensures the customer's data, operations, and resources are separate and protected while supporting scalability and customization.

To create a partition

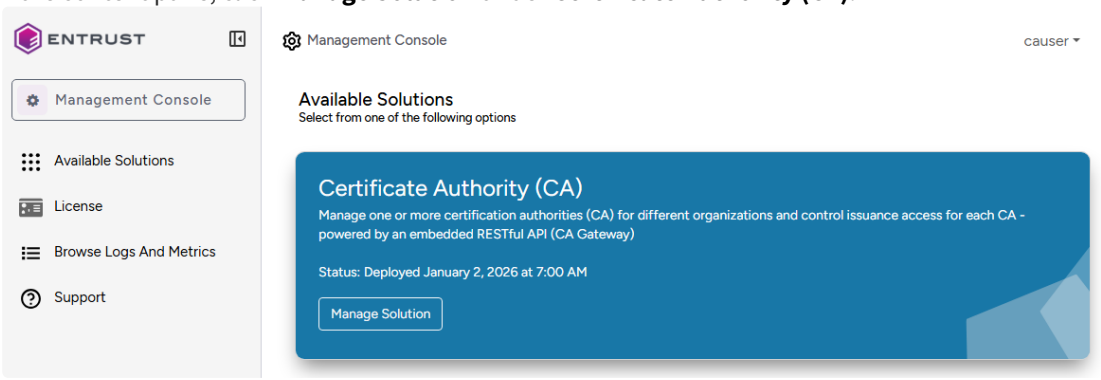
1. Open the following URL in a Web browser.

   ```
   https://<machine>:8443/management-console
   ```

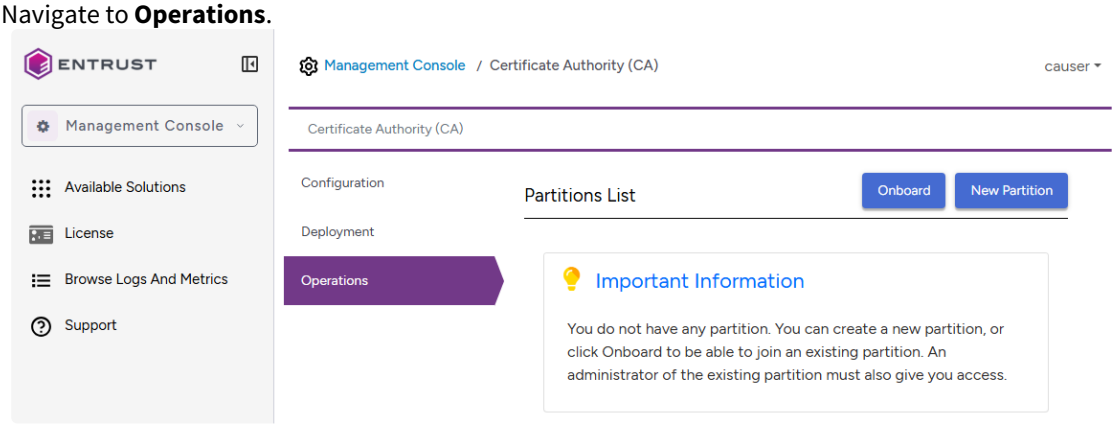
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

> ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the content pane, click **Manage Solution** under **Certificate Authority (CA)**.



4. Navigate to **Operations**.



5. If not yey onboarded, click **Onboard**.
6. Click **New Partition**.
7. Enter a unique partition identifier in the Create Partition dialog.

> ⚠ The partition identifier must be between 3 and 14 characters long and contain only letters a-z or numbers.

8. Click **Create** to confirm the partition creation.

Onboarding and adding partition administrators

See below for onboarding and adding administrators to an existing partition.

- Onboarding partition administrators
- Adding partition administrators

> ℹ As explained in Creating partitions, users who create a partition are automatically onboarded and added as administrators of the new partition.

Onboarding partition administrators

Onboard administrators before adding them to an existing partition.

To onboard a partition administrator

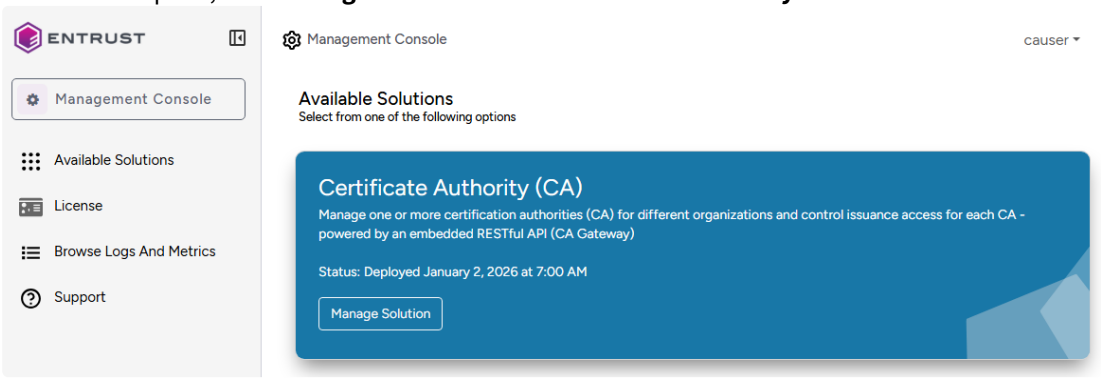
1. Create a user with the settings described in Creating partition administrators.
2. Open the following URL in a Web browser.

```
https://<machine>:8443/management-console
```

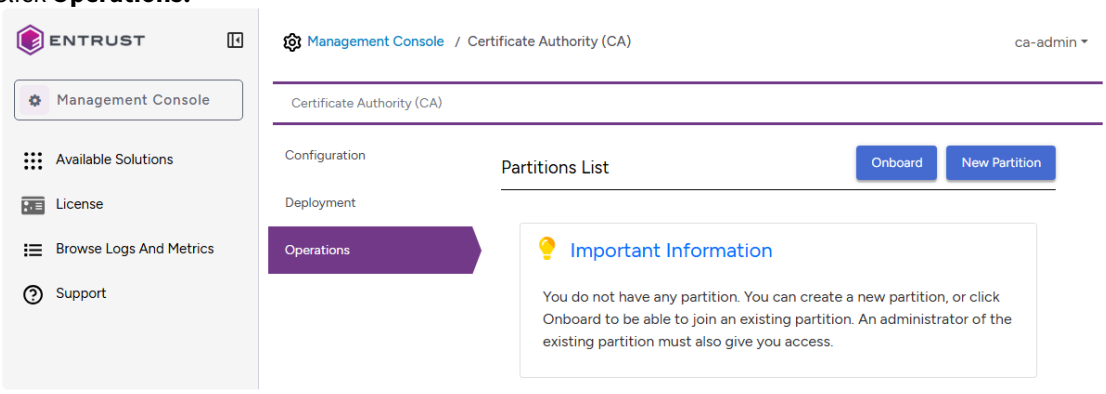
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

> ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

3. Log in to the Management Console as the new user.
4. In the content pane, click **Manage Solution** under **Certificate Authority**.



5. Click **Operations.**



6. Click **Onboard**.

Adding partition administrators

Once onboarded, administrators can be added to an existing partition.

To add a partition administrator

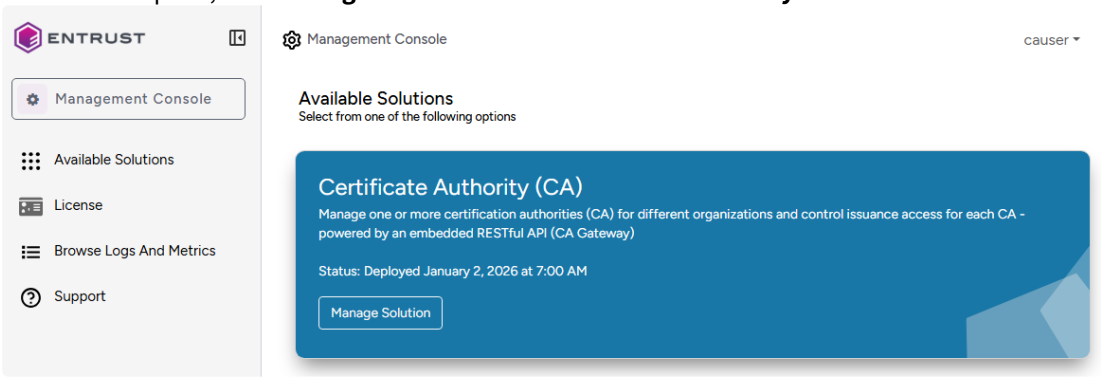
1. Open the following URL in a Web browser.

```
https://<machine>:8443/management-console
```

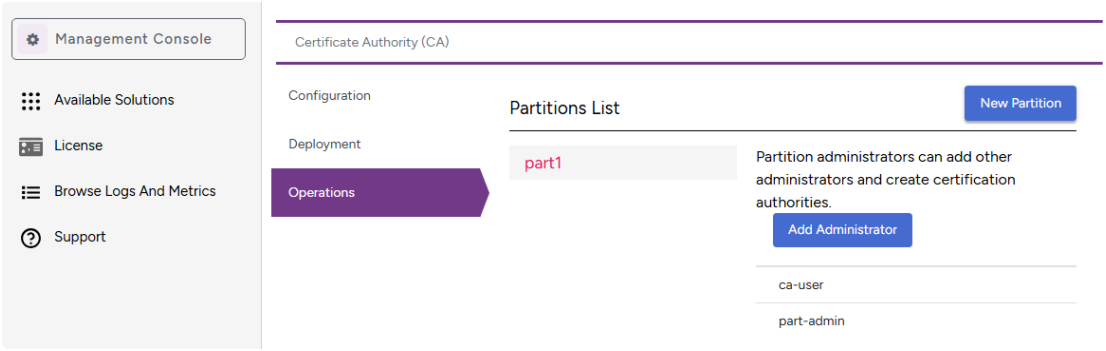
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

> ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

2. Log in to the Management Console as a partition administrator – for example, as the user who created the partition.
3. In the content pane, click **Manage Solution** under **Certificate Authority**.



4. Click **Operations.**



5. Click **Add Administrator**.
6. Enter the name of a user who has been previously onboarded, as explained in Onboarding partition administrators.
7. Click **Add**.

Using Certificate Authority

See below for using Certificate Authority to manage your certificate authorities and certificates.

- Managing certificate authority instances
- Managing certificate profiles
- Managing Certificate Authority users
- Managing certificates
- Integrating client applications

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

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

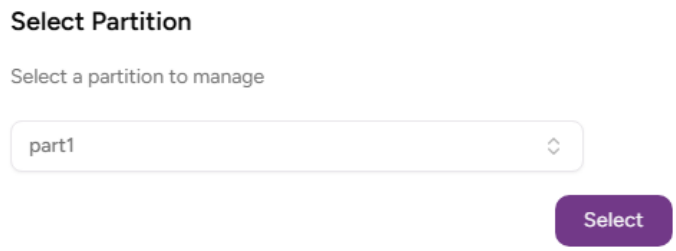
1. Open the following URL in a Web browser.

   ```
   https://<machine>/v2/
   ```

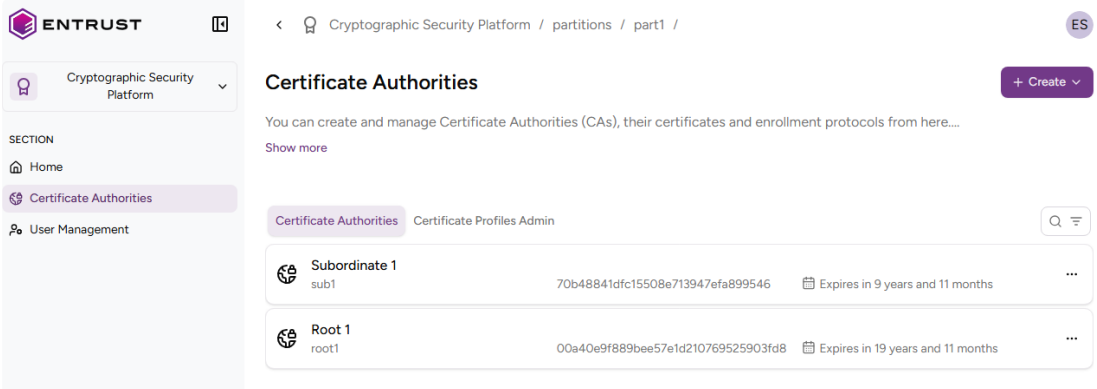
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > ⚠ Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.

4. Click **Select**.
5. Click **Certificate Authorities** on the sidebar.

6. Click **Create > Certificate Authority**.

7. Configure the following settings.
    - CA Type
    - CA Identifier
    - Friendly Name
    - Signing Key Type
    - Expiration Date
    - Certificate Profiles
    - Subject
8. Click **Create** to create the new Certificate Authority.

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

Select a combination of cryptosystem and hash algorithm for the new CA to sign certificates.

- The available algorithms on this list depend on the configured cryptographic module.
- 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

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
RSA-2048+PKCS15-SHA256	RSA2048	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-2048+PSS-SHA256	RSA2048	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
RSA-3072+PKCS15-SHA256	RSA3072	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-3072+PSS-SHA256	RSA3072	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-4096+PKCS15-SHA512	RSA4096	sha512WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-4096+PSS-SHA512	RSA4096	sha512WithRSAPSS	RSA2048	sha256WithRSAPSS
ECDSAP256+SHA256	ECDSAP256	ecdsa-with-SHA256	RSA2048	sha256WithRSAEncryption
ECDSAP384+SHA384	ECDSAP384	ecdsa-with-SHA384	RSA2048	sha256WithRSAEncryption
ECDSAP521+SHA512	ECDSAP521	ecdsa-with-SHA512	RSA2048	sha256WithRSAEncryption
ML-DSA-44	ML-DSA-44	ML-DSA-44	RSA2048	sha256WithRSAEncryption
ML-DSA-65	ML-DSA-65	ML-DSA-65	RSA2048	sha256WithRSAEncryption
ML-DSA-87	ML-DSA-87	ML-DSA-87	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	RSA2048	sha256WithRSAEncryption
Falcon-512	Falcon-512	Falcon-512	RSA2048	sha256WithRSAEncryption
Falcon-1024	Falcon-1024	Falcon-1024	RSA2048	sha256WithRSAEncryption

Mandatory: Yes.

Expiration Date

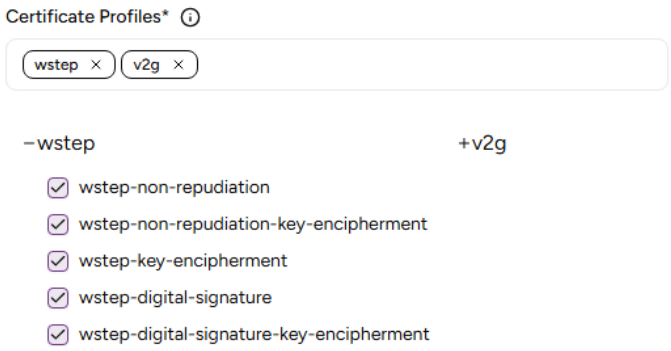
The expiration date for the certificate signing certificate of the Certificate Authority.

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

Certificate Profiles

The profiles the Certificate Authority will support for issuing certificates. After selecting a profile group in the Certificate Profiles field, click the plus sign (“+”) to view, select, and unselect the profiles in that group.



See a complete reference of these profiles at the Entrust PKIaaS online guide.

Profiles	URL
Profiles for issuing authority certificates	https://docs.pkiaas.entrust.com/profiles/browse/authority
Profiles for issuing subscriber certificates	https://docs.pkiaas.entrust.com/profiles/browse/subscriber

Mandatory: Select at least one profile.

Subject

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.

Adding an external root certificate authority

See below for adding an external root 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.

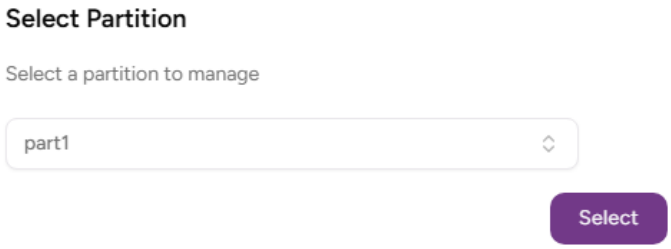
   ```
   https://<machine>/v2/
   ```

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

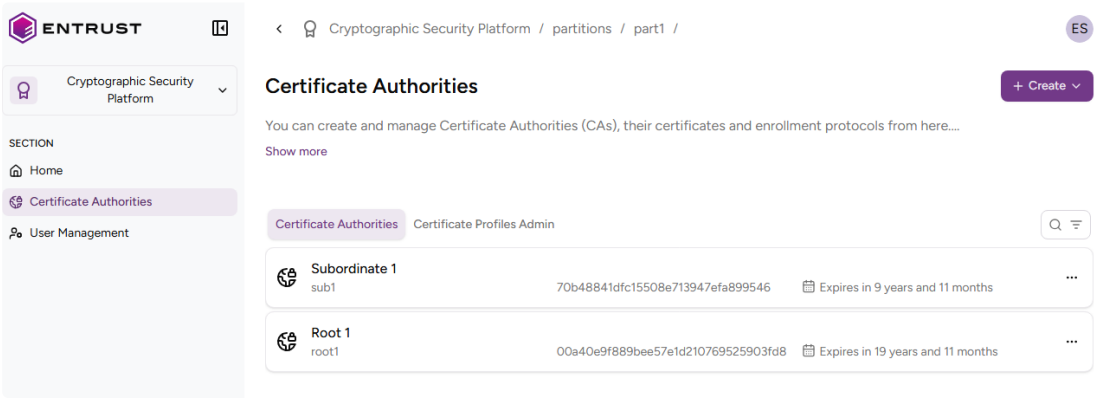
   > Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.

3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.



4. Click **Select**.
5. Click **Certificate Authorities** on the sidebar.



6. Click **Create > Certificate Authority**.
7. Configure the following settings.
   - CA Type
   - CA Identifier
   - Friendly Name
   - Root CA Certificate
8. Click **Create** 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.

Root CA Certificate

Click Choose file and import the PEM-encoded certificate of the external CA.

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 instructions on creating an intermediate CA.

> If the root CA of the new CA is an external CA, you must have at hand the certificate issued by the external CA for the new CA.

To create an intermediate certificate authority

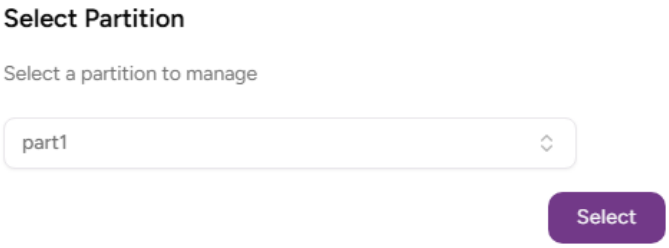
1. Open the following URL in a Web browser.

   ```
   https://<machine>/v2/
   ```

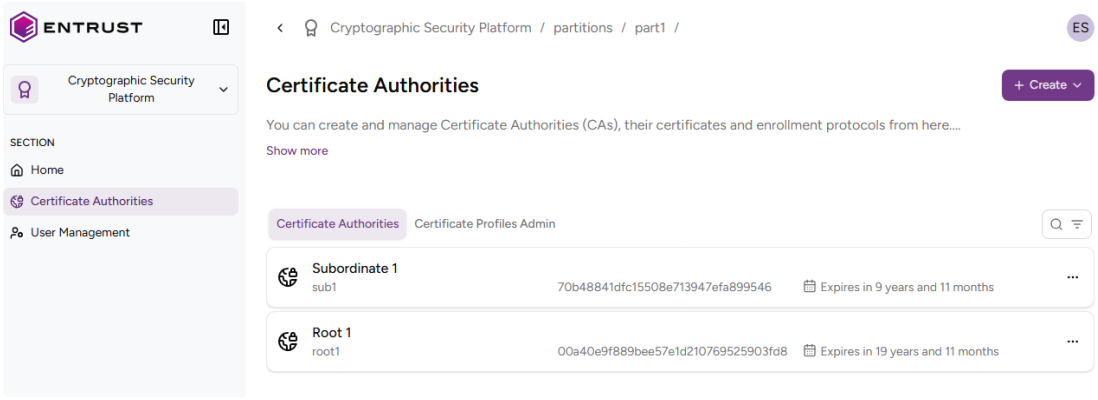
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > Do not omit the ending forward slash "/" on this URL.

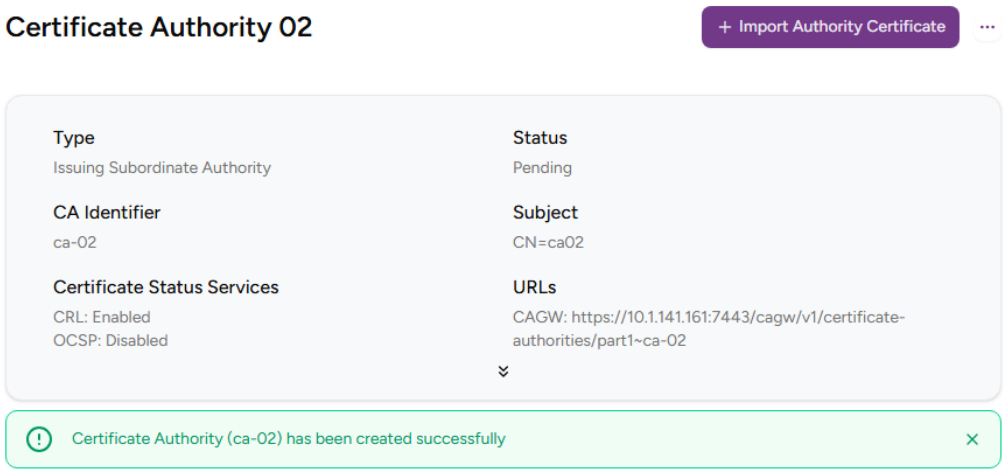
2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.

4. Click **Select**.
5. Click **Certificate Authorities** on the sidebar.



6. Click **Create > Certificate Authority**.
7. Configure the following settings.
    - CA Type
    - CA Identifier
    - Friendly Name
    - Parent CA Identifier
    - Signing Key Type
    - Expiration Date
    - Certificate Profiles
    - Subject
8. Click **Create** to create the new Certificate Authority.
9. If the parent CA is an external CA:
    a. Click **Import Authority Certificate**.



    b. Select a file that contains the PEM-encoded certificate for the new CA, signed by the external CA.

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.

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.

Parent CA Identifier

The identifier of the parent Certificate Authority.

⚠ The selector list only includes root or intermediate authorities with the Intermediate authority certificate profile enabled.

Mandatory: Yes.

Signing Key Type

Select a combination of cryptosystem and hash algorithm for the new CA to sign certificates.

- The available algorithms on this list depend on the configured cryptographic module.
- 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

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
RSA-2048+PKCS15-SHA256	RSA2048	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-2048+PSS-SHA256	RSA2048	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-3072+PKCS15-SHA256	RSA3072	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-3072+PSS-SHA256	RSA3072	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-4096+PKCS15-SHA512	RSA4096	sha512WithRSAEncryption	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
RSA-4096+PSS-SHA512	RSA4096	sha512WithRSAPSS	RSA2048	sha256WithRSAPSS
ECDSAP256+SHA256	ECDSAP256	ecdsa-with-SHA256	RSA2048	sha256WithRSAEncryption
ECDSAP384+SHA384	ECDSAP384	ecdsa-with-SHA384	RSA2048	sha256WithRSAEncryption
ECDSAP521+SHA512	ECDSAP521	ecdsa-with-SHA512	RSA2048	sha256WithRSAEncryption
ML-DSA-44	ML-DSA-44	ML-DSA-44	RSA2048	sha256WithRSAEncryption
ML-DSA-65	ML-DSA-65	ML-DSA-65	RSA2048	sha256WithRSAEncryption
ML-DSA-87	ML-DSA-87	ML-DSA-87	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	RSA2048	sha256WithRSAEncryption
Falcon-512	Falcon-512	Falcon-512	RSA2048	sha256WithRSAEncryption
Falcon-1024	Falcon-1024	Falcon-1024	RSA2048	sha256WithRSAEncryption

Mandatory: Yes.

Expiration Date

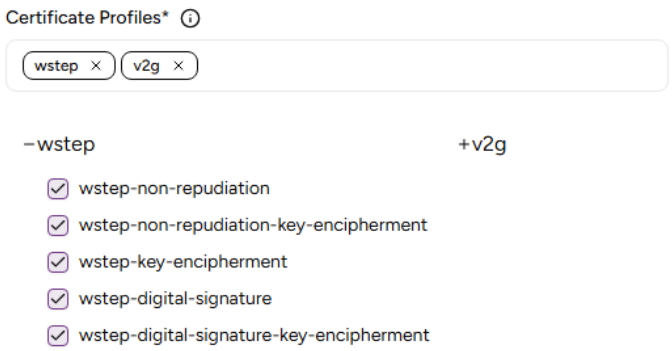
The expiration date for the certificate signing certificate of the Certificate Authority.

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

Certificate Profiles

The profiles the Certificate Authority will support for issuing certificates. After selecting a profile group in the Certificate Profiles field, click the plus sign (“+”) to view, select, and unselect the profiles in that group.



See a complete reference of these profiles at the Entrust PKIaaS online guide.

Profiles	URL
Profiles for issuing authority certificates	https://docs.pkiaas.entrust.com/profiles/browse/authority
Profiles for issuing subscriber certificates	https://docs.pkiaas.entrust.com/profiles/browse/subscriber

Mandatory: Select at least one profile.

Subject

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.

Creating an issuing certificate authority

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

> If the root CA of the new CA is an external CA, you must have at hand the certificate issued by the external CA for the new CA.

To create an issuing certificate authority

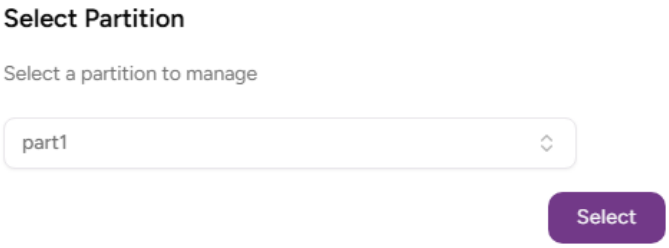
1. Open the following URL in a Web browser.

   ```
   https://<machine>/v2/
   ```

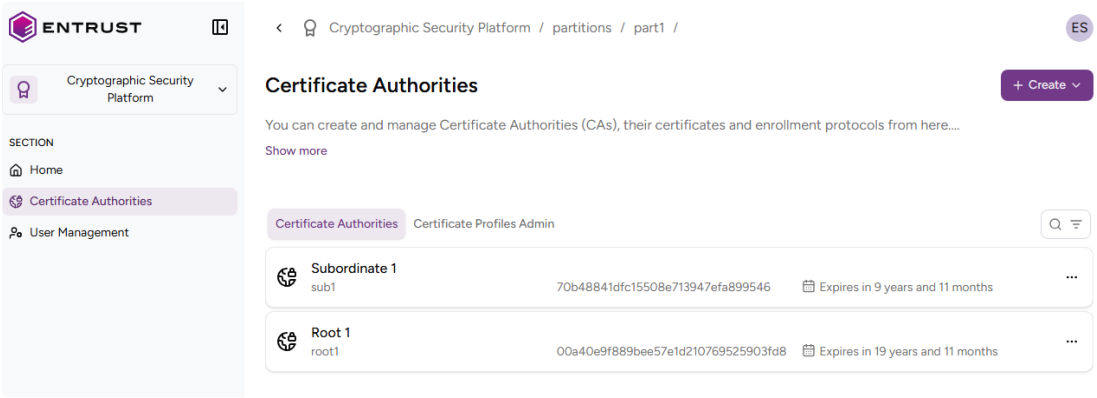
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > Do not omit the ending forward slash "/" on this URL.

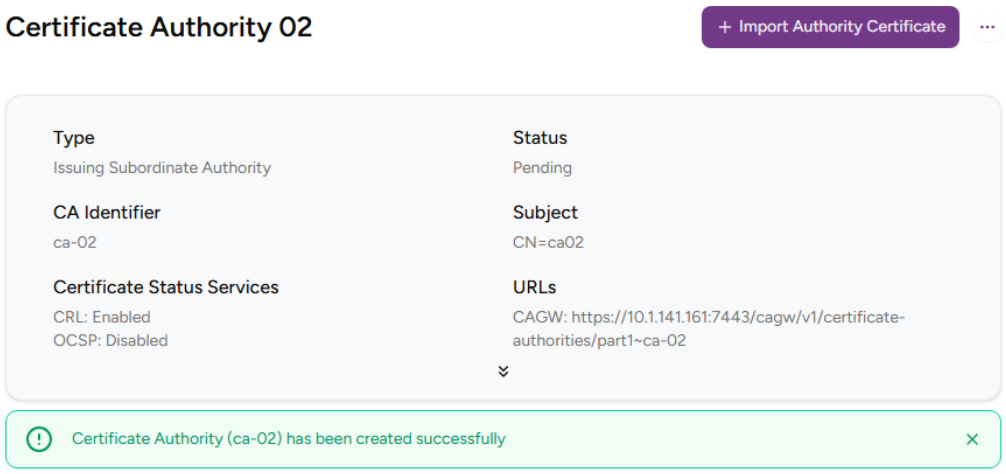
2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.

4. Click **Select**.
5. Click **Certificate Authorities** on the sidebar.



6. Click **Create > Certificate Authority**.
7. Configure the following settings.
    - CA Type
    - CA Identifier
    - Friendly Name
    - Parent CA Identifier
    - Signing Key Type
    - Certificate Profiles
    - Expiration Date
    - Subject
8. Click **Create** to create the new Certificate Authority.
9. If the parent CA is an external CA:
    a. Click **Import Authority Certificate**.



    b. Select a file that contains the PEM-encoded certificate for the new CA, signed by the external CA.

CA Type

Click **Issuing 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.

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.

Parent CA Identifier

The identifier of the parent Certificate Authority.

⚠ The selector list only includes root or intermediate authorities with the Basic authority certificate profiles or Intermediate authority certificate profile enabled.

Mandatory: Yes.

Signing Key Type

Select a combination of cryptosystem and hash algorithm for the new CA to sign certificates.

- The available algorithms on this list depend on the configured cryptographic module.
- 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

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
RSA-2048+PKCS15-SHA256	RSA2048	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-2048+PSS-SHA256	RSA2048	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-3072+PKCS15-SHA256	RSA3072	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-3072+PSS-SHA256	RSA3072	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-4096+PKCS15-SHA512	RSA4096	sha512WithRSAEncryption	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
RSA-4096+PSS-SHA512	RSA4096	sha512WithRSAPSS	RSA2048	sha256WithRSAPSS
ECDSAP256+SHA256	ECDSAP256	ecdsa-with-SHA256	RSA2048	sha256WithRSAEncryption
ECDSAP384+SHA384	ECDSAP384	ecdsa-with-SHA384	RSA2048	sha256WithRSAEncryption
ECDSAP521+SHA512	ECDSAP521	ecdsa-with-SHA512	RSA2048	sha256WithRSAEncryption
ML-DSA-44	ML-DSA-44	ML-DSA-44	RSA2048	sha256WithRSAEncryption
ML-DSA-65	ML-DSA-65	ML-DSA-65	RSA2048	sha256WithRSAEncryption
ML-DSA-87	ML-DSA-87	ML-DSA-87	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	RSA2048	sha256WithRSAEncryption

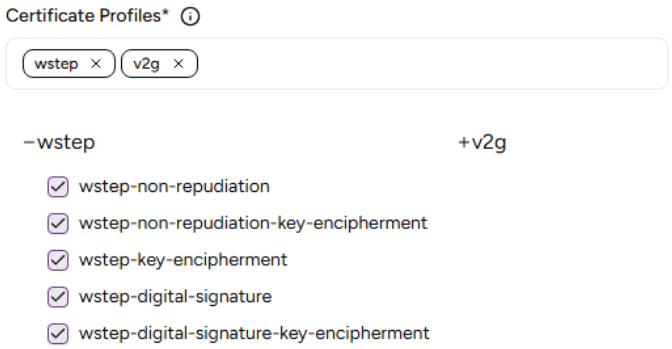
Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	RSA2048	sha256WithRSAEncryption
Falcon-512	Falcon-512	Falcon-512	RSA2048	sha256WithRSAEncryption
Falcon-1024	Falcon-1024	Falcon-1024	RSA2048	sha256WithRSAEncryption

Mandatory: Yes.

Certificate Profiles

The profiles the Certificate Authority will support for issuing certificates. After selecting a profile group in the Certificate Profiles field, click the plus sign (“+”) to view, select, and unselect the profiles in that group.



See a complete reference of these profiles at the Entrust PKIaaS online guide.

Profiles	URL
Profiles for issuing authority certificates	https://docs.pkiaas.entrust.com/profiles/browse/authority
Profiles for issuing subscriber certificates	https://docs.pkiaas.entrust.com/profiles/browse/subscriber

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

Subject

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.

Managing certificate profiles

See below for managing certificate profiles.

- Browsing certificate profiles
- Creating certificate profiles
- Updating the certificate profiles of a certificate authority

Browsing certificate profiles

See below for browsing existing certificate profiles.

To browse certificate profiles

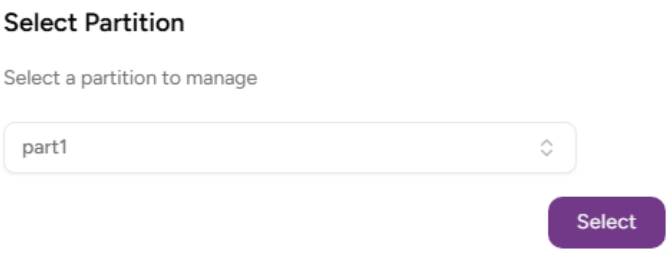
1. Open the following URL in a Web browser.

   ```
   https://<machine>/v2/
   ```

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

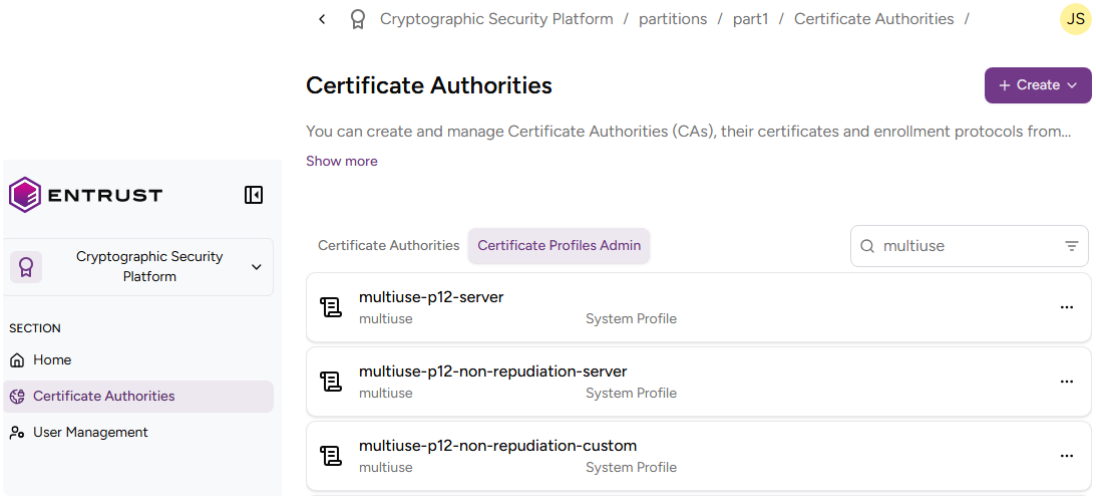
   > ⚠ Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.

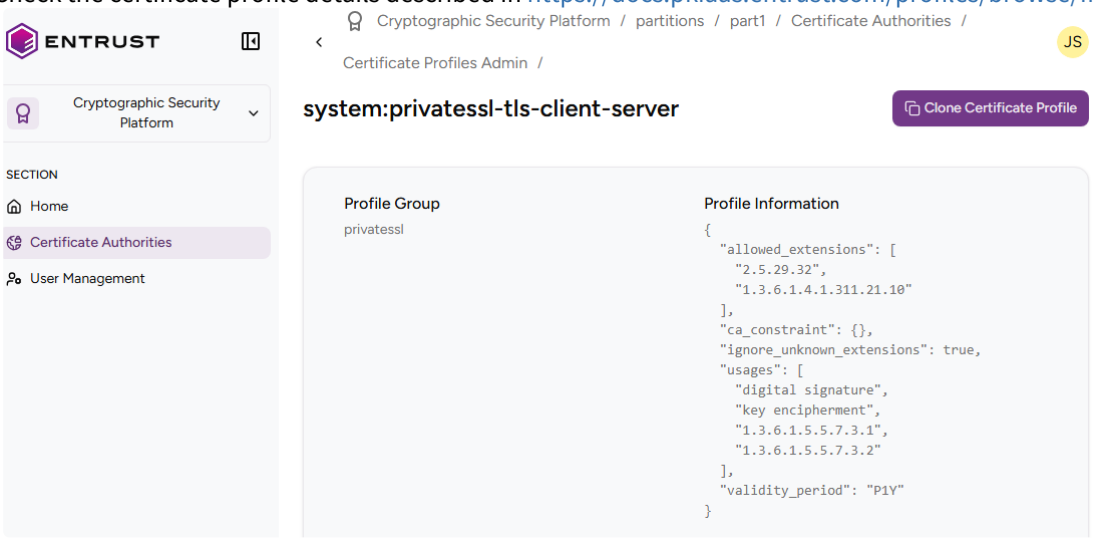
   

4. Click **Select**.

5. Click **Certificate Authorities** in the sidebar and select the **Certificate Profiles Admin** tab.



6. Browse the list of certificate profiles.
7. Click the name of a certificate profile.
8. Check the certificate profile details described in https://docs.pkiaas.entrust.com/profiles/browse/fields



Creating certificate profiles

See below for creating certificate profiles.

To create certificate profiles

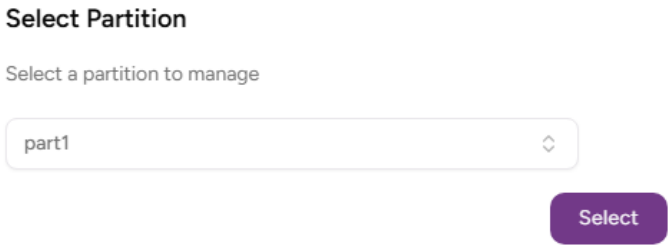
1. Open the following URL in a Web browser.

```
https://<machine>/v2/
```

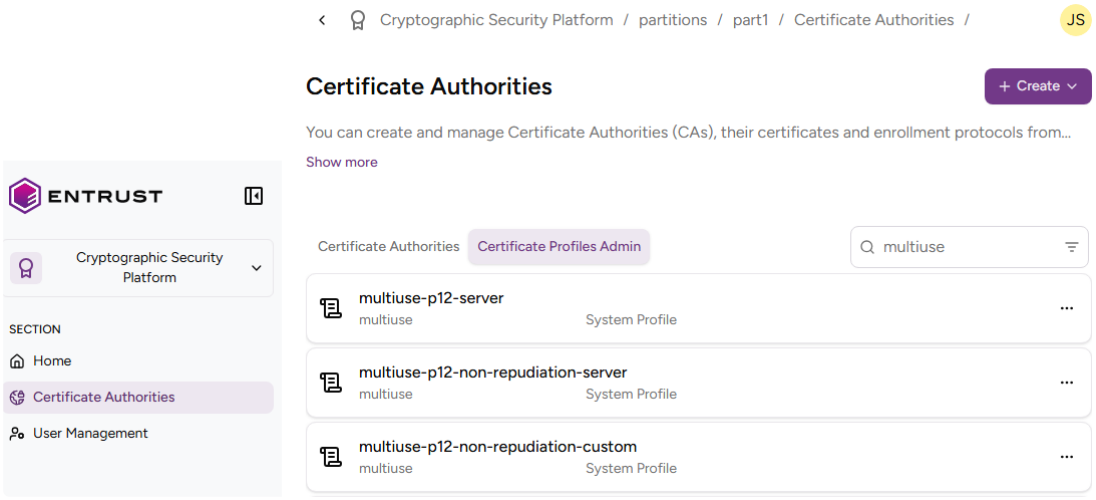
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

> ⚠ Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.



4. Click **Select**.
5. Click **Certificate Authorities** in the sidebar and select the **Certificate Profiles Admin** tab.



6. Browse the list of certificate profiles.
7. Click the name of a certificate profile you will use as a template for the new profile.
8. Check the certificate profile details described in https://docs.pkiaas.entrust.com/profiles/browse/fields



9. Click **Clone Certificate Profile**.
10. Define the properties of the new certificate profile.
11. Click **Clone**.

Updating the certificate profiles of a certificate authority

See below for adding or removing certificate profiles from an already-created certificate authority.

To update the certificate profiles of a certificate authority

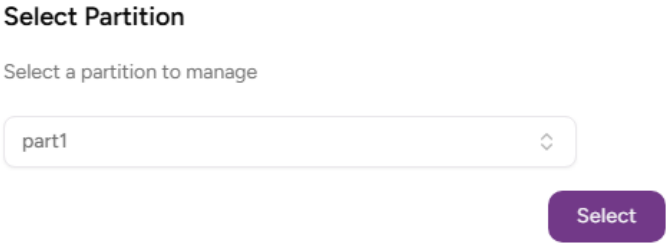
1. Open the following URL in a Web browser.

   ```
   https://<machine>/v2/
   ```

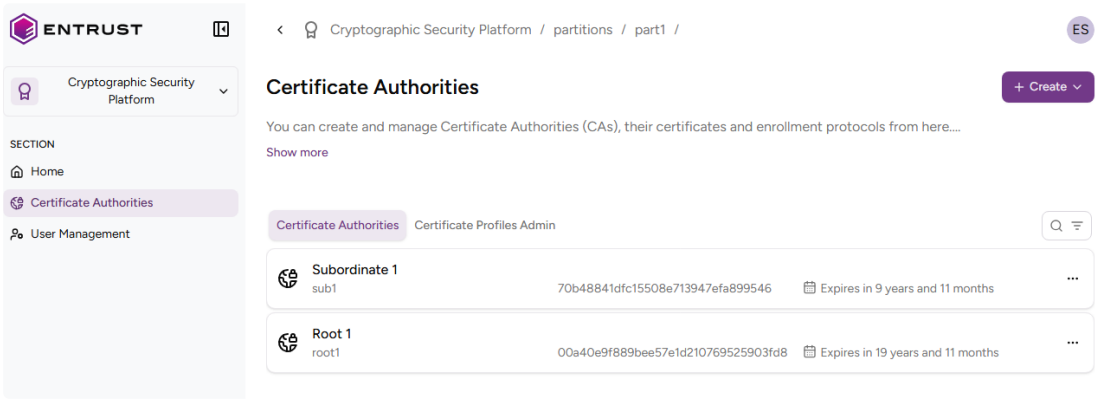
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > ⚠ Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.

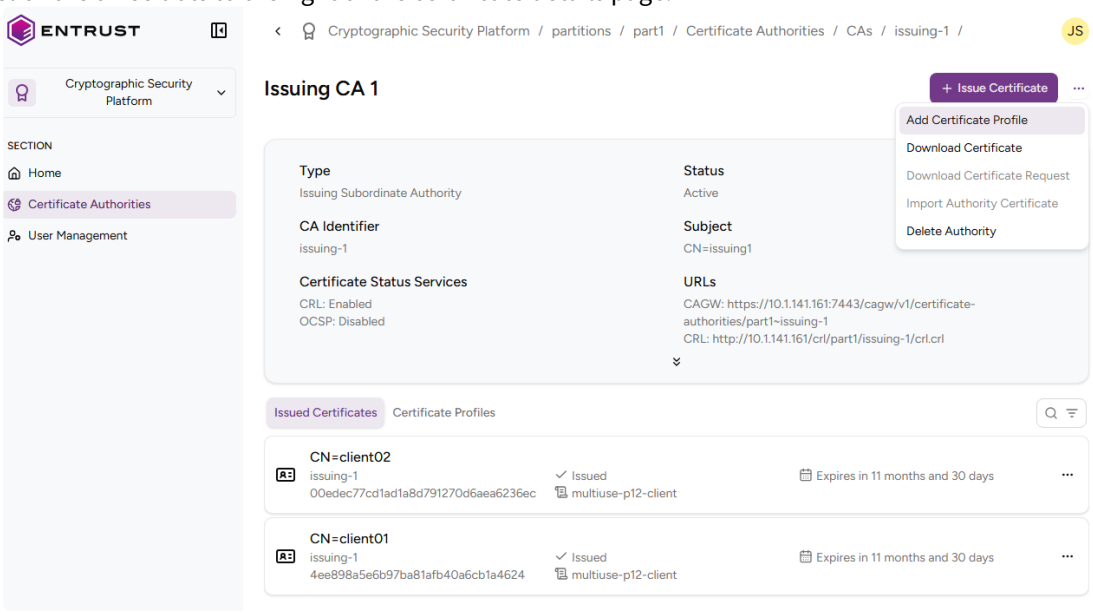
   

4. Click **Select**.
5. Click **Certificate Authorities** on the sidebar.

6. In the certificate authorities grid, click the name of a certificate authority.

7. Click the three dots to the right of the certificate details page.



8. Select **Add Certificate Profiles**.
9. Use the **Update Authority Profiles** page to add or remove certificate profiles.

Managing Certificate Authority users

See below for managing the users of the Certificate Authority solution.

- Browsing users
- Browsing and assigning roles
- Managing CAGW credentials

> See Onboarding and adding partition administrators for how to add users to a partition.

Browsing users

See below for browsing the users of the Certificate Authority solution.

To browse Certificate Authority users

1. Open the following URL in a Web browser.

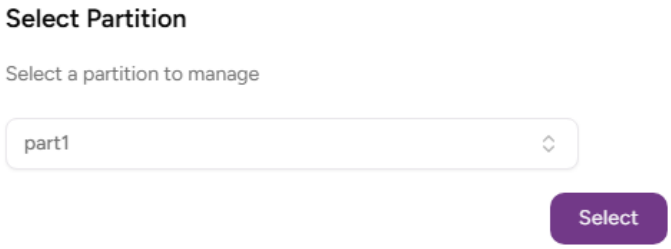
   ```
   https://<machine>/v2/
   ```

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

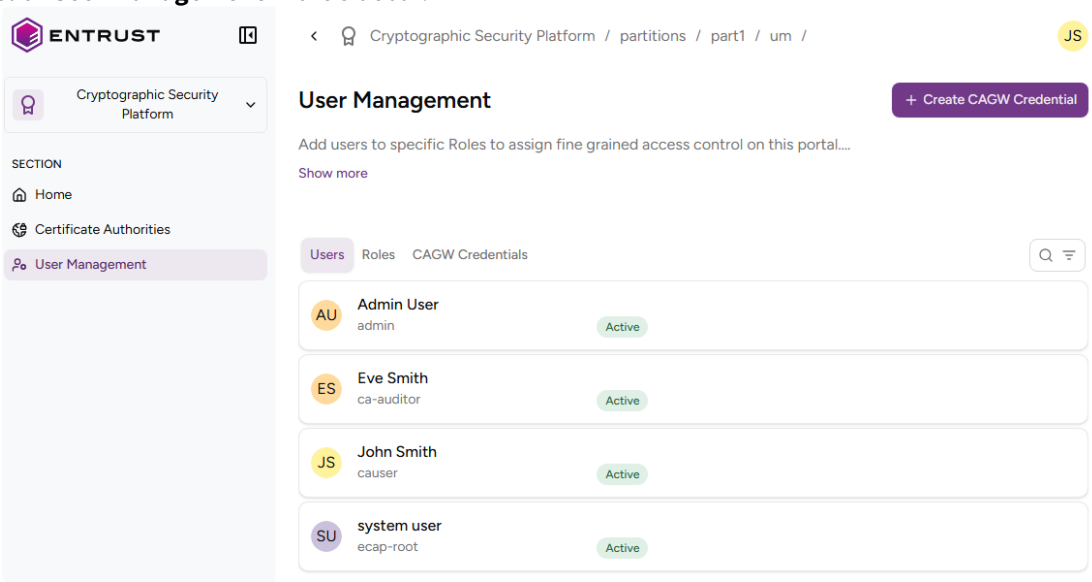
   > Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.

3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.



4. Click **Select**.
5. Click **User Management** in the sidebar.



6. Browse the list of users with permissions on the selected partition.
7. Click the name of a user to check more details.

Browsing and assigning roles

See below for browsing and assigning user roles.

To browse and assign roles

1. Open the following URL in a Web browser.

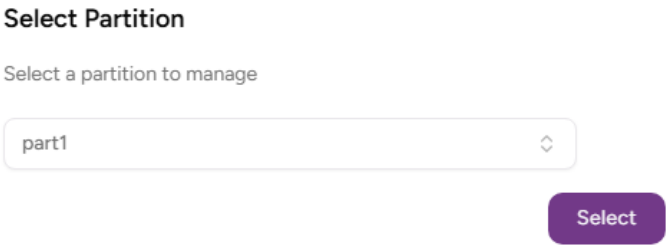
```
https://<machine>/v2/
```

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

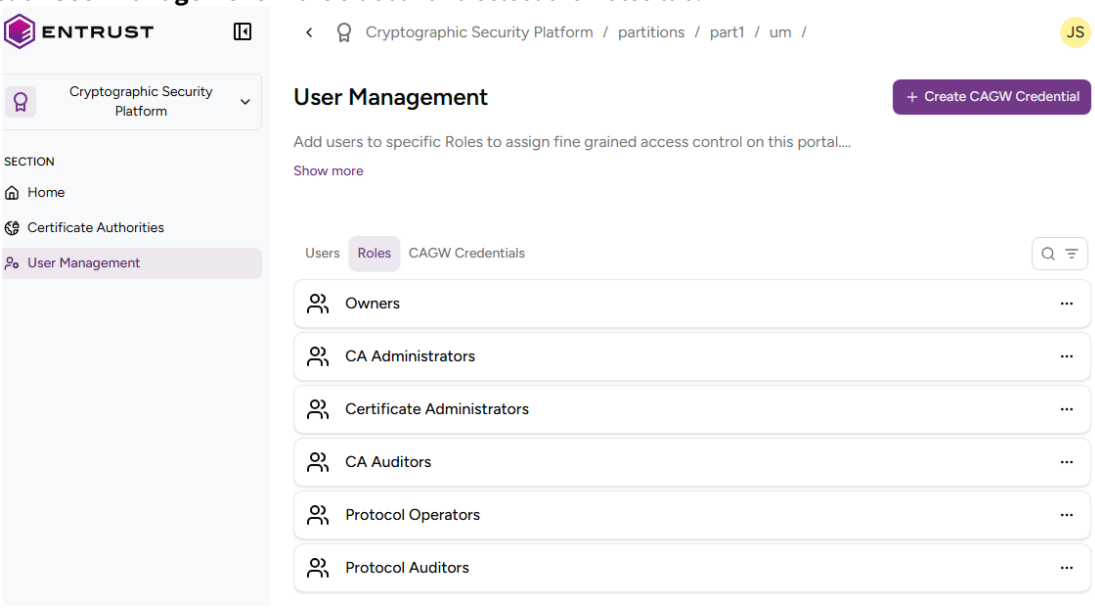
> ⚠ Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.

3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.



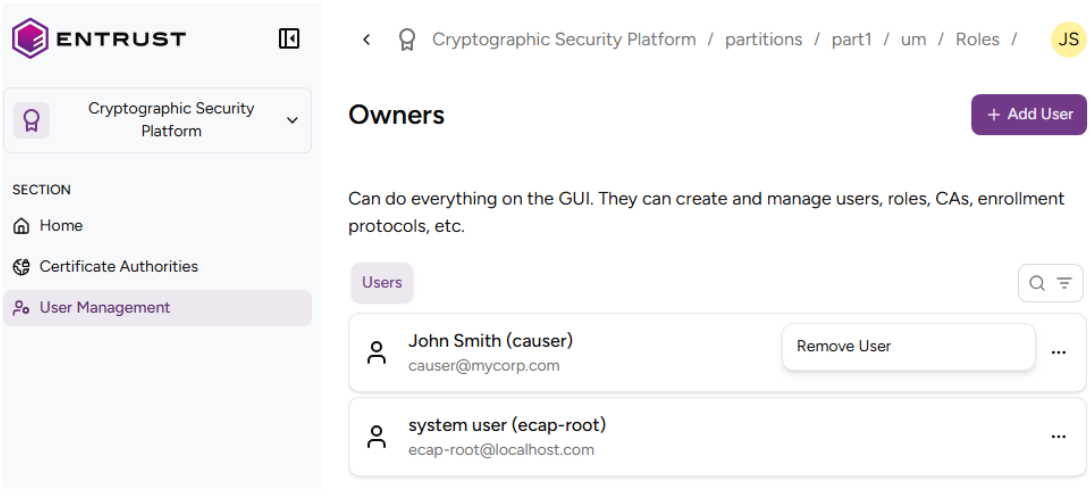
4. Click **Select**.
5. Click **User Management** in the sidebar and select the **Roles** tab.



Browse the list of role users.

- Owners
- CA Administrators
- Certificate Administrators
- CA Auditors
- Protocol Operators
- Protocol Auditors

6. Click the name of a role to check the list of users with this role.



7. Manage the list of users with the role:
   - Click **Add User** to grant the roles to new users.
   - Click the three dots to the right of a user, and select **Remove User**.

Owners

Users with this role can perform all the supported operations.

CA Administrators

Users with this role can perform the following operations on certificate authorities.

- Create
- Configure
- Delete

Certificate Administrators

Users with this role can perform the following operations on certificates.

- Issue
- Browse
- Export
- Revoke
- Suspend
- Unsuspend

CA Auditors

Users with this role can:

- Browse certificate authorities
- Browse certificates
- Download certificates
- Browse users
- Browse certification profiles
- Browse CA Gateway credentials

Protocol Operators

Users with this role can enroll certificates using a client application.

Protocol Auditors

Users with this role can audit certificate enrollment configuration.

Managing CAGW credentials

CAGW (CA Gateway) credentials grant third-party users permission to issue certificates or manage certificate authorities.

- Creating CAGW credentials
- Adding certificate authorities to CAGW credentials
- Renewing CAGW credentials

> The CAGW credential validity period is set to one year.

Creating CAGW credentials

See below for generating and downloading a CAGW (CA Gateway) credential in PKCS#12 format.

To create a CAGW credential

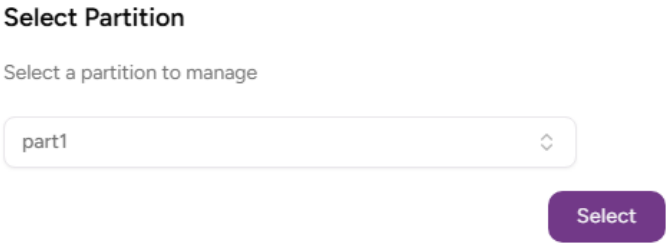
1. Open the following URL in a Web browser.

   ```
   https://<machine>/v2/
   ```

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

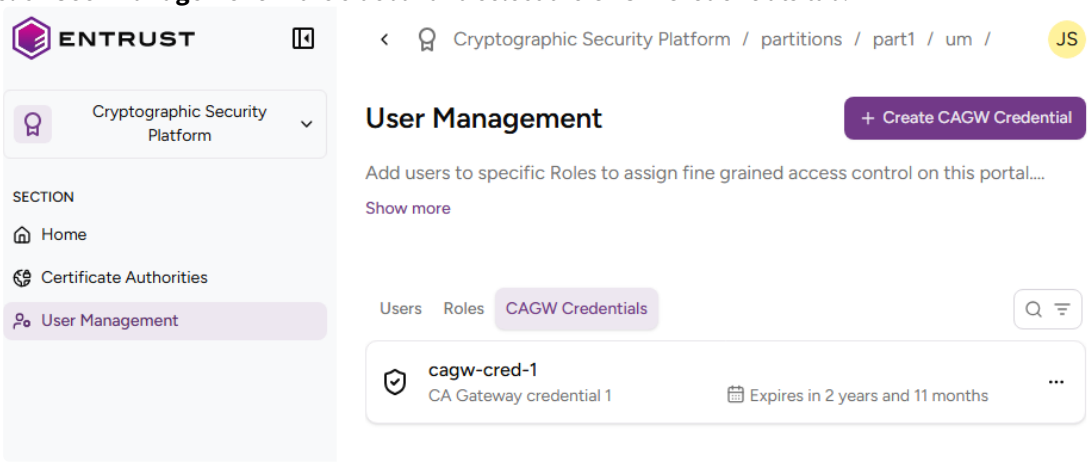
   > Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.

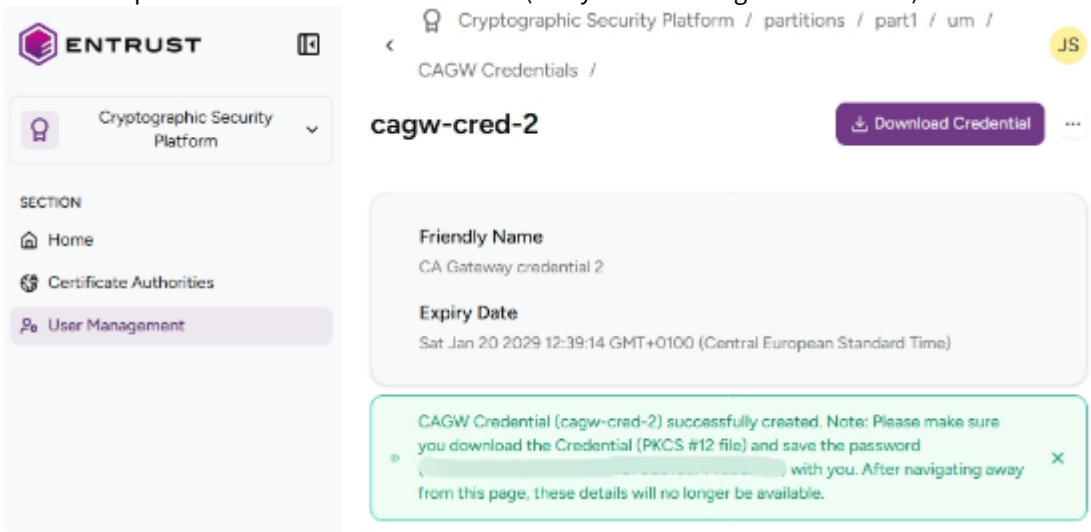
   

4. Click **Select**.

5. Click **User Management** in the sidebar and select the **CAGW Credentials** tab.



6. Click **Create CAGW Credential**.
7. Enter an identifier and a friendly name for the new credential.
8. Click **Create** and wait while the new credential automatically downloads.
9. Check the expiration date of the new credential (one year after the generation date).



10. Copy the password displayed in the credential details page.

> ⚠ As indicated in the warning message when leaving this page, you won't be able to copy the credential password again. If you don't copy this password now, you will be forced to generate a new credential.

Adding certificate authorities to CAGW credentials

See below for selecting the certificate authorities on which CAGW (CA Gateway) credential holders will have permissions.

To add a certificate authority to a CAGW credential

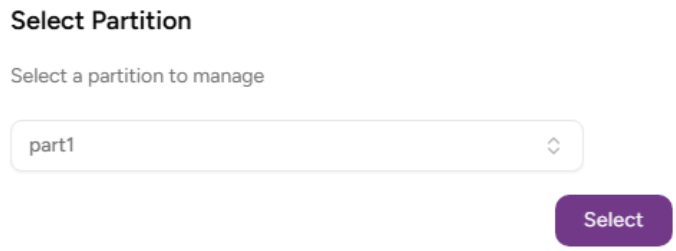
1. Open the following URL in a Web browser.

```
https://<machine>/v2/
```

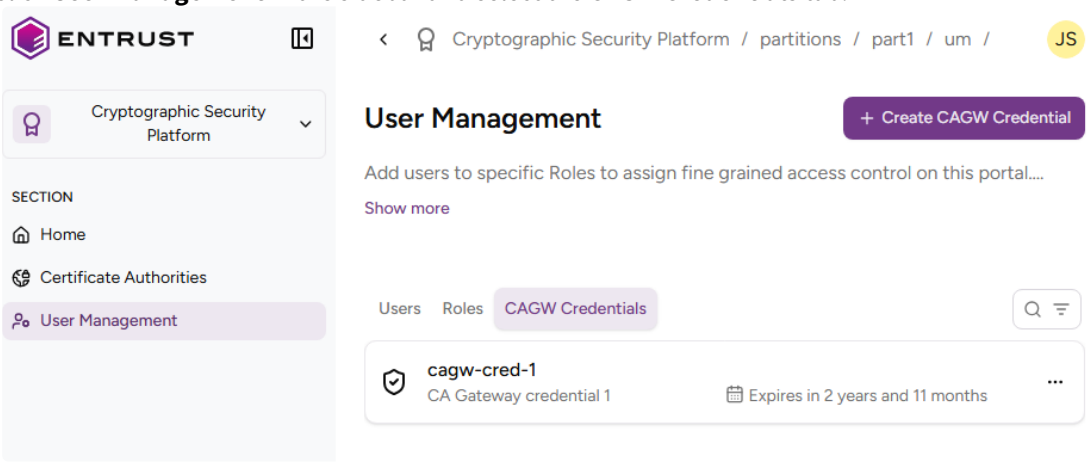
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

> ⚠ Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.



4. Click **Select**.
5. Click **User Management** in the sidebar and select the **CAGW Credentials** tab.



6. Click the three buttons to the right of a credential and select **Add Certificate Authority**.
7. In the **Add Certificate Authority** dialog, select:
   - The certificate authority to which the credential will grant access
   - The roles of the credential holders on the certificate authority.
8. Click **Add**.

Renewing CAGW credentials

As explained in Creating CAGW credentials, CA Gateway credentials expire one year after issuance. See below for renewing a credential before this date.

To renew a CAGW credential

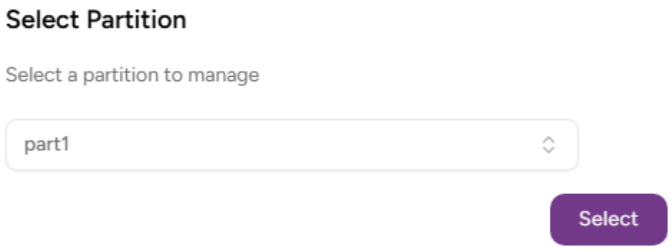
1. Open the following URL in a Web browser.

```
https://<machine>/v2/
```

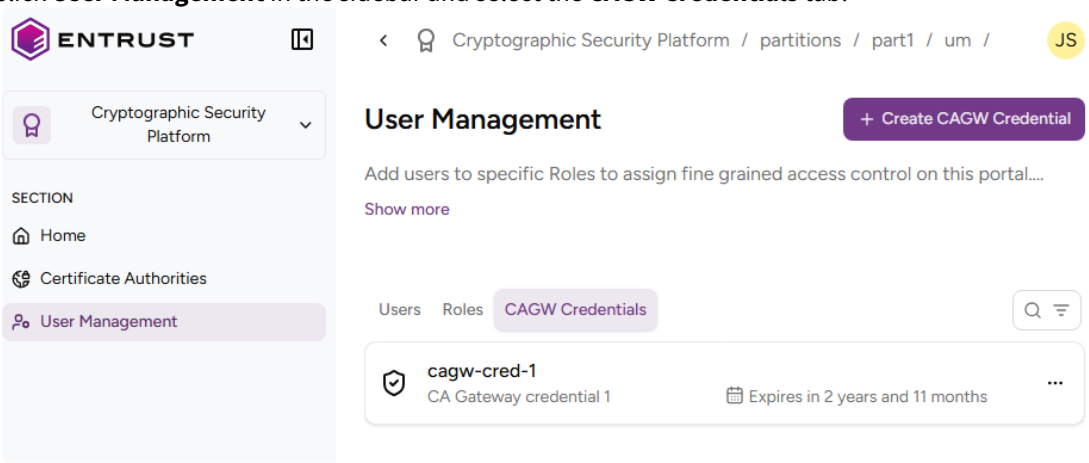
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

> ⚠ Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.



4. Click **Select**.
5. Click **User Management** in the sidebar and select the **CAGW Credentials** tab.



6. Click the three buttons to the right of a credential and select **Renew CAGW credential**.
7. Review the credential details and click **Renew**.
8. Check the expiration date of the renewed credential (one year after the renewal date).
9. Copy the password displayed in the credential details page.

> ⚠ As indicated in the warning message when leaving this page, you won't be able to copy the credential password again. If you don't copy this password now, you will be forced to generate a new credential.

Managing certificates

See below for issuing and managing certificates using the Certificate Authority console.

- Issuing certificates and key pairs on a PKCS #12
- Issuing certificates for client-generated keys
- Browsing and downloading certificates
- Managing the validity or a certificate

Issuing certificates and key pairs on a PKCS #12

See below for issuing certificates and key pairs on a PKCS #12 file.

To issue certificates from the Certificate Authority console

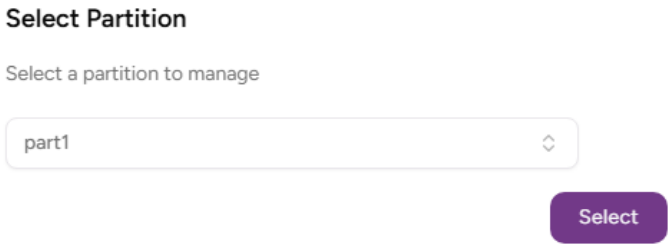
1. Open the following URL in a Web browser.

   ```
   https://<machine>/v2/
   ```

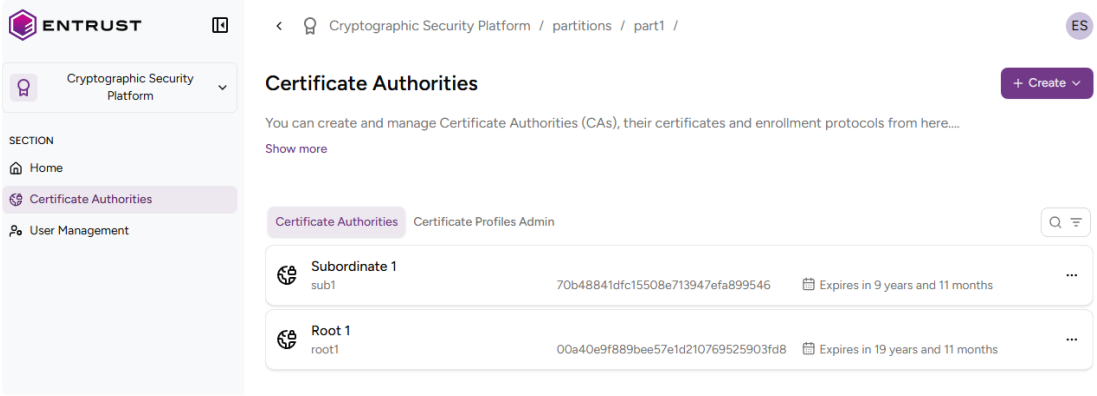
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > ⚠ Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.

4. Click **Select**.
5. Click **Certificate Authorities** on the sidebar.

6. In the certificate authorities grid, click the name of a certificate authority.
7. Click **Issue certificate**.
8. Configure the following settings.
   - Certificate Type
   - Certificate Profile
   - PKCS #12 Password
   - Subject DN Attributes
   - Subject Alternative Names
9. Click **Create**.
10. Click **Download your PKCS #12**.

    > ⚠ As indicated in the warning message when leaving this page, you won't be able to download the PKCS #12 file again.

Certificate Type

Select **Server-side Generated Key Certificate (PKCS #12)**.

Mandatory: Yes.

Certificate Profile

The certificate profile for issuing the certificate.

> This list only displays profiles configured in the issuing certificate authority.

Mandatory: Yes.

PKCS #12 Password

Enter and confirm the password that will protect the PKCS #12 generated file.

Mandatory: No.

Subject DN Attributes

Select the required Distinguished Name (DN) attributes.

> You must enter at least the `CN` attribute value.

Mandatory: Yes.

Subject Alternative Names

The list of subject alternative names (SAN) for the certificate.

Mandatory: No.

Issuing certificates for client-generated keys

See below for issuing certificates for key pairs generated on the client side.

To issue certificates from the Certificate Authority console

1. Open the following URL in a Web browser.

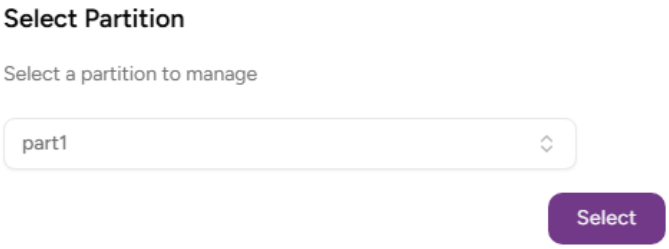
   ```
   https://<machine>/v2/
   ```

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

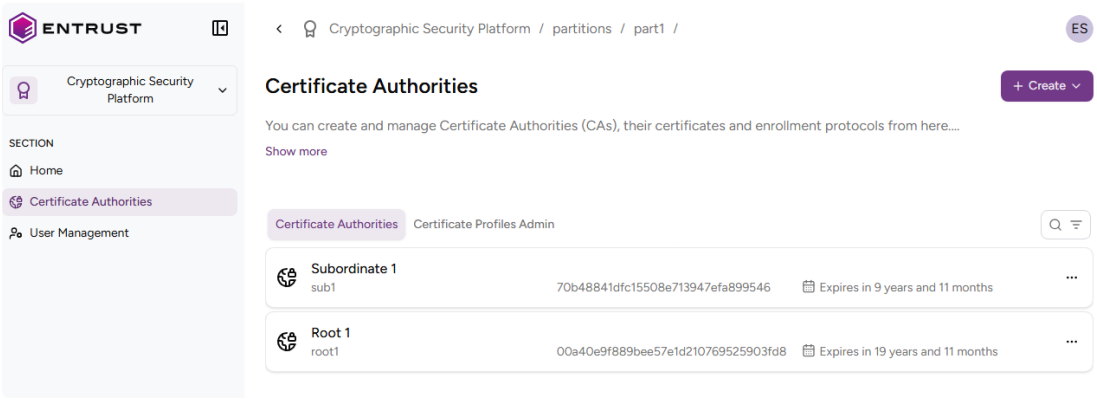
   > Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.

3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.



4. Click **Select**.
5. Click **Certificate Authorities** on the sidebar.



6. In the certificate authorities grid, click the name of a certificate authority.
7. Click **Issue certificate**.
8. Configure the following settings.
   - Certificate Type
   - Certificate Profile
   - Certificate Signing Request (CSR)
   - Use subject from CSR
   - Subject DN Attributes
   - Subject Alternative Names
9. Click **Create**.

Certificate Type

Select **Client-side Generated Key Certificate (X.509 cert)**.

Mandatory: Yes.

Certificate Profile

The certificate profile for issuing the certificate.

> This list only displays profiles configured in the issuing certificate authority.

Mandatory: Yes.

Certificate Signing Request (CSR)

The PEM or Base64 encoding of a CSR (Certificate Signing Request).

Mandatory: Yes.

Use subject from CSR

Enable this field to use the subject included in the certificate request as the subject of the issued certificate.

Subject DN Attributes

Select the required Distinguished Name (DN) attributes.

> ⚠ You must enter at least the `CN` attribute value.

Mandatory: When not enabling the **Use subject from CSR** field.

Subject Alternative Names

The list of subject alternative names (SAN) for the certificate.

Mandatory: No.

Browsing and downloading certificates

See below for browsing and downloading certificates.

To issue certificates from the Certificate Authority console

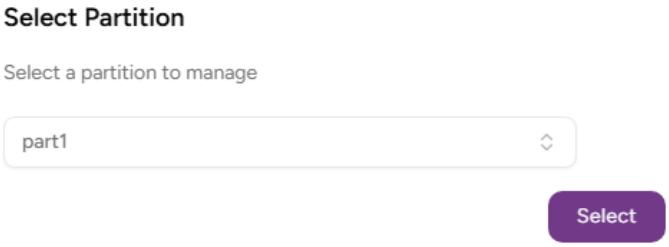
1. Open the following URL in a Web browser.

   ```
   https://<machine>/v2/
   ```

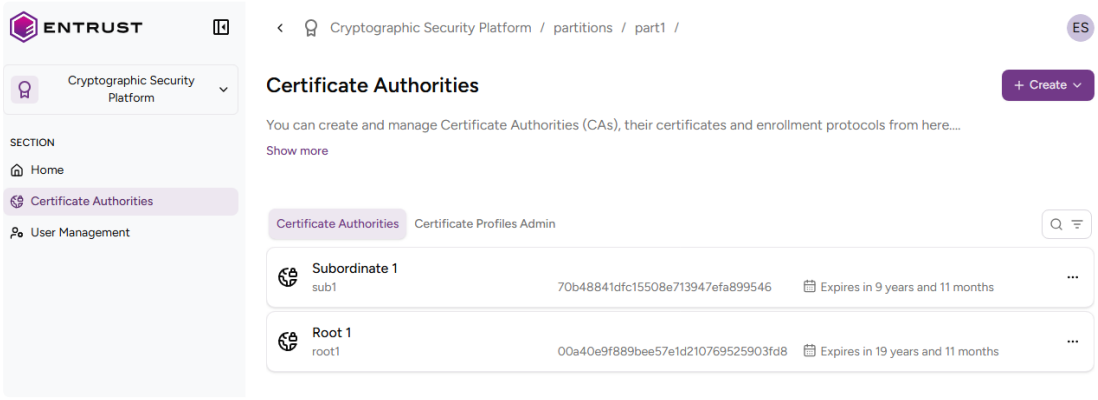
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > ⚠ Do not omit the ending forward slash "/" on this URL.

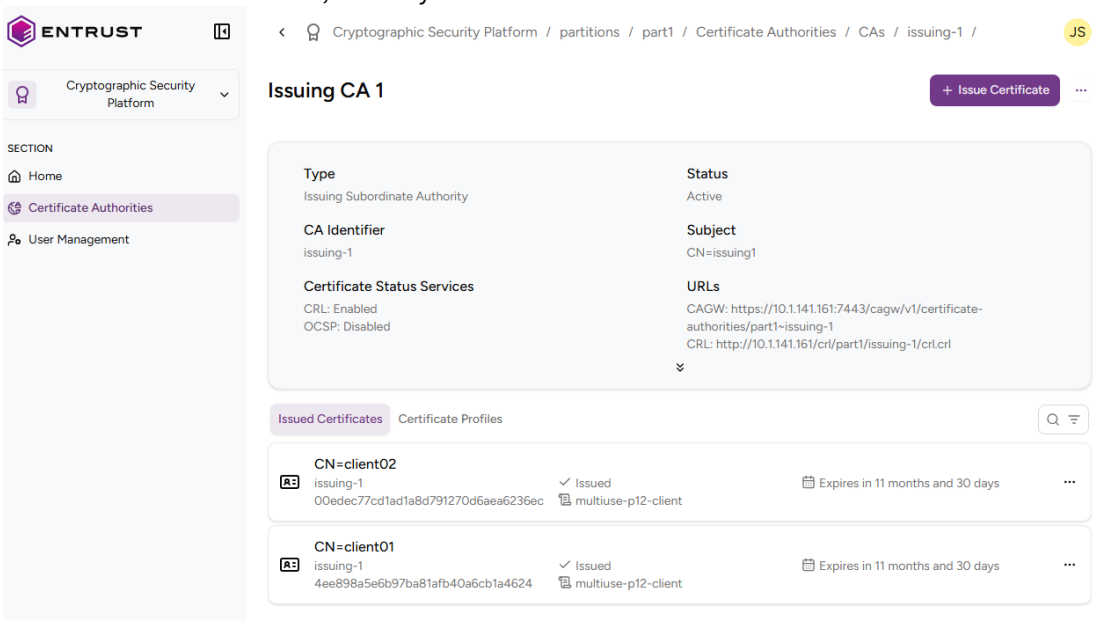
2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.

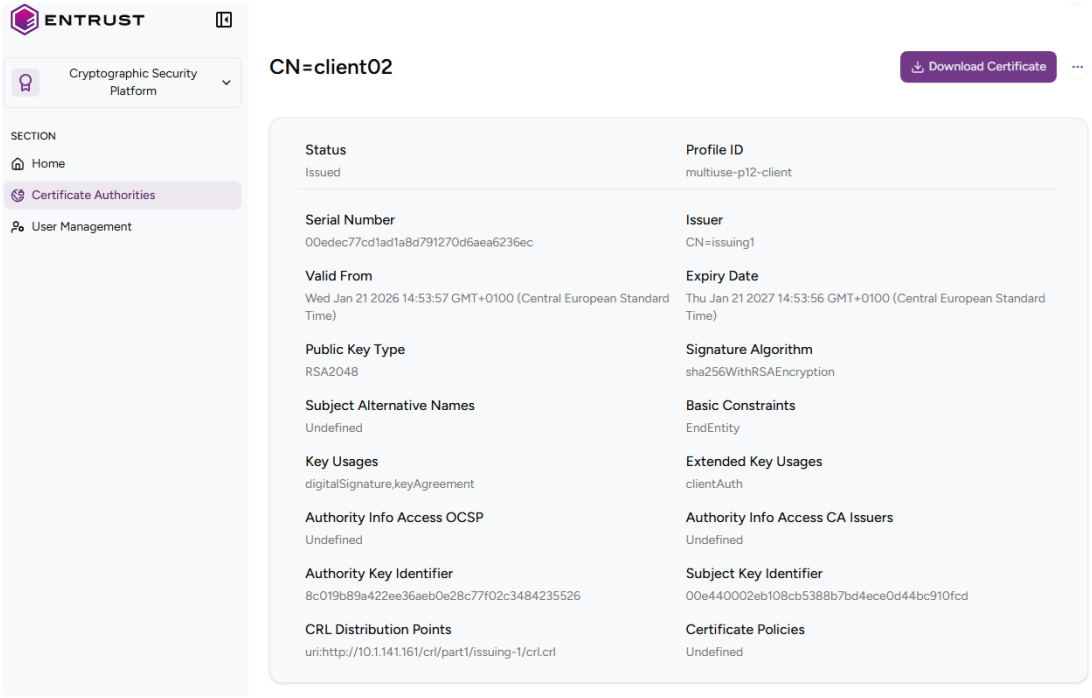
4. Click **Select**.
5. Click **Certificate Authorities** on the sidebar.



6. In the certificate authorities grid, click the name of a certificate authority.
7. In the **Issued Certificates** tab, click any of the listed certificates.



8. Check the certificate details.



9. Click **Download Certificate** to download the certificate in a PEM-encoded X.509 file.

Managing the validity or a certificate

See below for changing the validity status of a certificate.

To change the validity status of a certificate

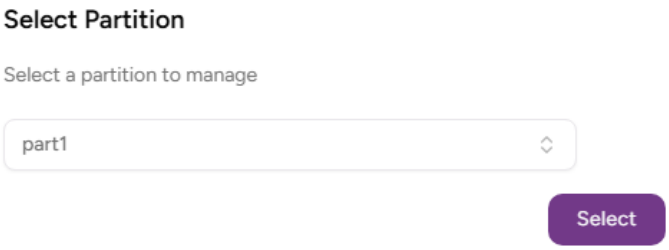
1. Open the following URL in a Web browser.

   ```
   https://<machine>/v2/
   ```

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

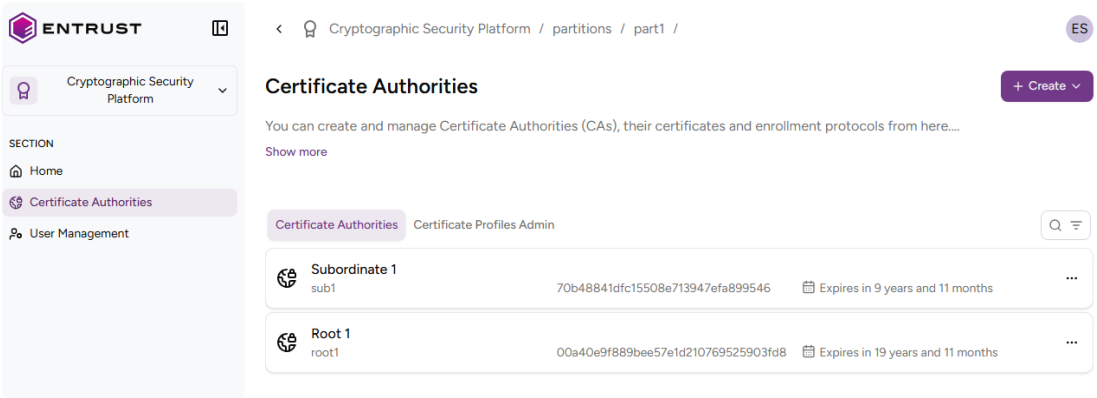
   > ⚠ Do not omit the ending forward slash "/" on this URL.

2. Log in to the Management Console as the user described in Creating partition administrators.
3. In the **Select Partition** dialog, select the partition on which to manage certificate authorities and certificates.

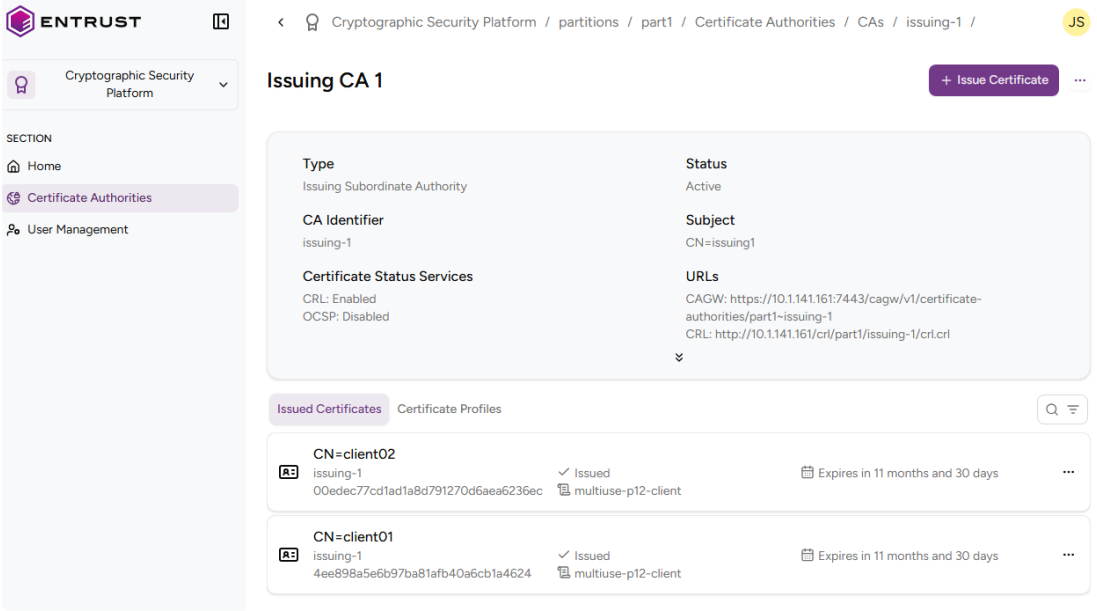


4. Click **Select**.

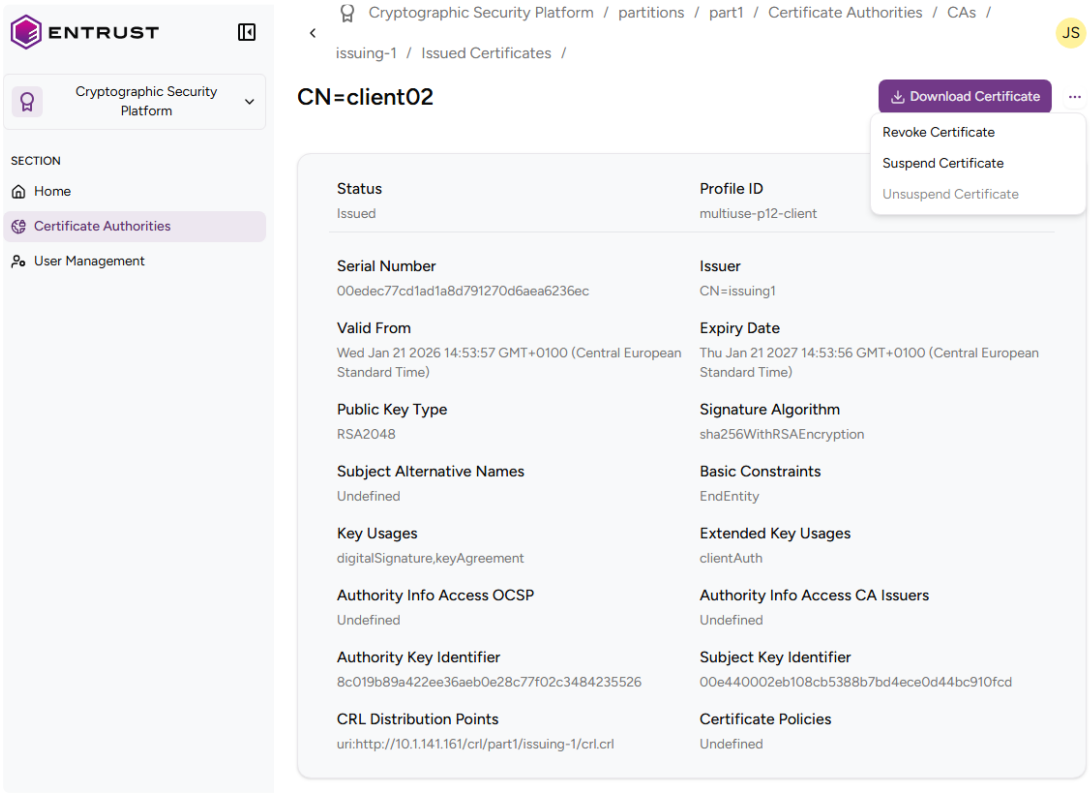
5. Click **Certificate Authorities** on the sidebar.



6. In the certificate authorities grid, click the name of a certificate authority.
7. In the **Issued Certificates** tab, click any of the listed certificates.



8. Check the certificate details.



9. Click the three dots to the right of the certificate details page.
10. Select:
    - **Revoke Certificate** to permanently invalidate a certificate.
    - **Suspend Certificate** to temporarily invalidate a certificate.
    - **Unsuspend Certificate** to rehabilitate a suspended certificate.

Integrating client applications

See below for how to issue certificates with client applications.

- 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 :

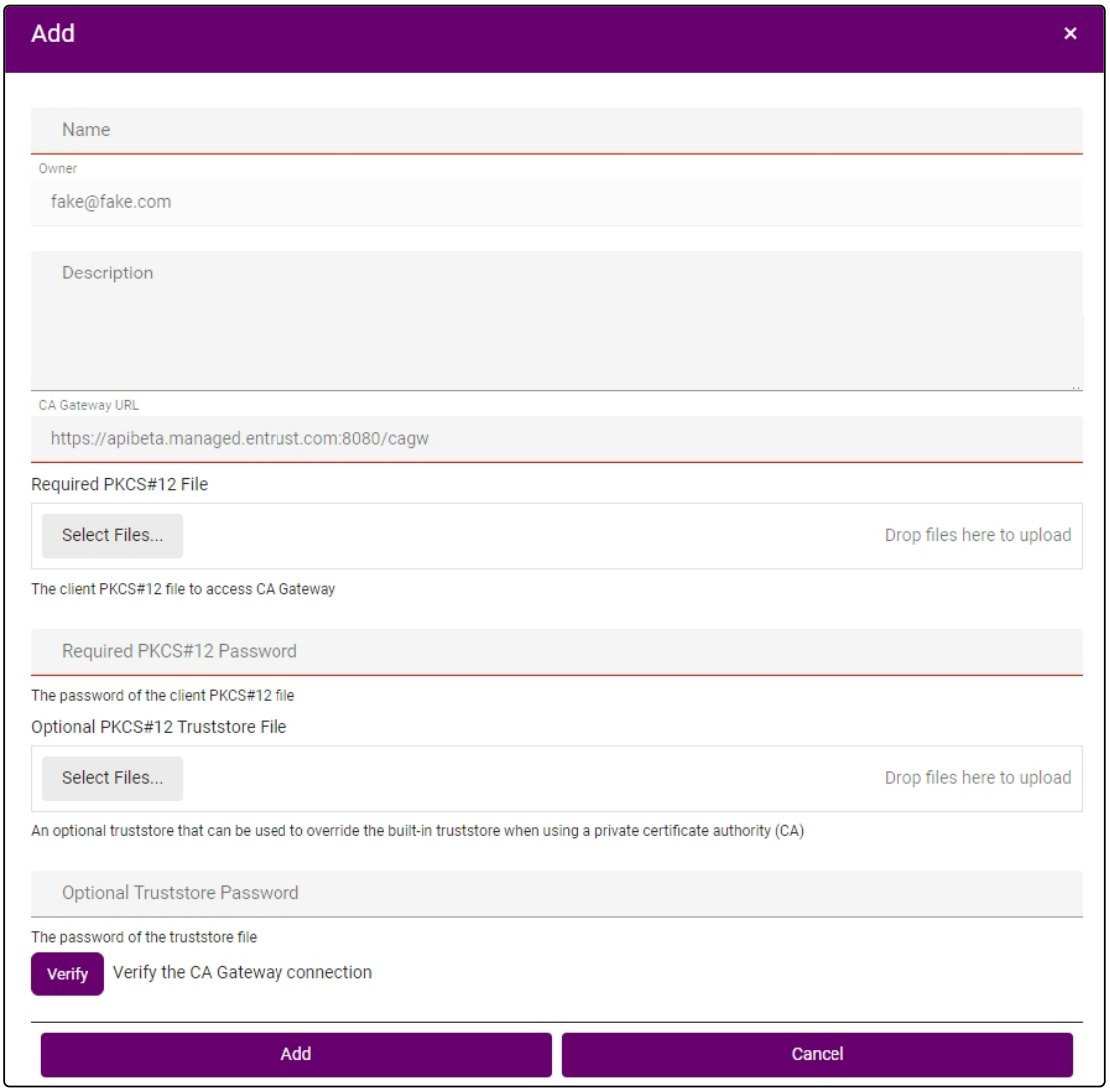
- `$P12` is the path of the PKCS#12 file described in Creating CAGW credentials.
- `$PWD` is the password of the PKCS 12 file described in Creating CAGW credentials.
- `$PKIHUB` is the hostname or IP address of the machine hosting Cryptographic Security Platform.
- `$ORG_ID` is the identifier of the 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



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 PKCS #12 file described in Creating CAGW credentials.

Required PKCS#12 Password

Enter the password of the PKCS#12 files described in Creating CAGW credentials.

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.

> 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**.

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 administrating 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:

- ACMEv2
- CMPv2
- EST
- Intune-SCEP
- MDM-SCEP
- MDMWS
- SCEP
- WSTEP

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 1.3.0. 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 > 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 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 Nonrepudation 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 Nonrepudation 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 Nonrepudation P12 certificate definition policy for EST enrollment

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

To create a Nonrepudation 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 Nonrepudation 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 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 EST Signing and Nonrepudation 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 Nonrepudation certificate type

See below to map an Entrust Certificate Authority certificate definition policy to the MDM SCEP Signing and Nonrepudation certificate type.

To map a certificate definition policy to the MDM SCEP Signing and Nonrepudation 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 Nonrepudation P12 certificate definition policy

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

To create a Nonrepudation 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 Nonrepudation certificate type

Mapping to the SCEP Encryption certificate type

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

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

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > SCEP Encryption > Encryption_p10**.
3. In the **Certificate definition Policy** drop-down list, select **Encryption_P10 policy**.
4. Click **Apply**.

5. If prompted, authorize the operation.

Mapping to the SCEP Signing certificate type

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

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

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > SCEP Signing > Verification_p10**.
3. In the **Certificate definition Policy** drop-down list, select **Verification_p10 Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the SCEP Signing and Encryption certificate type

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

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

1. Log in to Entrust Certificate Authority Administration.
2. In the tree view, expand **Security Policy > Certificate Categories > Enterprise > SCEP Signing and Encryption > Dual Usage**.
3. In the **Certificate definition Policy** drop-down list, select **Dual Usage Policy**.
4. Click **Apply**.
5. If prompted, authorize the operation.

Mapping to the SCEP Signing and Nonrepudation certificate type

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

To map a certificate definition policy to the SCEP Signing and Nonrepudation 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

> 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----
MIIDejCCAmKgAwIBAgIQQ8e7ock59Y21Mtcy7rGJUDANBgkqhkiG9w0BAQs...
-----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.

Test	Purpose
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).
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.

Test	Purpose
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.
Protection.rejectUnprotected	Ensure unprotected messages are not allowed.
PasswordBasedMac.applyProtection	Ensure that the protection defined in the response header is applied to the message response.

Test	Purpose
PasswordBasedMac.checkApplyAlgorithm	Ensure PBM protection algorithms defined in the response header are supported by the system.
PasswordBasedMac.checkVerifyAlgorithm	Ensure PBM protection algorithms defined in the request header are supported by the system.
PasswordBasedMac.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

> 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

> 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.

> 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 1.3.0 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 1.3.0 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 1.3.0.
<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 1.3.0 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 1.3.0 – 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 1.3.0 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 1.3.0. 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 1.3.0 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]:
```

   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 1.3.0 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 1.3.0 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-----
MIIDqQYJKoZIhvcNAQcCoIIDmjCCA5YCAQExADALBgkqhkiG9w0BBwGgggN...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----
MIIDejCCAmKgAwIBAgIQQ8e7ock59Y21Mtcy7rGJUDANBgkqhkiG9w0BAQs...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----
MIQ0EgRW50cnkwHhcNMjMwMjA4MTUxNzEwWhcNMzMwMjA4MTU0NzEwWjAyM...
-----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 Cryptographic Security Platform.

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 Platofrm 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>:8443/management-console
   ```

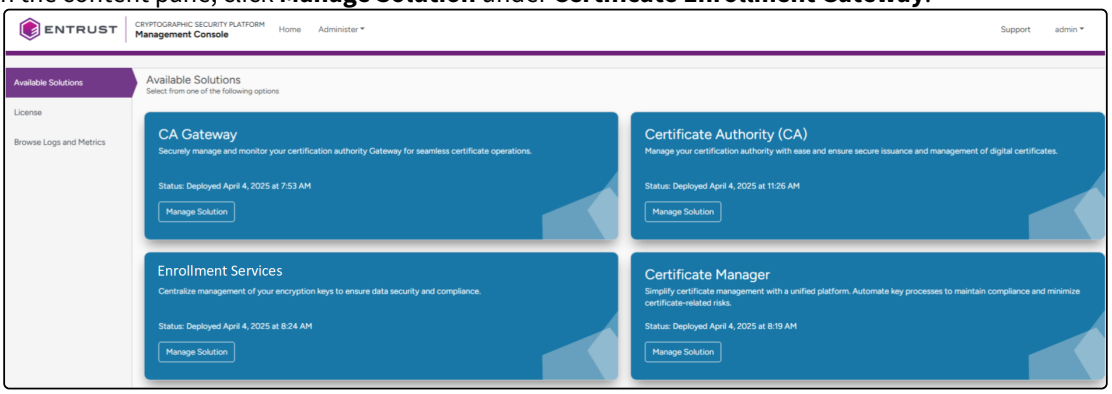
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

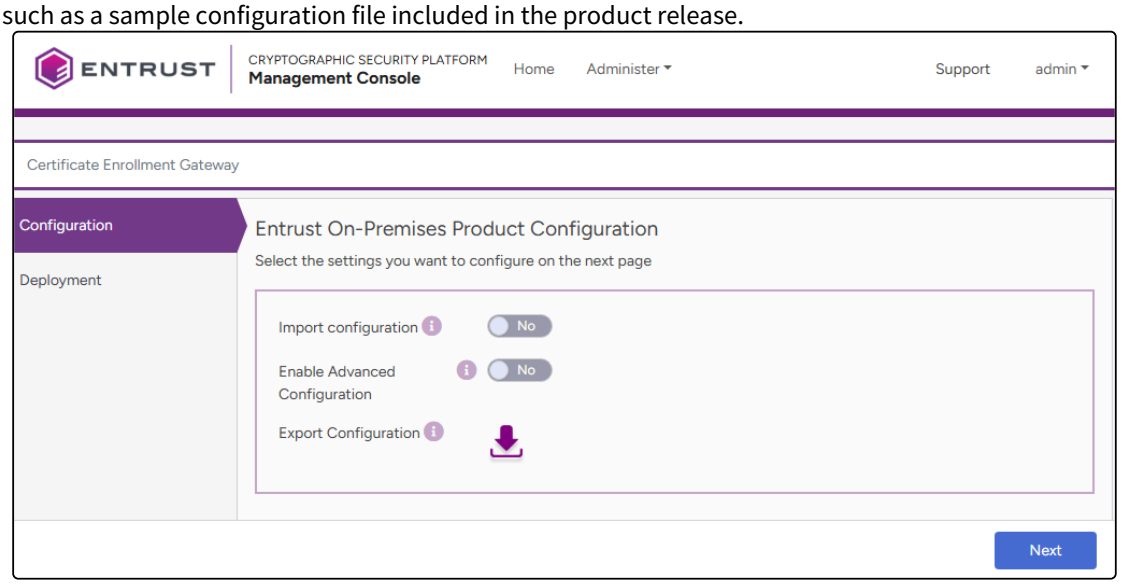
2. Log in to the Management Console as a user belonging to a role with Certificate Enrollment Gateway management permissions – for example, the initial `admin` administrator user.

   ℹ See Managing identities 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)

> ℹ 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: ***verify-full, ****verify-ca** or ***disable** (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	**enable** to enable SSL security for connecting, **disable** 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 `jdbc:` 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 `/opt/entrust/ceg/pvc_rwx_config/db` 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 partition administrators.
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	**Yes** to validate the vendor certificate against a CRL; **No** 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.

> 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

> 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.

> 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.

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.

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 1.3.0 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/0mj615kbbkkb/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/0mj615kbbkkb/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:

The following Intune-SCEP enrollment URL requires the trailing forward slash (/). To support macOS (Apple) devices, the URL must start with `http` instead of `https`.

```
http://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/intune/
https://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/intune/
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the SCEP client.
- `<profile-ID>` is the profile ID defined in CA Gateway that defines the certificate type issued to the SCEP client. For Entrust PKI as a Service, the profile ID is one of the following:
  - intune-digital-signature-key-encipherment
  - intune-digital-signature
  - intune-key-encipherment
  - intune-non-repudiation

For example:

```
http://cegserver.example.com/scep/tenant1/example_ca1/intune-digital-signature-key-
encipherment/intune/
https://cegserver.example.com/scep/tenant1/example_ca1/intune-digital-signature-key-
encipherment/intune/
```

MDM-SCEP enrollment URL

MDM-SCEP clients must use one of the following URLs to communicate with Certificate Enrollment Gateway:

To support macOS (Apple) devices, the URL must start with `http` instead of `https`.

```
http://<CEG-server>/scep/<tenant-ID>/<digitalid-config>/mdm
https://<CEG-server>/scep/<tenant-ID>/<digitalid-config>/mdm
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<digitalid-config>` is a digital ID configuration defined in the CEG Service.

For example:

```
http://cegserver.example.com/scep/tenant1/digitalid-config1/mdm
https://cegserver.example.com/scep/tenant1/digitalid-config1/mdm
```

MDMWS enrollment URL

Mobile Device Management products must use the following URL to communicate with Certificate Enrollment Gateway:

```
https://<CEG-server>/mdm/services/<tenant-ID>
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.

For example:

```
https://cegserver.example.com/mdm/services/tenant1
```

SCEP enrollment URL

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

> 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 ACMv2 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>:8443/management-console
   ```

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

   > ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

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

   > ℹ See Managing identities 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.

> 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.

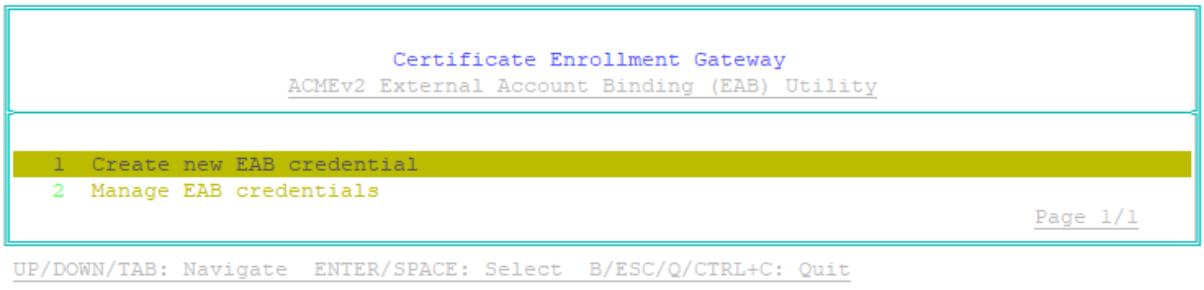
Multiple ACMEv2 clients can use the same External Account Binding credential to create an account and perform ACMEv2 operations.

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:



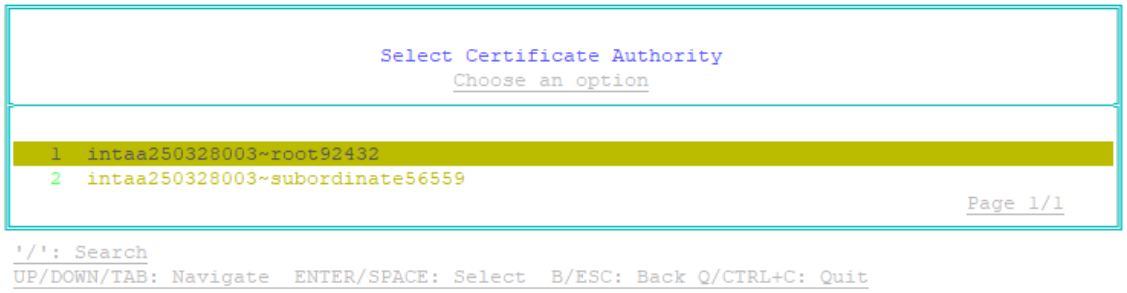
4. Select **Create new EAB credential**, then press Enter.
   The **Create New EAB Credential** page appears.



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.



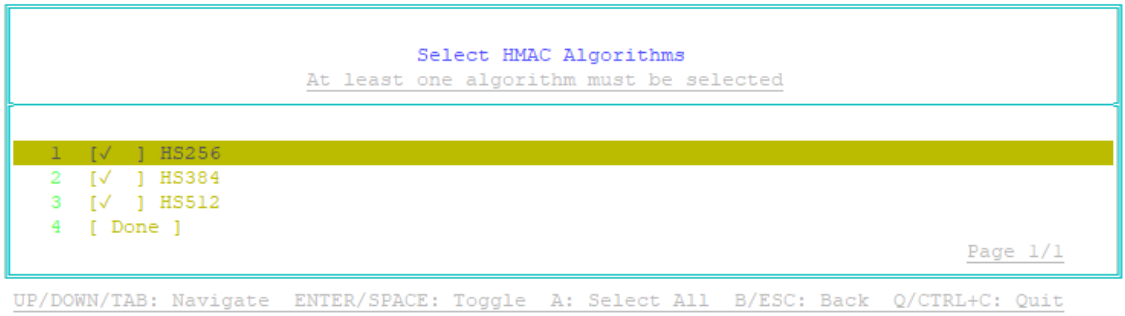
   b. Select a Certification Authority from the list, then press Enter.
7. Select the certificate profile defined in CA Gateway that will be used to issue the certificate to the ACMEv2 clients:

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



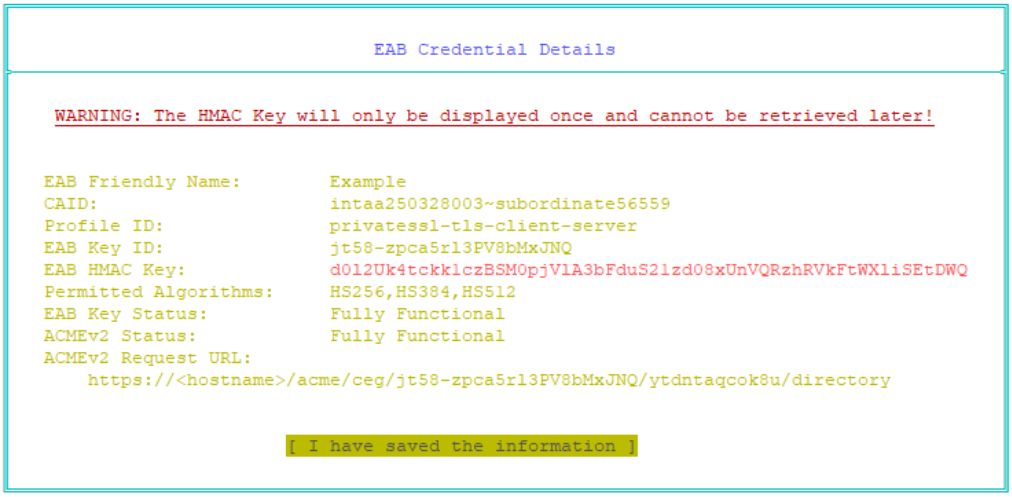
b. Select the certificate profile that will issue the certificate to the ACMEv2 clients, and then press Enter.
For Entrust PKI as a Service, the profile ID is one of the following:
- privatessl-tls-client-server
- privatessl-tls-server
- privatessl-tls-client

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.



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.



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.

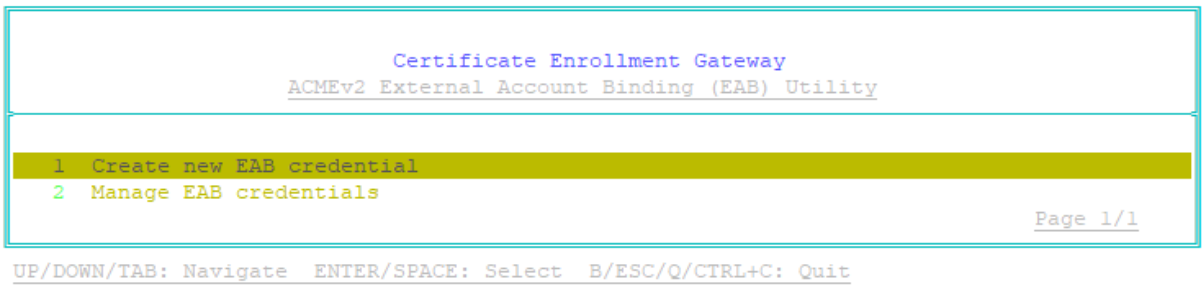
> The EAB Utility will display the HMAC key for an External Account Binding credential only when you create the credential. The EAB Utility will not display the key when viewing details about an External Account Binding credential.

To view details about an External Account Binding credential

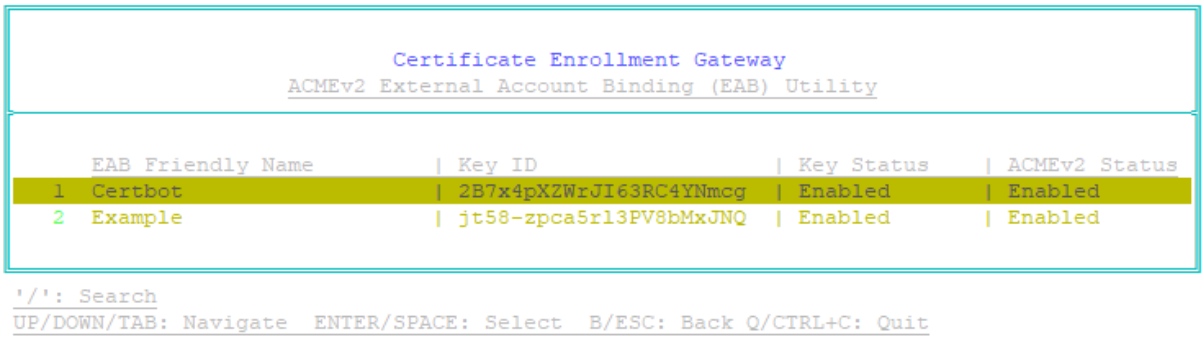
1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

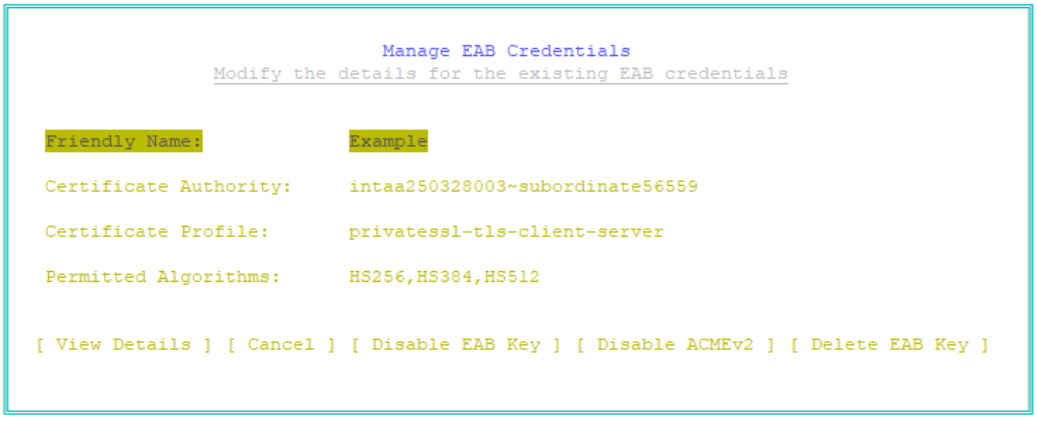


4. Select **Manage EAB credentials**, and then press Enter.
   A list of External Account Binding credentials appears. For example:



   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.

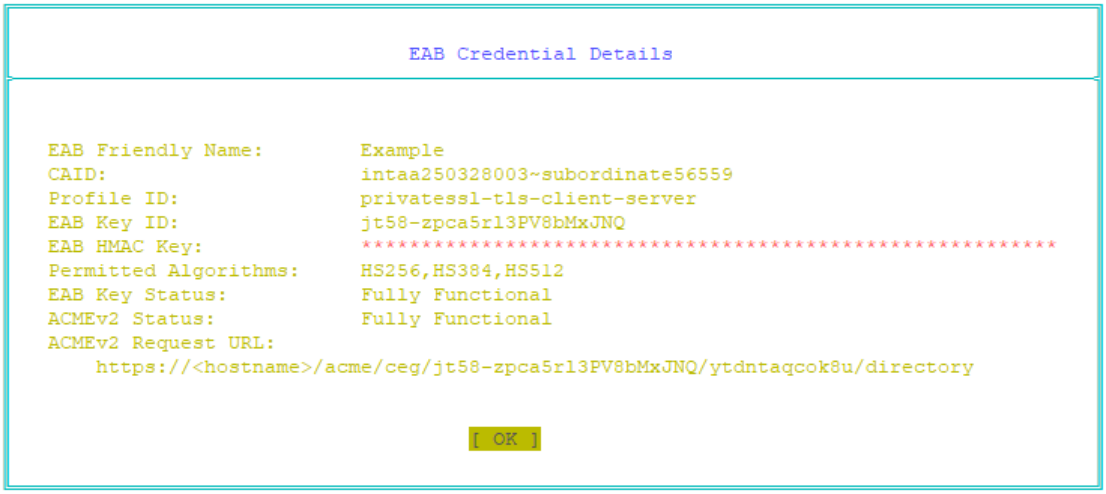
5. Select the credential you want to edit, and then press Enter.
   A **Manage EAB Credentials** page appears. For example:



   - **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:



- **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.

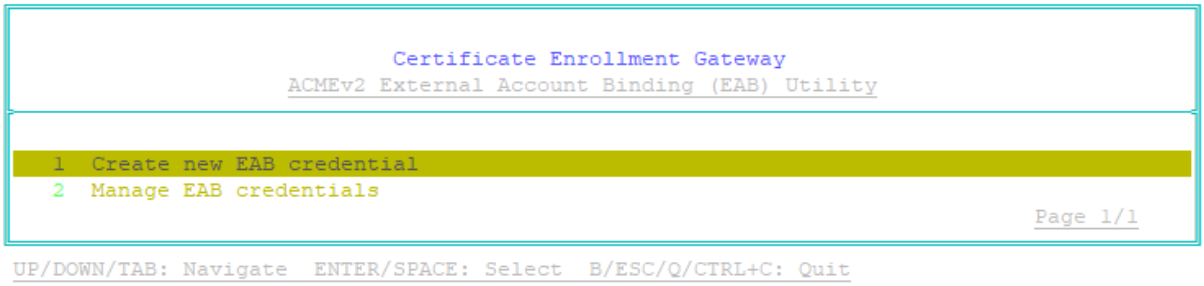
You cannot change the HMAC (Hash-Based Message Authentication Code) key or ACMEv2 Request URL used by ACMEv2 clients. The key and URL were automatically generated when the credential was created and cannot be changed.

To modify an External Account Binding credential

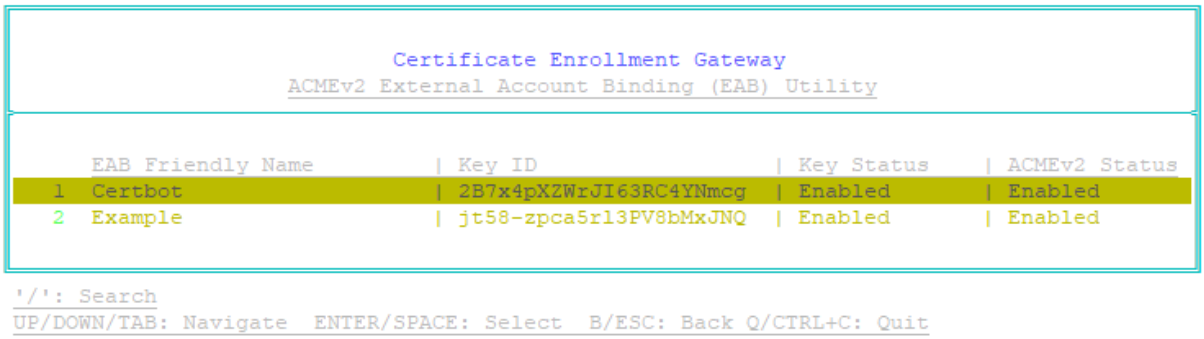
1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

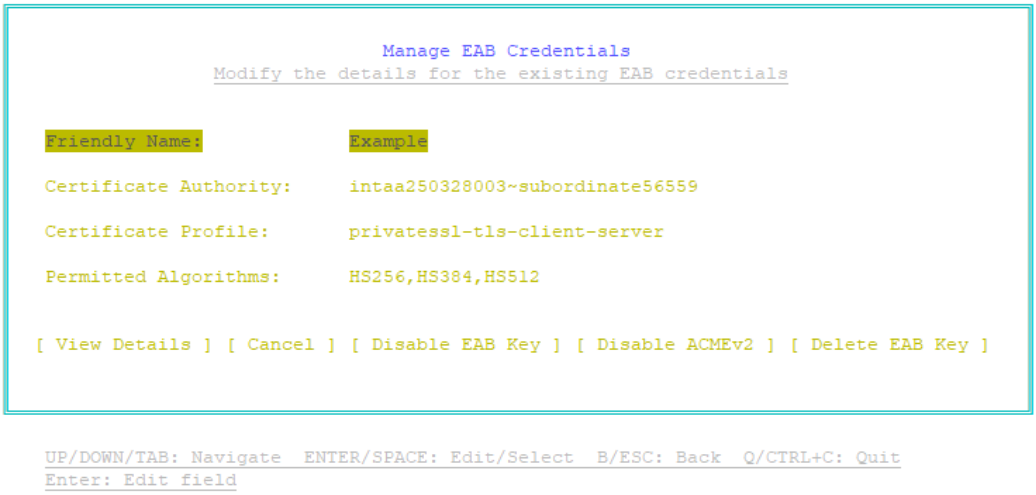
3. The main menu appears:



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



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



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.



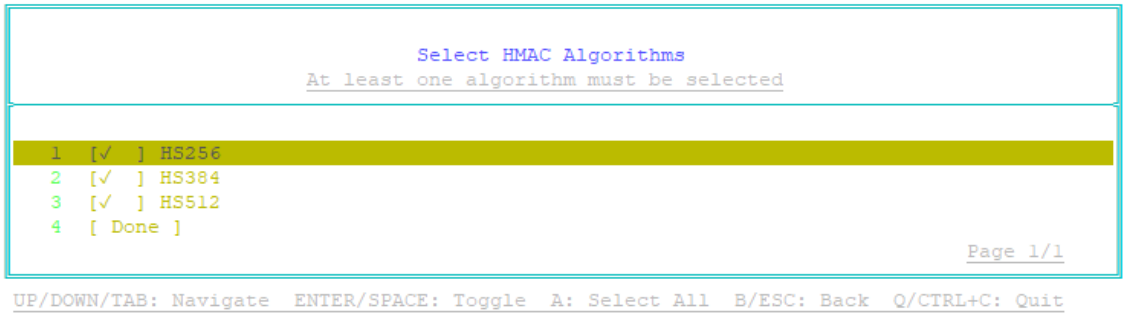
   b. Select a Certification Authority from the list, then press Enter.
8. To change the certificate profile defined in CA Gateway that will be used to issue the certificate to the ACMEv2 client:

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



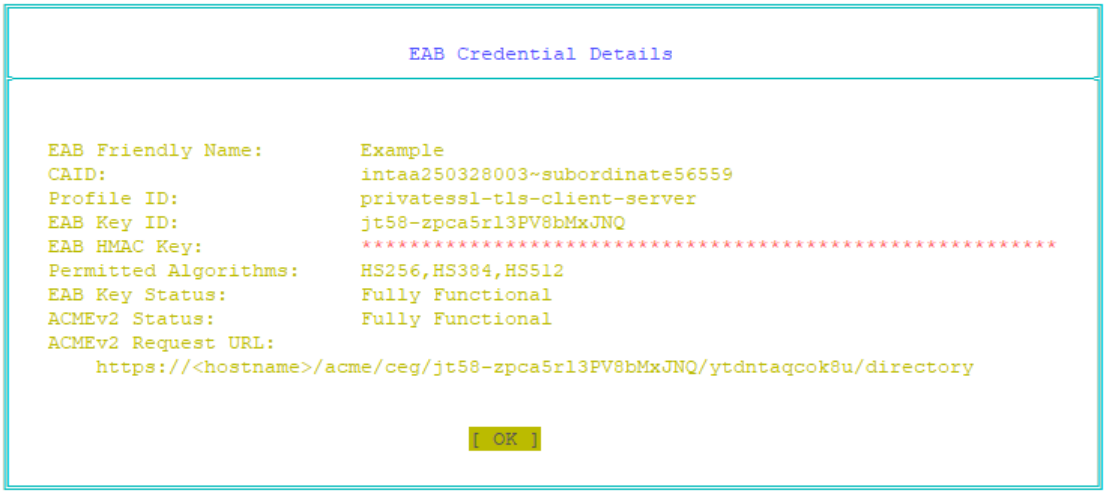
b. Select the certificate profile that will issue the certificate to the ACMEv2 client, and then press Enter.

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.



   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.



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.

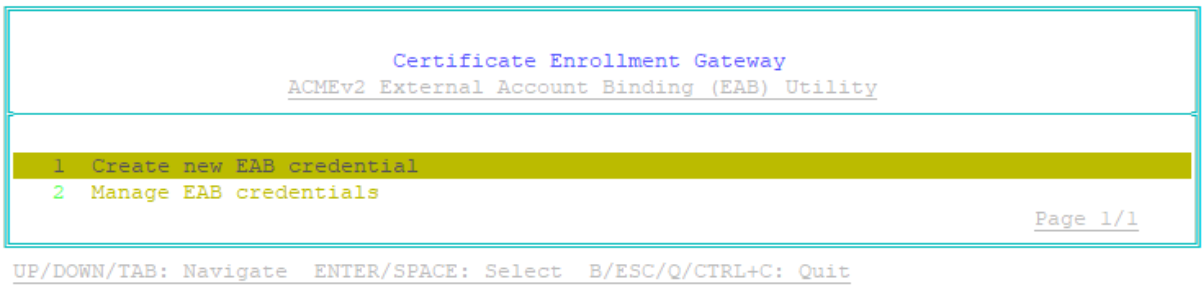
You can disable the HMAC key for an External Account Binding credential. Disabling a key will block new ACMEv2 clients from using the key to create an account with External Account Binding credential. ACMEv2 clients that have already used the key to create an account can still perform ACMEv2 operations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

To disable the HMAC key for an External Account Binding credential

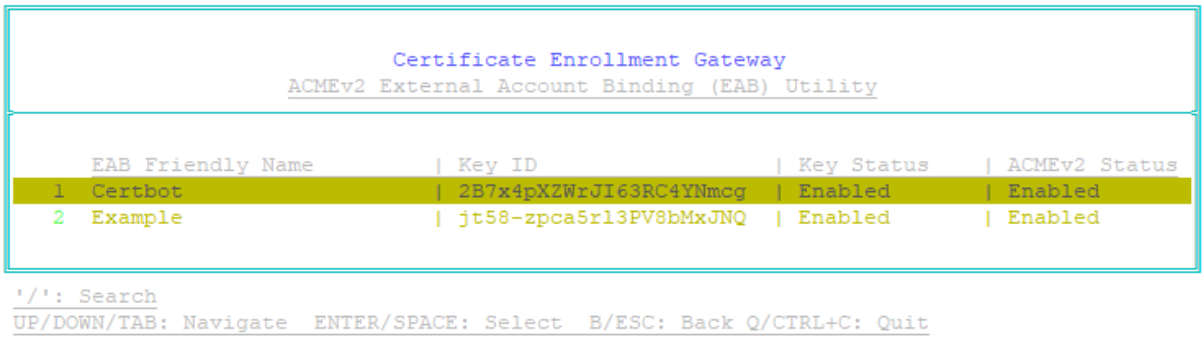
1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

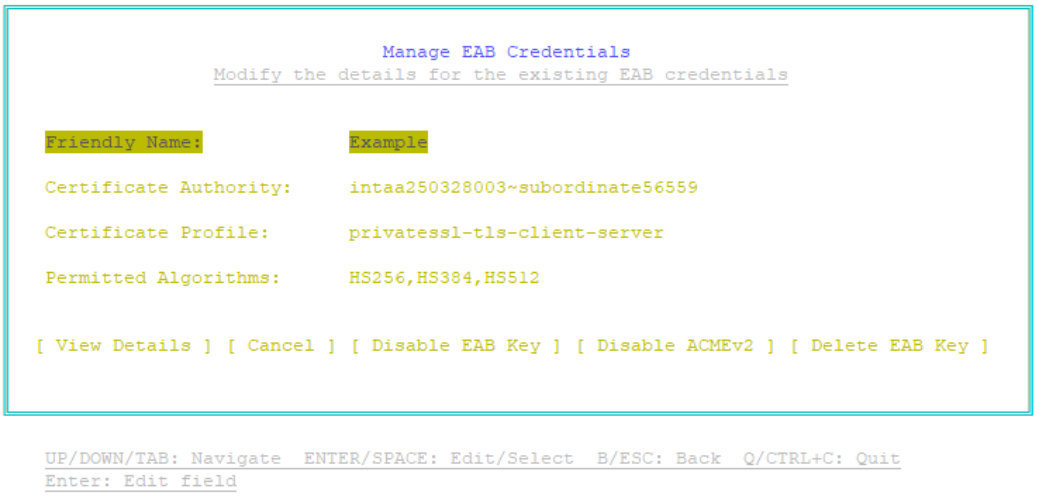


4. Select **Manage EAB credentials**, and then press Enter.
   A list of External Account Binding credentials appears. For example:

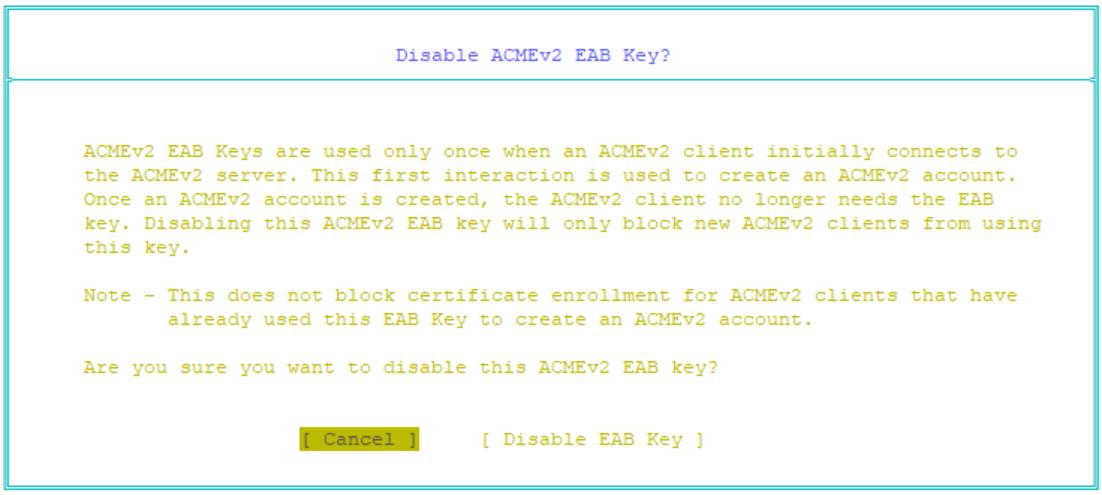


The **Key Status** column displays the status of the HMAC key for each External Account Binding credential, either Enabled or Disabled.

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



6. Select **Disable EAB Key**, and then press Enter.
   The **Disable ACMEv2 EAB Key** page appears.



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.

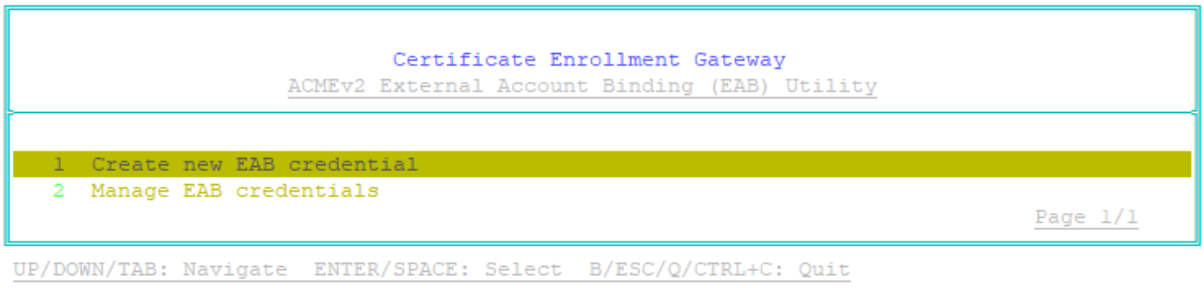
You can enable a key that has been disabled for an External Account Binding credential. When you enable a key, new ACMEv2 clients can use the key to create a new ACMEv2 account.

To enable the HMAC key for an External Account Binding credential

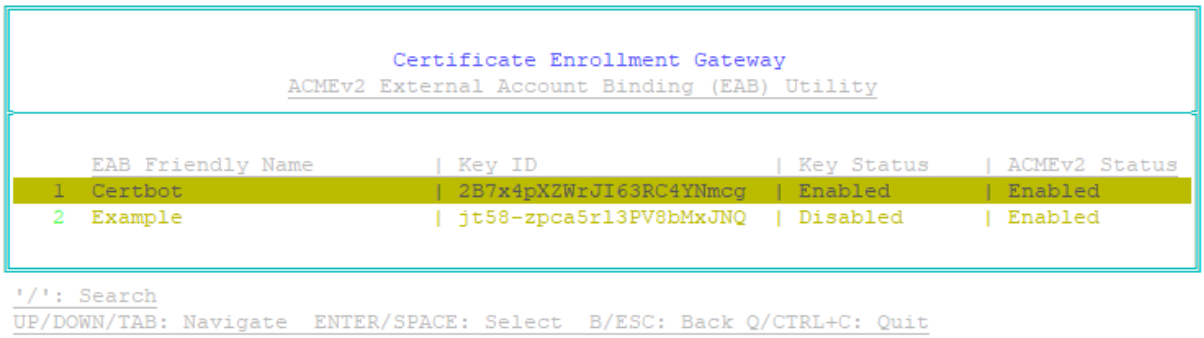
1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

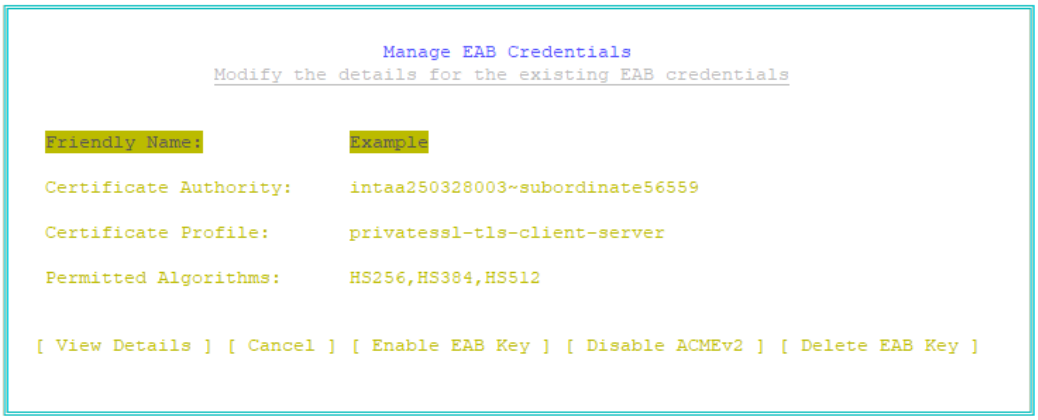


4. Select **Manage EAB credentials**, and then press Enter.
   A list of External Account Binding credentials appears. For example:

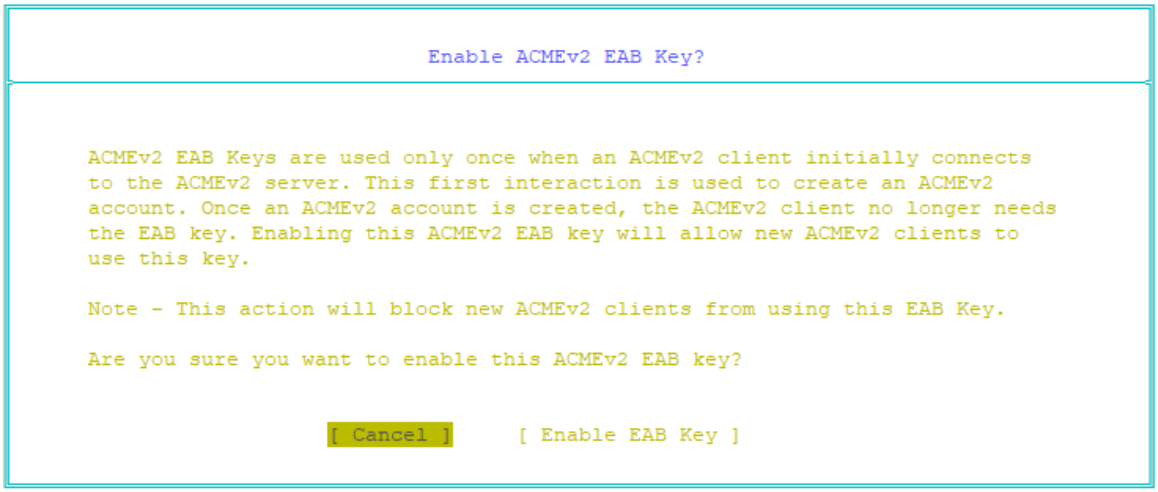


   The **Key Status** column displays the status of the HMAC key for each External Account Binding credential, either Enabled or Disabled.

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



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.

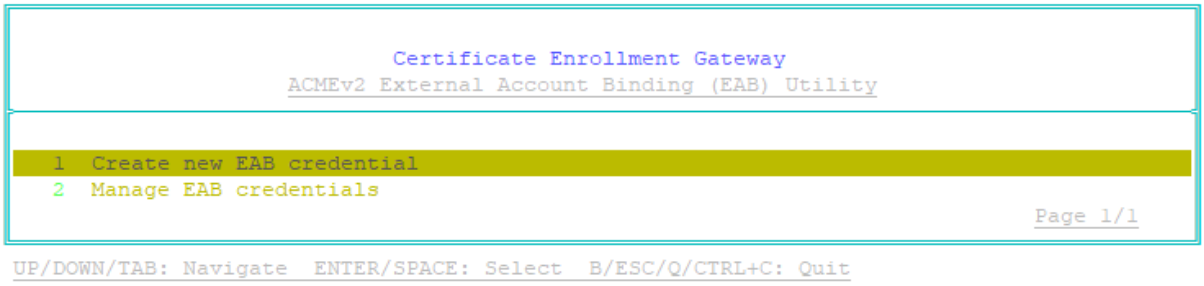
You should disable ACMEv2 operations for an External Account Binding credential if you want to temporarily prevent any ACMEv2 clients from using the External Account Binding credential. If you want to permanently prevent ACMEv2 clients from using an External Account Binding credential, delete the HMAC key for the credential (see Deleting HMAC keys for External Account Binding credentials).

To disable ACMEv2 operations for an External Account Binding credential

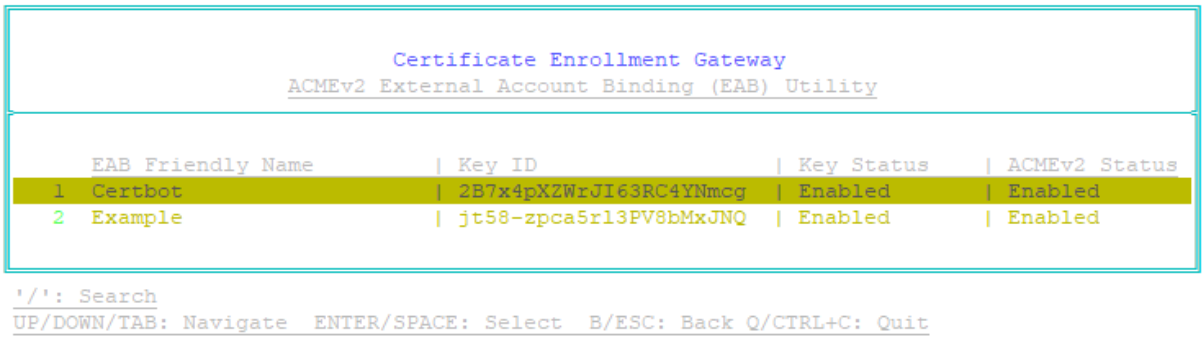
1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

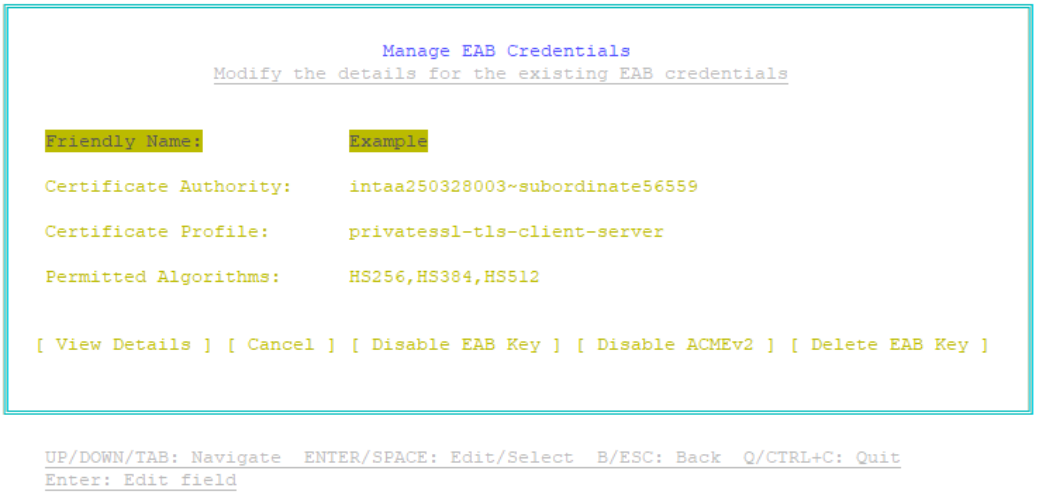
3. The main menu appears:



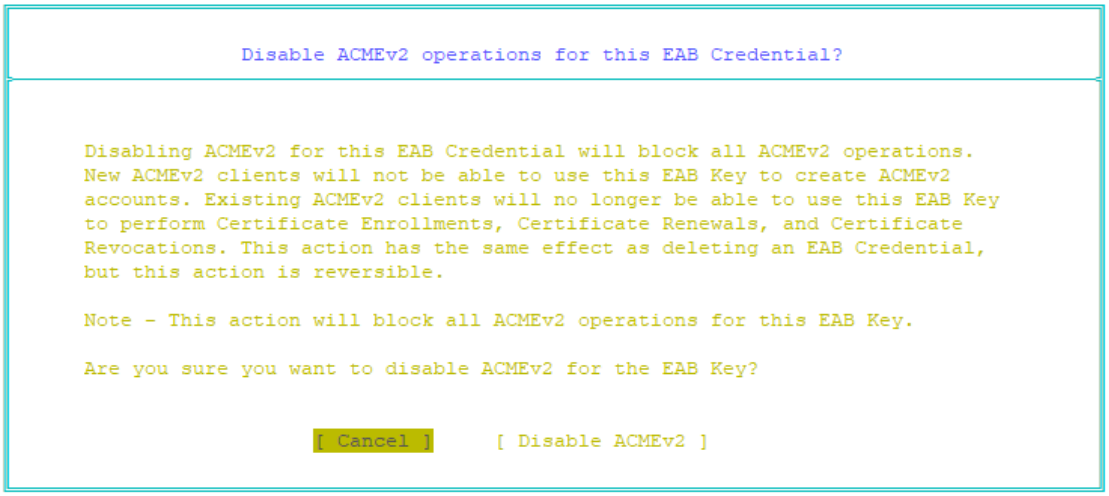
4. Select **Manage EAB credentials**, and then press Enter.
   A list of External Account Binding credentials appears. For example:



   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:



6. Select **Disable ACMEv2** and press Enter.
   The **Disable ACMEv2 operations for this EAB Credential** page appears.



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.

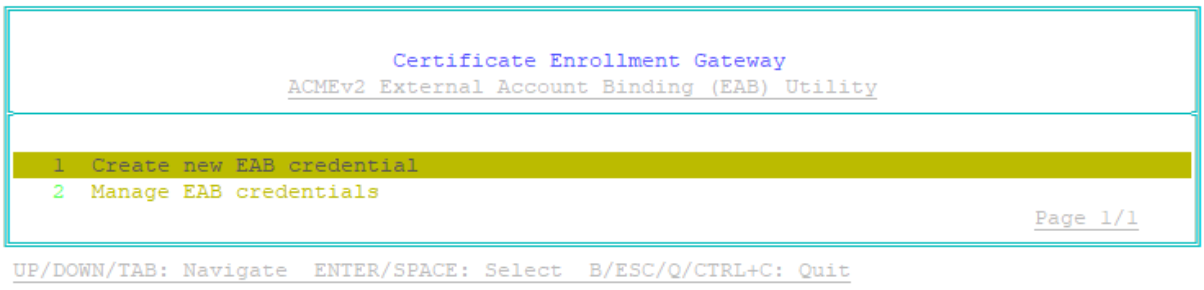
You can enable ACMEv2 operations that have been disabled for an External Account Binding credential. When you enable ACMEv2 operations for an External Account Binding credential, ACMEv2 clients with an existing account can perform ACMEv2 operations with the credential, and new ACMEv2 clients can use the credential to create an account if the HMAC key is enabled.

To enable ACMEv2 operations for an External Account Binding credential

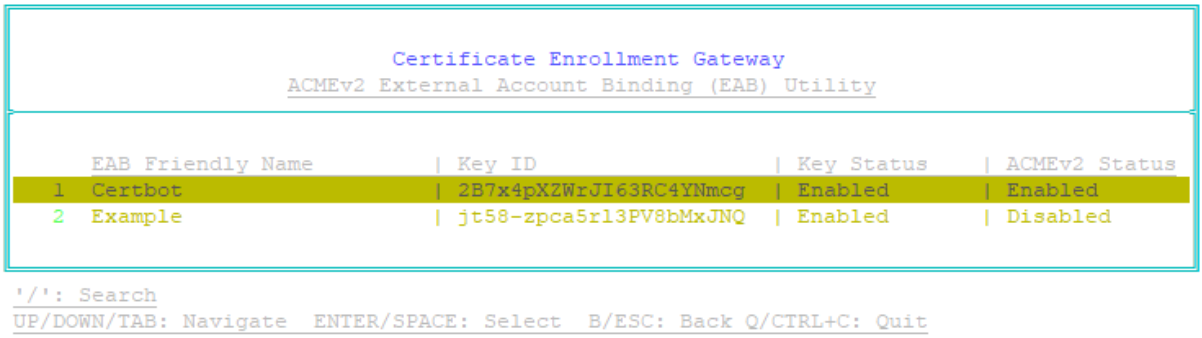
1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

3. The main menu appears:

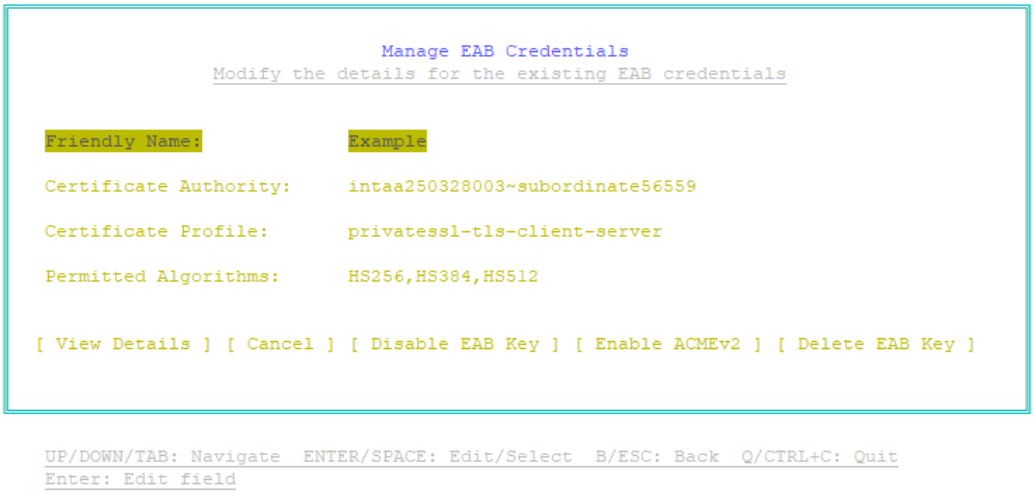


4. Select **Manage EAB credentials**, and then press Enter.
   A list of External Account Binding credentials appears. For example:

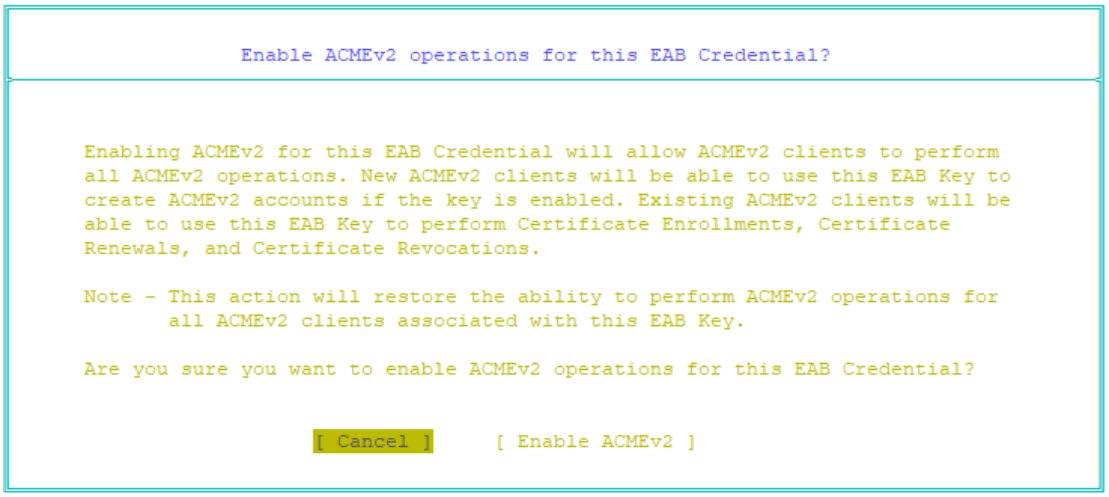


The **ACMEv2 Status** column displays the status of ACMEv2 operations for each External Account Binding credential, either Enabled or Disabled.

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



6. Select **Enable ACMEv2** and press Enter.
   The **Enable ACMEv2 operations for this EAB Credential** page appears.



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 the remove the HMAC key 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.

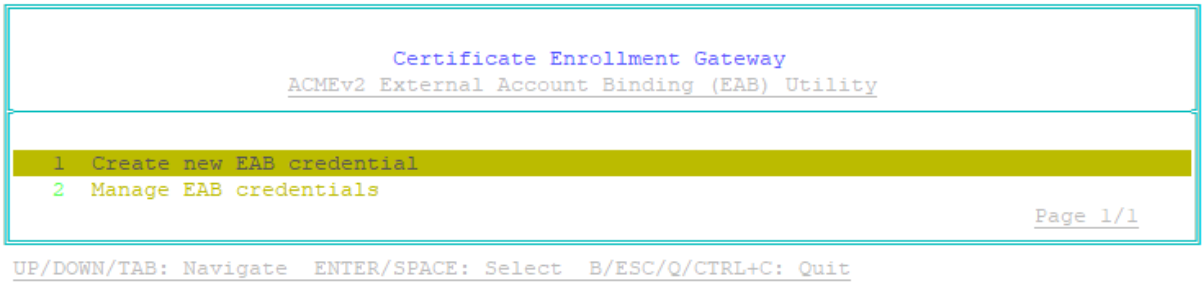
If you want to temporarily prevent an External Account Binding credential from being used by ACMEv2 clients, disable ACMEv2 operations for the credential instead (see Disabling ACMEv2 operations for External Account Binding credentials).

To delete an External Account Binding credential

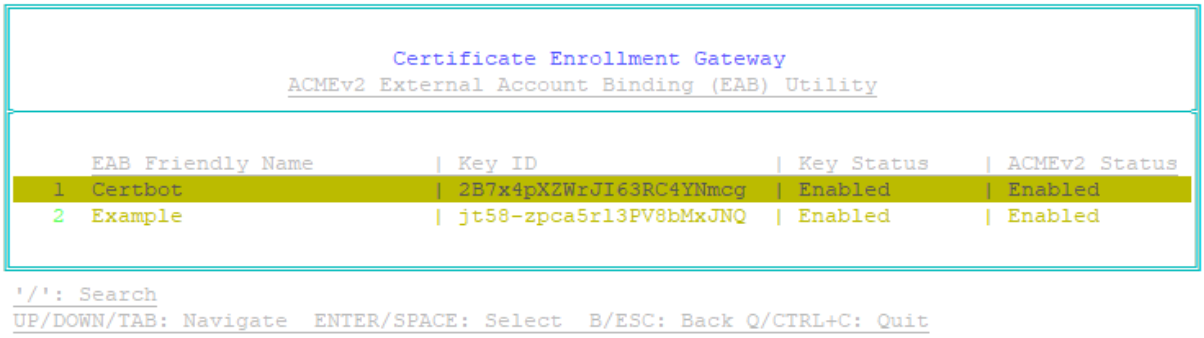
1. On the Entrust Deployment Manager or Cryptographic Security Platform node hosting the EAB Utility, log in as sysadmin.
2. Enter the following command to launch the EAB Utility:

```
sudo eab-util
```

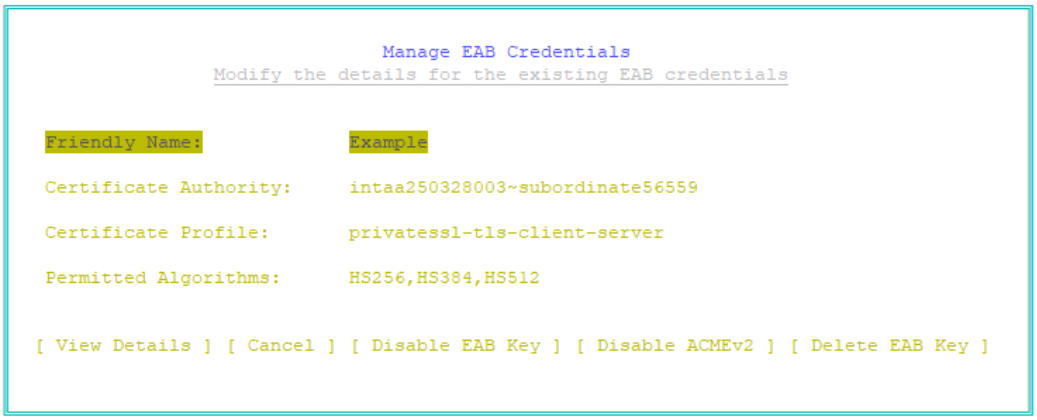
3. The main menu appears:



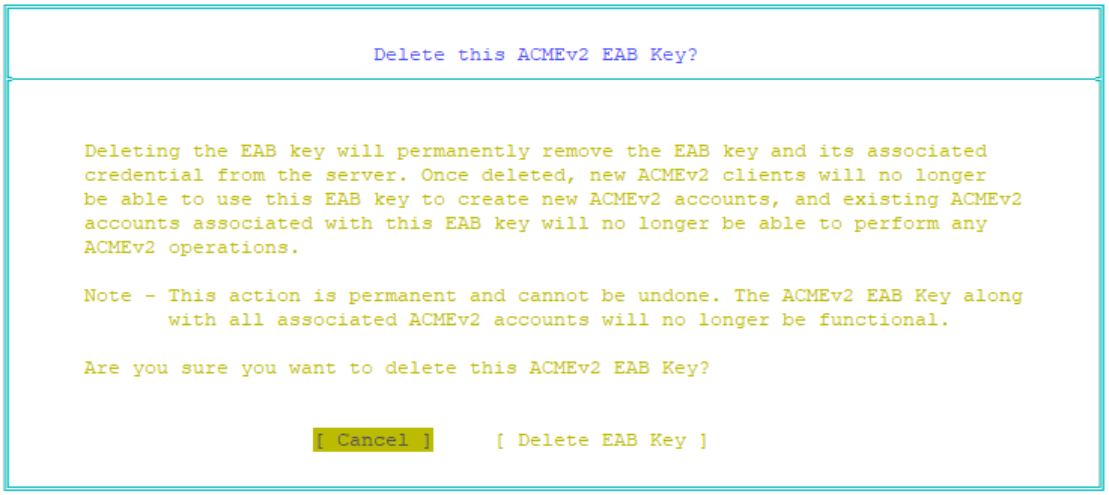
4. Select **Manage EAB credentials**, and then press Enter.
   A list of External Account Binding credentials appears. For example:



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



6. Select **Delete EAB Key** and press Enter.
   The **Delete this ACMEv2 EAB Key** page appears.



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/0mj615kbbkkb/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/0mj615kbbkkb/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:

Method	Required configuration
DNS-01	Certificate Enrollment Gateway and the ACMEv2 client must point to the same DNS server. Certificate Enrollment Gateway must be able to query for DNS TXT records generated by the ACMEv2 client.
HTTP-01	Certificate Enrollment Gateway must resolve the hostname of the FQDN in the CSR. The hostname must resolve to the IP address of the ACMEv2 client. The ACMEv2 client must listen on port 80 to use HTTP-01 validation.

About CSRs with an empty Subject DN

Some ACMEv2 clients may send a CSR with an empty Subject DN. However, certificates issued by Entrust Certificate Authority instances will have a non-empty Subject DN. If an ACMEv2 client sends a CSR with an empty Subject DN, Certificate Enrollment Gateway will use the first Subject Alternative Name value in the CSR as the Subject DN.

Certificate Enrollment Gateway will not modify the Subject DN in the CSR. Certificate Enrollment Gateway will send the CSR unaltered to CA Gateway for processing, and send the Subject DN separately as a CA Gateway request parameter.

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.

- Cert-manager.io prerequisites

- Preparing Linux for HTTPS (optional)
- Deploying Kubernetes and Cert-manager.io
- Configuring Cert-manager.io for Certificate Enrollment Gateway with ACMEv2

> 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.

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 Enrollment URLs for Certificate Enrollment Gateway. You need this URL later when configuring Cert-manager.io.

Preparing Linux for HTTPS (optional)

> This section is required only if the Kubernetes cluster that will host Cert-manager.io will use a trusted HTTPS connection to connect to Certificate Enrollment. If you will not use a trusted HTTPS connection, you can skip this section. You must complete this step before deploying the Kubernetes cluster.

To configure Linux to trust a CA certificate chain, complete the following steps.

To configure Linux to trust a CA certificate chain

1. Transfer Certificate Enrollment Gateway's trust certificate chain (from the issuing CA certificate to the root CA certificate) to the Linux server that will host Cert-manager.io. The certificate files must be in PEM format.
2. Log in to the Linux server that will host Cert-manager.io.
3. Copy the certificates (trust chain) into the following directory:

```
/etc/pki/ca-trust/source/anchors
```

4. Enter the following command to update the file permissions for `ca-bundle.crt` so everyone can read the file:

```
sudo chmod +r ./ca-bundle.crt
```

5. Run the following command to update the `ca-bundle.crt` file at the operating system level:

```
sudo update-ca-trust extract
```

6. Verify that the certificates were added to the following file:

```
/etc/pki/tls/certs/ca-bundle.crt
```

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:/user/local/bin
```

2. Enable the use of kubectl permanently, by ensuring that `/usr/local/bin` appears as part of the `PATH` environment variable in the `~/.bash_profile` file.
3. Install Helm by running the following commands:

```
curl https://raw.githubusercontent.com/helm/helm/master/scripts/get-helm-3 |
bash
echo "export KUBECONFIG=/etc/rancher/k3s/k3s.yaml" >> ~/.bash_profile
export KUBECONFIG=/etc/rancher/k3s/k3s.yaml
```

4. Add the Cert-manager.io repository to Helm by running the following commands:

```
helm repo add jetstack https://charts.jetstack.io
helm repo update
```

5. Install Cert-manager.io using Helm by entering the following command:

```
helm upgrade -i -n cert-manager cert-manager jetstack/cert-manager --set
installCRDs=true --create-namespace --version v1.6.0-beta.0 --wait
```

6. (Secure HTTP Only) If you want to use Cert-manager.io with trusted HTTPS connections, then you must add the TLS CA certificate chain into the cluster. Create a `private-ca-bundle.pem` file.
    a. This file contains a concatenation of all PEM certificates in the CA certificate chain, starting with the issuing CA first and ending with the root CA last. For example:

```
-----BEGIN CERTIFICATE-----
MIIF0TCCA7mgAwIBAgIQCy...
...
V8HUOts=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFUDCCAzigAwIBAgIQRv...
...
XLy202FpMk40JO31gqbnDOusrY8=
-----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.

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 default ACMv2 enrollment URL or an ACMEv2 External Account Binding
credential 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 ACMEv2 account private key
```

```
    privateKeySecretRef:
      name: ceg-acme-account-key-http
    # Enable the HTTP-01 challenge provider
    solvers:
    - http01:
        ingress:
          class:  traefik
    # These lines are required for External Account Binding.
    # Remove these lines if External Account Binding is disabled in Certificate
Enrollment Gateway.
    # Replace the keyID value with the Key ID of the External Account Binding
credential.
    externalAccountBinding:
      keyID: Agu-fwShl2jDXsMYe4Ti3w
      keySecretRef:
        name: eab-secret
        key: secret
```

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. To use External Account Binding with Certificate Enrollment Gateway, enter the following command to create Kubernetes secret that contains the HMAC key for the External Account Binding credential:

```
kubectl create secret generic eab-secret --from-literal \ secret=<HMAC-key>
```

   Where `<HMAC-key>` is the HMAC key. For example:

```
kubectl create secret generic eab-secret --from-literal \
secret=YWxCcVJKeG00cXZsc2x3OHZaNzNwRTdTX3hJeVh3dllTSXJxeFQ1Rngxcw
```

2. 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
```

3. 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.
4. 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
```

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> (--eab-kid <key-ID> --eab-hmac-key <HMAC-key>)
```

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 Enrollment URLs for Certificate Enrollment Gateway.
- `<ca-file>` is the path and file name of the CA certificate bundle, used to verify the Certificate Enrollment Gateway server certificate.
- `<key-ID>` is the Key ID of the External Account Binding credential.
- `<HMAC-key>` is the HMAC key of the External Account Binding credential.

Examples:

```
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

acme.sh --issue --standalone -d example.com -d www.example.com --server https://
cegserver.example.com/acme/ceg/Agu-fwShl2jDXsMYe4Ti3w/0mj615kbbkkb/directory --ca-
bundle /tmp/root-ca.crt --eab-kid Agu-fwShl2jDXsMYe4Ti3w --eab-hmac-key
YWxCcVJKeG00cXZsc2x3OHZaNzNwRTdTX3hJeVh3dllTSXJxeFQ1Rngxcw
```

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. Parameters in parentheses are required to create an account with an External Account Binding credential, but must not be specified when External Account Binding is disabled in Certificate Enrollment Gateway. Parameters in square brackets are optional parameters.

   ```
   wacs.exe --baseuri <CEG-ACME-URL> --accepttos --source manual --host <hosts> --
   force (--eab-key-identifier <key-ID> --eab-key <HMAC-key> [--eab-algorithm
   <algorithm>])
   ```

   Where:
   - `<CEG-ACME-URL>` is the ACMEv2 enrollment URL used to request a certificate from Certificate Enrollment Gateway. For details, see Enrollment URLs for Certificate Enrollment Gateway.
   - `--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-separate list of host names to include the 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.
   - `<key-ID>` is the Key ID of the External Account Binding credential.
   - `<HMAC-key>` is the HMAC key of the External Account Binding credential.
   - `<algorithm>` is the HMAC algorithm is the algorithm to use for External Account Binding. If not specified, it defaults to HS256. The algorithm must be permitted by the External Account Binding credential.

5. Examples:

   ```
   wacs.exe --baseuri https://cegserver.example.com/acme/tenant1/example_ca1/
   privatessl_tls_client/directory --accepttos --source manual --host
   www.example.com,example.com --force
   ```

```
wacs.exe --baseuri https://cegserver.example.com/acme/ceg/Agu-
fwShl2jDXsMYe4Ti3w/0mj615kbbkkb/directory --acceptto s --source manual --host
www.example.com,example.com --force --eab-key-identifier Agu-fwShl2jDXsMYe4Ti3w
--eab-key YWxCcVJKeG00cXZsc2x3OHZaNzNwRTdTX3hJeVh3dllTSXJxeFQ1Rngxcw
```

6. 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
```

7. Enter `N` to create a new certificate with the default settings.
8. 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):
```

9. Enter an email address. Certificate Enrollment Gateway will not send email messages to this email address.
10. 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> --server <CEG-ACME-URL> --standalone --no-eff-email --
agree-tos -m <email-address> (--eab-kid <key-ID> --eab-hmac-key <HMAC-key>)
```

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.
- `<key-ID>` is the Key ID of the External Account Binding credential.
- `<HMAC-key>` is the HMAC key of the External Account Binding credential.

Examples:

```
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

certbot certonly -d example.com -d www.example.com --server https://
cegserver.example.com/acme/ceg/Agu-fwShl2jDXsMYe4Ti3w/0mj615kbbkkb/directory --
standalone --no-eff-email --agree-tos -m notifications@example.com --eab-kid Agu-
fwShl2jDXsMYe4Ti3w --eab-hmac-key
YWxCcVJKeG00cXZsc2x3OHZaNzNwRTdTX3hJeVh3dllTSXJxeFQ1Rngxcw
```

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>:8443/management-console
   ```

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

   ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

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

   ℹ See Managing identities 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:

ℹ 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-----
MIIDqQYJKoZIhvcNAQcCoIIDmjCCA5YCAQExADALBgkqhkiG9w0BBwGgggN...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----
MIIDejCCAmKgAwIBAgIQQ8e7ock59Y21Mtcy7rGJUDANBgkqhkiG9w0BAQs...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----
MIQ0EgRW50cnkwHhcNMjMwMjA4MTUxNzEwWhcNMzMwMjA4MTU0NzEwWjAyM...
-----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-----
MIIDqQYJKoZIhvcNAQcCoIIDmjCCA5YCAQExADALBgkqhkiG9w0BBwGgggN...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----
MIIDejCCAmKgAwIBAgIQQ8e7ock59Y21Mtcy7rGJUDANBgkqhkiG9w0BAQs...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----
MIQ0EgRW50cnkwHhcNMjMwMjA4MTUxNzEwWhcNMzMwMjA4MTU0NzEwWjAyM...
-----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>:8443/management-console
   ```

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

   > ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

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

   > ℹ See Managing identities 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 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>:8443/management-console
   ```

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

   ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

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

   > See Managing identities 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 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 1.3.6.1.4.1.311.30.2.2).
k. For **Renewal threshold (%)**, enter the percentage of the certificate lifetime that remains before the certificate should be renewed.
l. For **SCEP Server URLs**, enter one of the following Certificate Enrollment Gateway URLs:

> The following Intune-SCEP enrollment URL requires a trailing forward slash (/). To support macOS devices, the URL must start with `http` instead of `https`.

```
https://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/intune/
http://<CEG-server>/scep/<tenant-ID>/<CA-ID>/<profile-ID>/intune/
```

See below for a description of each field.
   - <CEG-server>
   - <tenant-ID>
   - <CA-ID>
   - <profile-ID>

For example:

```
https://cegserver.example.com/scep/tenant1/example-ca1/intune-digital-signature/intune/
http://cegserver.example.com/scep/tenant1/example-ca1/intune-digital-signature/intune/
```

m. Enter values for any other settings as required.
11. Click **OK**.
12. Click **Create** to create the SCEP certificate profile.
13. Click **Assignments**.
14. For **Include**, select the Azure Active Directory groups you want to include with the certificate profile.

15. For **Exclude**, select the Azure Active Directory groups you want to exclude from the certificate profile.
16. Click **Save**.

<CEG-server>

The hostname or IP address of the Certificate Enrollment Gateway server.

<tenant-ID>

The unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.

<CA-ID>

The CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the SCEP client.

<profile-ID>

The profile ID defined in CA Gateway that defines the certificate type issued to the SCEP client. For Entrust PKI as a Service, the profile ID is one of the following:

- intune-digital-signature-key-encipherment
- intune-digital-signature
- intune-key-encipherment
- intune-non-repudiation

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>:8443/management-console
   ```

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

   ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

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

   ℹ See Managing identities 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>:8443/management-console
```

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

> ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

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

> ℹ See Managing identities 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>:8443/management-console
   ```

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

   > ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

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

   > ℹ See Managing identities 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:

> 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 ChomeOS is a cloud-first operating system for Chromebooks and other Google devices. ChromeOS devices can request certificates from the Certificate Enrollment Gateway using the SCEP protocol. SCEP enrollment for ChromeOS is controlled using Google Admin, a Web-based interface for managing users and groups for an organization.

- ChromeOS integration requirements
- Configuring Google Admin for SCEP enrollment
- Downloading and installing the Google Cloud Certificate Connector
- Testing SCEP enrollment with ChromeOS

ChromeOS integration requirements

Google Admin requirements:

- Google Admin requires either the Chrome Enterprise Upgrade or the Chrome Education Upgrade.
- Google Admin requires the CA certificate chain (from the root CA certificate to the issuing CA certificate) for the on-premises Managed CA or Entrust PKI as a Service (PKIaas).

Google Cloud Certificate Connector requirements:

- The Google Cloud Certificate Connector must be installed on Domain-joined Windows server.
- The Google Cloud Certificate Connector requires outbound network connectivity to Google Admin.
- The Google Cloud Certificate Connector requires outbound network connectivity to Entrust Certificate Enrollment Gateway.

Entrust Certificate Enrollment Gateway requirements:

> Static challenge passwords are not secure. To increase security, it is recommended that you configure the firewall on the Certificate Enrollment Gateway server to limit incoming traffic for the SCEP service to only the Google Cloud Certificate Connector.

- The SCEP service must be configured with a static challenge password.
- Certificate Enrollment Gateway requires inbound connectivity from the Google Cloud Certificate Connector.

ChromeOS requirements:

- ChromeOS must be enrolled with Google Admin using the **Enterprise enrollment** option. See the Google documentation for instructions about enrolling a device using the **Enterprise enrollment** option (https://support.google.com/chrome/a/answer/1360534).
- ChromeOS requires outbound connectivity to Google Admin without the interference of SSL decryption.

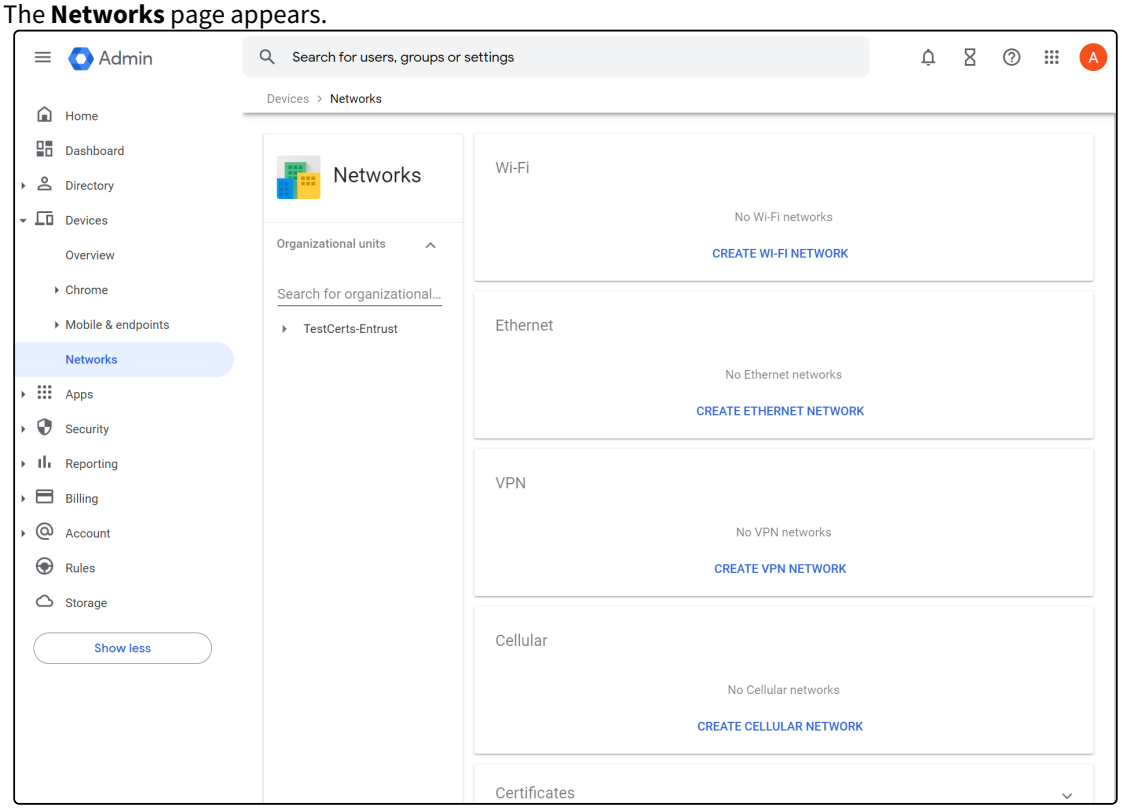
Configuring Google Admin for SCEP enrollment

SCEP enrollment for ChromeOS is controlled using Google Admin, a Web-based interface for managing users and groups for an organization.

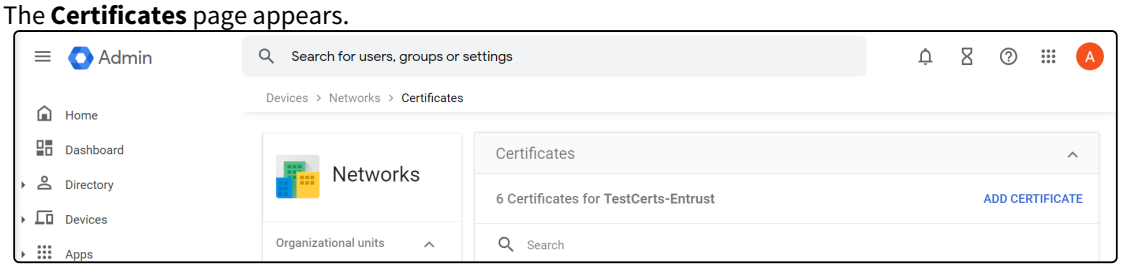
To configure Google Admin for SCEP enrollment

1. Log in to Google Admin (https://admin.google.com).

2. Navigate to **Devices > Networks**.
   The **Networks** page appears.

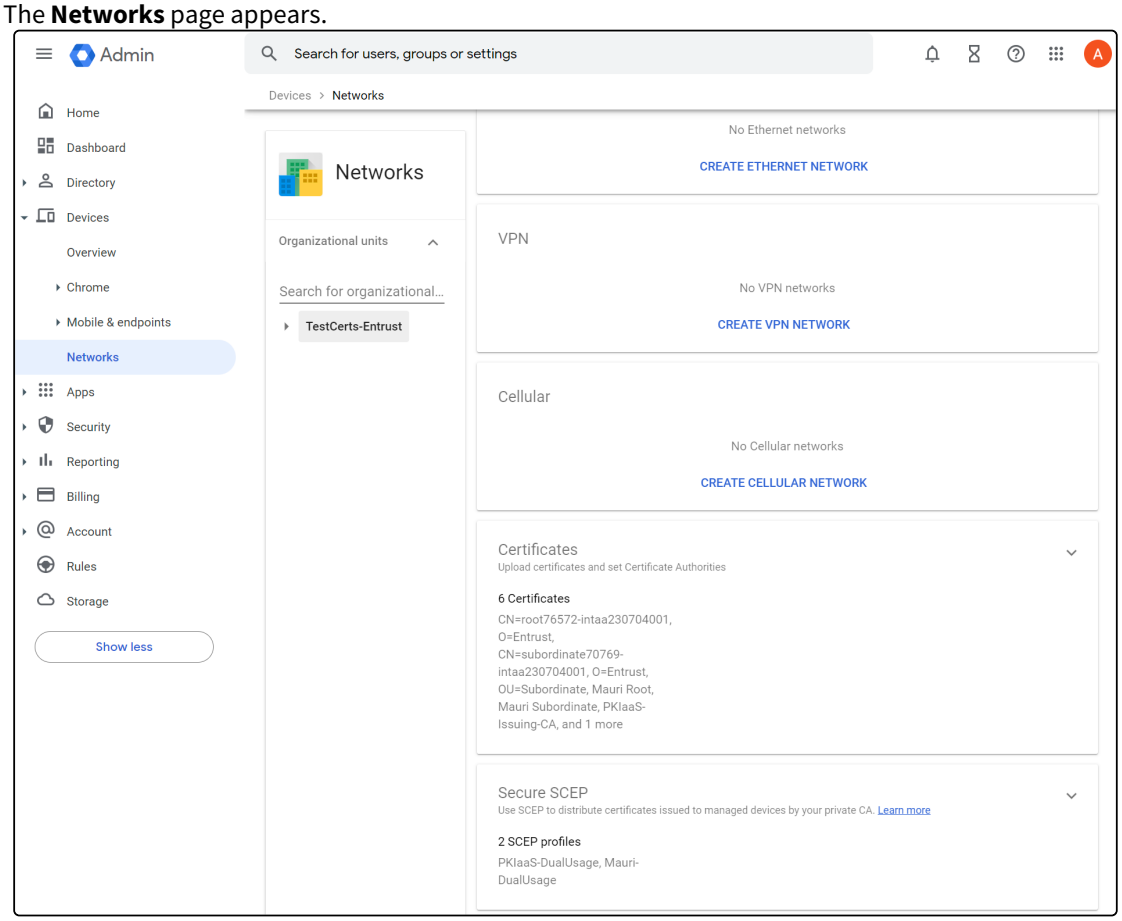


3. Click on the **Certificates** pane.
   The **Certificates** page appears.

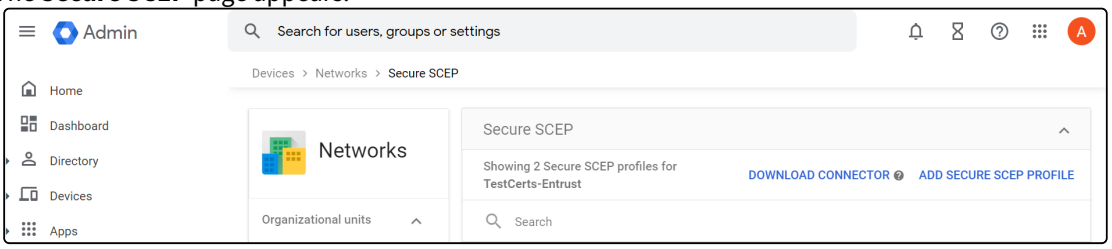


4. Add the entire CA certificate chain (from the root CA to the issuing CA) for the Managed CA. To add a CA certificate:
   a. Click **Add Certificate**. The **Add Certificate** page appears.
   b. In the **Name** field, enter a unique friendly name for the CA certificate,
   c. Click **Upload** and then select the CA certificate you want to upload.
   d. Select **Chromebook**.
   e. Click **Add**.
5. Navigate to **Devices > Networks**.

6. The **Networks** page appears.



7. Click on the **Secure SCEP** pane.
   The **Secure SCEP** page appears.



8. Create a SCEP profile:
   a. Click **ADD SECURE SCEP PROFILE**. The **Edit Secure SCEP** page appears.
   b. 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.
   c. For **SCEP profile name**, enter a unique name for the SCEP profile.
   d. For **Subject name format**, define the desired Subject Name format.

> 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`.

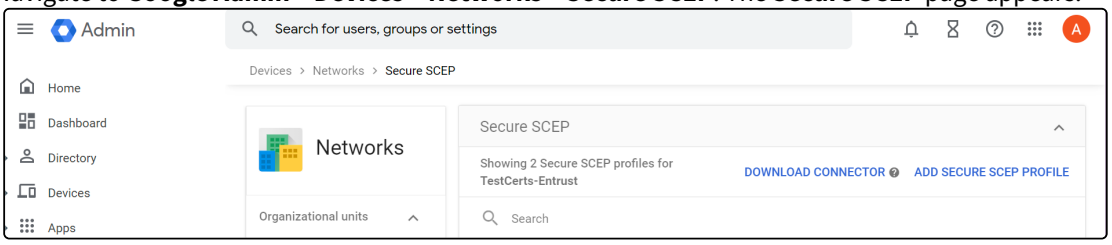
e. For **Key Usage**, select each key usage that will be included in the issued certificates.
f. For **Key size (bits)**, select a key size for the issued certificates.
g. For **Security**, select the security level (attestation requirement) for the issued certificates.
h. In the **SCEP server URL** 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

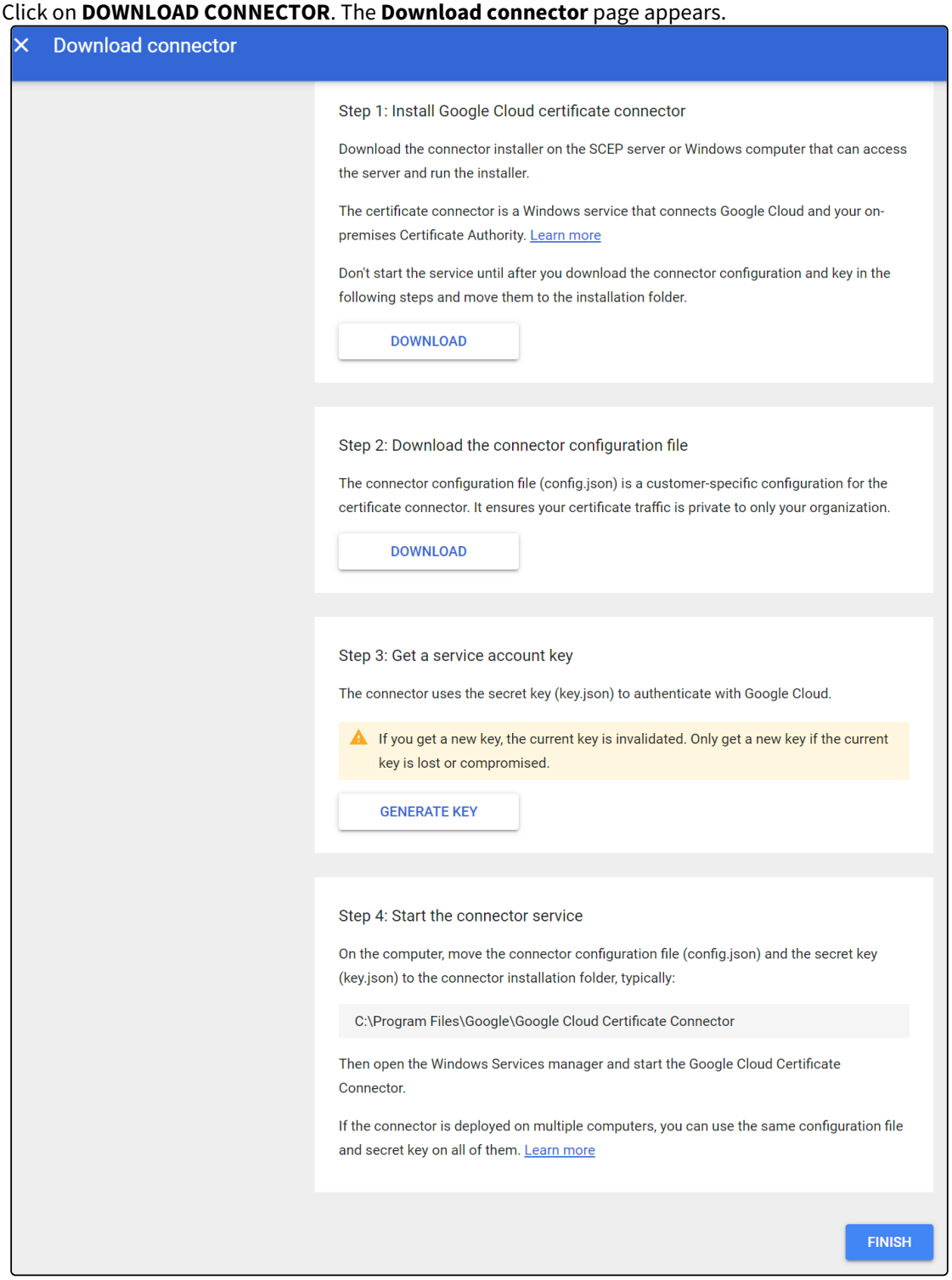
The Google Cloud Certificate Connector is a Windows service that securely distributes certificates and authentication keys from a SCEP server to users' devices. The Google Cloud Certificate Connector must be installed on Domain-joined Windows server.

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.



4. In the **Step 1** pane, click **DOWNLOAD** to download the installer for Google Cloud Certificate Connector.
5. In the **Step 2** pane, click **DOWNLOAD** to download the configuration file (`config.json`) for Google Cloud Certificate Connector.
6. In the **Step 3** pane, click **GENERATE KEY** to generate and download a key file (`key.json`) for Google Cloud Certificate Connector.

7. Copy the installer, configuration file (`config.json`), and key file (`key.json`) to a Domain-joined Windows server.
8. On the Domain-joined Windows server, run the installer to install Google Cloud Certificate Connector.
9. Copy the `config.json` and `key.json` files into the Google Cloud Certificate Connector installation folder.
10. Start Google Cloud Certificate Connector. Open the Services administrative tool (select **Start** > **Windows Administrative Tools** > **Services**), and start **Google Cloud Certificate Connector**.

Testing SCEP enrollment with ChromeOS

To test SCEP enrollment with ChromeOS:

1. Enroll a Chromebook into Google Admin using the Enterprise Enrollment option.
2. Log in to the Chromebook.
3. Open Google Chrome.
4. Browse to chrome://policy.
5. Ensure that a device or user policy for client certificates exists (either **RequiredClientCertificateForDevice** or **RequiredClientCertificateForUser**).
   - The **RequiredClientCertificateForDevice** policy corresponds to the **Chromebook (device)** device platform in the SCEP profile.
   - The **RequiredClientCertificateForUser** policy corresponds to the **Chromebook (user)** device platform in the SCEP profile.
6. Browse to chrome://certificate-manager.
7. The name of the SCEP certificate should appear in the list.
8. Click on the SCEP certificate to view details.
9. Validate that no errors are displayed for the certificate.

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 Configuring

the Group Policy for cross-forest deployments), 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.

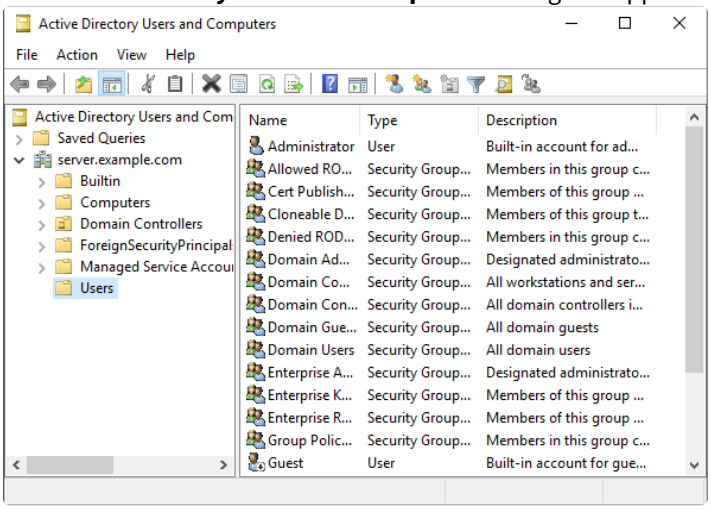
A Kerberos Service Account is a standard Active Directory user which belongs to the top-level parent domain. No special permissions are required for this user account.

> 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.

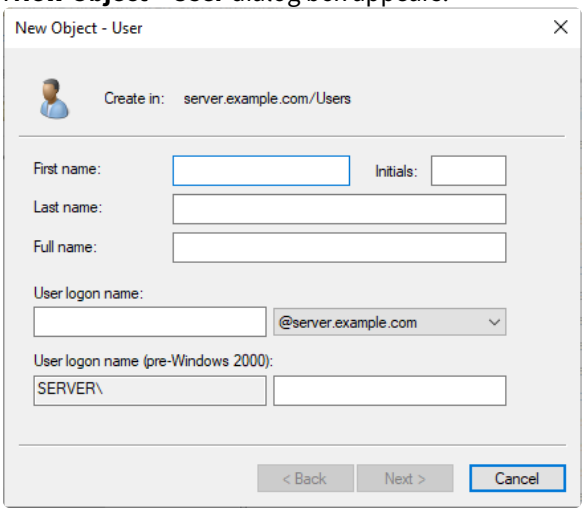
You must create the same Kerberos account for all forests in cross-forest deployments.

To create a Kerberos Service Account

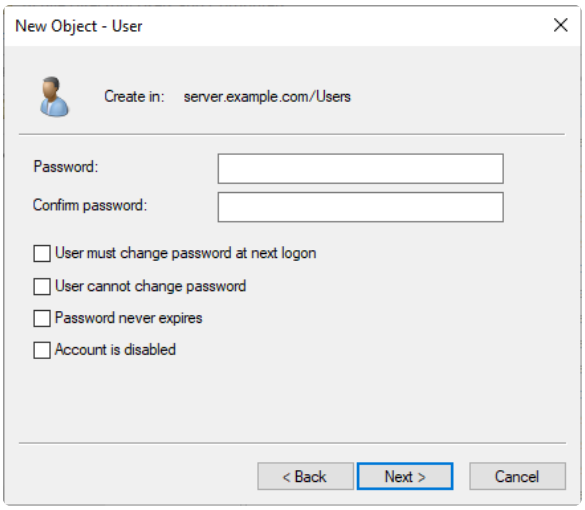
1. Log in to the server hosting the Active Directory domain controller as a domain administrator or a user who is a member of the built-in Account Operators domain group.
2. Open the Active Directory Users and Computers administrative tool (select **Start > Windows Administrative Tools > Active Directory 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.

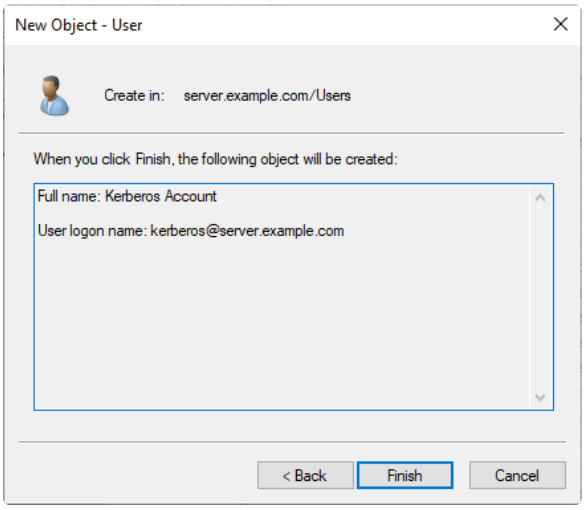


4. Using the **First name**, **Last name**, and **Full name** fields, enter a name for the new user account.
   At a minimum, you must enter a value into the **Full name** field. Entering values into the **First name** and **Last name** field will automatically fill the **Full name** field.
5. In the **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**.

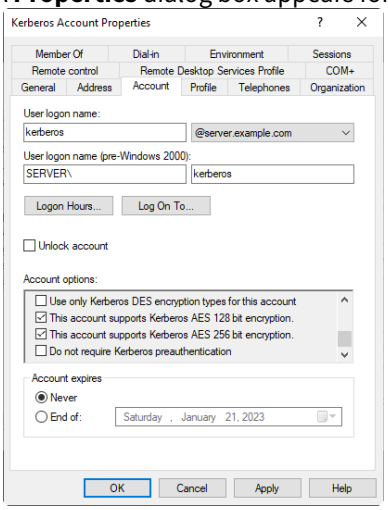


8. In the **Password** field, enter a password for the user account.
9. In the **Confirm password** field, enter the password again to confirm the password.
10. Deselect **User must change password at next logon**.
11. To avoid service interruptions because of an expired password, select **Password never 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:

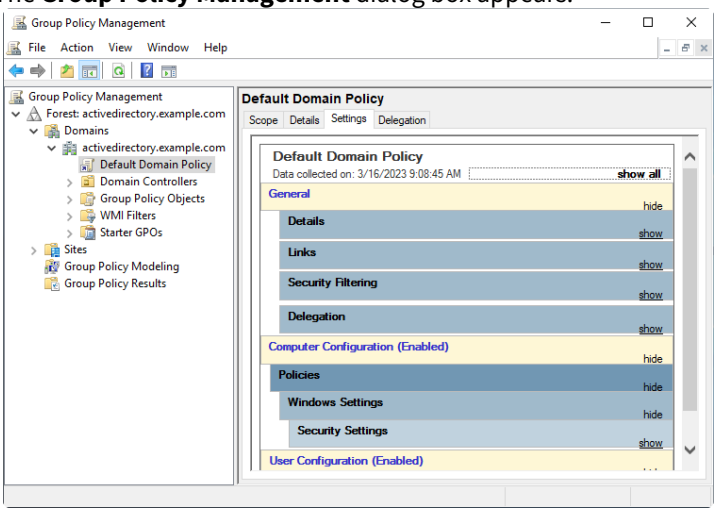
```
HTTP/server.example.com@EXAMPLE.COM
```

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.

> To ensure consistent behavior, the Global Policy settings must be supported and set identically on all domain controllers in the domain.

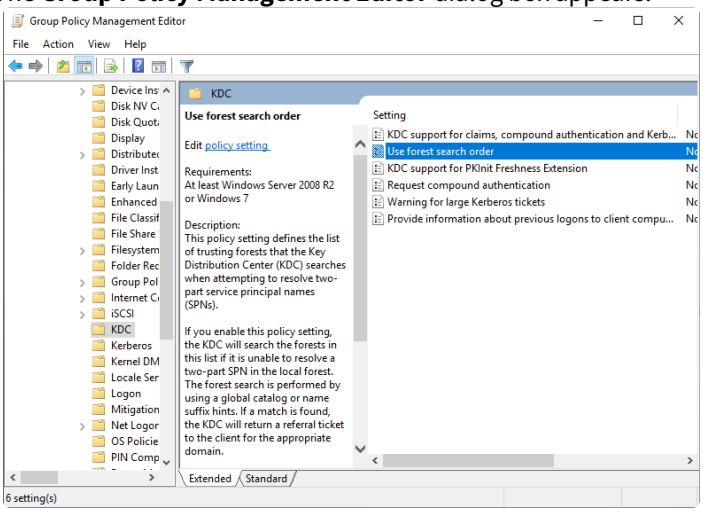
To configure the Group Policy for cross-forest deployments

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.

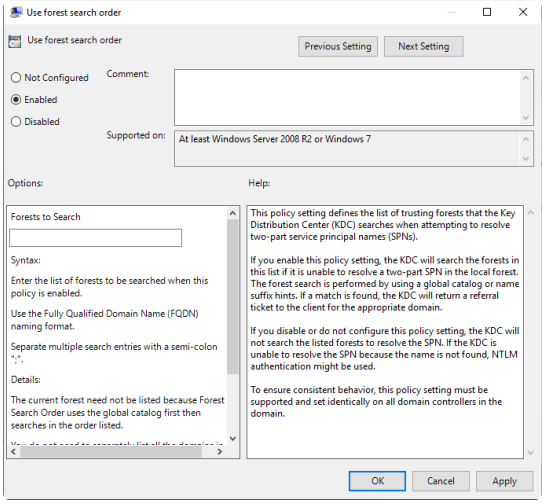


3. In the tree view, select **Group Policy Management** > **Forest: <forest>** > **Domains** > **<domain>** > **Default Domain Policy**.
   Where **<forest>** is the FQDN (fully qualified domain name) of the forest, and **<domain>** is the FQDN of the domain.

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.

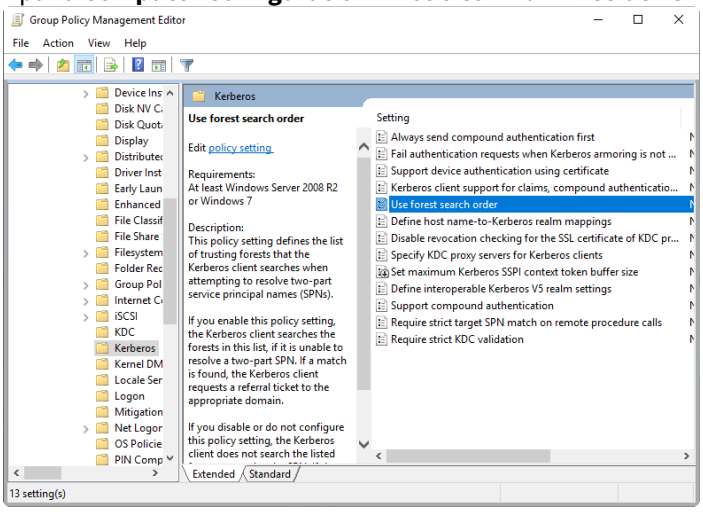


8. Select **Enabled**.
9. In the **Options** pane, in the **Forests to Search** field, enter the list of trusted forests that the Key Distribution Center (KDC) will search when attempting to resolve a two-part SPN that does not exist in the local forest. Separate each forest with a semicolon. For example:

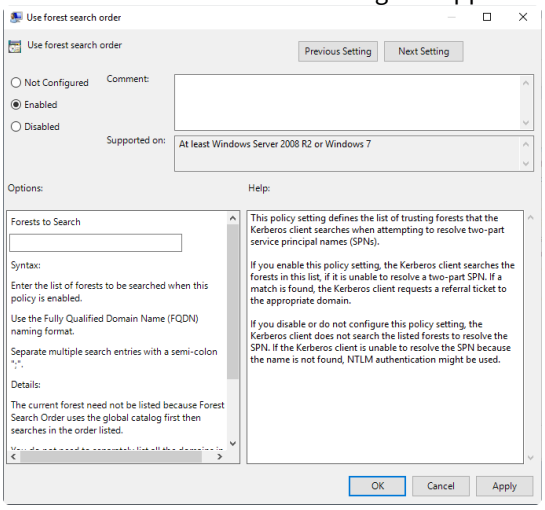
```
example.com;example.net;example.org
```

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**.

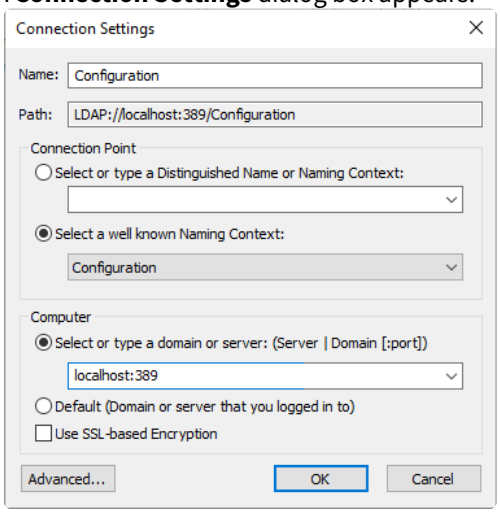
Adding referrals for cross-forest deployments

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.

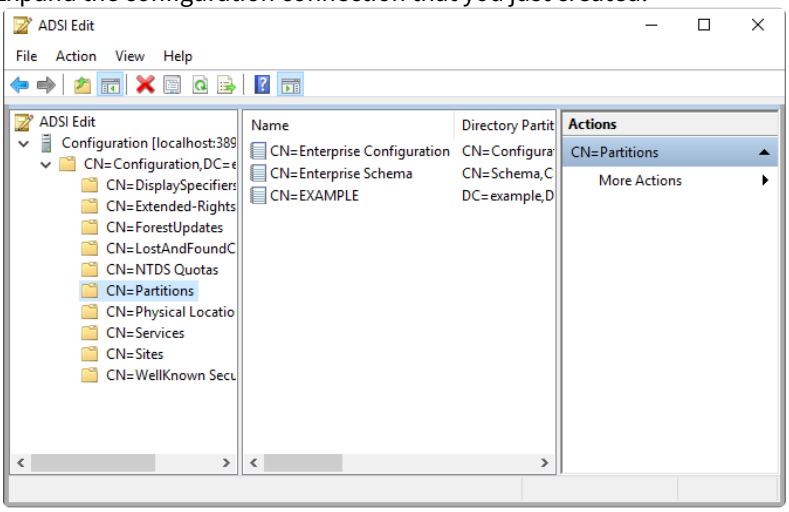
For cross-forest deployments with WSTEP enrollment, you must manually add a crossRef object into the domain controller for each cross-forest domain that you must support.

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.

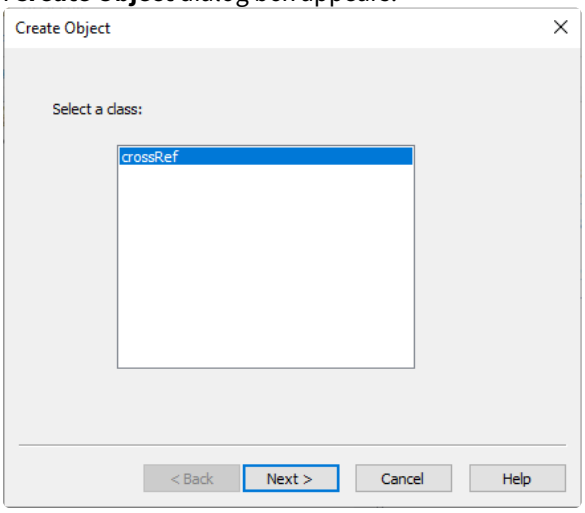


   b. In the **Name** field, enter a unique name for the connection.
   c. Under **Connection Point**, click **Select a well known Naming Context**, and then select **Configuration**.
   d. Under **Computer**, click **Select or type a domain or server**, and then enter the server and port of the domain 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.

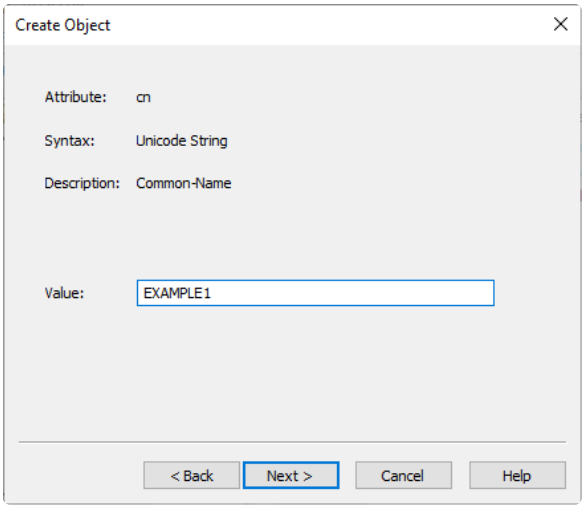


4. Expand **CN=Configuration,<suffix>** > **CN=Partitions**.
   Where **<suffix>** is the suffix (distinguished name) of the domain controller.

5. Select **CN=Partitions**, and then select **Action** > **New** > **Object**.
   A **Create Object** dialog box appears.

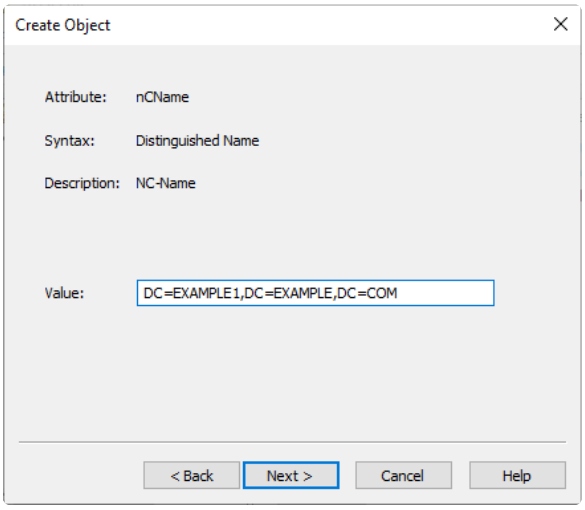


6. Select **crossRef**.
7. Click **Next**.

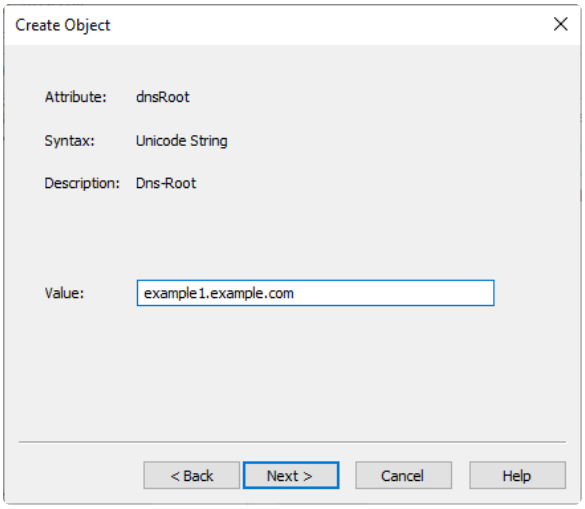


8. In the **Value** field, enter the NetBIOS name of a cross-forest domain.

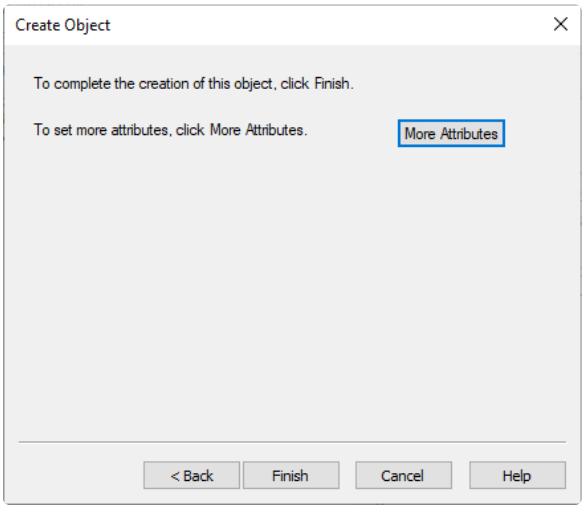
9. Click **Next**.



10. In the **Value** field, enter the distinguished name of the cross-forest domain.
11. Click **Next**.



12. In the **Value** field, enter the DNS name of the cross-forest domain.
13. Click **Next**.



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.

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.

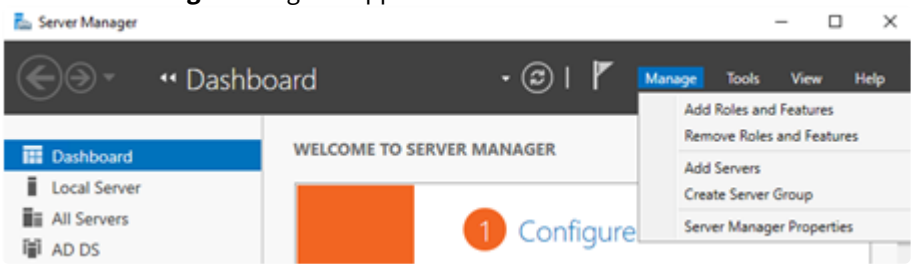
```
C:\Windows\System32\certtmpl.msc
```

5. Answer **Yes** when prompted to install the templates into Active Directory.

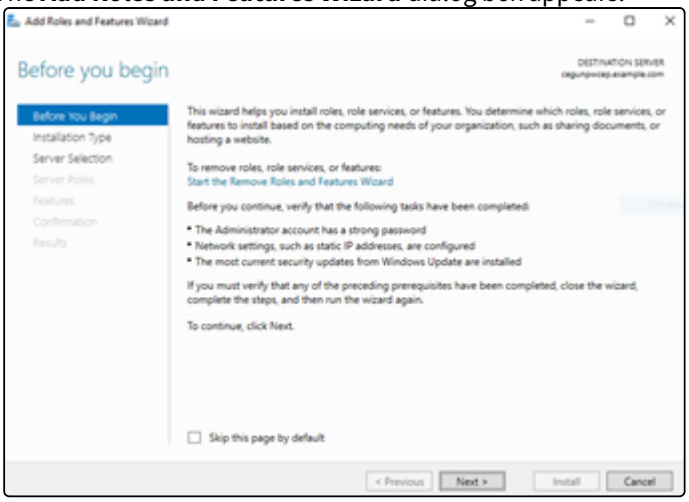
Adding the certificate templates feature using the Windows graphical interface

To add Certificate Templates using the Windows graphical interface, complete the following procedure.

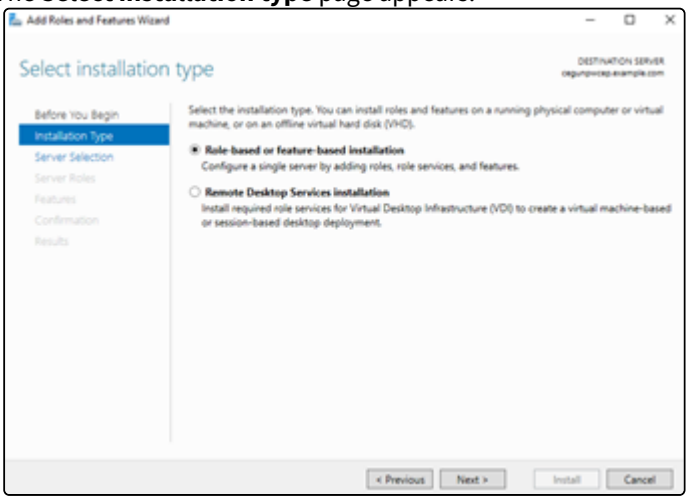
1. Log in to the server hosting Active Directory as a member of the Domain Admins and Enterprise Admins groups.
2. Open Server Manager. Select **Start > Server Manager**.
   The **Server Manager** dialog box appears.



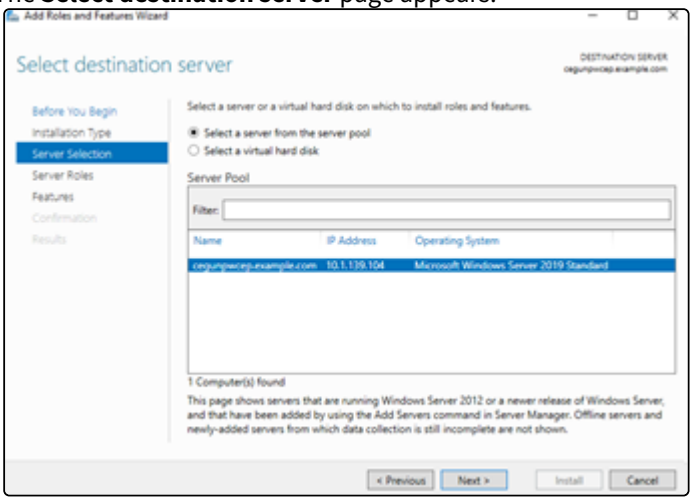
3. Select **Manage > Add Roles and Features**.
   The **Add Roles and Features Wizard** dialog box appears.



4. If the **Before you Begin** page appears, click **Next**.
   The **Select installation type** page appears.

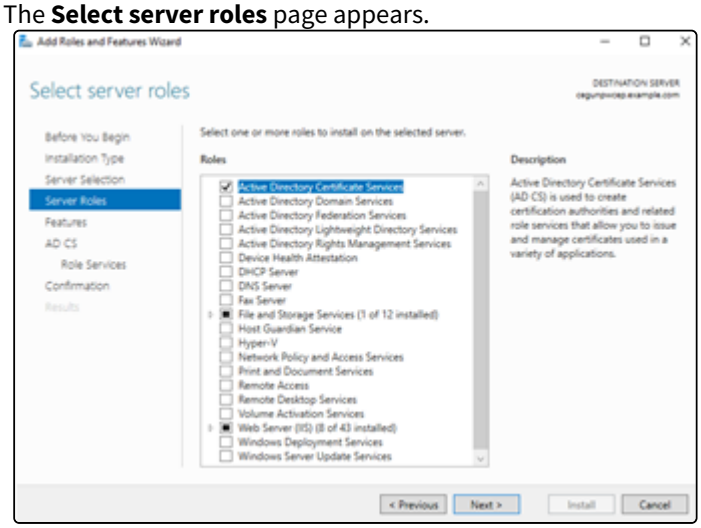


5. Select **Role-based or feature-based installation**.
6. Click **Next**.
   The **Select destination server** page appears.

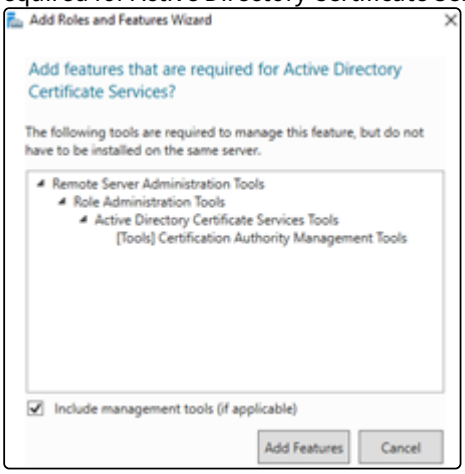


7. Click **Select a server from the pool**.
8. In the **Server Pool** list, select the server.

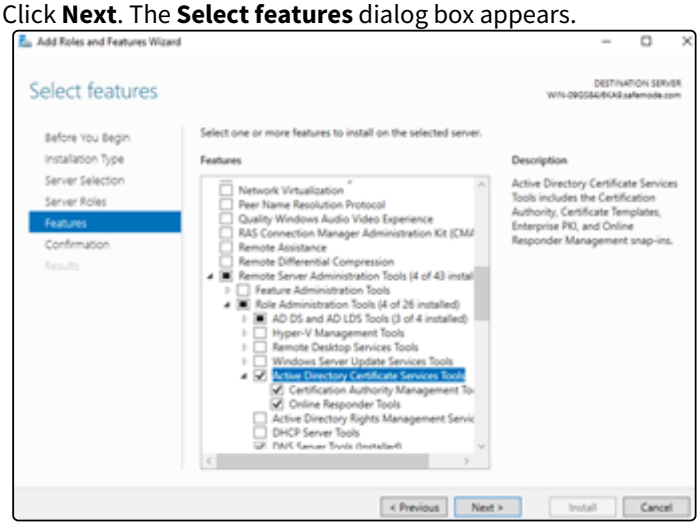
9. Click **Next**.
   The **Select server roles** page appears.



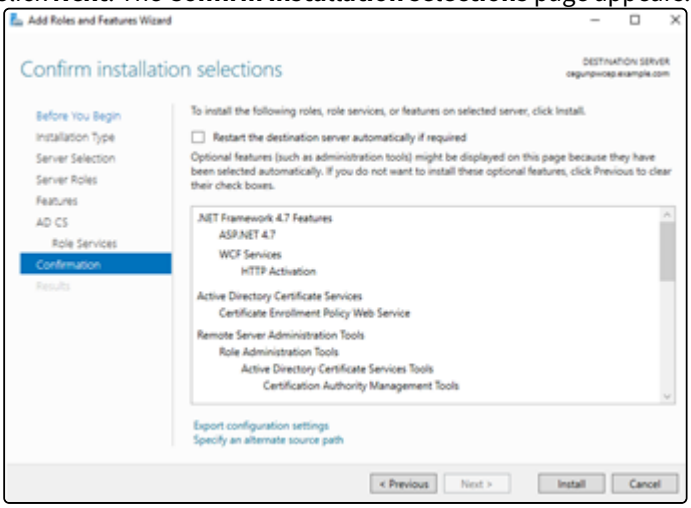
10. Select **Active Directory Certificate Services**.
    Another **Add Roles and Features Wizard** dialog box may appear, informing you that some features are required for Active Directory Certificate Services.



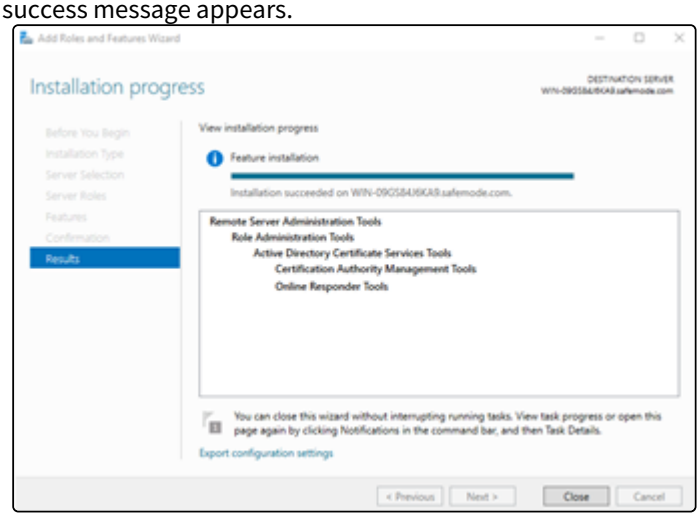
11. Click **Add Features** to add these required features and close the dialog box.
12. Click **Next**. The **Select features** dialog box appears.



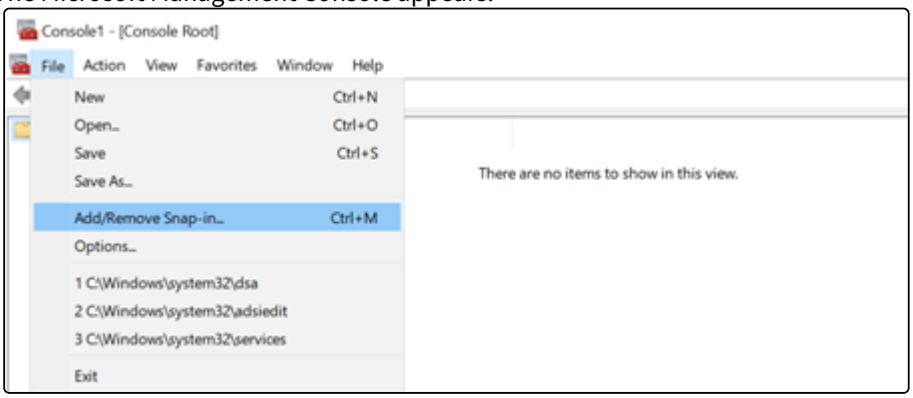
13. Expand **Remote Server Administration Tools > Role Administration Tools, then select Active Directory Certificate Services Tools**.
14. Click **Next**. The **Confirm installation selections** page appears.



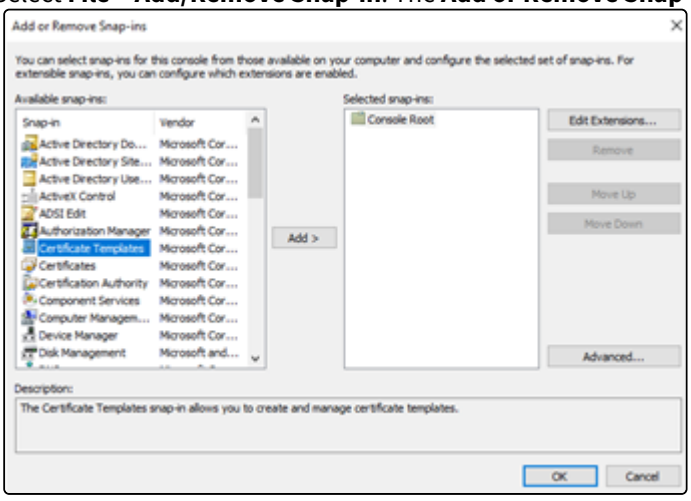
15. Click **Install**. The **Installation Progress** page appears.
    A progress indicator displays the progress of the installation. After the roles and features are installed, a success message appears.



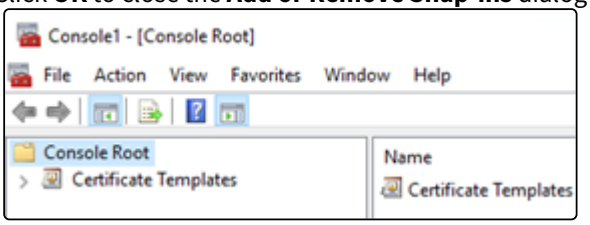
16. Click **Close**.
17. Run `mmc.exe`.
    The Microsoft Management Console appears.



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

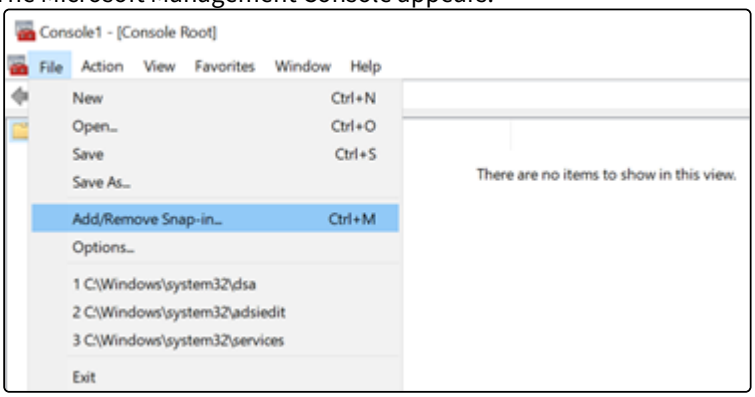
The Entrust WSTEP Service is a component of Certificate Enrollment Gateway. The Entrust WSTEP Service is Certificate Enrollment Gateway's implementation of the WSTEP protocol.

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).

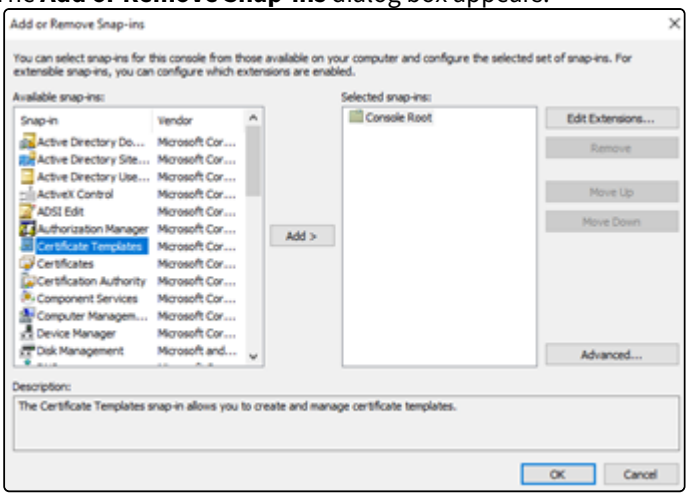
To create a Windows certificate template for WSTEP

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.

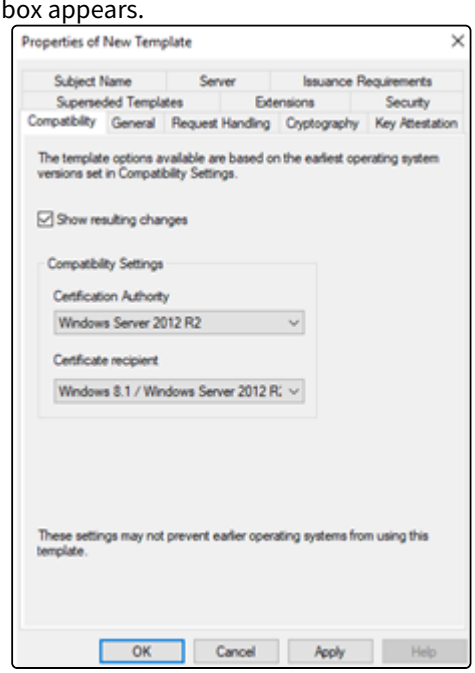


3. Select **File > Add/Remove Snap-in**.
   The **Add or Remove Snap-ins** dialog box appears.



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 If you install a Windows Server 2016 CA, read the following Microsoft troubleshooting guide: Cannot select Windows Server 2016 CA-compatible certificate templates from Windows Server 2016 or later-based CAs or CEP servers.
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 **Template display name** field but without spaces. We recommend using this value. The name must contain only alphanumeric characters (a-z, A-Z, 0-9).
Validity Period	Yes	Any value allowed by the validity policy of the issuing CA.
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 **Domain Users** group to use a copy of the **User certificate** template. If the group is not listed, click **Add** to add the group to the list.
Permissions for Authenticated Users	Set the following **Allow** permissions for the selected group: Read, Enroll, Autoenroll.

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 **RegisteredID** is not supported. The **Subject name** types **Title** and **Initials** 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	For User certificate templates, the following formats are supported: • **Common name**. • **Fully distinguished name**. This value is not supported when Certificate Enrollment Gateway has mapped the Windows certificate template to a Profile ID in CA Gateway. For Computer or Domain Controller certificate templates, the following formats are supported: • **Common name**. • **DNS**. • **Fully distinguished name**. This value is not supported when Certificate Enrollment Gateway has mapped the Windows certificate template to a Profile ID in CA Gateway.
Include e-mail name in subject name	No	
E-mail name	Yes	
DNS name	Yes	
User principal name (UPN)	Yes	
Service principal name (SPN)	Yes	

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 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.

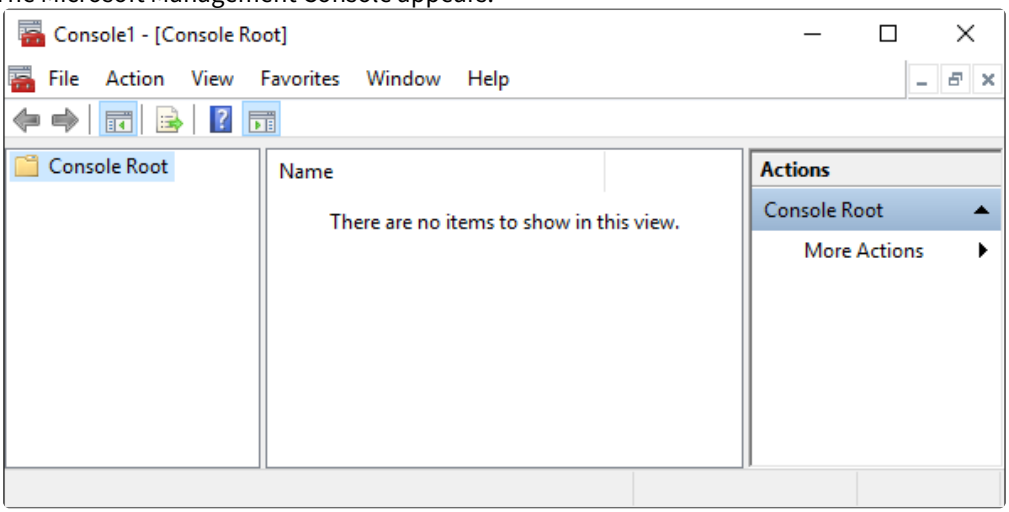
- Creating a CSR for an Active Directory server certificate
- Installing the CA certificate chain for the Active Directory certificate
- Issuing the Active Directory server certificate with Entrust PKI as a Service
- Issuing the Active Directory server certificate with an on-premises CA
- Installing 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

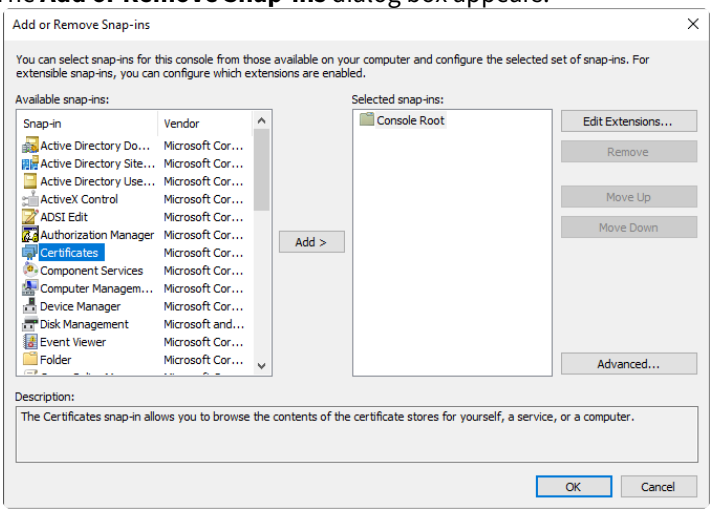
Active Directory requires a server certificate to secure communications to the directory over LDAPS. The following procedure describes how to to create a certificate signing request (CSR) an Active Directory server certificate. A CSR contains information that the issuing CA will use to create the certificate. 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.

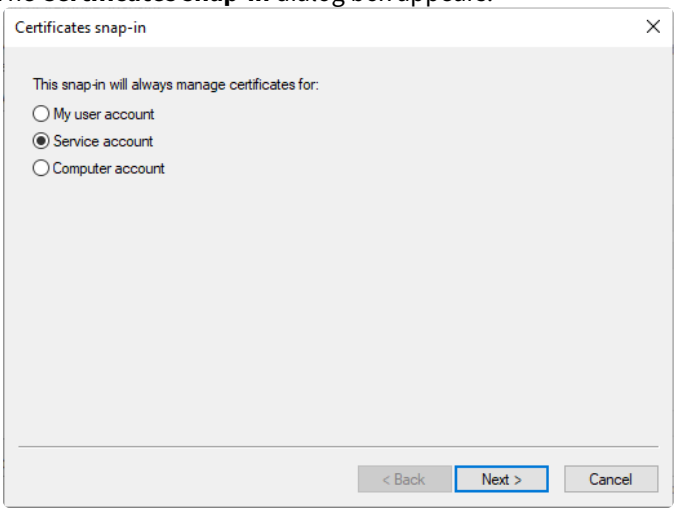


3. Select **File > Add/Remove Snap-in**.
   The **Add or Remove Snap-ins** dialog box appears.

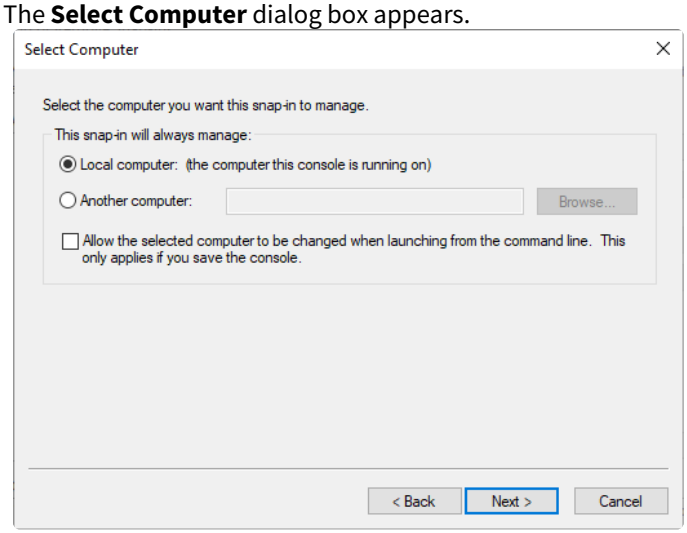


4. In the **Available snap-ins** list, select **Certificates**.

5. Click **Add**.
   The **Certificates snap-in** dialog box appears.

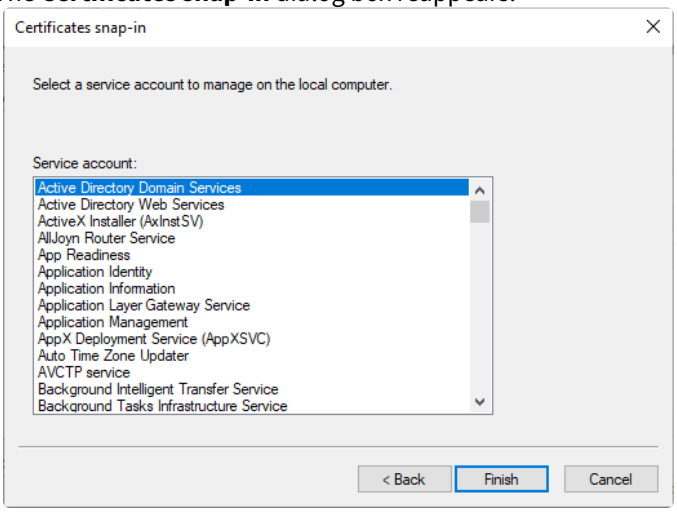


6. Select **Service account**.
7. Click **Next**.
   The **Select Computer** dialog box appears.

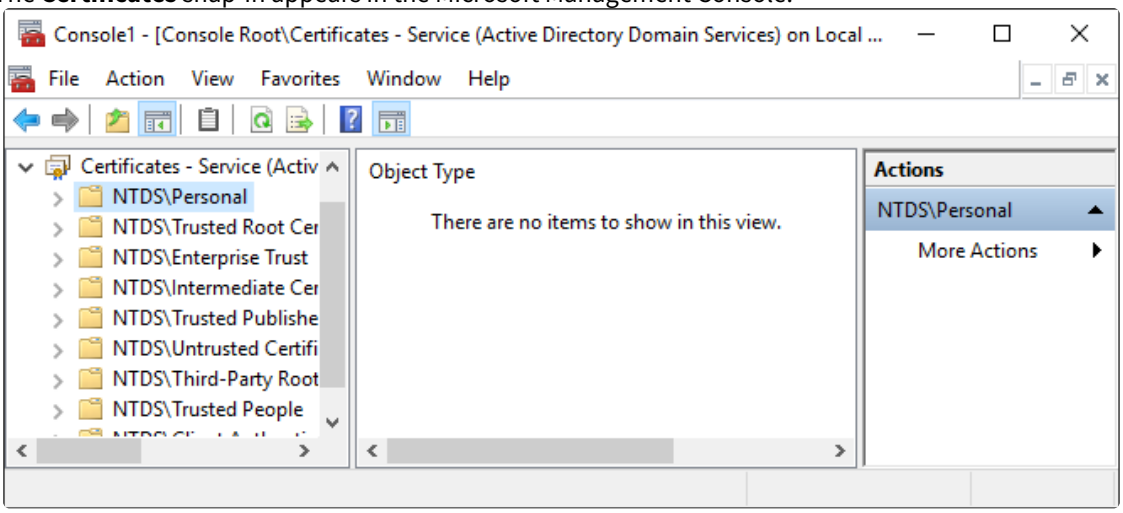


8. Select **Local computer**.

9. Click **Next**.
   The **Certificates snap-in** dialog box reappears.

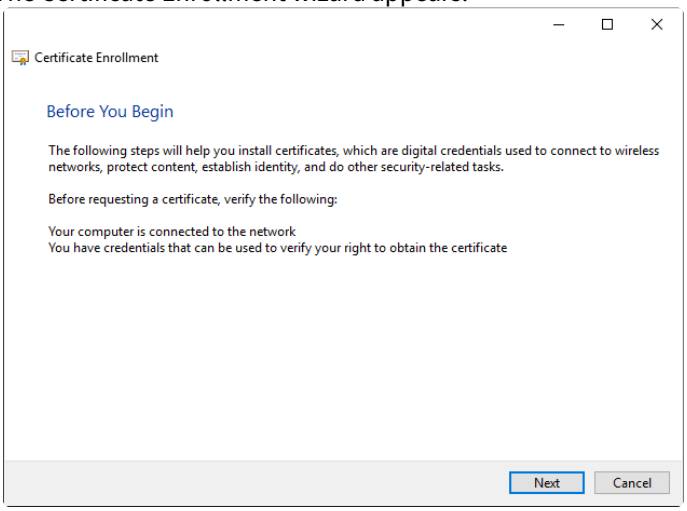


10. Select **Active Directory Domain Services**.
11. Click **Finish**.
    The **Certificates** snap-in as added to the list of Selected snap-ins.
12. Click **OK**.
    The **Certificates** snap-in appears in the Microsoft Management Console.

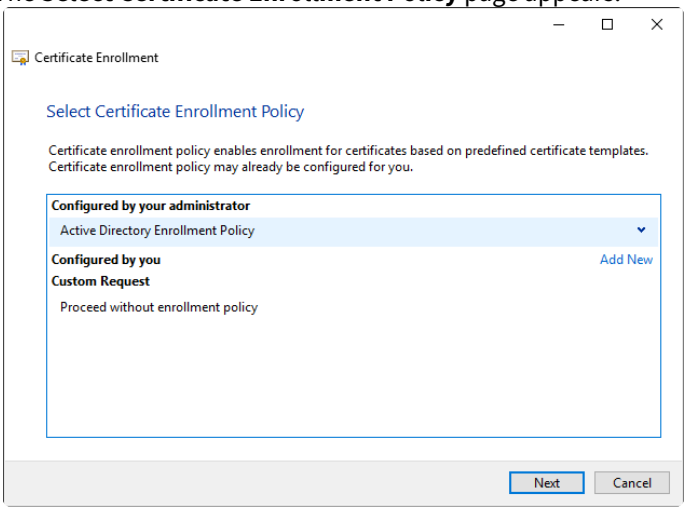


13. In the tree view, select **Certificates** > **NTDS\Personal**.

14. Select **Action** > **All Tasks** > **Advanced Operations** > **Create Custom Request**.
    The Certificate Enrollment wizard appears.

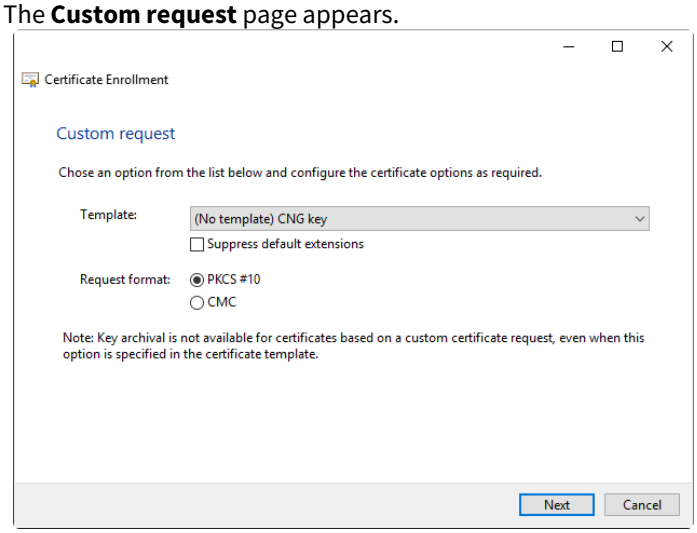


15. Click **Next**.
    The **Select Certificate Enrollment Policy** page appears.

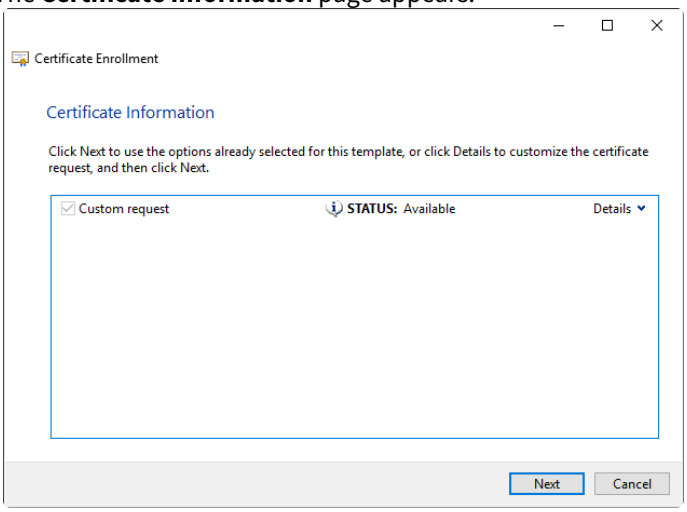


16. Under **Configured by your administrator**, select **Active Directory Enrollment Policy**.

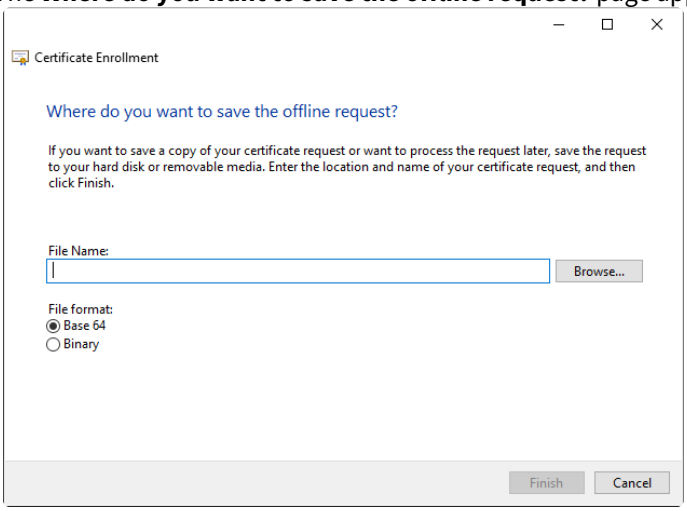
17. Click **Next**.
    The **Custom request** page appears.



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.



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**.

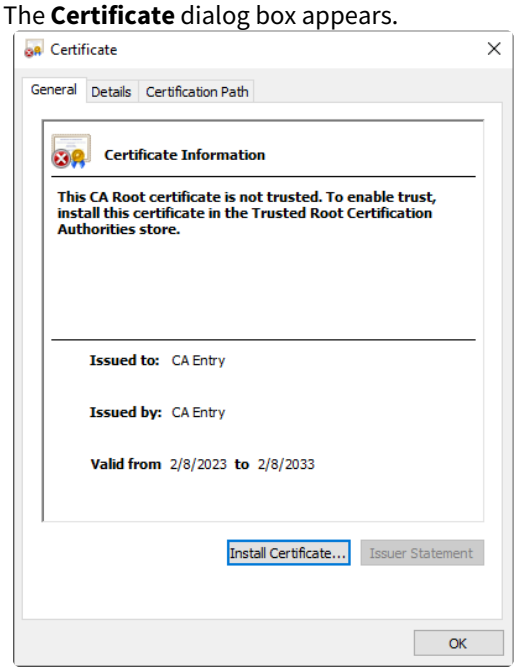
Installing the CA certificate chain for the Active Directory certificate

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.

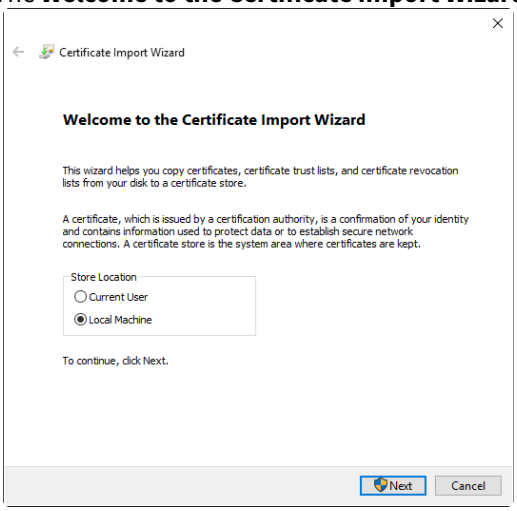
To install a CA certificate into Active Directory

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.

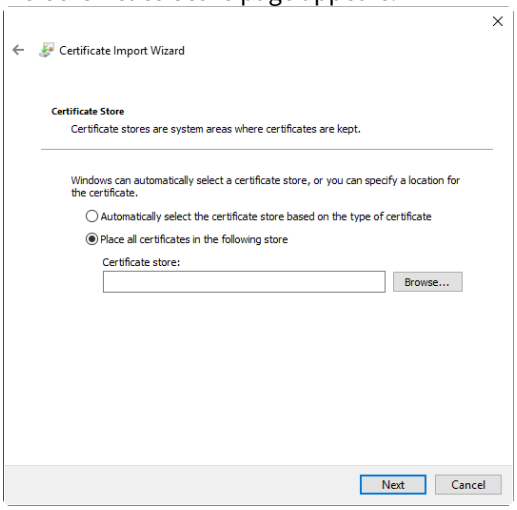


4. Click **Install Certificate**.
   The Certificate Import Wizard appears.
5. The **Welcome to the Certificate Import Wizard** page appears.

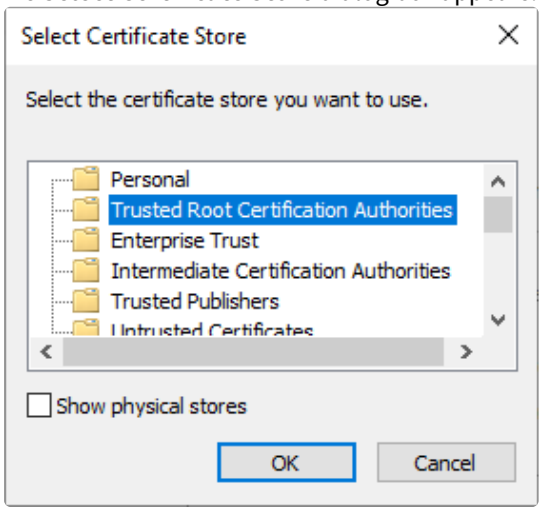


   a. For **Store Location**, select **Local Machine**.
   b. Click **Next**.

6. The **Certificate Store** page appears.

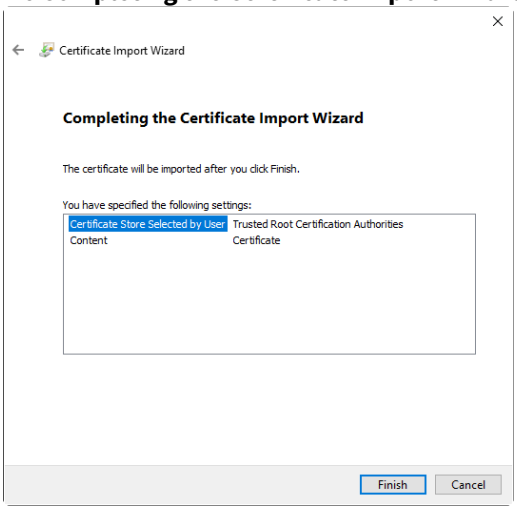


a. Select **Place all certificates in the following store**.
b. Click **Browse**.
The **Select Certificate Store** dialog box appears.



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**.

7. The **Completing the Certificate Import Wizard** page appears.



8. 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

1. Log in the Entrust Certificate Services interface.
2. Select **Create** > **PKIaas**.
   The Select **Certificate Authority** pane appears.
3. From the **Certificate Authority** drop-down list, select the CA you want to issue the TLS certificate.
4. From the **Certificate Profile** drop-down list, select the certificate profile you want to use for the TLS certificate. The certificate profile must include Digital Signature for TLS certificates.
5. Click **Next**.
   The **Certificate Details** pane appears.
6. In the **Subject DN** field, enter a value for the certificate's subject DN. The value should be the DNS name of the domain controller. For example, `cn=activedirectory.example.com`.
7. For **Certificate Expiry**, provide an expiry date for TLS certificate. It is recommended that the TLS certificate be valid for 1 year or less.
8. Under **Subject Alternative Names**, add one or more DNS Name components to the Subject Alternative Name (subjectAltName) extension in the certificate. The subjectAltName extension must have a DNS Name component for each DNS name that may be used by the domain controller.
   To add a DNS Name component the Subject Alternative Name extension:
   a. For **SAN type**, select **DNS Name**.
   b. In the **Value** field, enter a DNS name that may be used by the domain controller.
   c. Click **Add** to add the DNS Name component to the Subject Alternative Name extension.
      The component is added to the list of components in the Subject Alternative Name extension
   d. To remove a component from the Subject Alternative Name extension, click **Remove** next to the extension that you want to remove.
9. Copy the contents of the CSR you generated earlier, and paste the contents into the **Certificate Signing Request (CSR)** text box.
10. Click **Submit**.
    If the certificate is generated successfully, a success message appears.
11. Click **Download the newly created certificate** to download the TLS certificate.

After processing the CSR, proceed to Installing the Active Directory server certificate.

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 1.3.6.1.4.1.311.30.2). 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

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
```

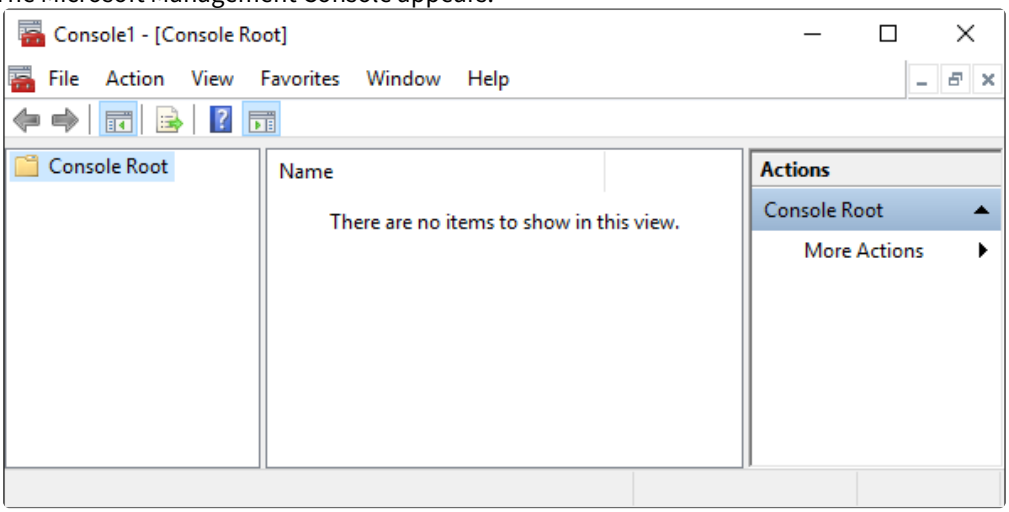
After processing the CSR and obtaining the certificate, proceed to Installing the Active Directory server certificate.

Installing the Active Directory server certificate

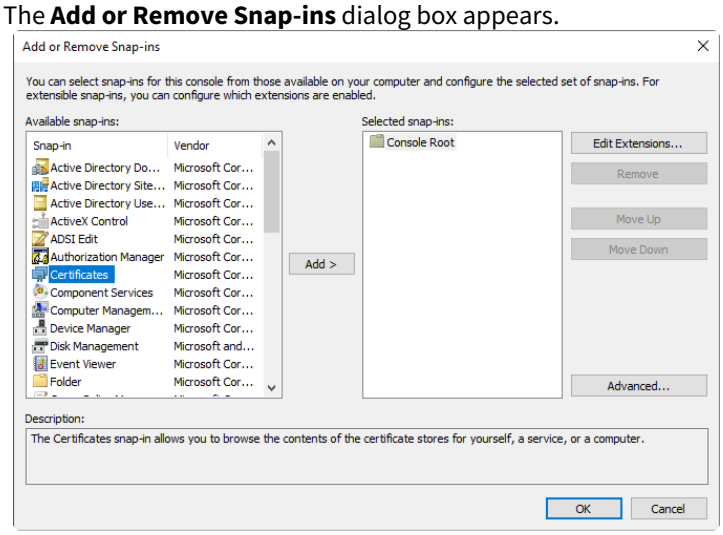
After obtaining the Active Directory server certificate, you must install the certificate into Active Directory. After processing the CSR with Entrust PKI as a Service or an on-premises CA, complete the certificate request to install the certificate into Active Directory. When the certificate is installed, 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.

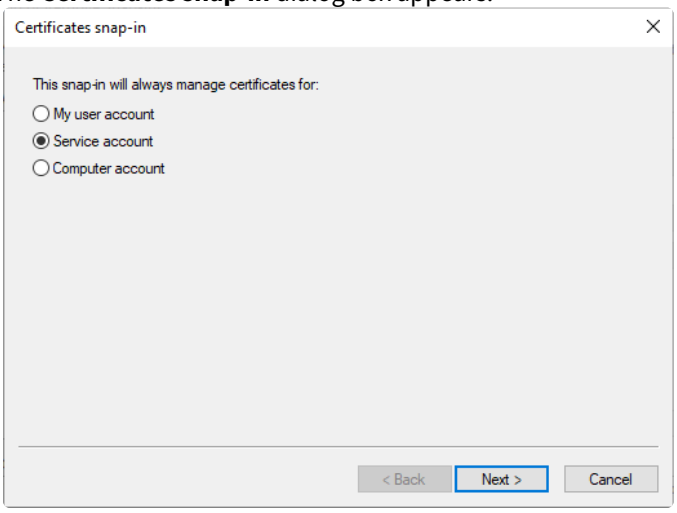


3. Select **File > Add/Remove Snap-in**.
   The **Add or Remove Snap-ins** dialog box appears.

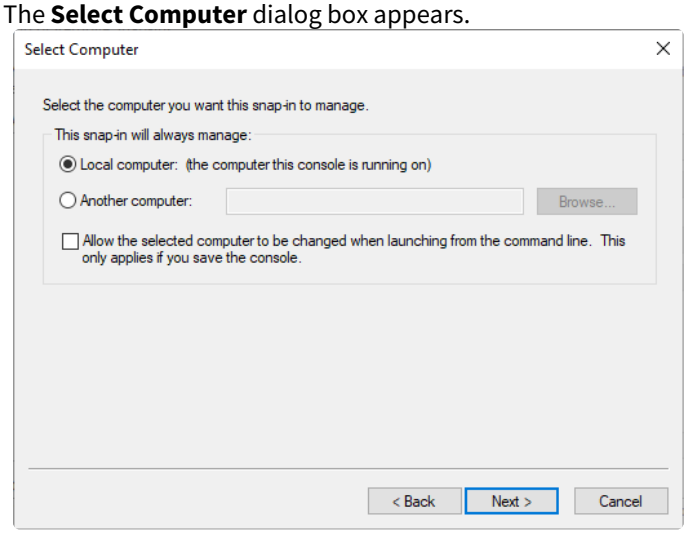


4. In the **Available snap-ins** list, select **Certificates**.

5. Click **Add**.
   The **Certificates snap-in** dialog box appears.

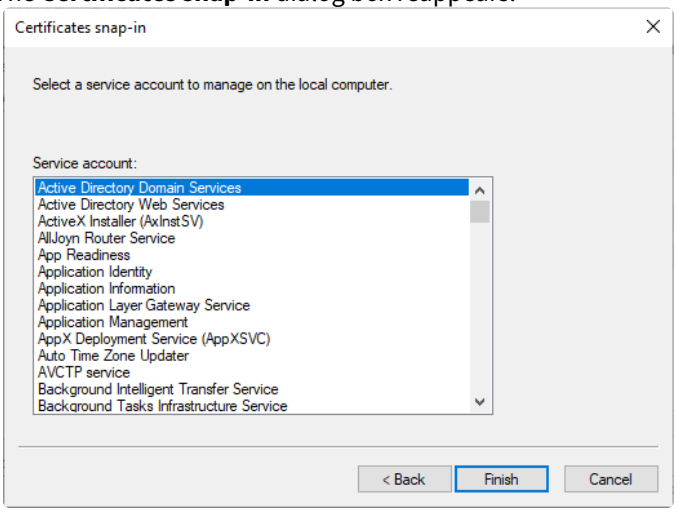


6. Select **Service account**.
7. Click **Next**.
   The **Select Computer** dialog box appears.

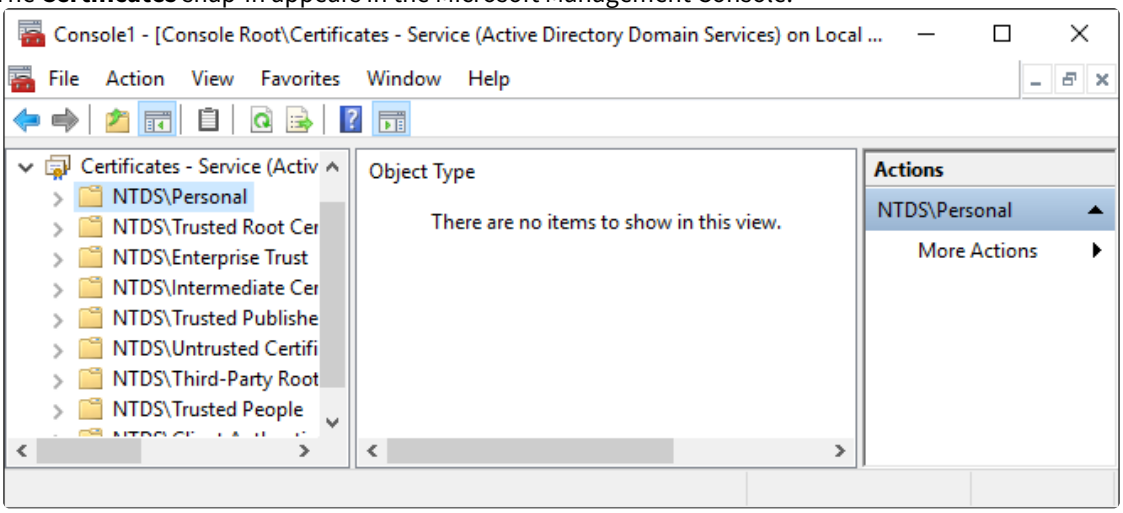


8. Select **Local computer**.

9. Click **Next**.
   The **Certificates snap-in** dialog box reappears.

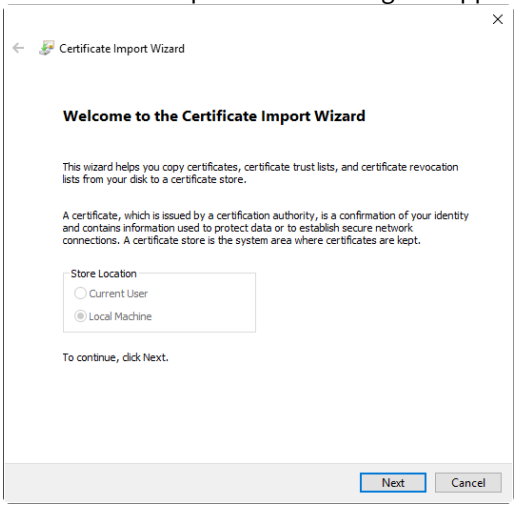


10. Select **Active Directory Domain Services**.
11. Click **Finish**.
    The **Certificates** snap-in as added to the list of Selected snap-ins.
12. Click **OK**.
    The **Certificates** snap-in appears in the Microsoft Management Console.

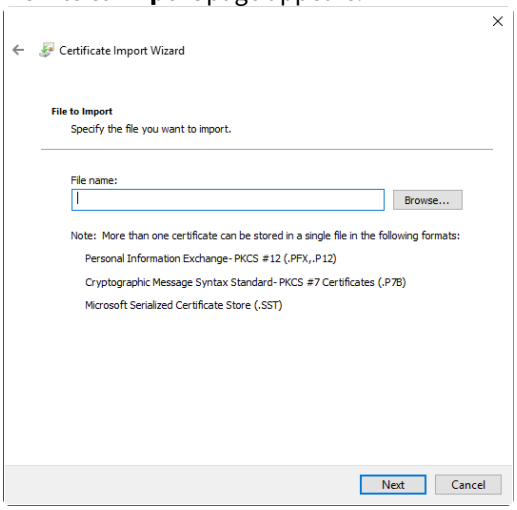


13. In the tree view, select **Certificates** > **NTDS\Personal**.

14. Select **Action** > **All Tasks** > **Import**.
    The Certificate Import Wizard dialog box appears.

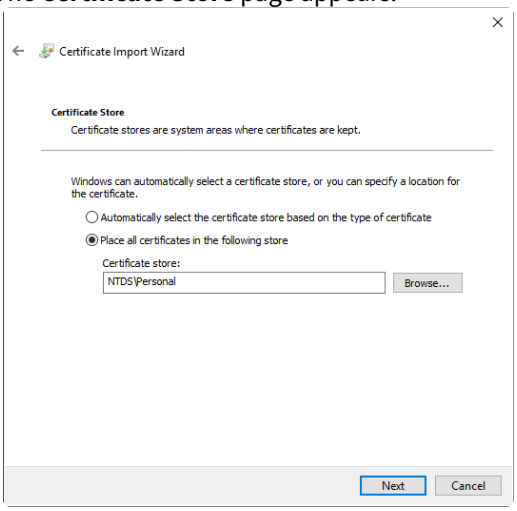


15. Click **Next**.
    The **File to Import** page appears.

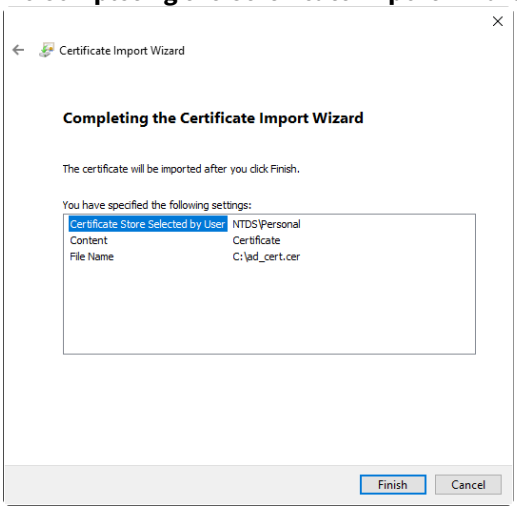


16. Click **Browse** and then select the Active Directory server certificate.

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). 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----
MIIDejCCAmKgAwIBAgIQQ8e7ock59Y21Mtcy7rGJUDANBgkqhkiG9w0BAQs...
-----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.

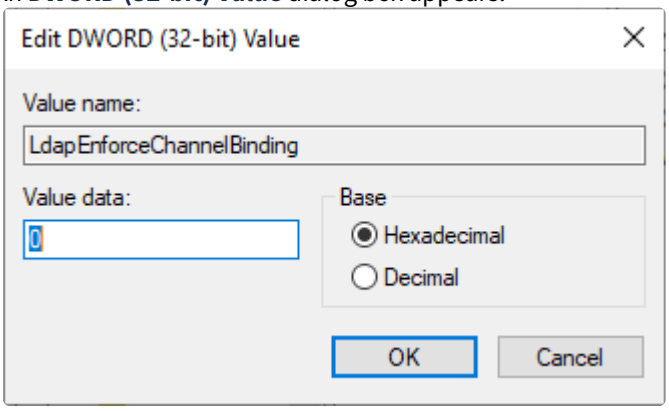
To configure channel binding enforcement to Active Directory

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>:8443/management-console
   ```

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

   ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

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

   ℹ See Managing identities 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

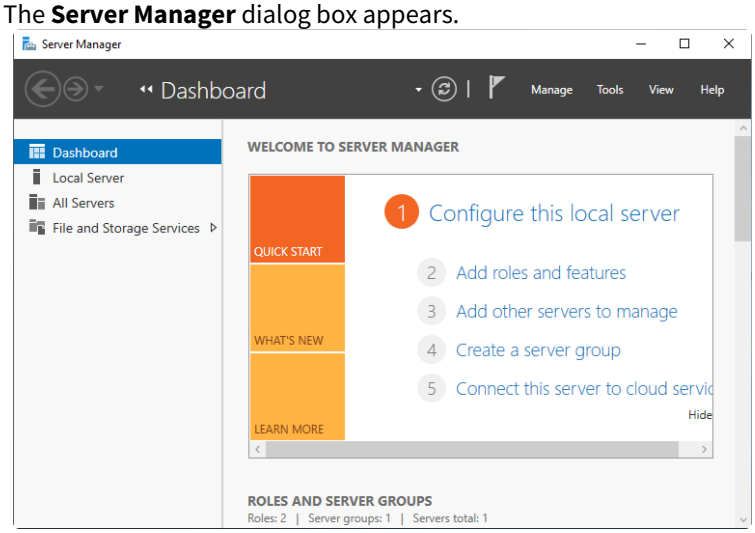
Installing Microsoft Internet Information Services

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.

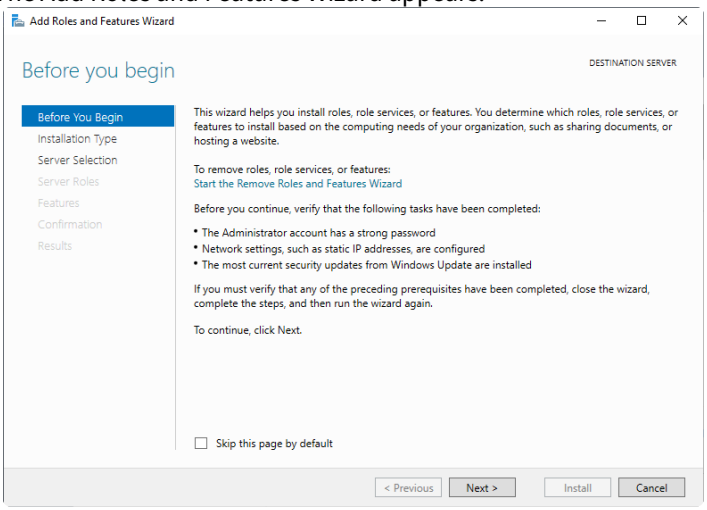
To install Microsoft Internet Information Services

1. Log in to the server that will host the Certificate Enrollment Policy Web Service.

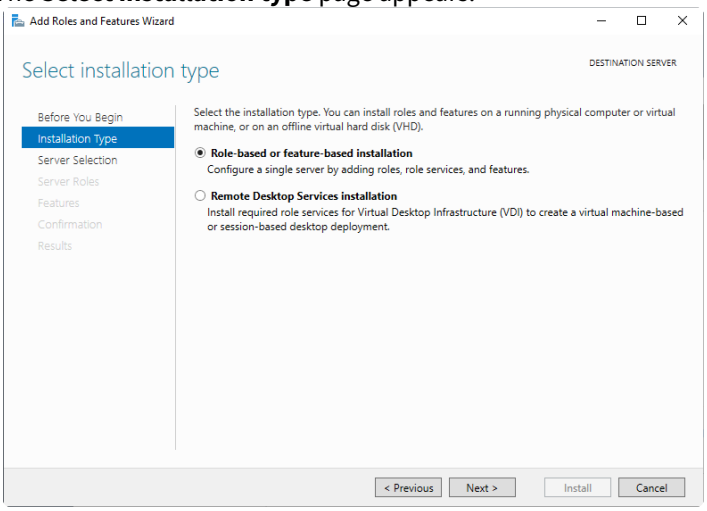
2. Open Server Manager. Select **Start** > **Server Manager**.
   The **Server Manager** dialog box appears.



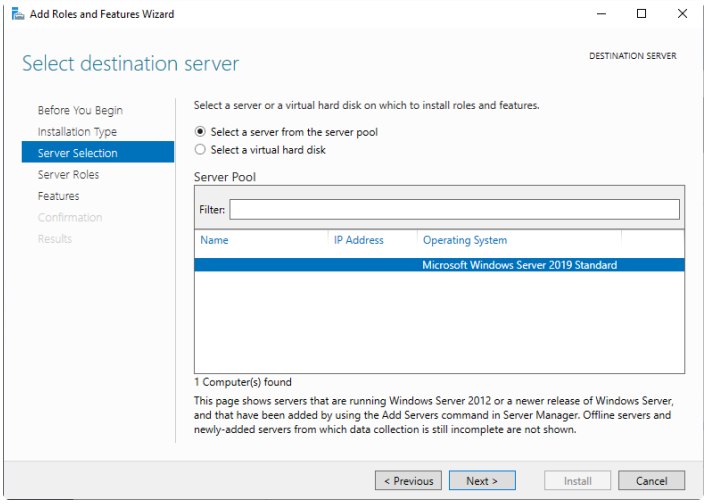
3. In the top navigation bar, select **Manage** > **Add Roles and Features**.
   The Add Roles and Features Wizard appears.



4. Click **Next**.
   The **Select installation type** page appears.

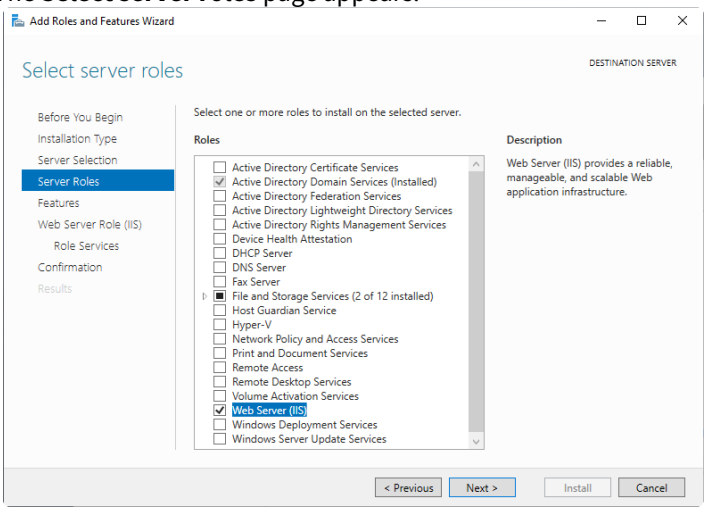


5. Click **Role-based or feature-based installation**. By default, this option is already selected.
6. Click **Next**.
   The **Select destination server** page appears.

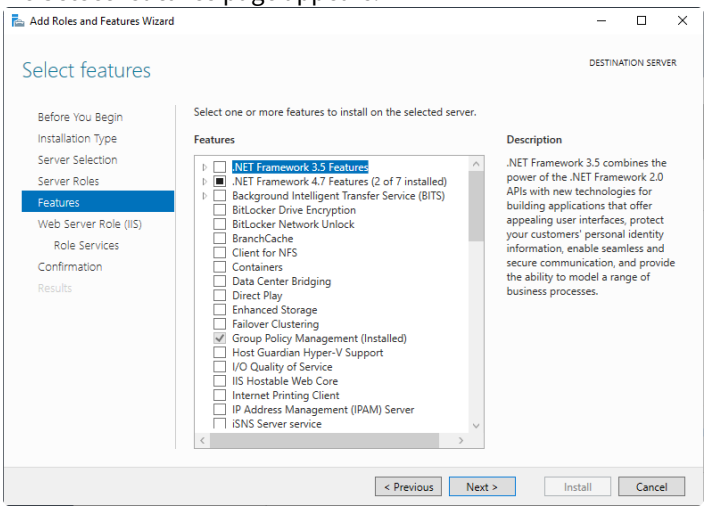


7. Click **Select a server from the server pool**. By default, this option should already be selected.
8. In the **Server Pool** list, select your server. By default, the server should already be selected.

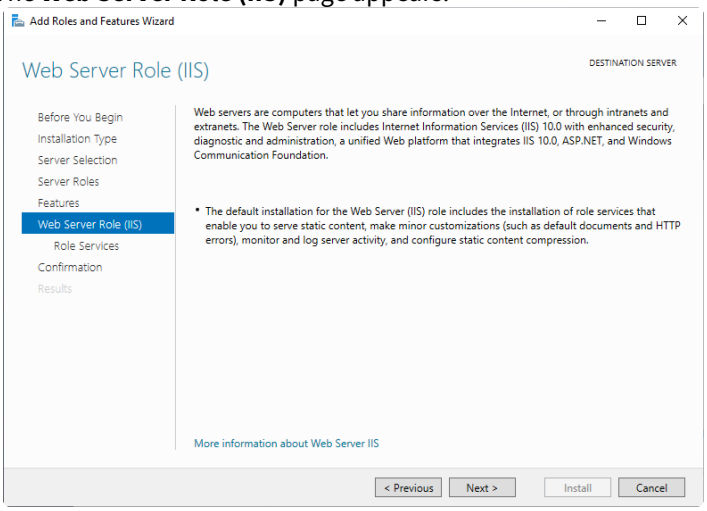
9. Click **Next**.
   The **Select server roles** page appears.



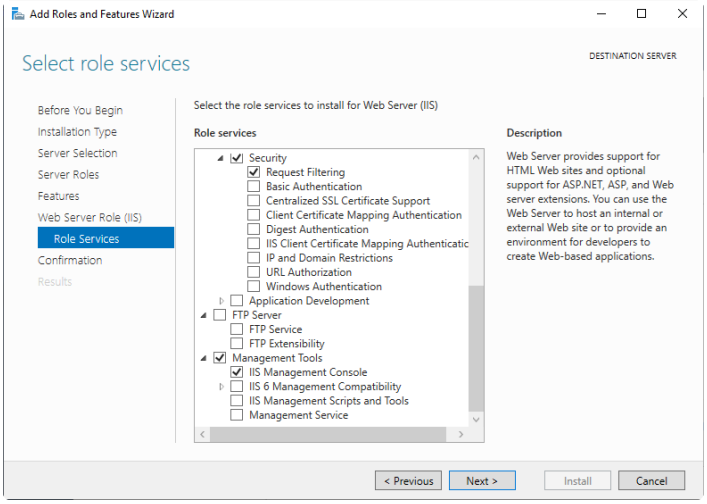
10. Select **Web Server (IIS)**.
11. A dialog box may appear, informing you that some features are required for Microsoft IIS. Click **Add Features** to add these required features and close the dialog box.
12. Click **Next**.
    The **Select features** page appears.



13. You do not need to add any features on this page. Click **Next**.
    The **Web Server Role (IIS)** page appears.

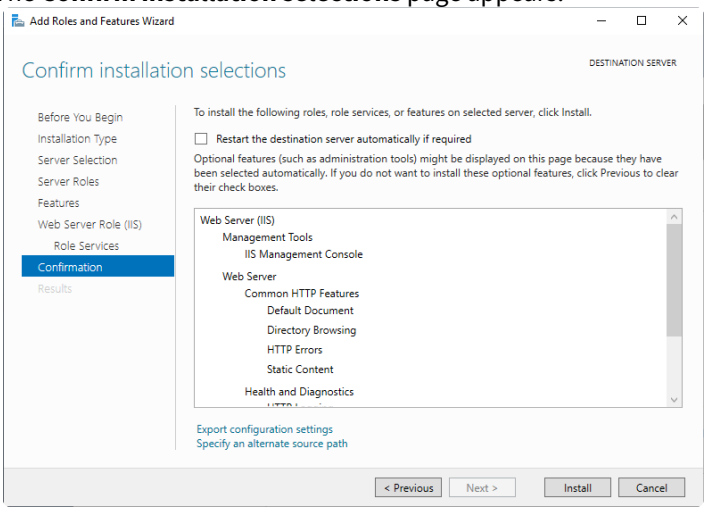


14. Click **Next**.
    The **Select role services** page appears.

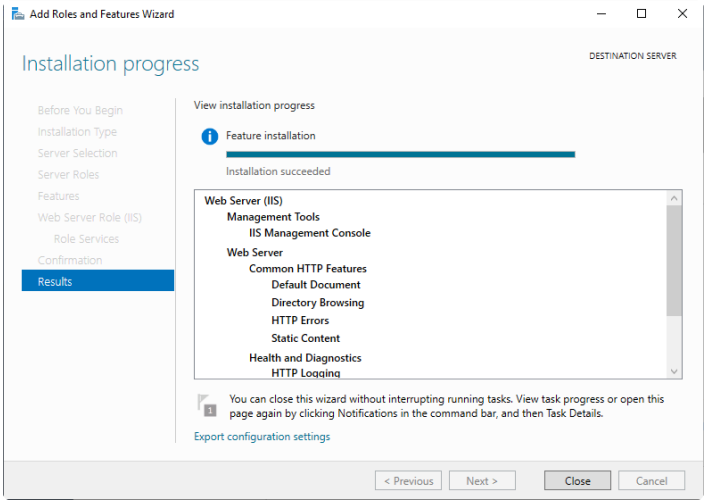


15. Under **Management Tools**, verify that **IIS Management Console** is selected.

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

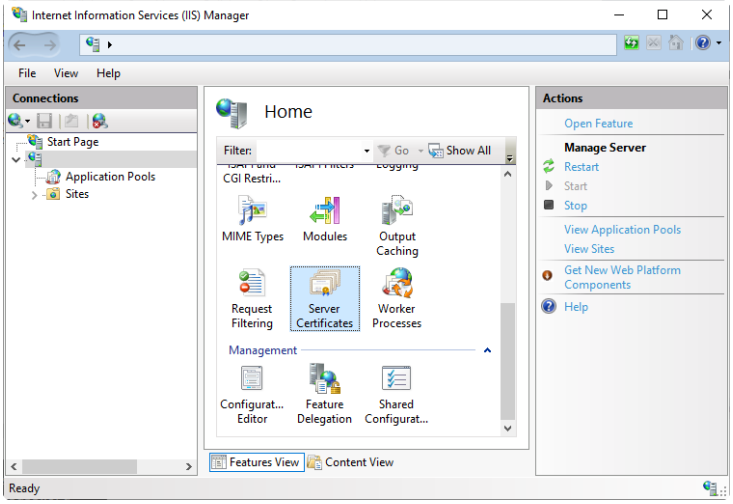
Creating a CSR for the Web server certificate

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.

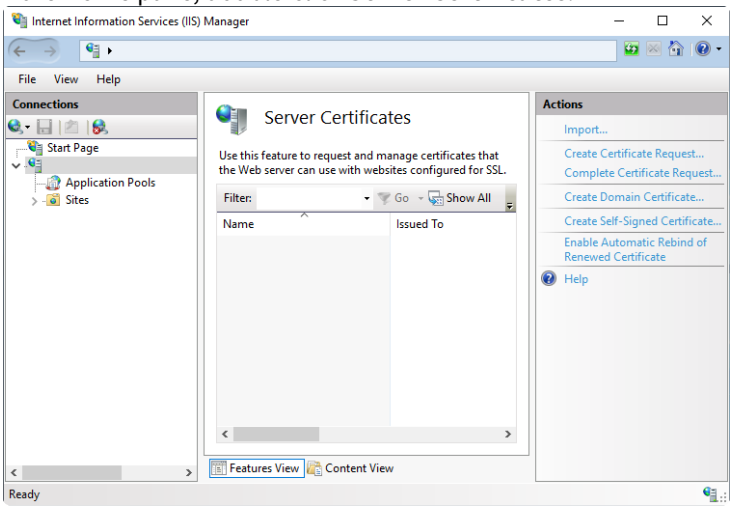
The following procedure describes how to to create a certificate signing request (CSR) in Microsoft IIS for a certificate. A CSR contains information that the issuing CA will use to create the certificate. Entrust PKI as a Service or an on-premises CA can process the CSR and issue the certificate.

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.

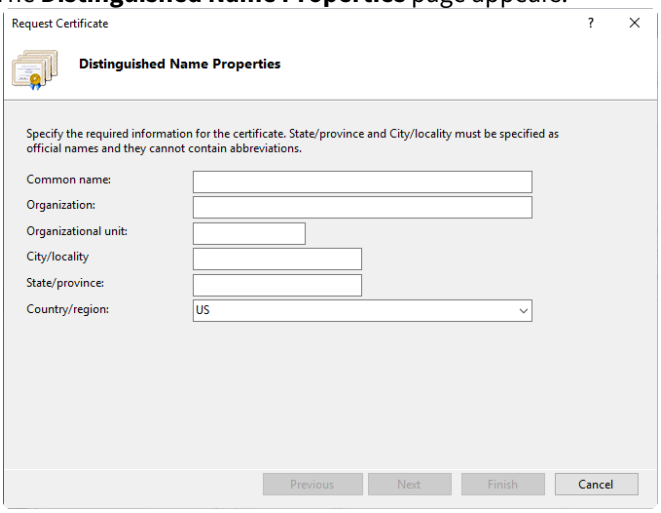


2. Under **Connections**, select the host name of the server.
3. In the **Home** pane, double-click **Server Certificates**.



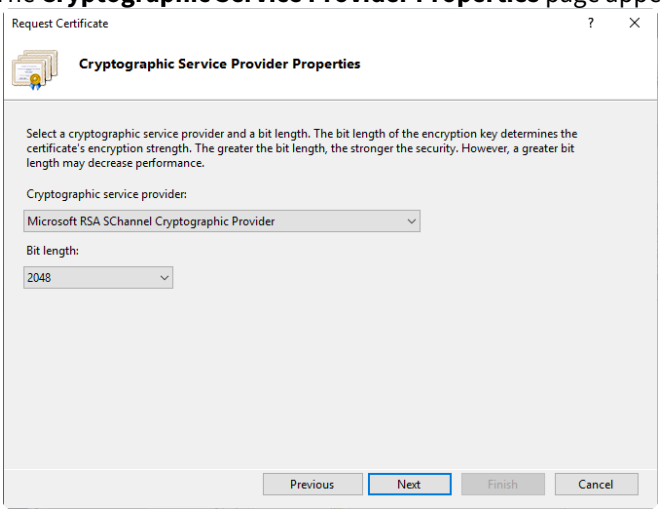
4. In the **Actions** pane, click **Create Certificate Request**.
   The **Request Certificate** wizard appears.

5. The **Distinguished Name Properties** page appears.



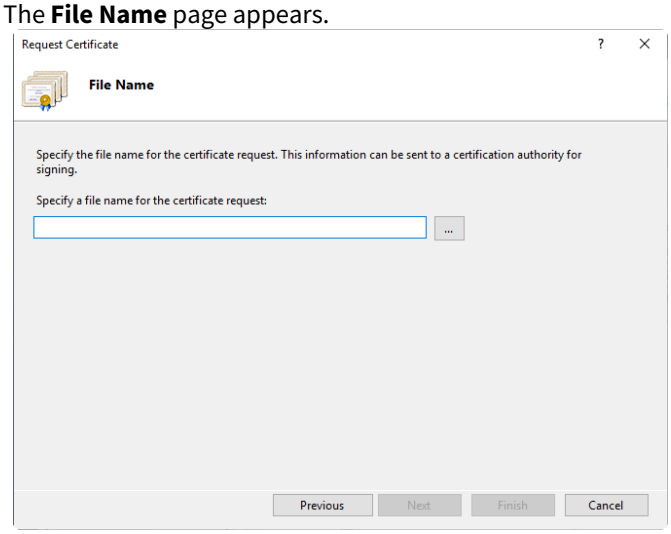
   a. In the provided fields, enter information that will be included in the CSR. Note that the issuing CA (either a CA in Entrust PKI as a Service, or an on-premises Entrust CA) will ignore this information.
   b. Click **Next**.

6. The **Cryptographic Service Provider Properties** page appears.



   a. From the **Cryptographic service provider** drop-down list, select a cryptographic service provider. It is recommended that you select **Microsoft RSA SChannel Cryptographic Provider**.
   b. In the **Bit length** list, select a bit length. It is recommended that you select 2048 as the bit length.
   c. 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 theEntrust Certificate Authority user being issued the certificate.
   - Under the **Users** permission category: **View** and **Perform PKIX** requests. Obtain the Entrust desktop profile (EPF file) from an Entrust Certificate Authority administrator.
3. Navigate to the directory containing the Profile Creation Utility.
4. Run the following command:

- On Windows, run `pcu.bat`.
- On Linux, run `pcu`.

5. The Profile Creation Utility main menu appears:

```
Main Menu
1. Exit
2. Help
3. Create Entrust profile
4. Recover Entrust profile
5. Inspect Entrust profile (read only)
6. Inspect and update Entrust profile (read/write)
7. Create Server Login credentials
8. Create PKCS #12 file (Entrust Certificate Authority)
9. Recover PKCS #12 file (Entrust Certificate Authority)
10. Create PKCS #12 file (3rdParty)
11. Update PKCS #12 file (3rdParty)
12. Process PKCS #10 Certificate Signing Request (CSR)
13. Generate/Process Certificate Signing Request on HSM (3rdParty)
14. Change password
Select an operation [3]:
```

> To return to the main menu at any time, enter a period (.). For help about using the Profile Creating Utility, enter 2 in the main menu.

Enter 12 to process the CSR.

6. The following prompt appears:

```
Take settings from an existing entrust.ini file (y/n) [y]:
```

- To use Certificate Authority (CA) connection settings from an existing `entrust.ini` file, enter `y`.
- To provide CA connection settings manually, enter `n`.

7. If you chose to use an existing `entrust.ini` file, you are prompted to enter the full path to the `entrust.ini` file:

```
Enter full path to entrust.ini file:
```

Enter the full path and file name of the `entrust.ini` file.

8. If you chose to enter CA connections setting manually, the following prompts appear:
   a. You are prompted to provide the host name (or IP address) and port of the CA server:

```
Enter the CA hostname or IP address and port in the form name:port:
```

   Enter the host name (or IPv4 address) and CMP port of the server hosting the CA in format of `<hostname>:<port>`. If you omit the port number, it defaults to 829.
   b. You are prompted to provide the host name (or IP address) and port of the directory server:

```
Enter the directory hostname or IP address and port in the form name:port:
```

Enter the host name (or IPv4 address) and LDAP port of the server hosting the directory in format of `<hostname>:<port>`. The name or address defaults to the same value that you entered for the CA address If you omit the port number, it defaults to 389.

9. You are prompted for the full path to an administration profile:

```
Enter full path to administration profile:
```

Enter the full path and file name of an administration profile.

10. You are prompted to enter the profile password:

```
Enter profile password:
```

Enter the profile password.

11. You are asked if the CSR is authenticated:

```
Is the CSR authenticated? (y/n)? [n]:
```

Enter `n`. The CSR is not authenticated.

12. You are prompted for the full path to the CSR:

```
Enter full path to CSR:
```

Enter the full path and file name of the CSR.

13. You are prompted to enter the reference number for the CSR:

```
Enter reference number:
```

Enter the reference number you recorded earlier.

14. You are prompted to enter the authorization code for the CSR:

```
Enter authorization code:
```

Enter the authorization code you recorded earlier.

15. You are prompted to enter a file name for the certificate:

```
Enter certificate file to create:
```

Enter the full path and file name for the certificate file.

16. You are prompted to enter the certificate definition required for the certificate:

```
Enter certificate definition required [Verification]:
```

Enter the certificate definition required for the certificate, such as Verification or Dual Usage.

17. The Profile Creation Utility processes the certificate. If the operation is successful,Entrust Certificate Authority issues a certificate and the Profile Creation Utility writes the certificate to a file.

```
Requesting certificate fromEntrust Certificate Authority...
Obtained new certificate with serial number 1340207625 from issuer
o=Example,c=US
Certificate written to c:\new_certificate.cer
```

18. After processing the CSR and obtaining the certificate, proceed to Installing the Web server certificate into Microsoft IIS.

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.

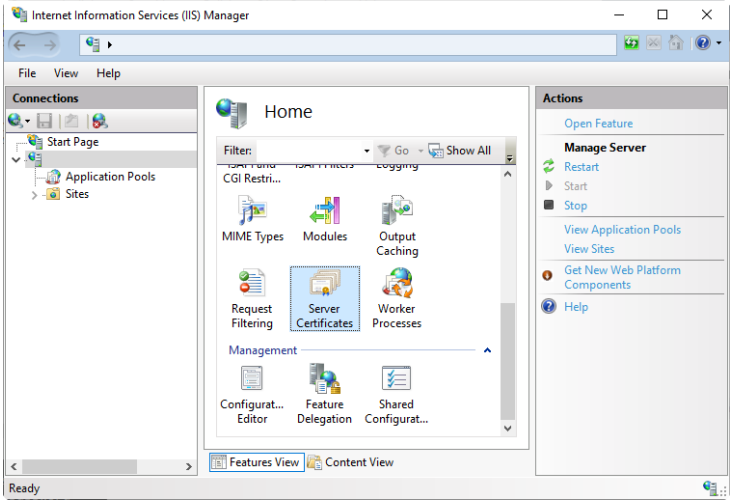
Installing the Web server certificate into Microsoft IIS

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.

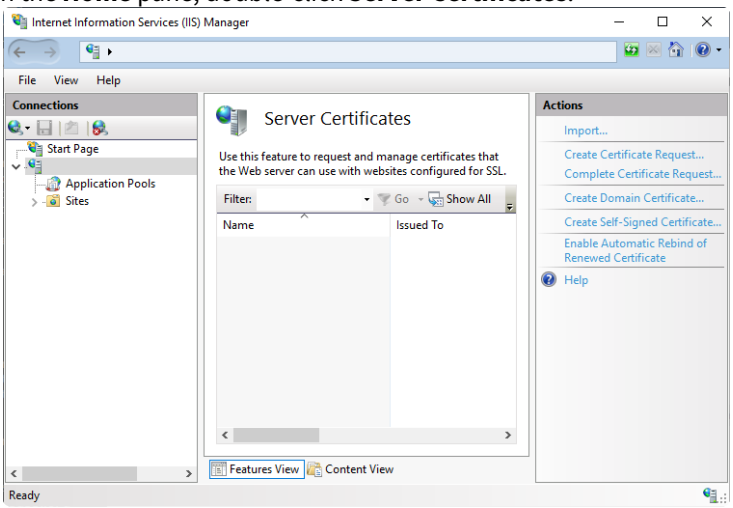
If you will use the Entrust-provided PowerShell scripts to install and configure the Certificate Enrollment Policy Web Service, keep the certificate file after installing the certificate into Microsoft IIS. The PowerShell script will prompt you to select an existing certificate or supply a new certificate for the Certificate Enrollment Policy Web Service. If the PowerShell script cannot find the certificate you install into Microsoft IIS, you must supply the certificate.

To complete a certificate request in Microsoft IIS

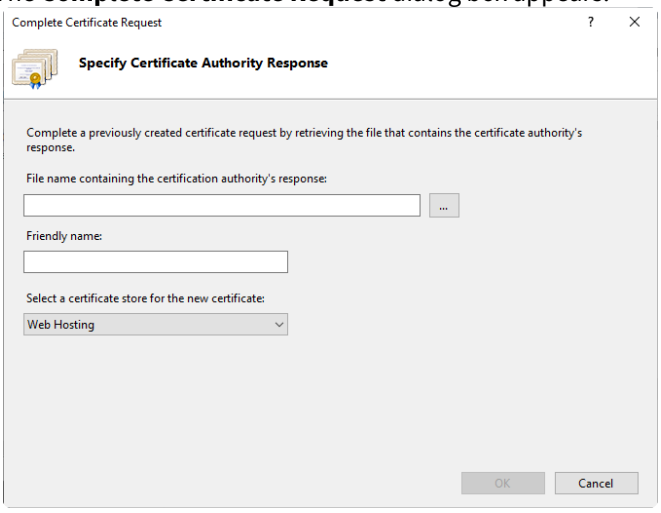
1. Open the Internet Information Services (IIS) Manager. Select **Start** > **Windows Administrative Applications** > **Internet Information Services (IIS) Manager**.
   The **Internet Information Services (IIS) Manager** dialog box appears.



2. Under **Connections**, select the host name of the server.
3. In the **Home** pane, double-click **Server Certificates**.



4. In the **Actions** pane, click **Complete Certificate Request**.
   The **Complete Certificate Request** dialog box appears.



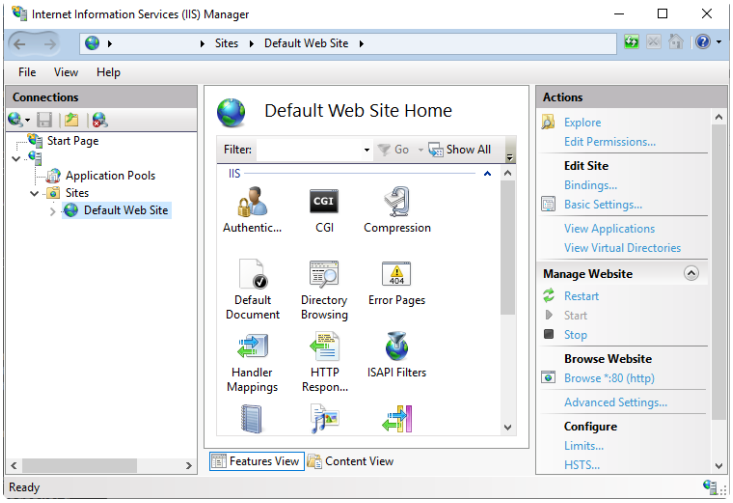
5. In the **File name containing the certification authority response** field, enter the full path and file name of the Web server certificate, or click the Browse button to select the certificate.
6. In the **Friendly name** field, enter a friendly name for the certificate. This friendly name will be used to identify the certificate in the IIS Manager interface.
7. From the **Select a certificate store for the new certificate** drop-down list, select **Web Hosting**.
8. Click **OK**.
   In the **Server Certificates** pane, the certificate appears in the list of server certificates. The certificate is listed by its friendly name.

Updating Microsoft IIS to use the Web server certificate

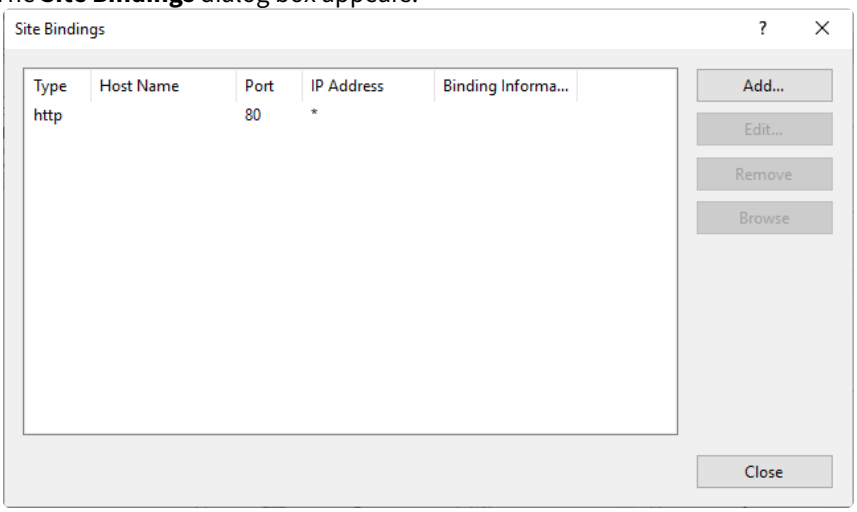
After installing the Web server certificate into Microsoft IIS, you must update the HTTPS site binding for the Web server in Microsoft IIS to use the TLS certificate.

To add an initial HTTPS site binding in Microsoft IIS to use the Web server certificate

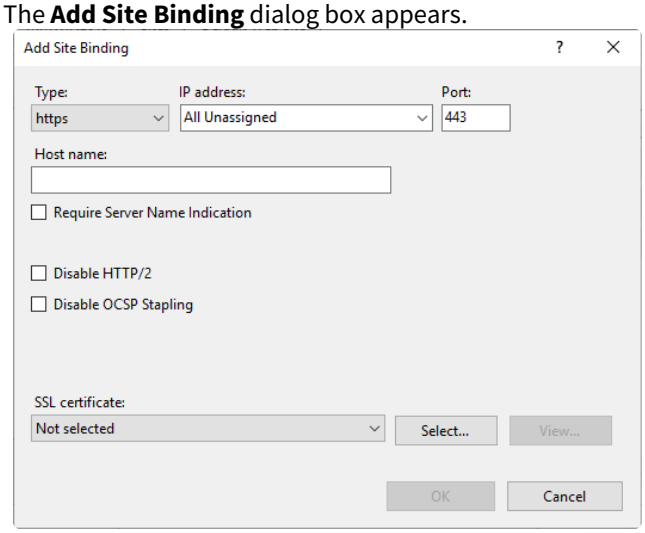
1. Open IIS Manager. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.
   The **Internet Information Services (IIS) Manager** dialog box appears.



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.

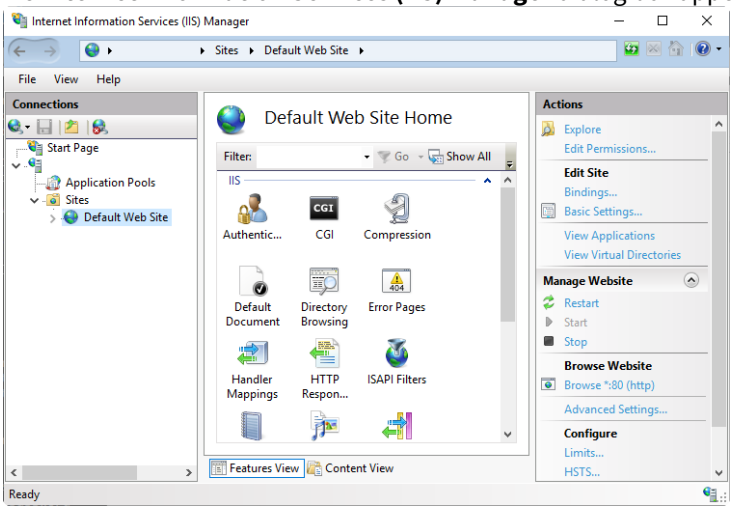


5. In the **Type** drop-down list, select **https**.
6. Keep **IP address** as **All Unassigned**.
7. For **Port**, keep the default 443.
8. From the **SSL certificate** drop-down list, select the Web server certificate you installed into Microsoft IIS earlier.
9. Click **OK**.
   The HTTPS binding is added to the list of site bindings.

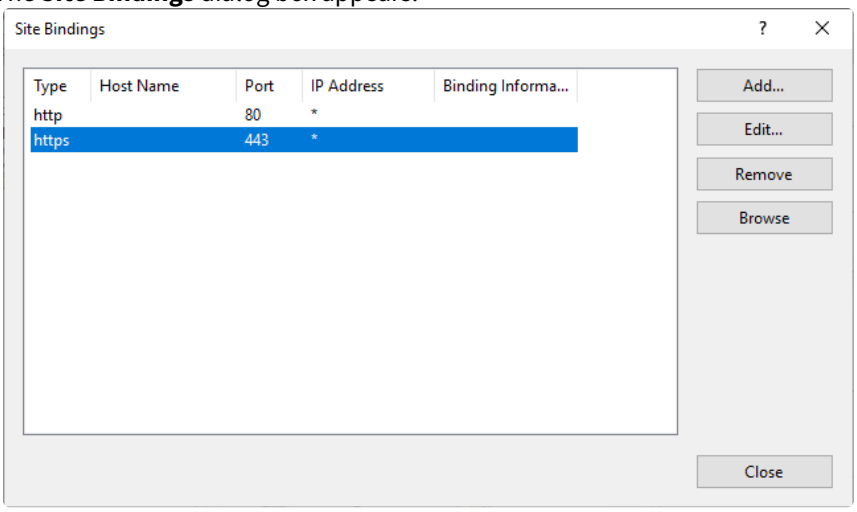
To update an existing HTTPS site binding in Microsoft IIS to use the Web server certificate

1. Open IIS Manager. Select **Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** dialog box appears.

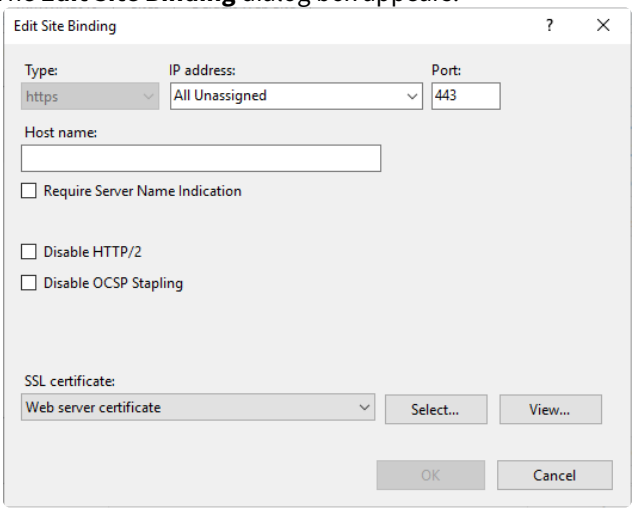


2. In the **Connections** pane, select **Sites > Default Web Site**.
   If the Certificate Enrollment Policy Web Service is installed, it appears as an application under the default Web site.
3. In the **Actions** pane, click **Bindings**.
   The **Site Bindings** dialog box appears.



4. 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**.

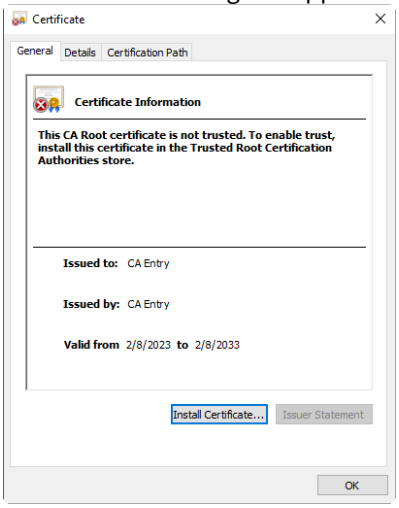
Installing the CA certificate chain for the Web server certificate

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.

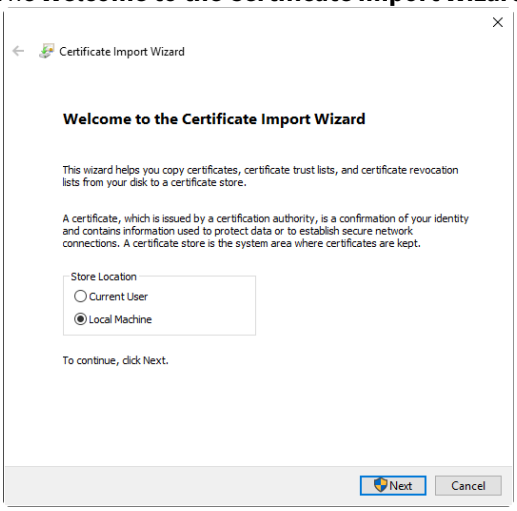
To install a CA certificate into the Web server

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.

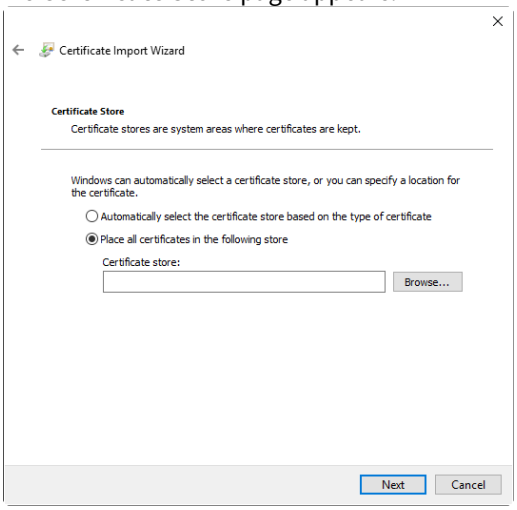


4. Click **Install Certificate**.
   The Certificate Import Wizard appears.
5. The **Welcome to the Certificate Import Wizard** page appears.

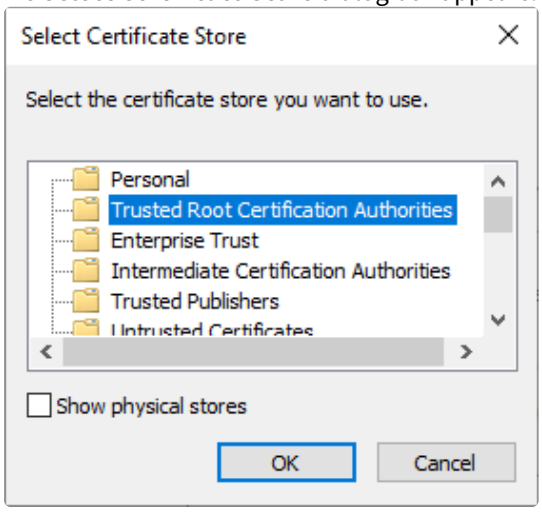


   a. For **Store Location**, select **Local Machine**.
   b. Click **Next**.

6. The **Certificate Store** page appears.

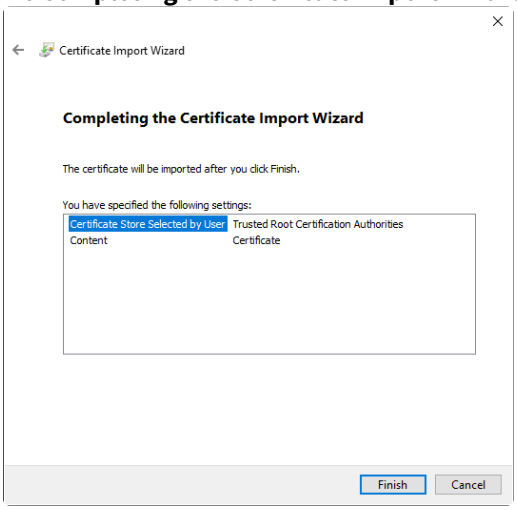


a. Select **Place all certificates in the following store**.
b. Click **Browse**.
The **Select Certificate Store** dialog box appears.



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:

> The PowerShell script was tested on specific versions of PowerShell. When validating the prerequisites, the PowerShell version my 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=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 : 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=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      :

Certificate Index : 2
-----------------
  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 : 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 : cepusername.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      :



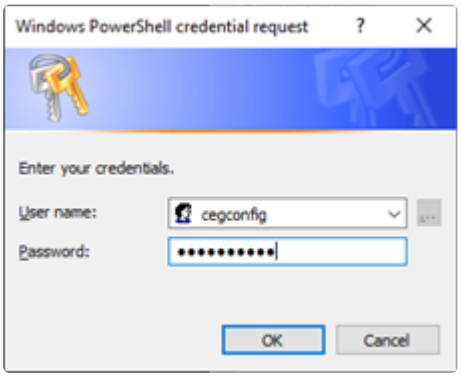
Choose from the following Options:
[S] Select Existing Cert  [N] Supply New Certificate  [C] Continue with
selected Certificate  [E] Exit  [?] Help
(default is "S"):
```

- 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 WSETP.
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 recommend 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

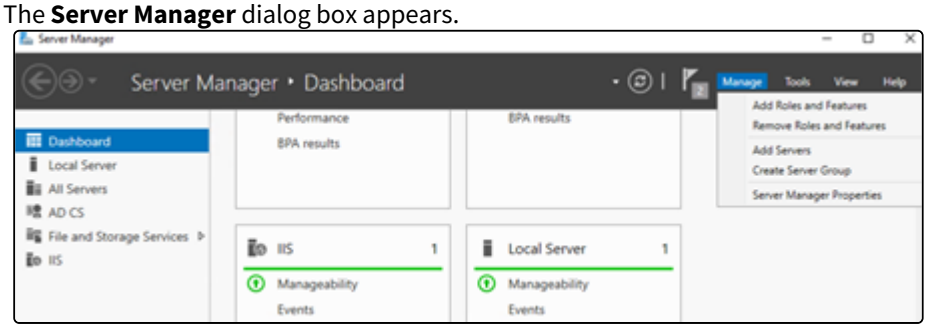
Installing the CEP Web Service using the Windows graphical interface

On a Windows server, install the Certificate Enrollment Policy Web Service.

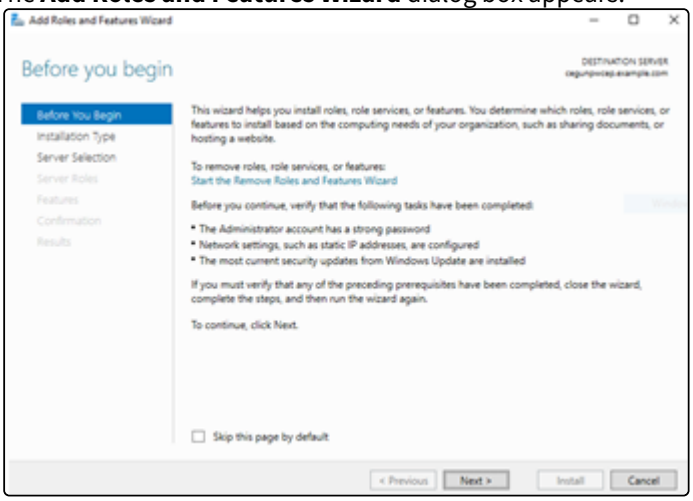
The Windows server hosting the Certificate Enrollment Policy Web Service can be the Active Directory server or any other server in the domain. However, it is recommended that you install and configure the Certificate Enrollment Policy Web Service on a different server than Active Directory.

To install the CEP Web Service using the Windows graphical interface

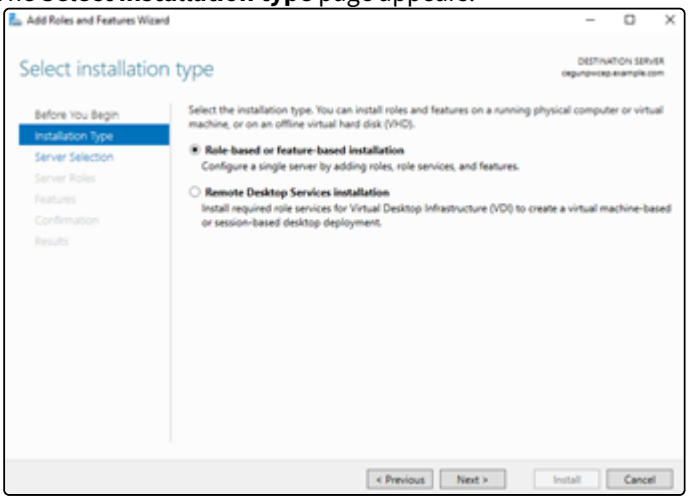
1. Log in to a Windows server hosting Microsoft IIS as a user with Domain Administrator and Enterprise Administrator permissions.
2. Open Server Manager. Select **Start > Server Manager**.
   The **Server Manager** dialog box appears.



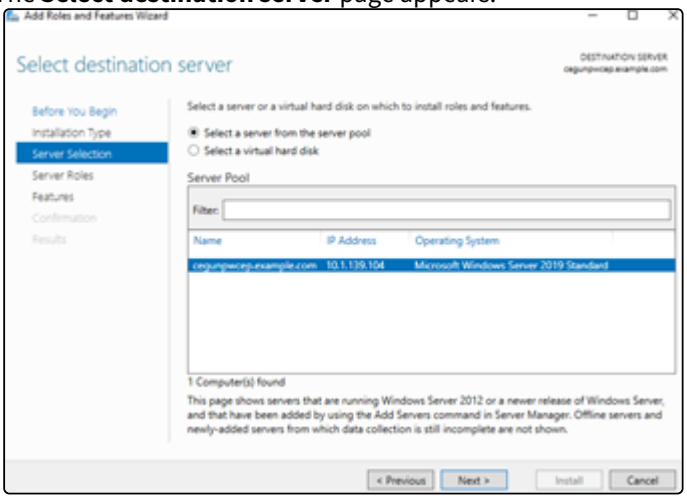
3. Select **Manage > Add Roles and Features**.
   The **Add Roles and Features Wizard** dialog box appears.



4. If the **Before you Begin** page appears, click **Next**.
   The **Select installation type** page appears.

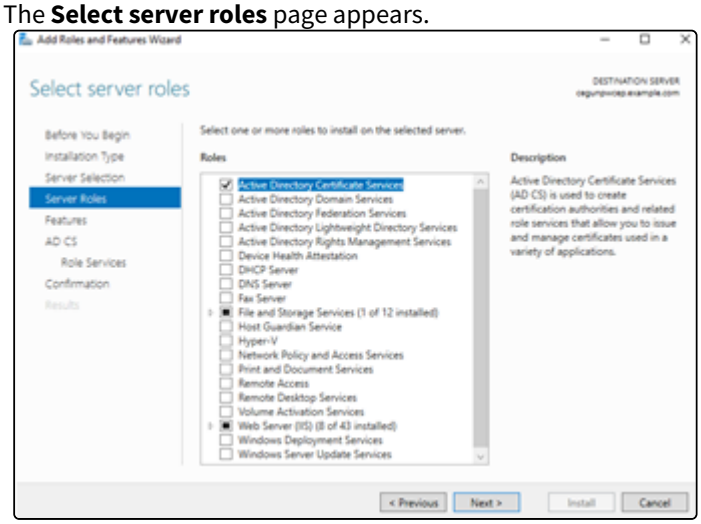


5. Select **Role-based or feature-based installation**.
6. Click **Next**.
   The **Select destination server** page appears.

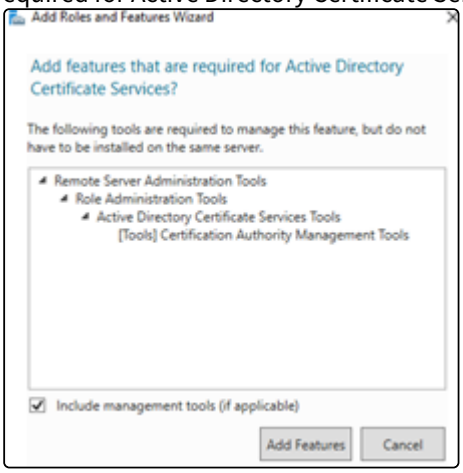


7. Click **Select a server from the pool**.
8. In the **Server Pool** list, select the server.

9. Click **Next**.
   The **Select server roles** page appears.

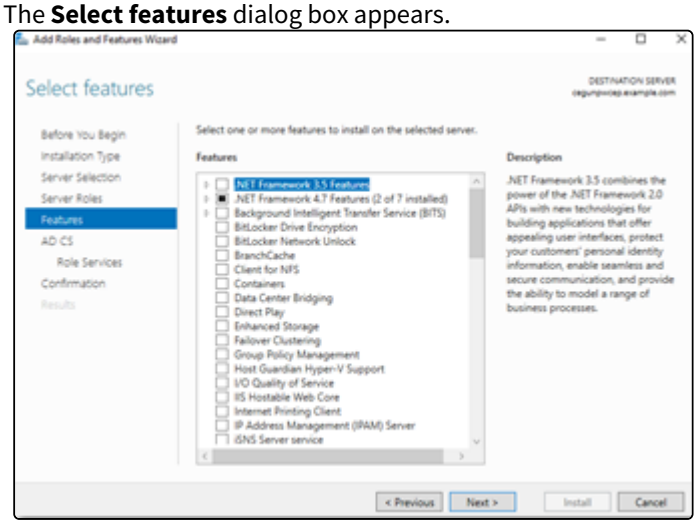


10. Select **Active Directory Certificate Services**.
    Another **Add Roles and Features Wizard** dialog box may appear, informing you that some features are required for Active Directory Certificate Services.

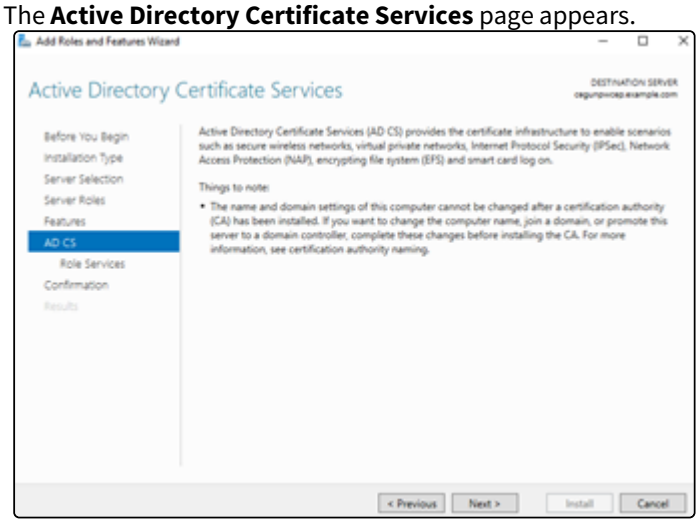


11. Click **Add Features** to add these required features and close the dialog box.

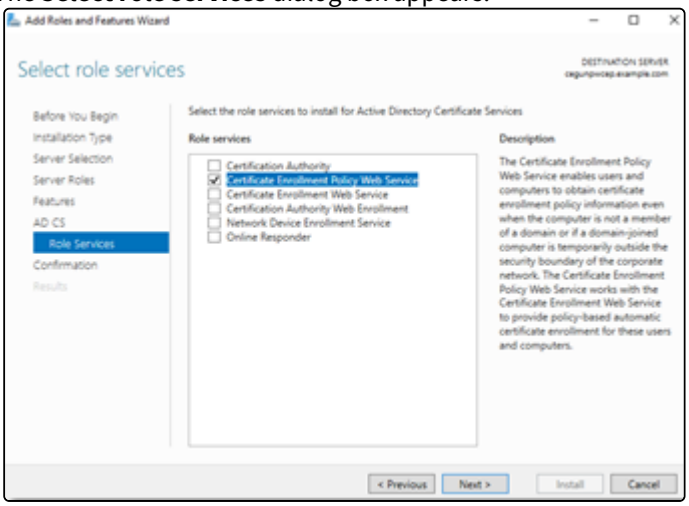
12. Click **Next**.
    The **Select features** dialog box appears.



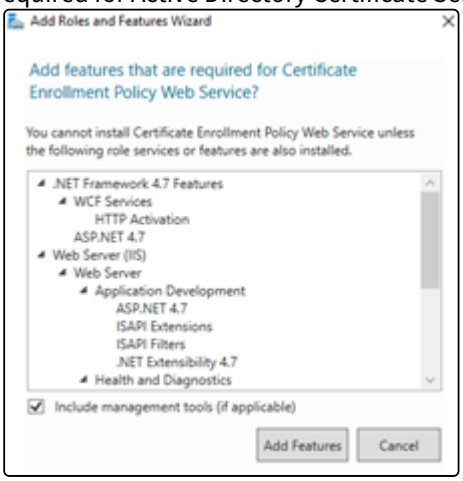
13. Click **Next**.
    The **Active Directory Certificate Services** page appears.



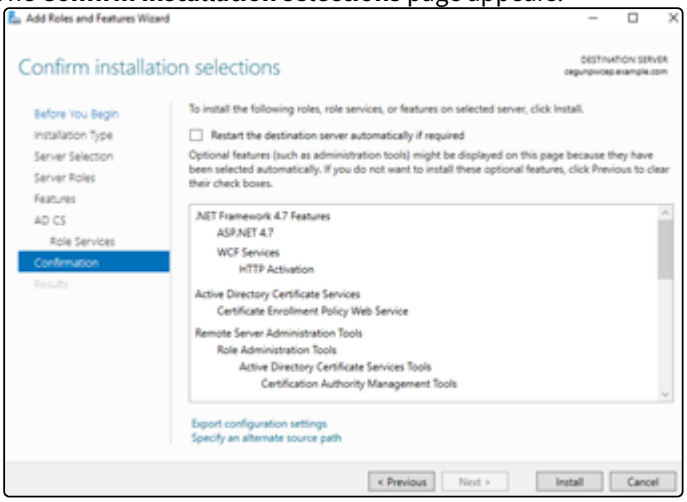
14. Click **Next**.
    The **Select role services** dialog box appears.



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.

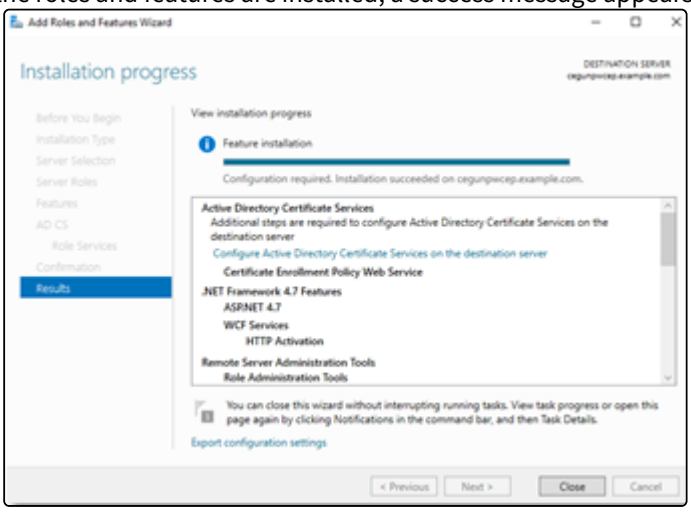


17. Click **Add Features** to add these required features and close the dialog box.
18. Click **Next**.
    The **Confirm installation selections** page appears.



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.

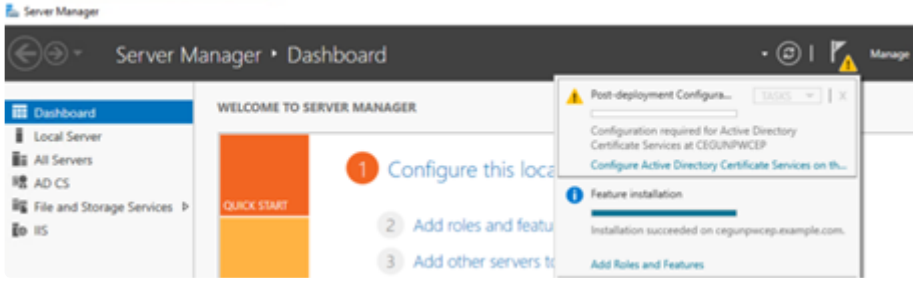
- username
- domain\username
- username@domain
- domainfqdn\username
- username@domainfqdn

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.

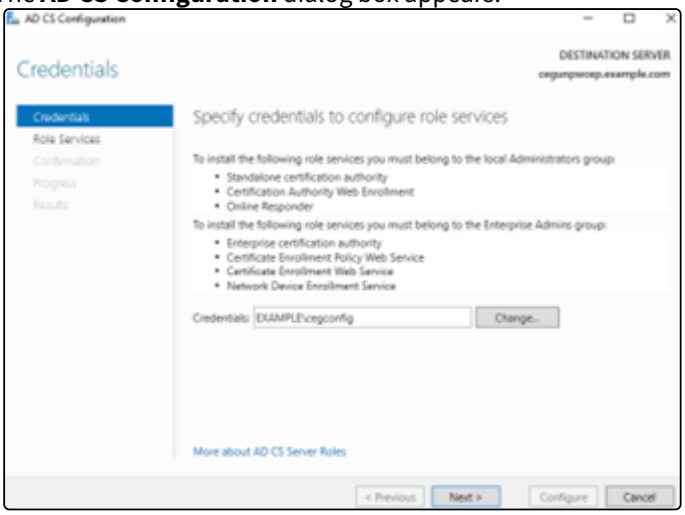
To select the authentication mode for the CEP Web Service using the Windows graphical interface

1. Log in to the server where you installed the Certificate Enrollment Policy Web Service.

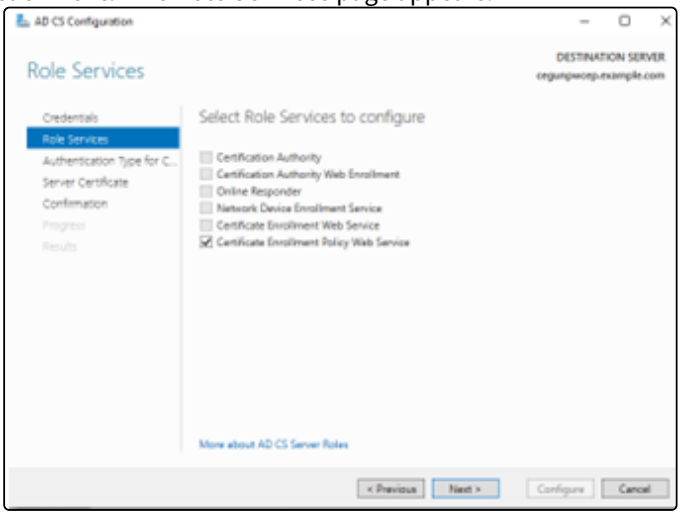
2. Open Server Manager. Select **Start > Server Manager**.
   The **Server Manager** dialog box appears.



3. Select **Notifications > Configure Active Directory Certificate Services** on the destination server.
   The **AD CS Configuration** dialog box appears.

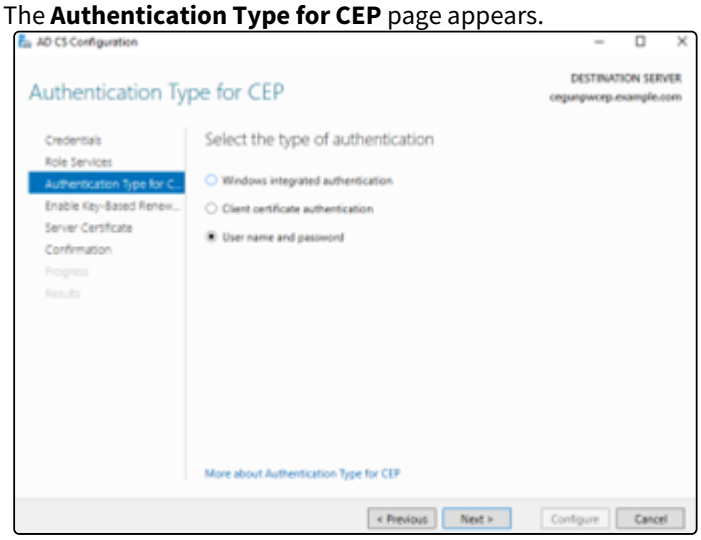


4. Enter or select the administrator credentials you will use to configure role services.
5. Click **Next.** The **Role Services** page appears.



6. Select **Certificate Enrollment Policy Web Service**.

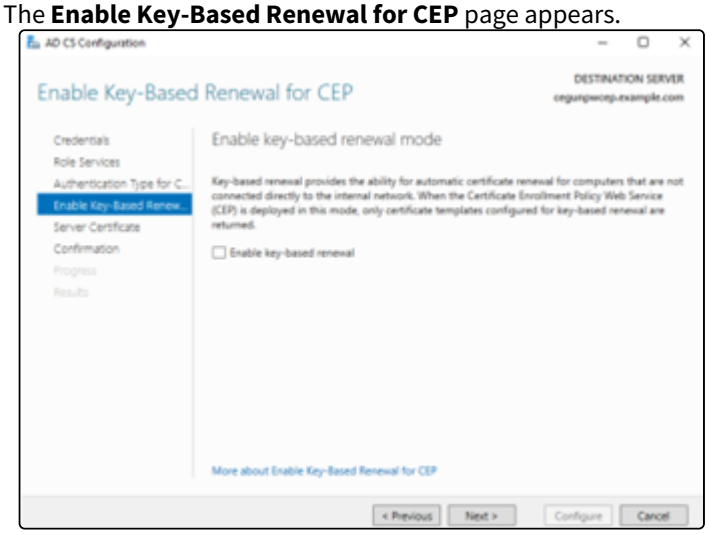
7. Click **Next**.
   The **Authentication Type for CEP** page appears.



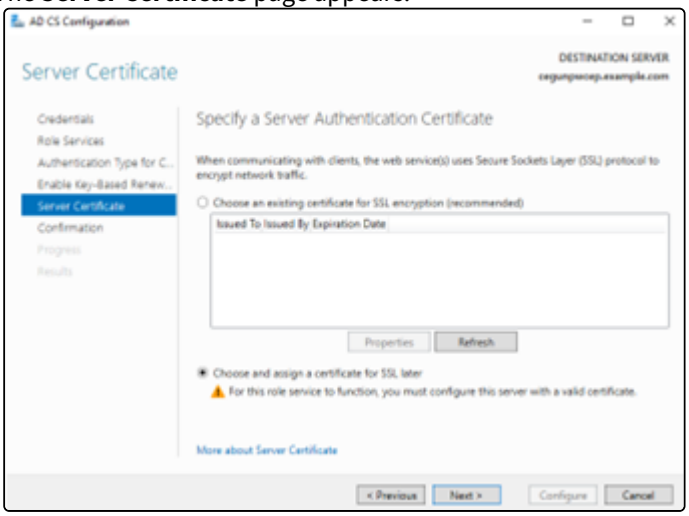
8. Select an authentication method supported by Certificate Enrollment Gateway.

   > Client certificate authentication is currently not supported by Certificate Enrollment Gateway.

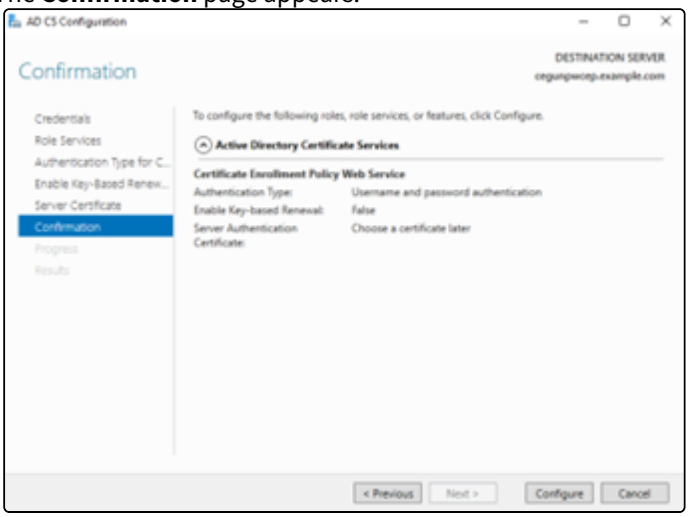
   If you support non-domain enrollment endpoints, you must select **User name and password** as the authentication method.
9. Click **Next**.
   The **Enable Key-Based Renewal for CEP** page appears.



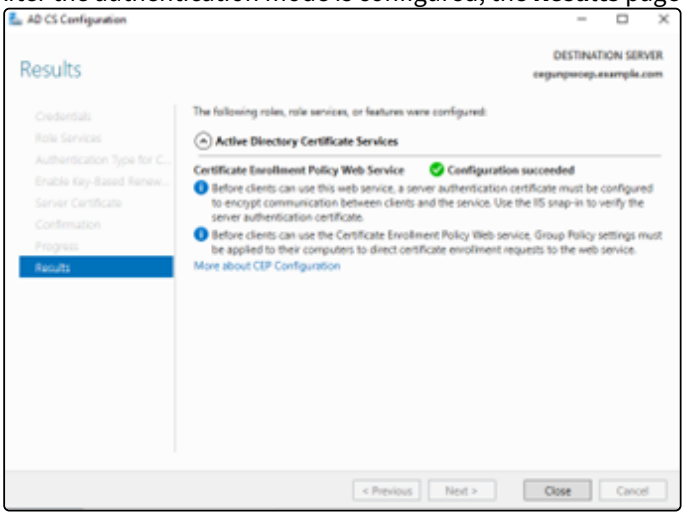
10. Do not select any options. Click **Next**.
    The **Server Certificate** page appears.



11. Select **Choose and assign a certificate for SSL later**.
12. Click **Next**.
    The **Confirmation** page appears.



13. Click **Configure**.
    After the authentication mode is configured, the **Results** page appears.



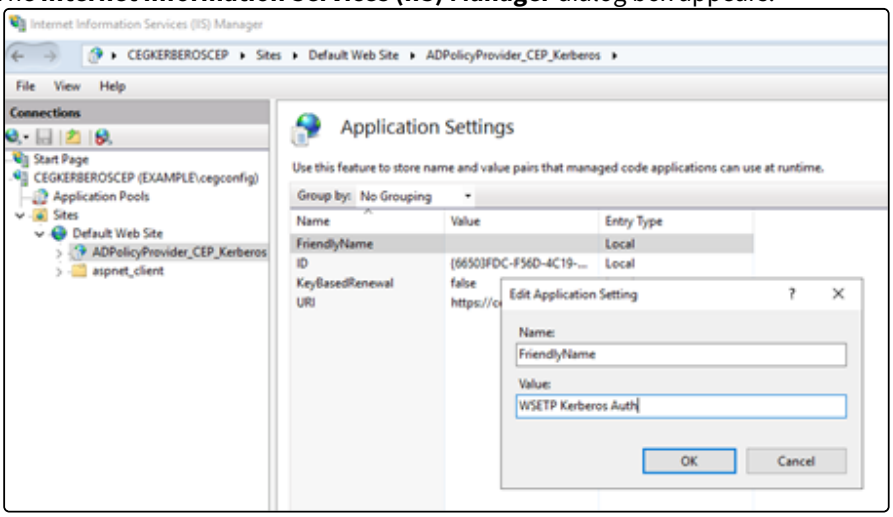
14. Click **Close**.

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"
   ```

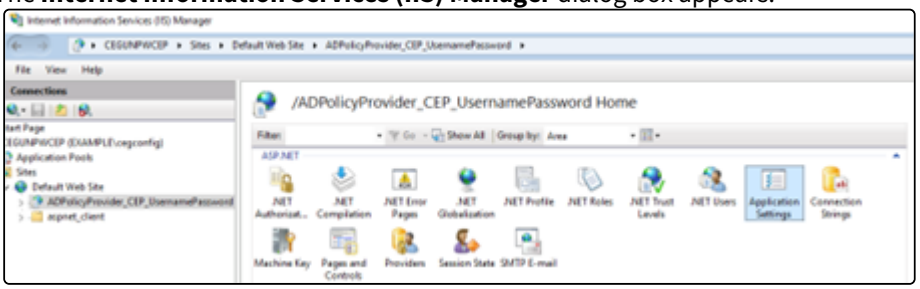
Assigning a unique Enrollment Policy Identifier with the Windows graphical interface

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**.

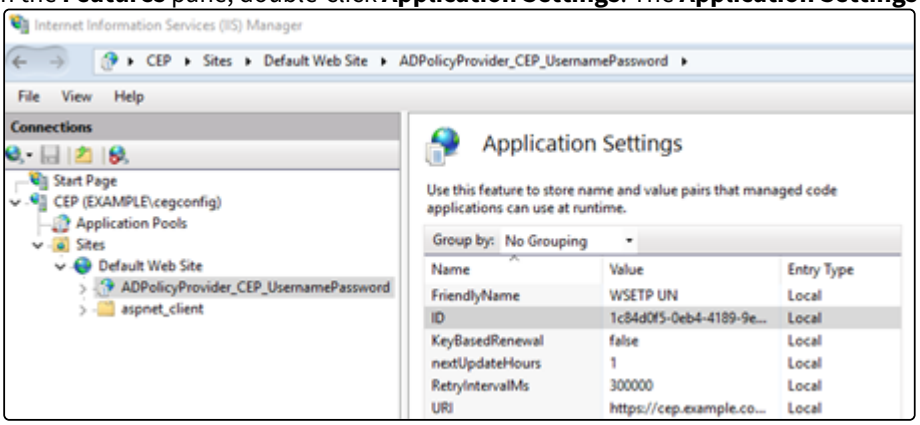
The **Internet Information Services (IIS) Manager** dialog box appears.



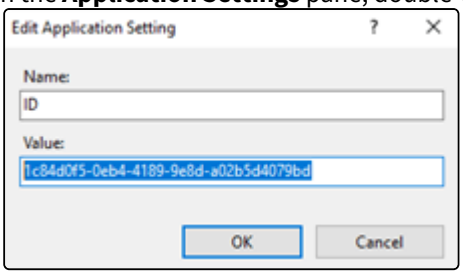
3. In the **Connections** pane, expand **Sites > Default Web Site**.
4. Select the name of the Certificate Enrollment Policy Web Service application.
   - If you configured user name and password authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider_CEP_UsernamePassword**.
   - 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 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 created an enrollment service with the InstallEnrollmentService.ps1 script

1. Log in to a Windows server that is joined to the Active Directory domain. It is recommended that you run the PowerShell script on a different server than the domain controller.
2. From Entrust TrustedCare, download the PowerShell scripts for Certificate Enrollment Gateway.
3. Extract the PowerShell scripts to a directory on the server.
4. PowerShell scripts downloaded from the Internet may be blocked from running. To unblock a PowerShell script:
    a. Right-click the PowerShell script > **Properties**.
    A **Properties** dialog box appears.
    b. Under the **General** tab, click **Unblock**.
5. Open an elevated PowerShell window. Select **Start** > **Windows PowerShell**, then right-click **Windows PowerShell** > **Run as administrator**.
6. Navigate to the directory where you extracted the PowerShell scripts.
7. Enter the following command to run the `InstallEnrollmentService.ps1` script:

```
.\InstallEnrollmentService.ps1
```

The script validates the pre-requisites and installs any missing Windows packages or features. For example:

> The PowerShell script was tested on specific versions of PowerShell. When validating the prerequisites, the PowerShell version my 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 propogate 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:

> The PowerShell script was tested on specific versions of PowerShell. When validating the prerequisites, the PowerShell version my be listed as Unverified, an "Unverified" version of PowerShell indicates that the script was not tested on that version of PowerShell. You can still use the script on an "Unverified" version of PowerShell.

```
Validating pre-requisites:
Script-Mode: Windows
Script Version: 1.5.1.19
    - Member of Domain:             Verified
    - Domain Admins privileges:     Verified
    - Enterprise Admins privileges: Verified
    - Windows Version:              Verified (Microsoft Windows NT
10.0.17763.0)
    - PowerShell Version:           Verified (5.1.17763.2931)

------------------------------------------------------------
Validating ldifde is installed.

ldifde.exe is installed.

Validating Windows Feature RSAT-ADCS-Mgmt is installed
Installing RSAT-ADCS-Mgmt
```

4. The script prompts you to select a management option:

```
Entrust Enrollment Service PowerShell

Using this PowerShell script, Enrollments servers can be created, removed
and Edited.

Please select from the following options to continue :
[N] New Service  [E] Edit Service  [Q] Quit  [?] Help (default is "N"):
```

   Enter `E` to edit an existing enrollment service.

5. If more than one enrollment service is defined in Active Directory, the script displays the list of enrollment services and asks you to select one of the enrollment services:

```
Select from the following List of defined Certificate Enrollment Gateway :

Index Enrollment Service Name
----- -----------------------
1     CEG WSTEP
2     Entrust WSTEP
```

```
Please select the Index to select an Enrollment Service. 0 to quit.:
```

Enter the number associated with the enrollment service you want to edit. If only one enrollment service exists, that service is automatically selected by the script.

6. The script displays the currently-selected enrollment service, and prompts you to choose from a list of options:

```
Currently Selected Enrollment Service : Entrust WSTEP

Choose from the following Options:
[E] Edit  [R] Remove  [P] Previous  [?] Help (default is "E"):
```

Enter `E` to edit the selected service.

7. The script prompts you to select an edit option:

```
Updating Enrollment Service : Entrust WSTEP

Menu to select between:
Updating the Enrollment Service URL(s)
Updating the Security Groups for the Enrollment Service.

Choose from the following Options:
[U] Update URL(s)  [S] Update Security Group(s)  [P] Previous  [?] Help
(default is "U"):
```

Enter `U` to update the enrollment URLs.

8. The script asks you to select an update option:

```
Editing the URL(s) for Enrollment Service : Entrust WSTEP

Choose from the following Options:
[A] Add URL  [D] Delete URL  [L] List URL  [P] Previous  [?] Help (default is
"L"):
```

- To list all enrollment URLs for the enrollment service, enter `L`.
- To delete an enrollment URL from the enrollment service, enter `D`.
- To add an enrollment URL to the enrollment service, enter `A`.

9. If you chose to list the enrollment URLs for the enrollment service, the script displays information about each enrollment URL for the enrollment service. For example:

```
Enrollment Service Name : Entrust WSTEP

   Priority     : 1
   Auth Type    : UserName
   Renewal Only : 0
   URL          : https://cegserver1.example.com:443/wstep/usertoken/services/
tenant1/example-ca1
```

For each URL, the script displays the following information:

- **Priority** displays the priority of the enrollment server. If multiple enrollment servers are defined, then the priority determines which enrollment server is preferred.
- **Auth Type** displays the authentication type, either **UserName** for user name and password authentication, or **Kerberos** for Kerberos authentication (integrated Windows authentication).
- **Renewal Only** indicates if the enrollment URL is for certificate renewal only.
  0 indicates that the enrollment URL is for both certificate enrollment and renewal.
  1 indicates that the enrollment URL is for certificate renewal only.
- **URL** displays the enrollment URL.

10. If you chose to delete an enrollment URL from the enrollment service:
    a. The script displays a list of enrollment URLs and asks you to select which URL to remove:

```
Selected Enrollment Service Name : Entrust WSTEP

Retrieving URl(s) from AD.

Index   URL
-----   ------------------------------------------------------------------
1       https://cegserver1.example.com:443/wstep/usertoken/services/
tenant1/example-ca1
Select the URL to remove. -1 to remove all, 0 to quit.:
```

    - To remove a specific enrollment URL, enter the number associated with the URL in the list.
    - To remove all enrollment URLs, enter -1.
    - To go back without removing any enrollment URLs, enter 0.

    b. The script asks you to confirm the removal of the URL or URLs. For example:

```
https://cegserver1.example.com:443/wstep/usertoken/services/tenant1/
example-ca1 is slated to be removed
Continue with removal of URL (y/n)?:
```

    - To confirm that you want remove the URL, enter `y`.
    - To cancel the removal, enter `n`.

11. If you chose to add an enrollment URL to the enrollment service, the script asks if you want to configure an enrollment URL for user name and password authentication:

```
Configure UserName Enrollment URL ? (y/n):
```

    - To configure an enrollment URL for user name and password authentication, enter `y`.
    - To skip configuring an enrollment URL for user name and password authentication, enter `n`.

12. If you chose to add an enrollment URL for user name and password authentication:
    a. The script prompts you to enter an enrollment URL:

```
Please enter the Enrollment Server URL :
```

    Enter the enrollment URL using the following format:

```
https://<CEG-server>:443/wstep/usertoken/services/<tenant-ID>/<CA-ID>
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the Windows endpoint.

For example:

```
https://cegserver1.example.com:443/wstep/usertoken/services/tenant1/
example-ca1
```

b. The script prompts you to specify the priority of the enrollment server:

```
The URI for the enrollment server which has the lowest priority number as
defined in the enrollment policy. If two enrollment servers have the same
priority then
   a. The URI with the following authentication type is preferred in
order:
      Kerberos, Anonymous, Username/Password cached in the vault or
      Client Auth Certificate cached in the vault, Username/Password or
      Client Auth Certificate.
   b. If all properties are equal then a URI is randomly selected.

Please enter the Priority of this Enrollment URL [Default : 1]:
```

If multiple enrollment servers are defined, then the priority determines which enrollment server is preferred. Enter the priority for the enrollment server.

c. The script asks if the URL will be used for certificate renewal only:

```
Will this URL be used for Renewal ONLY ? (y/n):
```

- If the enrollment URL is for certificate renewal only, enter `y`.
- If the enrollment URL is for certificate enrollment and renewal, enter `n`.

d. The script displays information about the enrollment URL and asks if you want to continue:

```
Enrollment Service  : Entrust WSTEP
Authentication Type : UserName
Enrollment URL      : https://cegserver1.example.com:443/wstep/usertoken/
services/tenant1/example-ca1
Priority            : 1
Modifiers           :
Continue with above settings? (y/n):
```

- To continue and add the enrollment URL, enter `y`.
- To go back and re-enter information about the enrollment URL, enter `n`.

13. If you chose to add an enrollment URL to the enrollment service, the script asks if you want to configure an enrollment URL for Kerberos (Windows integrated) authentication:

```
Configure Kerberos Enrollment URL ? (y/n):
```

- To configure an enrollment URL for Kerberos authentication, enter `y`.
- To skip configuring an enrollment URL for Kerberos authentication, enter `n`.

14. If you chose to add an enrollment URL for Kerberos authentication:
    a. The script prompts you to enter an enrollment URL:

```
Please enter the Enrollment Server URL :
```

Enter the enrollment URL using the following format:

```
https://<CEG-server>:443/wstep/kerberos/services/<tenant-ID>/<CA-ID>
```

Where:

- `<CEG-server>` is the hostname or IP address of the Certificate Enrollment Gateway server.
- `<tenant-ID>` is the unique identifier of a tenant defined in Certificate Enrollment Gateway. The value is case-sensitive.
- `<CA-ID>` is the CA ID of the Certificate Authority (CA) defined in CA Gateway that will issue certificates to the Windows endpoint.

For example:

```
https://cegserver1.example.com:443/wstep/kerberos/services/tenant1/
example-ca1
```

    b. The script prompts you to specify the priority of the enrollment server:

```
The URI for the enrollment server which has the lowest priority number as
defined in the enrollment policy. If two enrollment servers have the same
priority then
   a. The URI with the following authentication type is preferred in
order:
      Kerberos, Anonymous, Username/Password cached in the vault or
      Client Auth Certificate cached in the vault, Username/Password or
      Client Auth Certificate.
   b. If all properties are equal then a URI is randomly selected.

Please enter the Priority of this Enrollment URL [Default : 1]:
```

If multiple enrollment servers are defined, then the priority determines which enrollment server is preferred. Enter the priority for the enrollment server.

    c. The script asks if the URL will be used for certificate renewal only:

```
Will this URL be used for Renewal ONLY ? (y/n):
```

- If the enrollment URL is for certificate renewal only, enter `y`.
- If the enrollment URL is for certificate enrollment and renewal, enter `n`.

d. The script displays information about the enrollment URL and asks if you want to continue:

```
Enrollment Service  : Entrust WSTEP
Authentication Type : Kerberos
Enrollment URL      : https://cegserver1.example.com:443/wstep/kerberos/
services/tenant1/example-ca1
Priority            : 1
Modifiers           :
Continue with above settings? (y/n):
```

- To continue and add the enrollment URL, enter `y`.
- To go back and re-enter information about the enrollment URL, enter `n`.

15. To exit the script after updating the enrollment URLs:

a. Keep entering `P` to return to a previous menu until you return to the main menu:

```
Entrust Enrollment Service PowerShell

Using this PowerShell script, Enrollments servers can be created, removed
and Edited.

Please select from the following options to continue :
[N] New Service  [E] Edit Service  [Q] Quit  [?] Help (default is "N"):
```

b. Enter `Q` to exit the script.

Updating the security groups for an enrollment service using a PowerShell script

Entrust provides an `InstallEnrollmentService.ps1` PowerShell script that allows you to create, edit, and remove enrollment services in Active Directory. When editing an enrollment service in Active Directory, you can update the security groups (access groups) assigned to the enrollment service. When updating the security groups assigned to an enrollment service, you can:

- List all the security groups that are assigned to the enrollment service.
- Add a security group to the enrollment service.
- Remove a security group from to the enrollment service.

To run the script, you must use a Windows user account with Domain Admin and Enterprise Admin permissions.

To update the security groups for an enrollment service using the InstallEnrollmentService.ps1 script

1. Open an elevated PowerShell window. Select **Start** > **Windows PowerShell**, then right-click **Windows PowerShell** > **Run as administrator**.
2. Navigate to the directory where you extracted the PowerShell scripts.
3. Enter the following command to run the `InstallEnrollmentService.ps1` script:

```
.\InstallEnrollmentService.ps1
```

The script validates the pre-requisites and installs any missing Windows packages or features. For example:

> The PowerShell script was tested on specific versions of PowerShell. When validating the prerequisites, the PowerShell version my 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:                       "cegmsca.example.com\CEGMSCA"
  Exchange Certificate:         ""
  Signature Certificate:        ""
  Description:                  ""
  Server:                       "cegmsca.example.com"
  Authority:                    "CEGMSCA"
  Sanitized Name:               "CEGMSCA"
  Short Name:                   "CEGMSCA"
  Sanitized Short Name:         "CEGMSCA"
  Flags:                        "1"
  Web Enrollment Servers:
1
4
0
https://cegserver1.example.com:443/wstep/usertoken/services/tenant1/example-ca1
0

1
2
0
https://cegserver1.example.com:443/wstep/kerberos/services/tenant1/example-ca1
0
CertUtil: -dump command completed successfully.
```

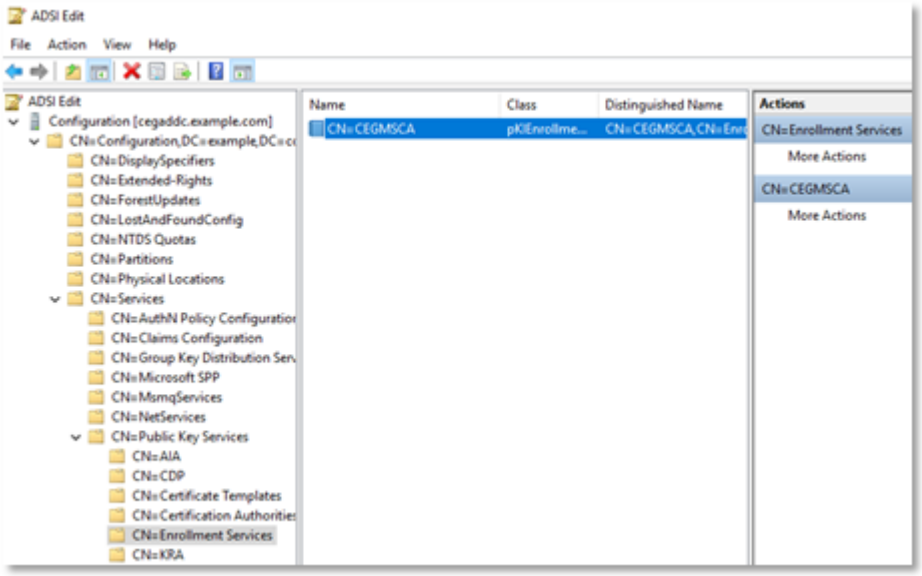
Changing the enrollment URL of the enrollment service using ADSI Edit

To add the enrollment service URL to Active Directory using ADSI Edit, complete the following procedure.

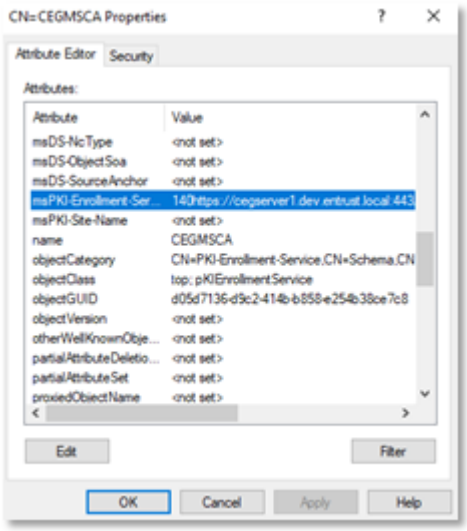
To add the enrollment service URL to Active Directory using ADSI Edit

1. Log in to the server hosting Active Directory.

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 **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.
7. Click **Edit**.
8. 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:

> The PowerShell script was tested on specific versions of PowerShell. When validating the prerequisites, the PowerShell version my 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"):
```

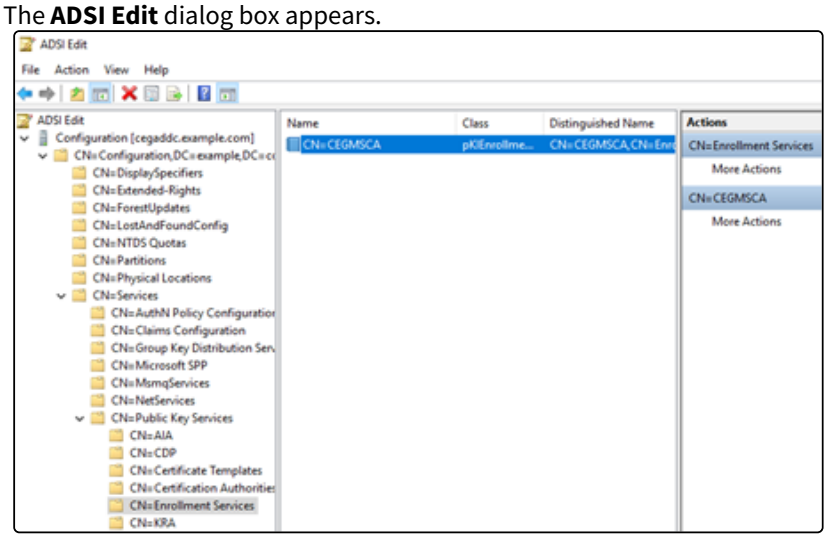
b. Enter `Q` to exit the script.

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.

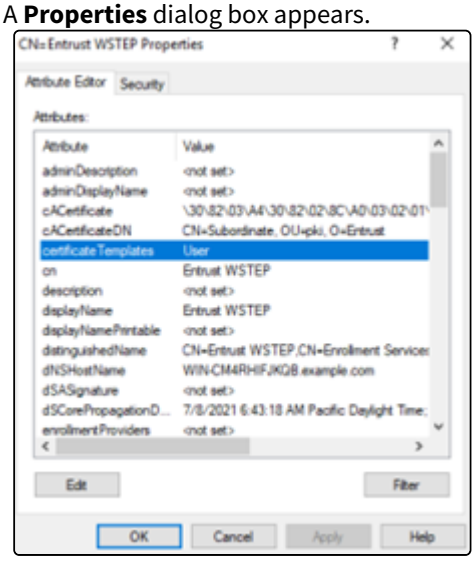
To add certificate templates to the enrollment service

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.

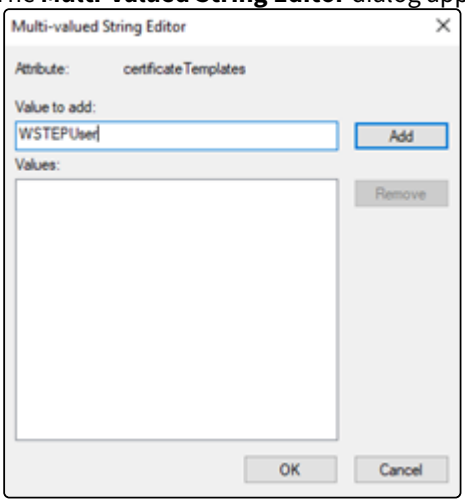


3. In the tree view, expand **ADSI Edit > Configuration > CN=Configuration,<suffix> > CN=Services > CN=Public Key Services > CN=Certificate Enrollment Gateway**.

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.

   > 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.

> 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.

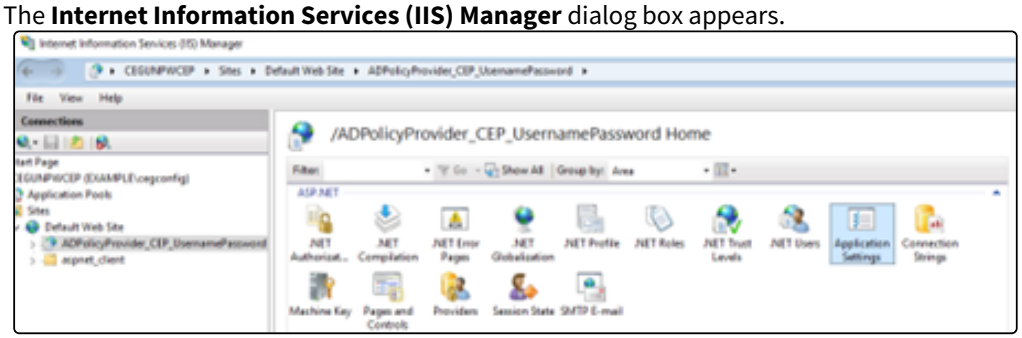
- Obtaining the URL of the Certificate Enrollment Policy Web Service
- Importing the CA certificate into Windows domain endpoints
- Configuring the Certificate Enrollment Policy Web Service for Windows users
- Configuring the Certificate Enrollment Policy Web Service for Windows domain endpoints
- Enabling 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.

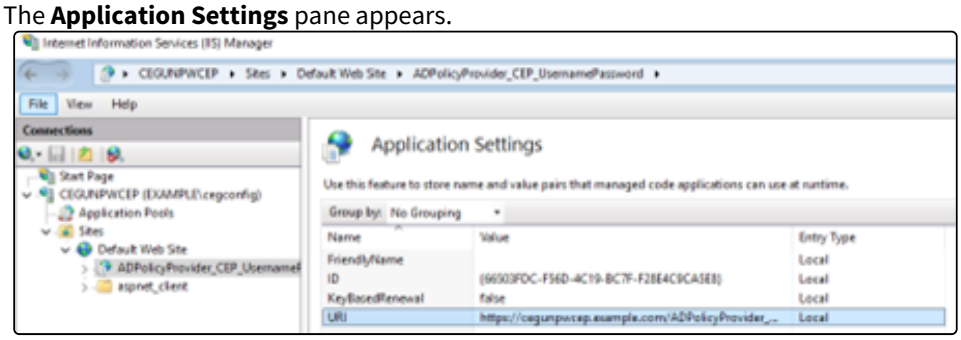
To obtain the URL of the Certificate Enrollment Policy Web Service

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.

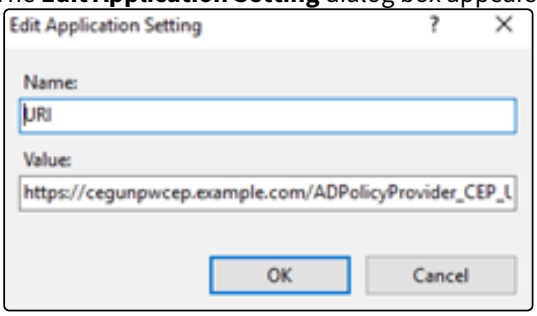


3. In the **Connections** pane, expand **Sites > Default Web site**.
4. Select the name of the Certificate Enrollment Policy Web Service application.
   - If you configured user name and password authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider_CEP_UsernamePassword**.
   - If you configured Kerberos (Windows integrated) authentication for the Certificate Enrollment Policy Web Service, the identifier is **ADPolicyProvider_CEP_Kerberos**.

5. In the Features pane, double-click **Application Settings**.
   The **Application Settings** pane appears.



6. In the **Application Settings** pane, right-click **URI > Edit**.
   The **Edit Application Setting** dialog box appears.



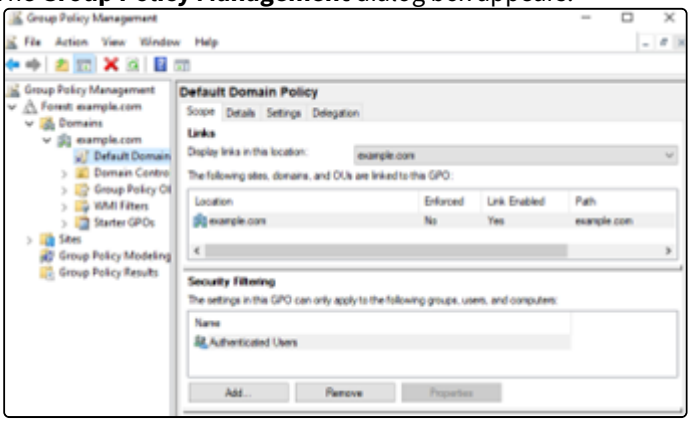
7. Copy the URL from the **Value** field.

Importing the CA certificate into Windows domain endpoints

In each Windows domain enrollment endpoint, import the root certificate of the CA that will issue certificates for the enrollment service.

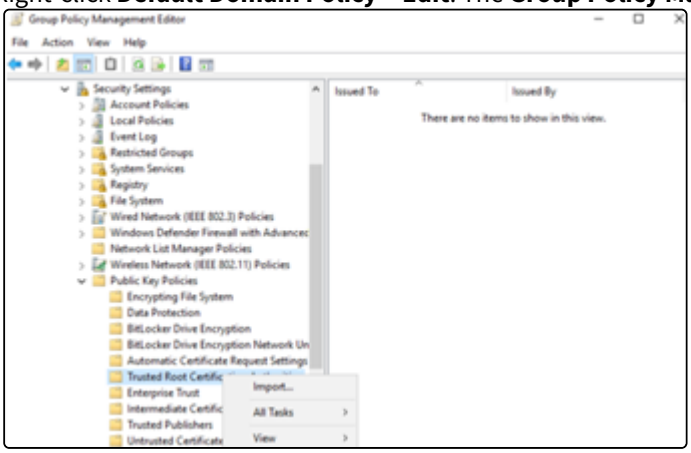
To import the CA certificate

1. Log in to the server hosting Active Directory.
2. Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.
   The **Group Policy Management** dialog box appears.

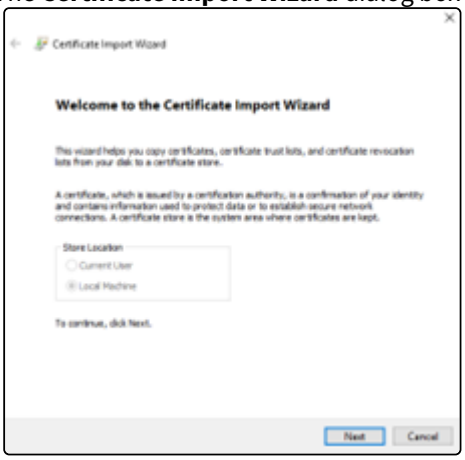


3. In the tree view, expand the Domain Controller you will modify.

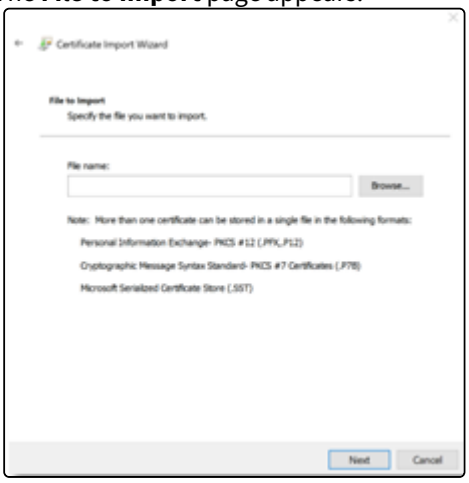
4. Right-click **Default Domain Policy > Edit**. The **Group Policy Management Editor** dialog box appears.



5. In the tree view, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
6. Right-click **Trusted Root Certification Authorities** and select **Import**.
   The **Certificate Import Wizard** dialog box appears.



7. Click **Next**.
   The **File to Import** page appears.



8. Click **Browse** and select the root certificate of the CA that will issue certificates for the enrollment service.

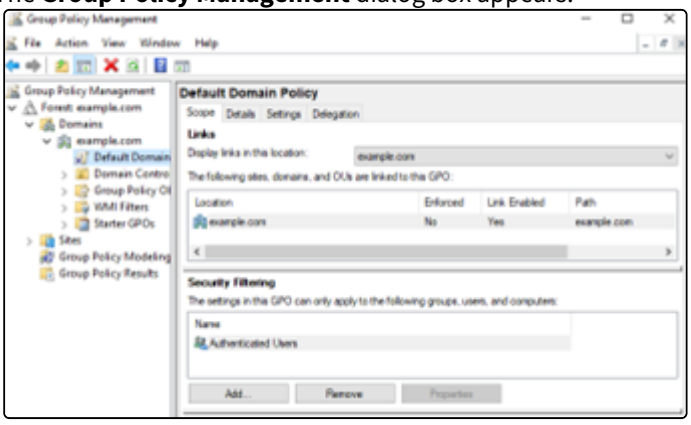
9. Click **Next**.
   The **Certificate Store** page appears.
10. The **Certificate Store** field is automatically set to **Trusted Root Certification Authorities**. Click **Next**.
    The **Completing the Certificate Import Wizard** page appears.
11. Click **Finish**.

Configuring the Certificate Enrollment Policy Web Service for Windows users

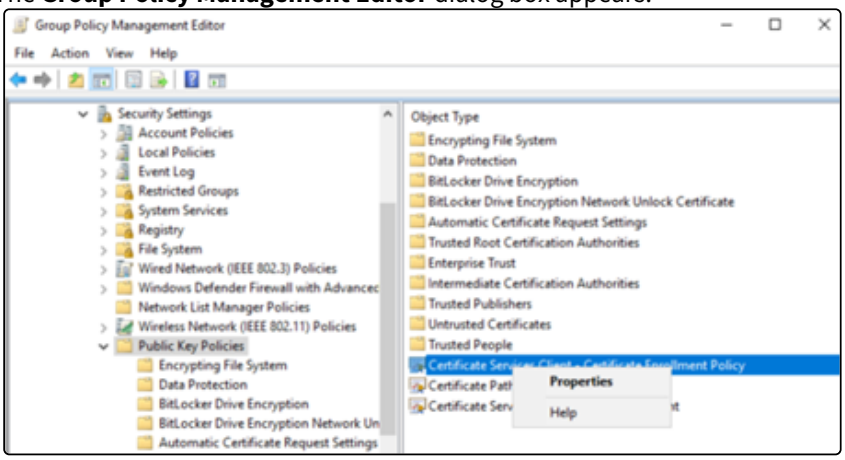
To work with Certificate Enrollment Gateway, Windows domain endpoints need the Certificate Enrollment Policy Web Service URL. Complete the following procedure to add the Certificate Enrollment Policy Web Service URL to Windows domain endpoints.

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.

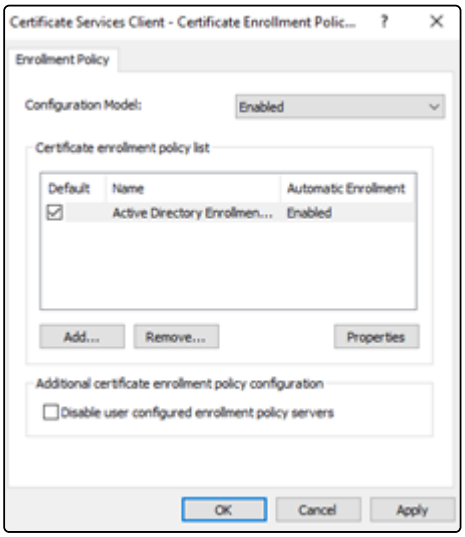


3. In the tree view, expand the Domain Controller you will modify.
4. Right-click **Default Domain Policy > Edit** .
   The **Group Policy Management Editor** dialog box appears.

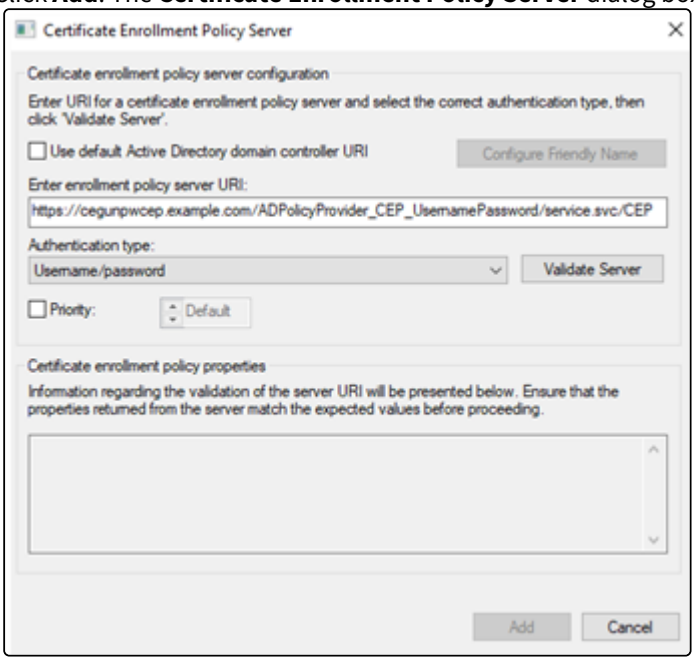


5. In the tree view, expand **User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.

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.

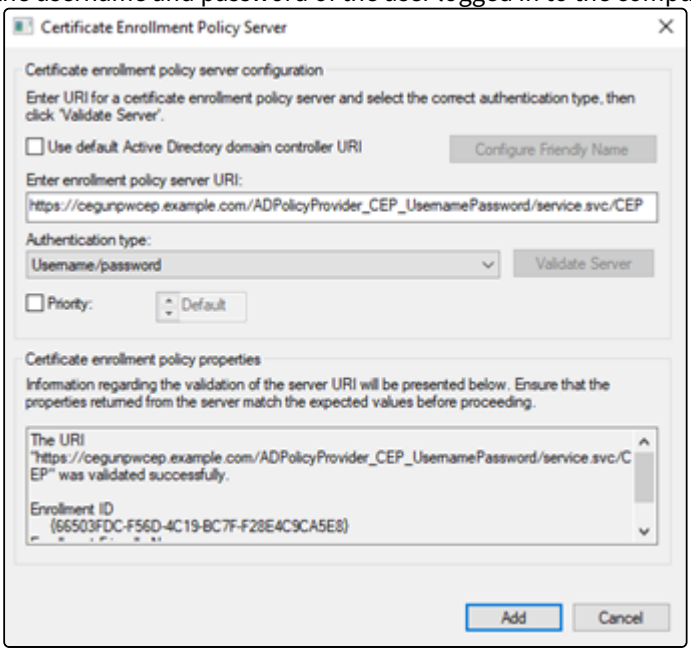


7. In the **Configuration Model** drop-down list, select **Enabled**.
8. If you are not installing WSTEP along with an existing Microsoft CA, select **Active Directory Enrollment** in the **Certificate enrollment policy list** pane, and then click **Remove**.
9. Click **Add**. The **Certificate Enrollment Policy Server** dialog box appears.

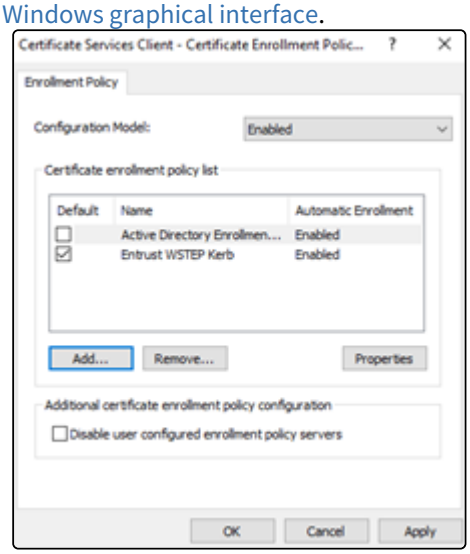


10. In the **Enter enrollment policy server URI** field, enter the Certificate Enrollment Policy Web Service URL that you obtained earlier.
11. In the **Authentication type** drop-down list, select the same authentication mode that you configured earlier in Selecting the authentication mode of the CEP 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.



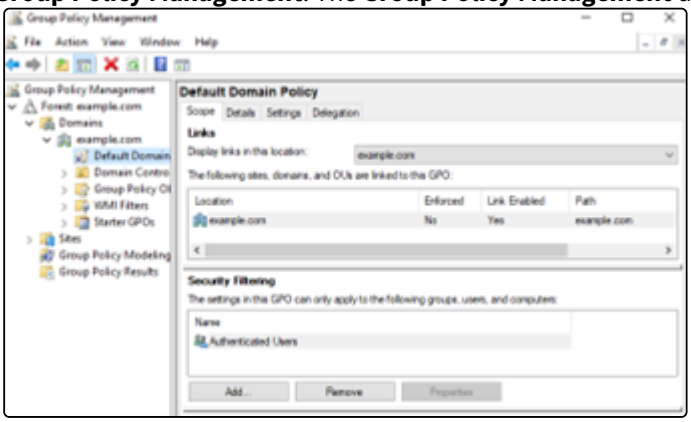
14. In the **Certificate enrollment policy list** pane, select the checkbox for the Certificate Enrollment Policy Web Service you just added to make it the default Certificate Enrollment Policy.
15. Click **OK**.

Configuring the Certificate Enrollment Policy Web Service for Windows domain endpoints

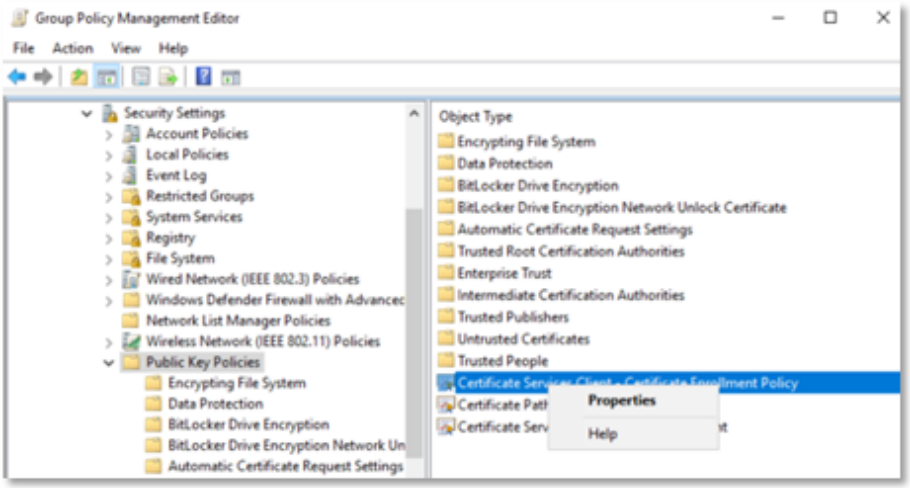
To work with Certificate Enrollment Gateway, Windows domain endpoints need the Certificate Enrollment Policy Web Service URL. Complete the following procedure to add the Certificate Enrollment Policy Web Service URL for Windows domain endpoints.

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.

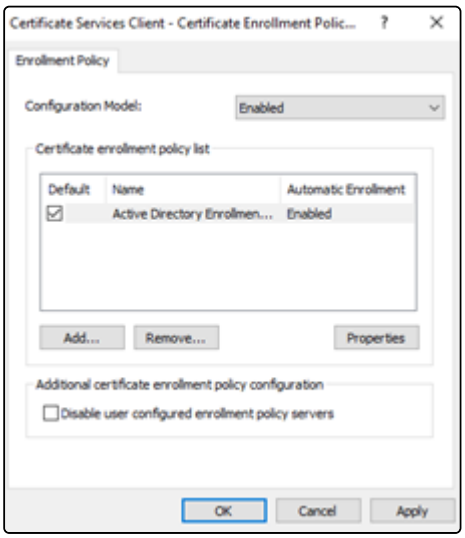


3. In the tree view, expand the Domain Controller you will modify.
4. Right-click **Default Domain Policy > Edit**. The **Group Policy Management Editor** dialog box appears.

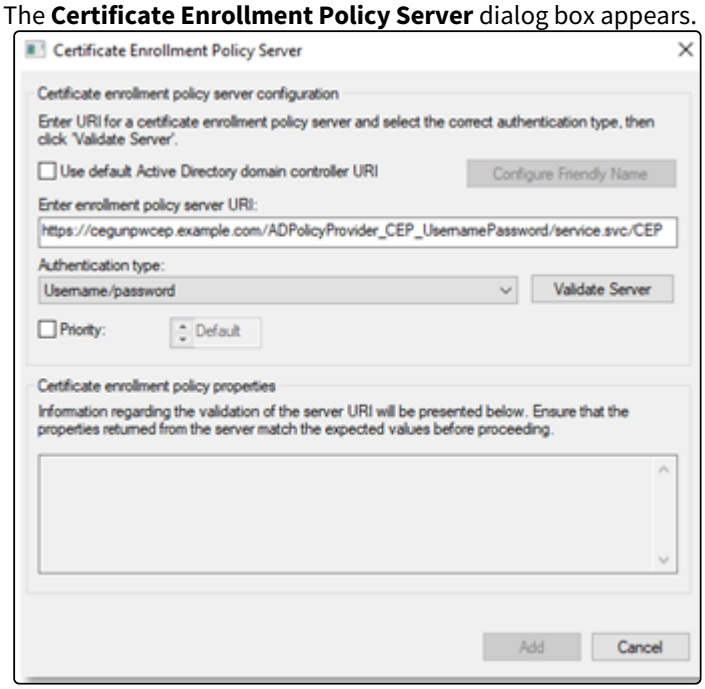


5. In the tree view, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.

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.

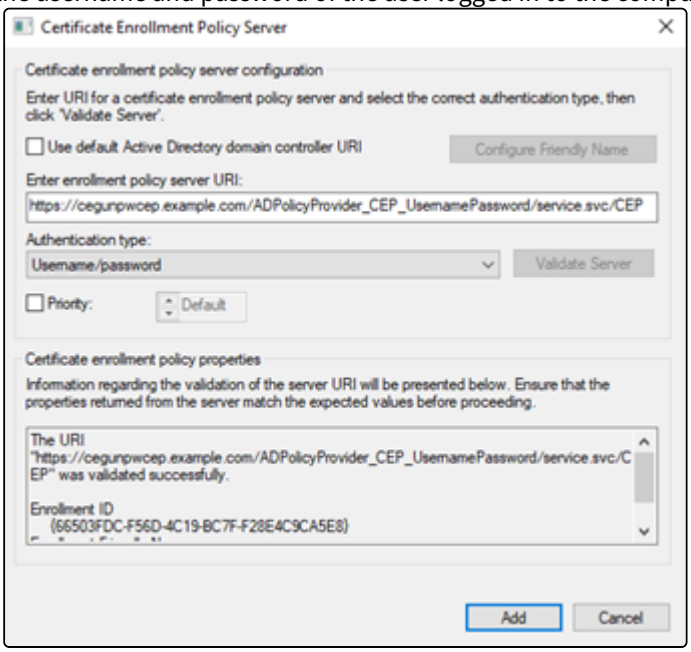


7. In the **Configuration Model** drop-down list, select **Enabled**.
8. If you are not installing WSTEP along with an existing Microsoft CA, select **Active Directory Enrollment** in the **Certificate enrollment policy list** pane, and then click **Remove**.
9. Click **Add**.
   The **Certificate Enrollment Policy Server** dialog box appears.

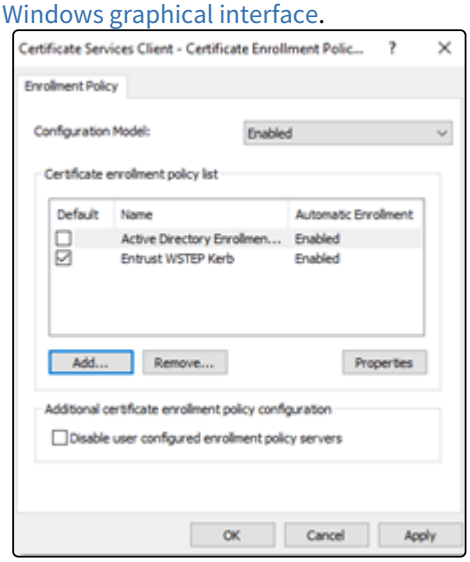


10. In the **Enter enrollment policy server URI** field, enter the Certificate Enrollment Policy Web Service URL that you obtained earlier.
11. In the **Authentication type** drop-down list, select the same authentication mode that you configured earlier in Selecting the authentication mode of the CEP 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**.

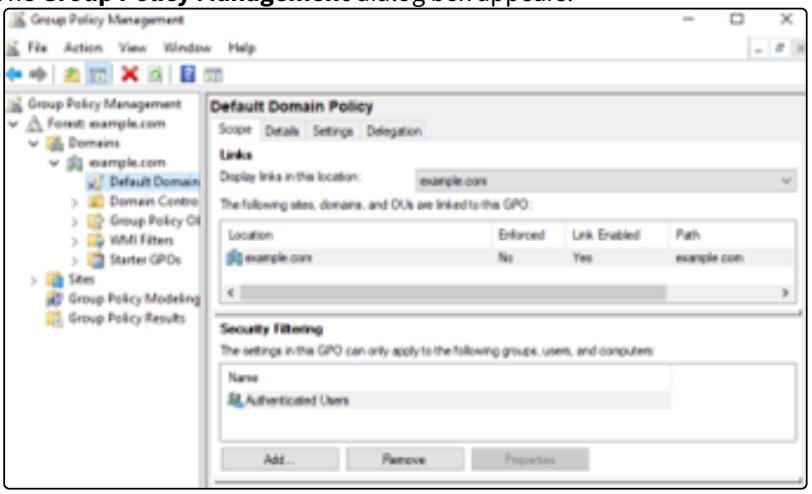
Enabling certificate auto-enrollment for users

In the Windows Domain, enable the certificate auto-enrollment for users.

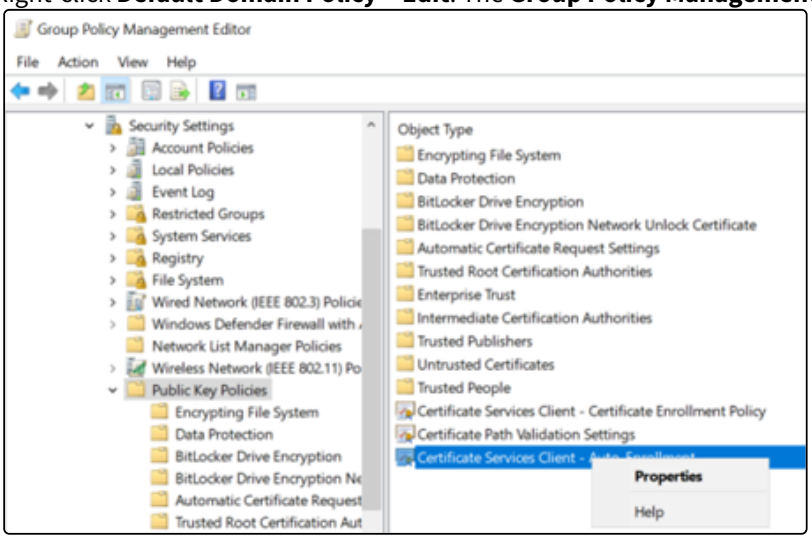
To enable the certificate auto-enrollment for users

1. Log in to the server hosting Active Directory.

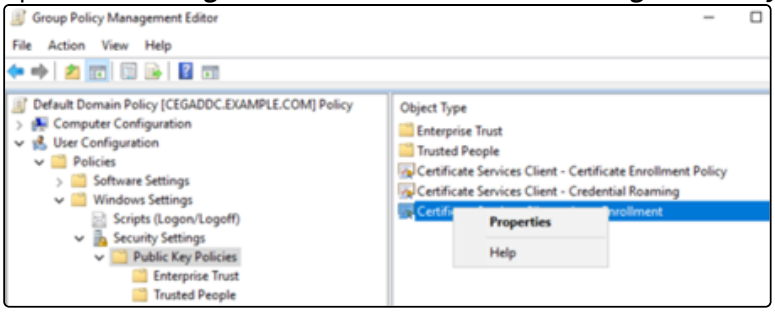
2. Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.
   The **Group Policy Management** dialog box appears.



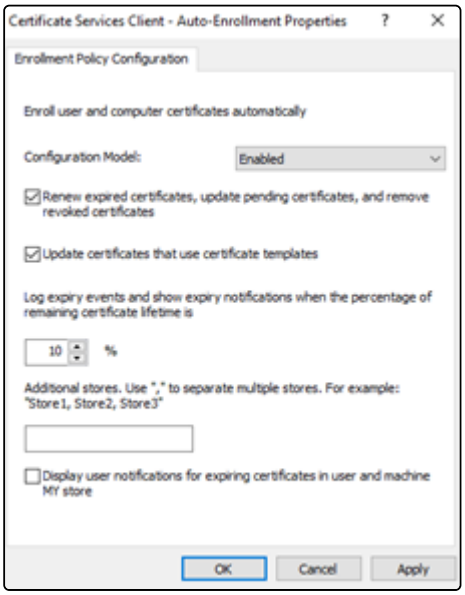
3. In the tree view, expand the Domain Controller you will modify.
4. Right-click **Default Domain Policy > Edit**. The **Group Policy Management Editor** dialog box appears.



5. Expand **User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.



6. In the content pane, right-click **Certificate Services Client Auto Enrollment > Properties**.
   The **Certificate Services Client Auto Enrollment Properties** dialog box appears.



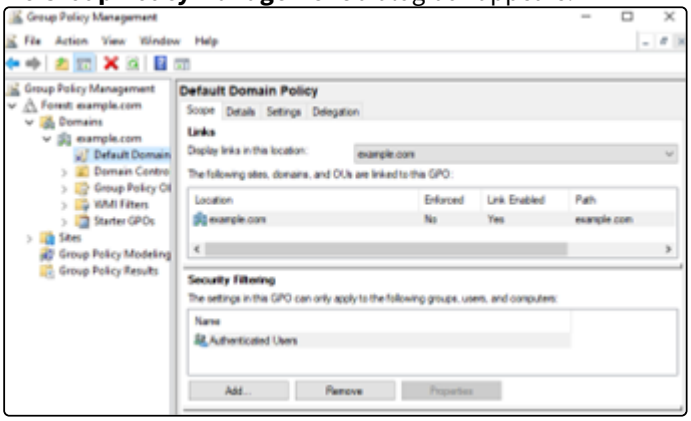
7. In the **Configuration Model** drop-down list, select **Enabled**.
8. Select **Renew expired certificates, update pending certificates, and remove revoked certificates**.
9. Select **Update certificates that use certificate templates**.
10. Click **OK**.

Enabling certificate auto-enrollment for computers and domain controllers

In the Windows domain, enable the certificate auto-enrollment for computers and domain controllers.

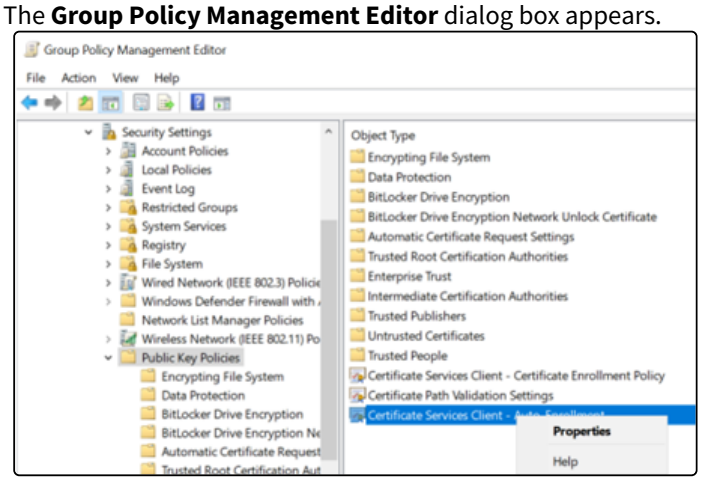
To enable certificate auto-enrollment for computers and domain controllers

1. Log in to the server hosting Active Directory.
2. Open the Group Policy Management administrative tool. Select **Start > Windows Administrative Tools > Group Policy Management**.
   The **Group Policy Management** dialog box appears.

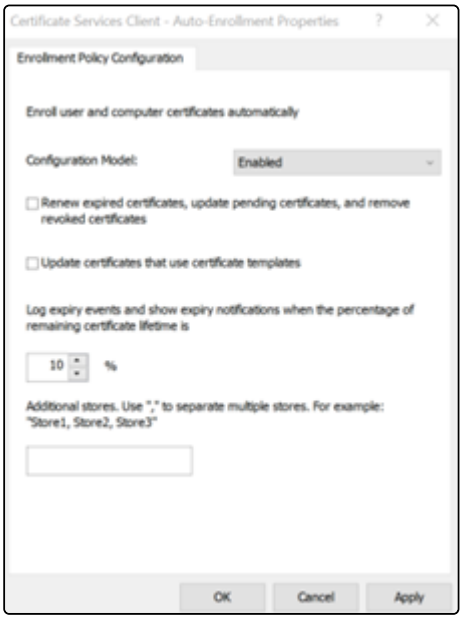


3. In the tree view, expand the Domain Controller you will modify.

4. Right-click **Default Domain Policy > Edit**.
   The **Group Policy Management Editor** dialog box appears.



5. Expand to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
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.

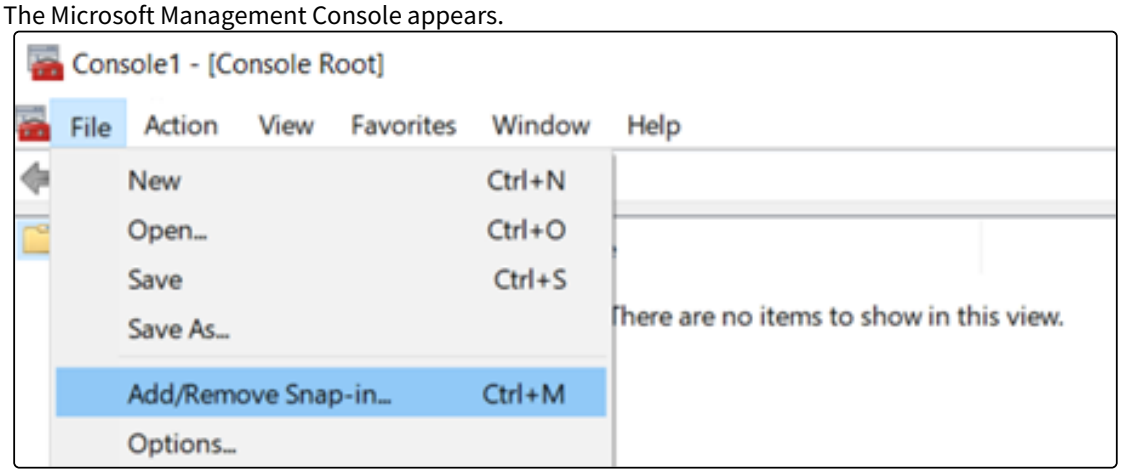
- Configuring the enrollment policy in non-domain endpoints
- Importing the root CA certificate into non-domain endpoints

Configuring the enrollment policy in non-domain endpoints

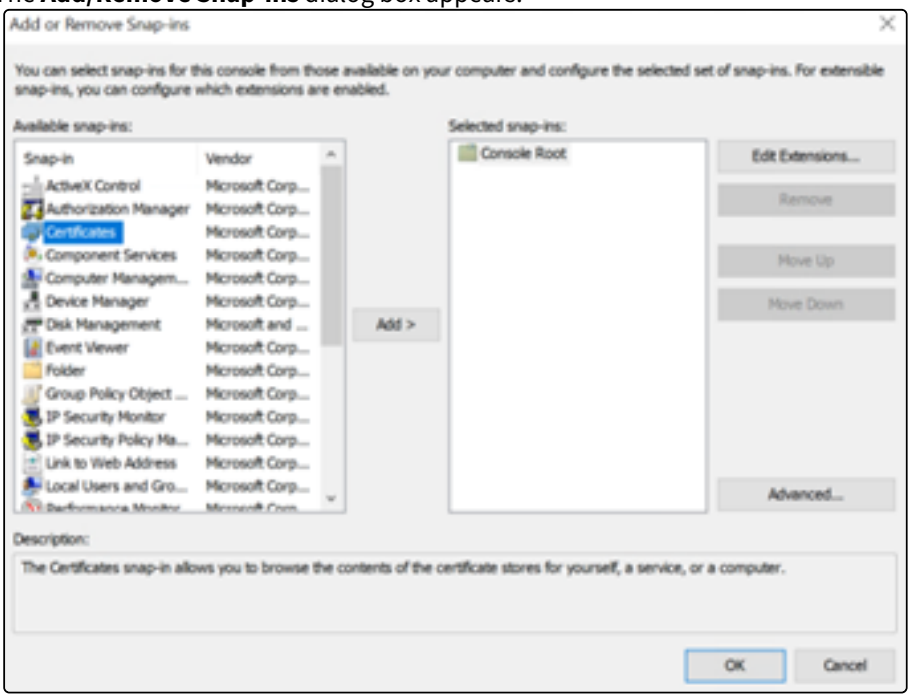
In the enrollment endpoints outside the Windows Domain, add the enrollment policy as described in the following procedure.

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.

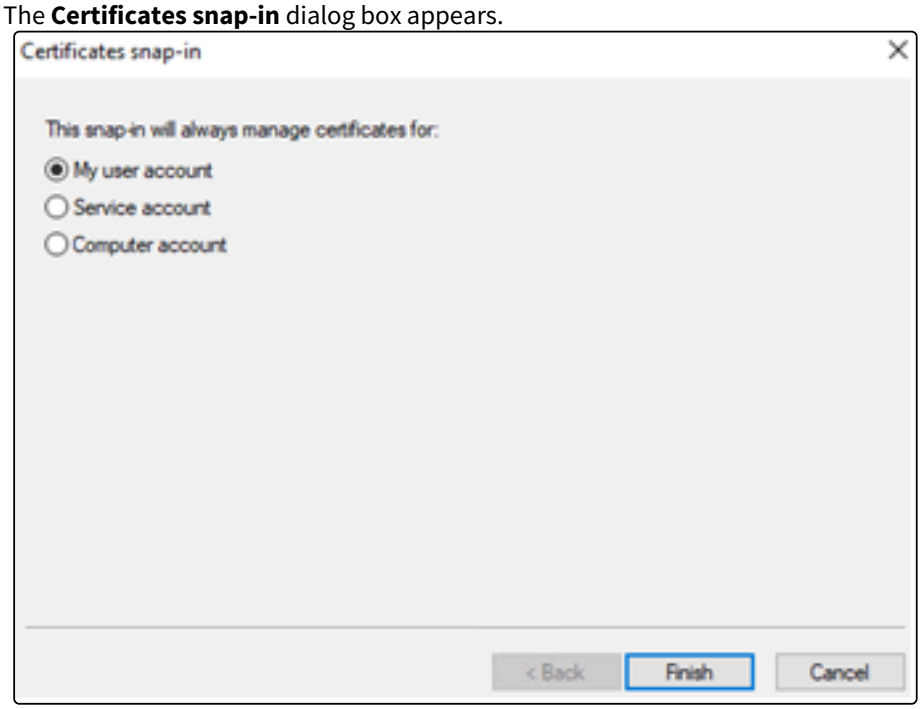


3. Select **File > Add/Remove Snap-in**.
   The **Add/Remove Snap-ins** dialog box appears.

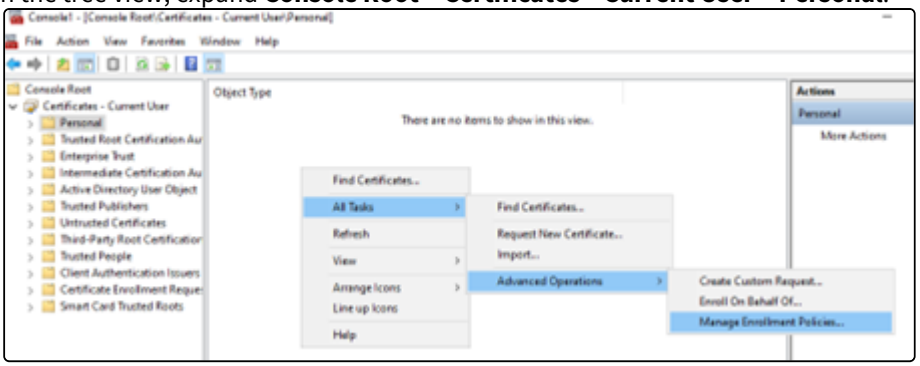


4. In the **Available snap-ins** list, select **Certificates**.

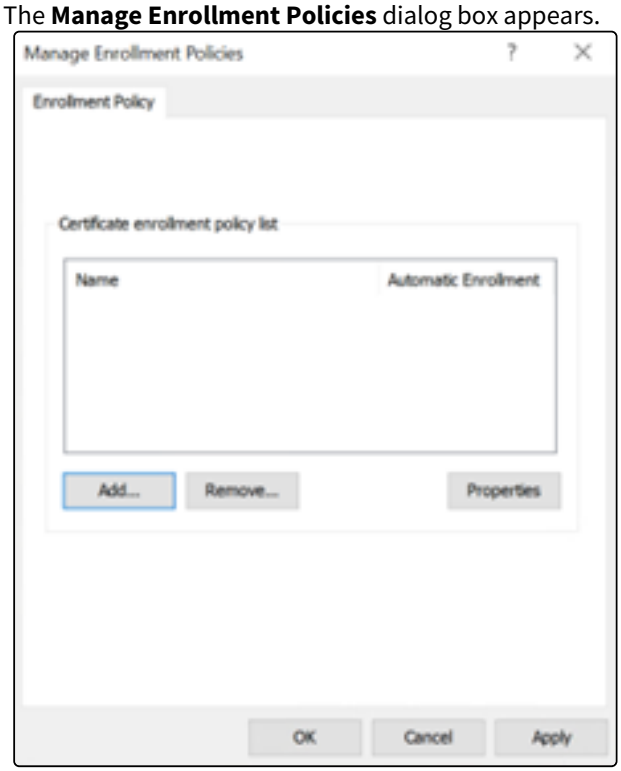
5. Click **Add**.
   The **Certificates snap-in** dialog box appears.



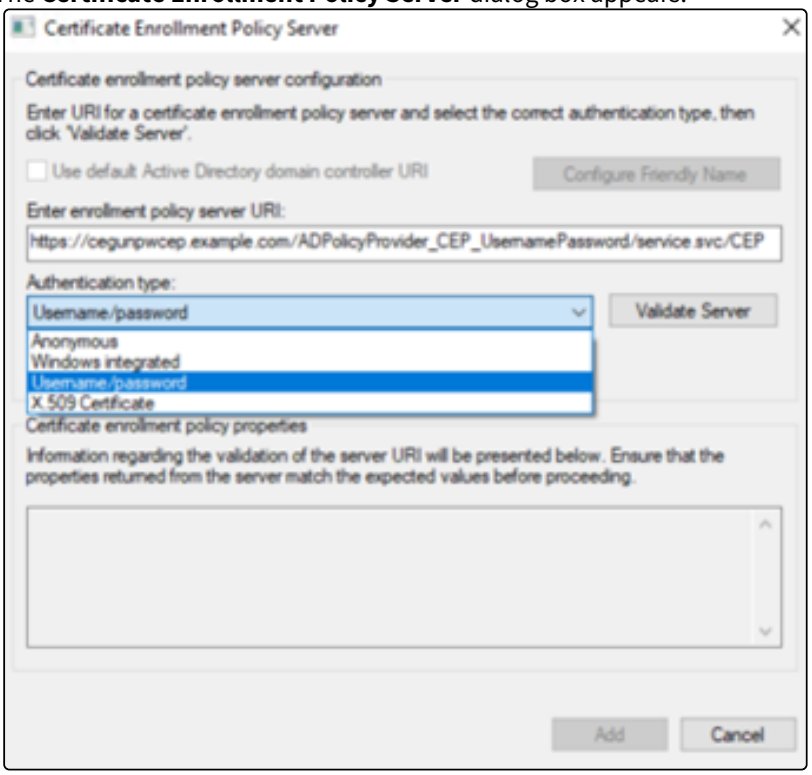
6. Select **My user account**.
7. Click **Finish** to close the **Certificates snap-in** dialog box.
8. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
9. In the tree view, expand **Console Root > Certificates – Current User > Personal**.



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

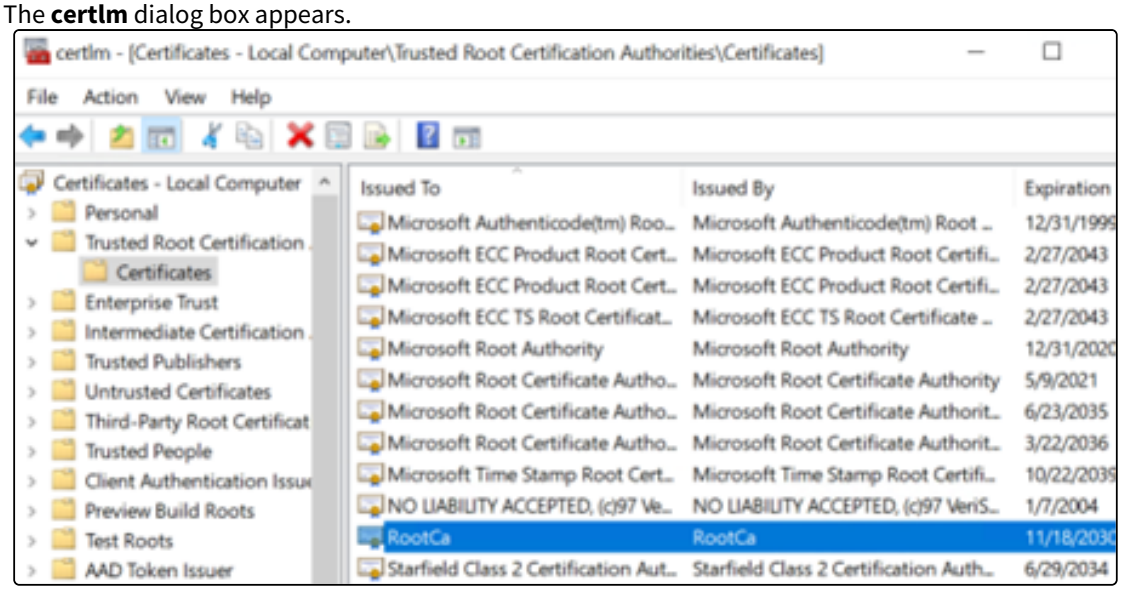
In the enrollment endpoints outside the Windows Domain, import the certificate of the CA that will issue certificates for the enrollment service.

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

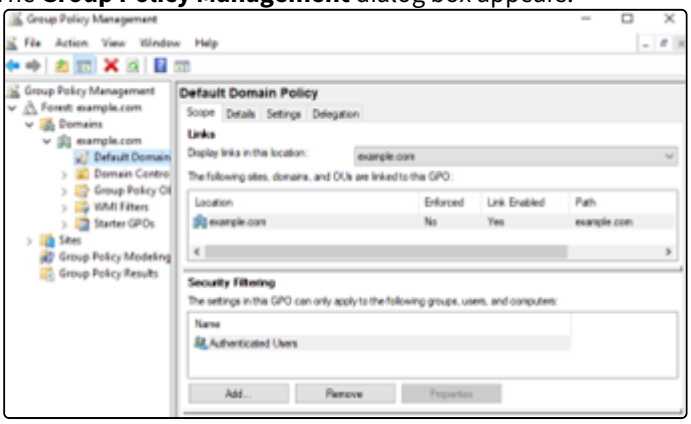
On the server hosting the Certificate Enrollment Policy Web Service, the TLS certificate installed on Microsoft IIS is irrelevant to Certificate Enrollment Gateway. Instead, what matters is that the issuing certificate chain is trusted by all devices on the domain, along with any non-domain WSTEP client.

- 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.

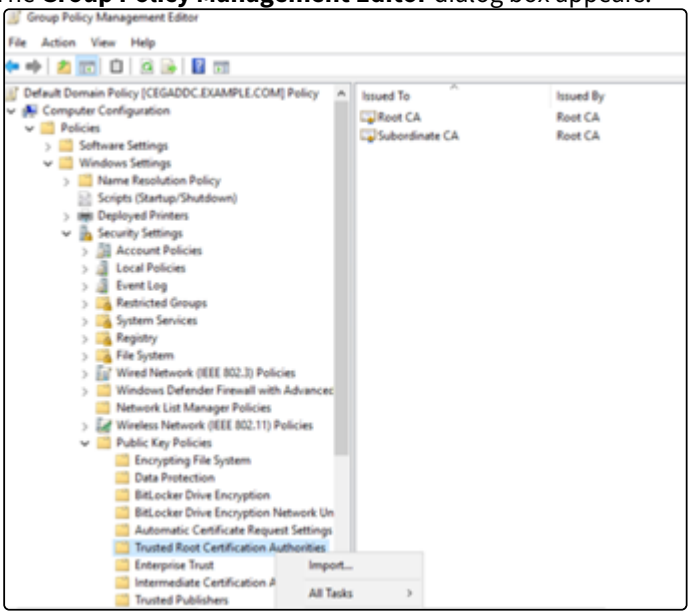
For CAs hosted by Entrust PKI as a Service, you should have obtain the CA certificates from the Entrust Certificate Services portal.

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 administrating 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.

> 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 Managing Certificate Authority, and select the built-in CA Gateway service of this CA.
External Certificate Authority	Start up the Entrust CA Gateway solution and connect it with the external CA as explained Managing CA Gateway.

Certificate Manager

Certificate Manager is a container-based set of services amenable to either customer premises or commercial cloud hosting. Certificate Manager provides:

- An API interface to the companion Certificate Manager browser UI.
- The underlying certificate database.
- The necessary background processes.

Configuring and deploying Certificate Manager

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

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>:8443/management-console
   ```

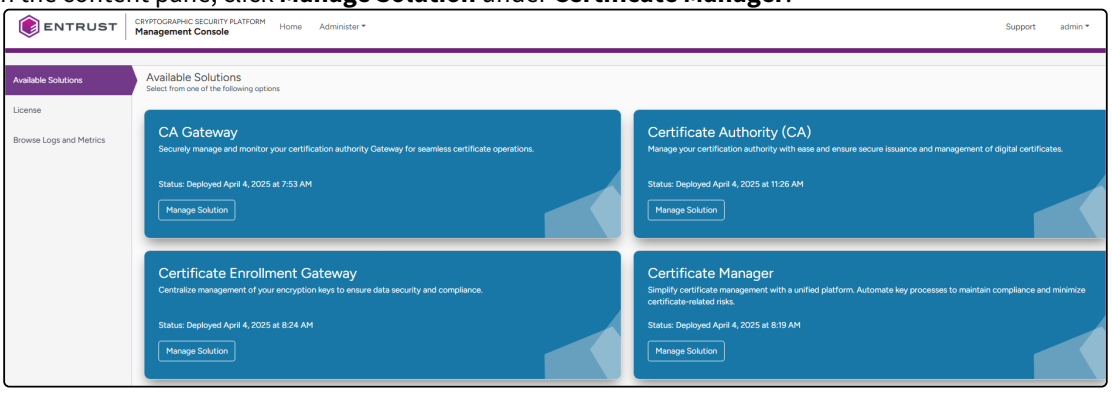
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   This release changes the URL port to 8443. Update your bookmarks accordingly.

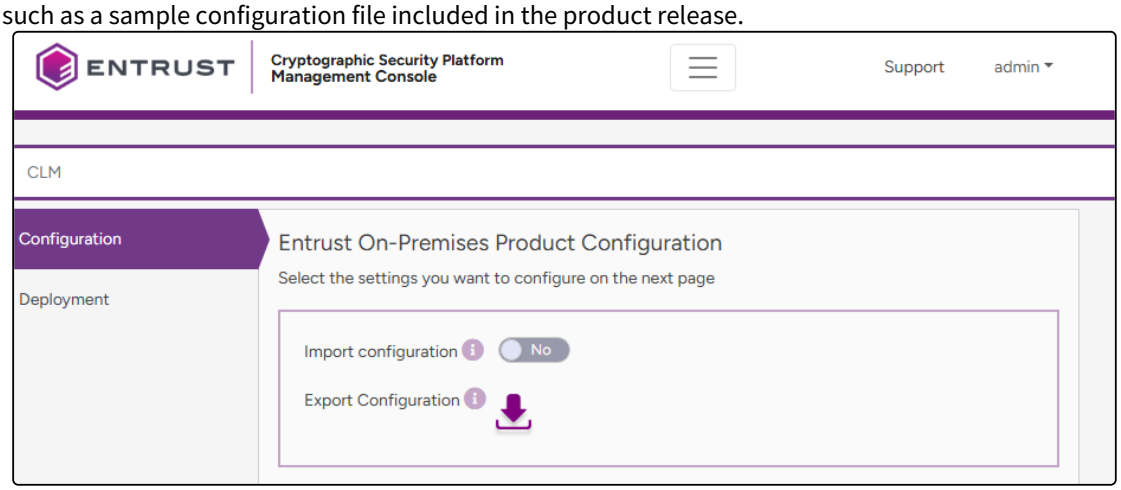
2. Log in to the Management Console as a user belonging to a role with Certificate Manager management permissions – for example, the initial `admin` administrator user.

   See Managing identities 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.

> ⛔ The databases for the cluster and the solutions can be hosted on the same DBMS. However, do not merge tables from different solutions into a single database. Both the cluster and each solution require their own dedicated 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

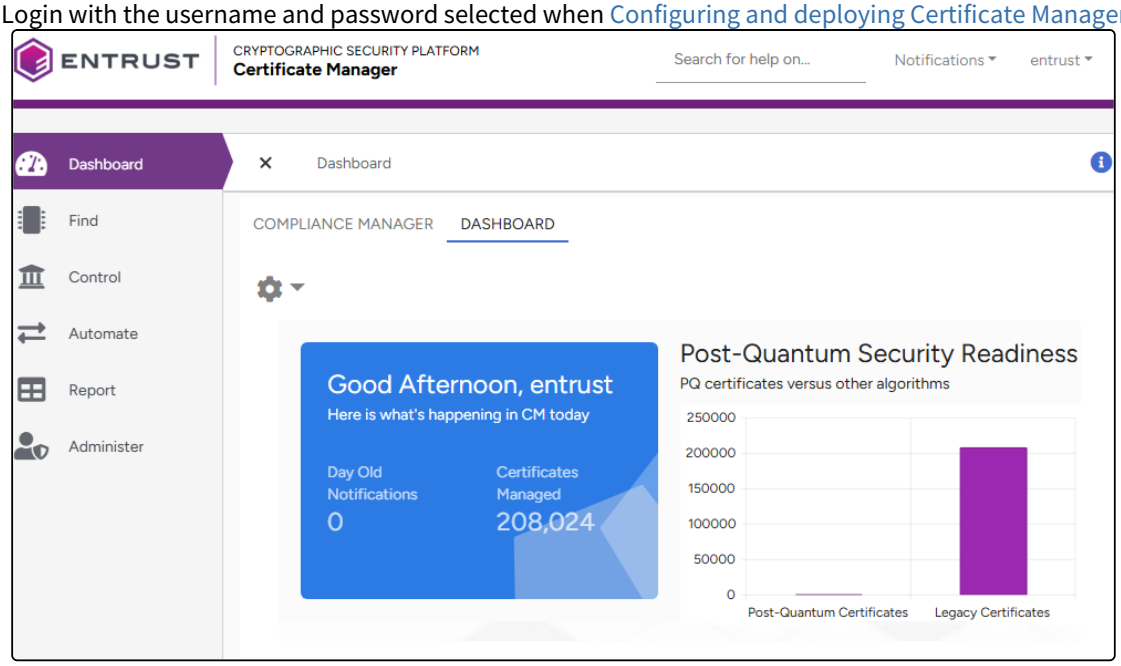
Once deployed, you can use Certificate Manager to manage certificate issuance and lifecycle.

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 https://www.entrust.com/resources/tools/entrust-discovery-scanner/download
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	www.example.com
An individual IP address	192.51.100.20
A comma-separated list of IP addresses or hostnames	www.example.com,192.51.100.2
A range of IP addresses using CIDR notation	192.51.100.0/24
A range of IP addresses, using a dash to separate the range	192.51.100.0-24

Schedule / Run Frequency

Select:

- **Manual** to run the scans when manually triggered.

- **Hourly, Daily, Weekly, Monthly**, to run the scans periodically at the specified moment.

Advanced / Hosts to Exclude

List of the hosts excluded from the scan, in any of the following formats.

```
192.0.2.0-100
```

```
192.0.2.0/24
```

```
www.example.com
```

```
www.example.com/16
```

Advanced / Resolve Hostnames

Configure the hostname resolution.

Option	Hostname resolution
Always	Performs a reverse DNS lookup of the hostname before contacting each host.
Never	Do not resolve hostnames. Select this option for better performance.

Advanced / Check If Host's Alive First

Select whether to ping the hosts to check whether they are alive.

Option	Scanned hosts
Check node before sc an	Only the hosts that respond to an initial ping.
Assume all hosts are a live	All hosts. The agent will attempt to perform scans on every host until the scan is successful or it times out. Select this option if the ping response is disabled in some hosts.

Advanced / Host Order

Select the scan order.

Option	Scan order
Normal	Order in which hosts appear in the list.
Randomized	Random order. This option slows the scan rate but prevents false alarms triggered by intrusion detection systems.

Advanced / Scan Rate

Select the rate of the queries executed by each scan to discover certificates.

Higher rates are resource-consuming and can trigger false alarms in intrusion detection systems.

Scan Rate	Initial scan delay (ms)	Max attempts to reach host port	Max time before sending another probe (ms)	Max scan delay (ms)
Slowest	300000	10	300000	300000
Slower	15000	10	15000	15000
Slow	400	10	10000	1000
Normal	0	10	10000	1000
Aggressive	0	6	1250	10
Very Aggressive	0	2	300	5

Adding a scan configuration to a Discovery Scanner

After Creating the first scan configuration of a Discovery Scanner, you can add new scan configurations as explained below.

To add a scanner configuration to a Discovery Scanner

1. Log in as an administrator with the global_admin role.
2. Go to **Find > Discovery**.
3. In the content pane, click the checkbox of the Discovery Scanner for which you want to add a configuration.
4. Click **Configure**.
5. In the **Configure** dialog, click **New**.
6. Configure the following scan settings.
    - Scan Name
    - Description
    - Priority
    - Custom Ports

- Custom Hosts
- Schedule / Run Frequency
- Advanced / Hosts to Exclude
- Advanced / Resolve Hostnames
- Advanced / Check If Host's Alive First
- Advanced / Host Order
- Advanced / Scan Rate

7. Click **Save**.

Scan Name

The name of the scan configuration.

Description

A brief description of the scan configuration.

Priority

If scans might overlap, this setting determines which scan (if any) should take precedence. Use this setting to avoid impacting the performance of other scheduled scans by over-stressing network bandwidth.

Priority	Scan execution
Low	Only run if no high or normal priority scan is running. Thus, when starting a normal or high-priority scan, low-priority scans stop executing until the other, higher-priority scans finish.
High	Always. Suspend any other normal or low-priority scans until they are complete.
Normal	When no high-priority scan runs, any normal-priority scans can run simultaneously.

Some configurations can prevent low-priority scans from running at all.

Custom Ports

The ports to run the certificate scan for every host listed in the **Custom Hosts** field. This field supports 255 characters in one of the following syntaxes.

- An individual port. For example 1443
- A comma-separated list of ports. For example 1400, 1443
- A port range. For example, 1400-1443

Please use a second scan if you require more space to specify ports.

The certificate scan will fail when providing invalid custom ports.

Custom Hosts

The hosts to scan for certificates. The value of this setting supports the following syntaxes.

Syntax	Example
An individual hostname	www.example.com
An individual IP address	192.51.100.20
A comma-separated list of IP addresses or hostnames	www.example.com,192.51.100.2
A range of IP addresses using CIDR notation	192.51.100.0/24
A range of IP addresses, using a dash to separate the range	192.51.100.0-24

Schedule / Run Frequency

Select:

- **Manual** to run the scans when manually triggered.
- **Hourly, Daily, Weekly, Monthly**, to run the scans periodically at the specified moment.

Advanced / Hosts to Exclude

List of the hosts excluded from the scan, in any of the following formats.

```
192.0.2.0-100
```

```
192.0.2.0/24
```

```
www.example.com
```

```
www.example.com/16
```

Advanced / Resolve Hostnames

Configure the hostname resolution.

Option	Hostname resolution
Always	Performs a reverse DNS lookup of the hostname before contacting each host.
Never	Do not resolve hostnames. Select this option for better performance.

Advanced / Check If Host's Alive First

Select whether to ping the hosts to check whether they are alive.

Option	Scanned hosts
Check node before sc an	Only the hosts that respond to an initial ping.
Assume all hosts are a live	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
Aggressi ve	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.

> 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	www.example.com
An individual IP address	192.51.100.20
A comma-separated list of IP addresses or hostnames	www.example.com,192.51.100.2
A range of IP addresses using CIDR notation	192.51.100.0/24
A range of IP addresses, using a dash to separate the range	192.51.100.0-24

Schedule / Run Frequency

Select:

- **Manual** to run the scans when manually triggered.

- **Hourly, Daily, Weekly, Monthly**, to run the scans periodically at the specified moment.

Advanced / Hosts to Exclude

List of the hosts excluded from the scan, in any of the following formats.

```
192.0.2.0-100
```

```
192.0.2.0/24
```

```
www.example.com
```

```
www.example.com/16
```

Advanced / Resolve Hostnames

Configure the hostname resolution.

Option	Hostname resolution
Always	Performs a reverse DNS lookup of the hostname before contacting each host.
Never	Do not resolve hostnames. Select this option for better performance.

Advanced / Check If Host's Alive First

Select whether to ping the hosts to check whether they are alive.

Option	Scanned hosts
Check node before sc an	Only the hosts that respond to an initial ping.
Assume all hosts are a live	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.

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://172.30.141.341:5696/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

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 **Profile Key Type** is **Unspecified**.

Mandatory: When requested by the selected **Profile**.

Select allowed key types

The key types supported by the Certificate Signing Requests.

Profile	Field visibility
A PKCS #12 profile (the CA generates the keys)	Never displayed.
A CSR profile	Only displayed when **Profile Key Type** is **Unspecified** or **Override key type** is enabled.

Mandatory: When requested by the selected **Profile**.

Minimum RSA Key Length

The minimum bit length for the RSA-type keys.

Profile	Field visibility
A PKCS #12 profile (the CA generates the keys)	Never displayed.
A CSR profile	Always displayed.

Mandatory: When requested by the selected **Profile**.

Editing a public enrollment form

See below for editing the settings of a public enrollment form.

To edit a public enrollment form

1. Log in as an administrator with either:
    - The global_admin role.
    - The <ca>_admin role for the certificate authority configured in the public enrollment form.
    - A Certificate Role for the same certificate authority and certificate profile configured in the public enrollment form.
2. Go to **Control > Public Enrollment Forms**.
3. Go to **Control > Custom fields**.
4. In the main grid, select a custom field.
5. click **Edit** to update the following settings.
    - Active
    - Name
    - Owner
    - Description
    - Custom Fields
    - Authority
    - Profile
    - Profile Key Type
    - Override required key type
    - Select allowed key types
    - Minimum RSA Key Length

Active

Check this box for the public enrollment form to be accessible; uncheck otherwise.

Name

The identifier of the public enrollment form.

Owner

The email address of the person responsible for the public enrollment form.

> The user who creates the public enrollment form is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the public enrollment form.

Custom Fields

The Custom Fields whose value will be requested by the public enrollment form.

Authority

The Authority to issue the enrolled certificates.

Profile

The certificate authority profile to issue the enrolled certificates.

Profile Key Type

The key type specified by the **Profile**, if any.

Override required key type

Whether to override the **Profile Key Type** and allow different key types.

Profile	Field visibility
A PKCS #12 profile (the CA generates the keys)	Never displayed.
A CSR profile	Only displayed when **Profile Key Type** is **Unspecified**.

Mandatory: When requested by the selected **Profile**.

Select allowed key types

The key types supported by the Certificate Signing Requests.

Profile	Field visibility
A PKCS #12 profile (the CA generates the keys)	Never displayed.
A CSR profile	Only displayed when **Profile Key Type** is **Unspecified** or **Override key type** is enabled.

Mandatory: When requested by the selected **Profile**.

Minimum RSA Key Length

The minimum bit length for the RSA-type keys.

Profile	Field visibility
A PKCS #12 profile (the CA generates the keys)	Never displayed.
A CSR profile	Always displayed.

Mandatory: When requested by the selected **Profile**.

Deleting public enrollment forms

See below for deleting public enrollment forms.

To delete public enrollment forms

1. Log in as an administrator with either:
   - The global_admin role.

- The <ca>_admin role for the certificate authority configured in the public enrollment forms.
- A Certificate Role for the certificate authority and certificate profile configured in the public enrollment form.

2. Go to **Control > Public Enrollment Forms**.
3. In the main grid, select one or more public enrollment forms.
4. Click **Delete** to remove the selected public enrollment forms.

Using public enrollment forms

As explained below, end-users can request certificates using public enrollment forms.

To request a certificate using a public enrollment form

1. Ask the administrator for the public link generated when Creating a public enrollment form.

   The administrator must share this link out-of-band because the form does not require access credentials.

2. Fill in the form fields.
3. Submit the form.
4. Copy the link displayed on the submission information page
5. Use this link to check the request processing status and eventually download the certificate.

Requests For Approval

Manage the "internal" and "external" pending certificate requests.

Request type	Description
Internal	Created as explained in Making a certificate request by registered Administrators logged in to Certificate Manager.
External	Created by non-registered users from a Public Enrollment Form configured by an Administrator and published to a publicly accessible URL.

See below for the supported operations.

- Browsing pending requests
- Approving a pending certificate request
- Rejecting a pending certificate request

The default retention period for certificate requests is 365 days. See General for how to change this period.

Browsing pending requests

See below for browsing the certificate issuance and renewal requests.

To browse pending requests

1. Log in as an administrator with one of the following roles.
   - The global_admin role.
   - The <ca>_admin role for the certificate authority configured in the requests.
   - A Certificate Role for the certificate authority and certificate profile configured in the requests.
2. Go to **Control > Requests For Approval**.

3. Define request views.
    - Unfold the **Columns** list to select the properties you want to display as columns.
    - Click **Show Filter Options** to display a filtering form below each column name.
    - Select **Show Filter Options / Remove all filters** to remove all filters.
    - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
    - Click **Show Filter Options** to hide the filtering options and keep the filters.
    - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
    - Click **Reset layout** to remove all the column and filter customizations.
    - Click the refresh icon to rerun the query with the current filters.

    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 Making a certificate request or Requesting a certificate renewal.
<public_form>	Request created by non-registered users using the Public Enrollment Form with `<public_form>` name.

Associated Certificate

The issued certificate (if any).

Actions

The actions supported by the pending request

- Approving a pending certificate request
- Rejecting a pending certificate request

Key Manager

The Key Manager that will generate the key pair, if any.

> This field is only available in PKCS#12 requests.

Request ID

The request identifier.

> Certificate Manager automatically generates this value.

BASIC INFO

Click the plus button and select the **BASIC INFO** tab to display additional basic information.

Setting	Description
Requestor	The email address entered by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request.
Description	The certificate description entered by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request.
Status	The status of the certificate requests are Pending, Approved and Rejected.
Comment	The reason behind rejecting a certificate request, if request gets rejected.
Date Created	The date when an end-user requested the certificate using a Public Enrollment Form published online, or an administrator requested the certificate as explained in Making a certificate request.
Last Modified	The date of the latest request modification, whether it should be request creation, request approval or request rejection.
Authority	The issuing certificate authority configured in a Public Enrollment Form published online, or selected by an administrator as explained in Making a certificate request.
Profile	The certificate authority profile configured for a Public Enrollment Form published online, or selected by an administrator as explained in Making a certificate request.

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 Public Enrollment Form published online, or pasted by an administrator as explained in Making a certificate request.
SAN	The subject alternative name (SAN) entered by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request.
Subject Variables	The certificate subject variables, if required by the selected profile defined by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request.

DESTINATIONS

Click the plus button ⊕ and select the **DESTINATIONS** tab to display the destination an administrator selected when Making a certificate request.

ACCESS TAGS

Click the plus button ⊕ and select the **ACCESS TAGS** tab to display the Certificate Access Tags:

- Entered by an administrator as explained in Making a certificate request.
- Entered by an administrator when approving the certificate request.

CUSTOM FIELDS

Click the plus button ⊕ and select the **CUSTOM FIELDS** tab to display the Custom Fields an administrator entered when Making a certificate request.

CSR INFORMATION

Click the plus button ⊕ and select the **CSR INFORMATION** tab to display additional request information.

ℹ 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 Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request.
Description	The certificate description entered by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request.
Status	The status of the certificate requests are Pending, Approved and Rejected.
Comment	The reason behind rejecting a certificate request, if request gets rejected.
Date Created	The date when an end-user requested the certificate using a Public Enrollment Form published online, or an administrator requested the certificate as explained in Making a certificate request.
Last Modified	The date of the latest request modification, whether it should be request creation, request approval or request rejection.
Authority	The issuing certificate authority configured in a Public Enrollment Form published online, or selected by an administrator as explained in Making a certificate request.
Profile	The certificate authority profile configured for a Public Enrollment Form published online, or selected by an administrator as explained in Making a certificate request.

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 Public Enrollment Form published online, or pasted by an administrator as explained in Making a certificate request.
SAN	The subject alternative name (SAN) entered by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request.
Subject Variables	The certificate subject variables, if required by the selected profile defined by an end-user on a Public Enrollment Form published online, or entered by an administrator as explained in Making a certificate request.

DESTINATIONS

Click the plus button ⊕ and select the **DESTINATIONS** tab to display the destination an administrator selected when Making a certificate request.

ACCESS TAGS

Click the plus button ⊕ and select the **ACCESS TAGS** tab to display the Certificate Access Tags:

- Entered by an administrator as explained in Making a certificate request.
- Entered by an administrator when approving the certificate request.

CUSTOM FIELDS

Click the plus button ⊕ and select the **CUSTOM FIELDS** tab to display the Custom Fields an administrator entered when Making a certificate request.

CSR INFORMATION

Click the plus button ⊕ and select the **CSR INFORMATION** tab to display additional request information.

ℹ 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

ℹ See Key Managers for creating key managers and techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Destinations

If required by the certificate profile, add one or more Destinations to publish the issued certificate.

⚠ If you selected a Key Manager, ensure the **Allow private key export** option is enabled on this Key Manager to add additional destinations for this certificate.

To add a destination

1. In the **Destinations** list, select a destination previously created as explained in the following sections.
   - Creating a HashiCorp Vault destination
   - Creating a Microsoft IIS web server destination
   - Creating an Apache web server destination
   - Creating an AWS Certificate Manager destination
   - Creating an Azure Key Vault destination
   - Creating an F5 BIG-IP destination
   - Creating an Nginx web server destination
   - Creating an SFTP destination
2. Click **Add** to confirm the selection.

   ⚠ Apache and Nginx destinations do not support adding several destinations or other key managers.
3. If required, configure destination-specific parameters.

- F5 BIG-IP destination-specific settings
- Microsoft IIS destination-specific settings

F5 BIG-IP destination-specific settings

Configure the following additional settings when adding a destination of the F5 BIG-IP type.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

See techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Microsoft IIS destination-specific settings

When adding a destination of the Microsoft IIS type, enter one or more site bindings in the **Site bindings** field. Define each binding with a line in the following syntax.

```
<name>;<host>;<port>
```

Where:

- `<name>` is the website name
- `<host>` is the website hostname or IP address
- `<port>` is the port for connecting to the website.

Select a certificate profile with "Web Server" or dual usage (key encipherment and digital signature) to deploy the certificate successfully.

Profile Options

Configure the following settings in the **Profile Options** form of the **Make Request** wizard.

- Certificate Signing Request (CSR)
- Password
- Subject Variable Requirements
- Subject Alternative Names
- Expected Subject DN

Certificate Signing Request (CSR)

The PEM or Base64 encoding of a CSR (Certificate Signing Request).

This field is only present when the selected certificate profile issues certificates from CSR. In this issuance mode:

- The user generates the key pair and the CSR.
- The CA processes the CSR and issues the certificate.
- The user downloads the certificate.

When selecting Apache, Nginx, or Microsoft IIS certificate destinations, Certificate Manager ignores any client-generated CSR and uses instead a CSR generated at the destination along with the key pair.

Password

A password for the generated P12.

This field is only present when the selected certificate profile issues certificates in P12 files. In this issuance mode:

1. The CA generates the key pair.
2. The user downloads both the certificate and the private key in a P12 file protected with the selected password.

Subject Variable Requirements

Variable values to build:

- The subject's distinguished name for the CSR, if using a Key Manager.
- The expected subject's distinguished name otherwise.

This field is mandatory when required by the selected profile.

Certificate renewals reuse the value of Subject variables, such as Subject DN, entered at issuance. Thus, the value of these variables is read-only during renewal.

Subject Alternative Names

The list of subject alternative names (SAN) for the certificate.

Expected Subject DN

The Subject DN (Distinguished Name) that Certificate Manager will generate using the configured values. This field is read-only.

Renewal

If supported by the selected profile, you can check the **Auto Renewal** box and configure the following settings.

- Renewal Period
- PKCS12 Password

Renewal Period

The day the certificate must be renewed, as a number of days before the certificate expiry. For a certificate that expires in E days and a **Renewal Period** set to P, the renewal starts in E-P days. At 12:00 AM UTC every day, a background process collects the certificates that:

- Must be renewed the same day because E-P=0
- Failed a previous renewal because E-P<0

For example, to force a certificate renewal the next day, set a P value equal to E-1 before 12:00 AM UTC. At 12:00 AM UTC, E-P will equal 0, and the certificate will be included in the renewal queue for that day.

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	Find
Imported into Certificate Manager	Importing certificates
Imported into Certificate Manager using the Certificate Manager API	Certificate Manager API
Issued using the Certificate Manager Web browser interface	Creating a certificate
Provided by a source and inserted with source synchronization operations	Sources
Imported with key manager synchronization operations	Key Managers

Operations you can take include:

- Browsing certificates
- Creating a certificate
- Automating certificate renewal
- Manually renewing a certificate
- Requesting a certificate renewal
- Editing a single certificate
- Editing certificates in bulk
- Revoking a certificate
- Revoking certificates in bulk
- Releasing a certificate from hold
- Exporting a certificate
- Importing certificates
- Archiving certificates
- Archiving certificates in bulk

Browsing certificates

See below for browsing the certificates managed by Certificate Manager.

To browse certificates

1. Go to **Control > Certificates**.
2. Click **Show Insights** at the top-right to display information such as:
    - The total number of issued certificates.
    - The total number of certificates issued, expired, renewed, suspended, revoked, or archived.

- The number of post-quantum certificates issued, expired, renewed, suspended, revoked, or archived.

3. Define grid certificate views.
   - Unfold the **Columns** list to select the properties you want to display as columns.
   - Click **Show Filter Options** to display a filtering form below each column name.
   - Select **Show Filter Options / Remove all filters** to remove all filters.
   - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
   - Click **Show Filter Options** to hide the filtering options and keep the filters.
   - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
   - Click **Reset layout** to remove all the column and filter customizations.
   - Click the refresh icon to rerun the query with the current filters.

   > 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 Source.
Serial	The serial number (SN) of the certificate.
Valid From	The **Not Before** date of the certificate.
Valid To	The **Not After** date of the certificate.
Last Modified	The time and date of the latest Key State modification.
SAN	The list of subject alternative names (SAN) of the certificate.
Key Length	The length of the certificate key.
Signature Algorithm	The hash signature algorithm and the Signing Algorithm Security Level
Key Algorithm	The key-pair generation algorithm and the Key Algorithm Security Level.
Validity	The certificate status: Empty for certificates from unknown sources (because either imported or discovered); **Issued** for certificates from known sources and still valid; **Revoked** for certificates from known sources and already revoked as explained in Revoking a certificate.
Requested Properties	Additional properties included in the certificate request.

ACCESS TAGS

The list of Certificate Access Tags.

> The Certificate Roles with any of these tags will grant permissions on the certificate.

CUSTOM FIELDS

The business-specific Custom Fields defined by your organization.

EXISTING DESTINATIONS

The list of Destinations where Certificate Manager has pushed the certificate.

RENEWAL DESTINATIONS

The list of Destinations where Certificate Manager will push the certificate upon auto-renewal.

DOMAINS

The **DOMAINS** tab to display the list of certified domains.

REPLACES

The certificate renewed by the current certificate.

ENDPOINTS

The Endpoint where a Discovery Scanner discovered the certificate (if any).

Setting	Description
Host Name	The name of the endpoint host.
Port	The endpoint port.
Service	The service exposed on the endpoint.
Service Vendor	The vendor of the service exposed on the endpoint.
Service Vendor Version	The version of the vendor services exposed on the endpoint.
Cipher Suites	The list of cipher suites that a service accepts.
OS Type	The operating system type of the endpoint.
Completed	The time and date the certificate discovery scan was completed.

CERTIFICATES

The PEM encoding of:

- The certificate.

- The certificate certification chain.
- The certificate signing request (CSR).

Creating a certificate

See below for creating a certificate in Certificate Manager.

To create a certificate

1. Log in as an administrator with one of the following roles.
   - The global_admin role.
   - The <ca>_admin role for the certificate authority that will issue the certificate.
   - A Certificate Role with permissions to create certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. Click **Create.**
4. Fill in the following forms of the **Create** wizard.
   - General
   - Destinations
   - Profile Options
   - Renewal
5. Click **Create** to create the certificate.
6. Wait until a notification in the bottom right corner of the Certificate Manager UI announces the certificate issuance.
7. Click the download link in the notification. You can also download the certificate from:
   - The list of notifications in the top-right **Notifications** menu.
   - The certificates view described in Browsing certificates.

General

Configure the following settings in the **General** form of the **Create** wizard.

- Owner
- Description
- <custom>
- Access Tags
- Certificate Authority
- Certificate Profile
- Use a key manager (KMS) to generate the key pair

Owner

The email address of the person responsible for the certificate – for example, the Web server operator.

Mandatory: Yes

Description

A brief description of the certificate purpose.

Mandatory: No

<custom>

Business-specific Custom Fields defined by your organization.

Mandatory: No

Access Tags

One or several Certificate Access Tags.

> Certificate Roles with any of these tags will grant permissions on the certificate.

Mandatory: No

Certificate Authority

The certificate authority that issues the certificate. See Authorities for how to register certificate authorities.

Mandatory: Yes

Certificate Profile

The certificate profile the certificate authority applies to issue the certificate. For certificates to be published in Destinations, consider the following profile limitations.

Destination	Limitations
Apache	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).
Azure	Does not support issuing certificates from a CSR.
Nginx	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).

> The selected certificate profile must be configured in CA Gateway for the Certificate Authority.

Mandatory: Yes

Use a key manager (KMS) to generate the key pair

To generate the certificate key pair with a key manager, check this box and select a key manager from the **Key Manager** list.

For the key managers described in Creating a F5 BIG-IP key manager, also configure the settings in the table below.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

> See Key Managers for creating key managers and techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Destinations

If required by the certificate profile, add one or more Destinations to publish the issued certificate.

> ⚠ If you selected a Key Manager, ensure the **Allow private key export** option is enabled on this Key Manager to add additional destinations for this certificate.

To add a destination

1. In the **Destinations** list, select a destination previously created as explained in the following sections.
   - Creating a HashiCorp Vault destination
   - Creating a Microsoft IIS web server destination
   - Creating an Apache web server destination
   - Creating an AWS Certificate Manager destination
   - Creating an Azure Key Vault destination
   - Creating an F5 BIG-IP destination
   - Creating an Nginx web server destination
   - Creating an SFTP destination
2. Click **Add** to confirm the selection.

   > ⚠ Apache and Nginx destinations do not support adding several destinations or other key managers.
3. If required, configure destination-specific parameters.
   - F5 BIG-IP destination-specific settings
   - Microsoft IIS destination-specific settings

F5 BIG-IP destination-specific settings

Configure the following additional settings when adding a destination of the F5 BIG-IP type.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

> ℹ See techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Microsoft IIS destination-specific settings

When adding a destination of the Microsoft IIS type, enter one or more site bindings in the **Site bindings** field. Define each binding with a line in the following syntax.

```
<name>;<host>;<port>
```

Where:

- `<name>` is the website name
- `<host>` is the website hostname or IP address

- `<port>` is the port for connecting to the website.

> ⚠ Select a certificate profile with "Web Server" or dual usage (key encipherment and digital signature) to deploy the certificate successfully.

Profile Options

Configure the following settings in the **Profile Options** form of the **Create** wizard.

- Certificate Signing Request (CSR)
- Password
- Requested Properties
- Subject Alternative Names
- Subject DN for CSR

Certificate Signing Request (CSR)

The PEM or Base64 encoding of a CSR (Certificate Signing Request).

This field is only present when the selected certificate profile issues certificates from CSR. In this issuance mode:

- The user generates the key pair and the CSR.
- The CA processes the CSR and issues the certificate.
- The user downloads the certificate.

> 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.

Requested Properties

Additional properties of the selected profile (if any).

Subject Alternative Names

The list of subject alternative names (SAN) for the certificate.

Subject DN for CSR

The distinguished name of the certificate subject. This field is mandatory when:

- The selected certificate profile issues certificates from CSRs, and
- The **Use Subject DN from CSR** checkbox is not marked.

Renewal

If supported by the selected profile, you can check the **Auto Renewal** box and configure the following settings.

- Renewal Period

- PKCS12 Password

Renewal Period

The day the certificate must be renewed, as a number of days before the certificate expiry. For a certificate that expires in E days and a **Renewal Period** set to P, the renewal starts in E-P days. At 12:00 AM UTC every day, a background process collects the certificates that:

- Must be renewed the same day because E-P=0
- Failed a previous renewal because E-P<0

For example, to force a certificate renewal the next day, set a P value equal to E-1 before 12:00 AM UTC. At 12:00 AM UTC, E-P will equal 0, and the certificate will be included in the renewal queue for that day.

> The restrictions imposed by Apache, Nginx, or Microsoft IIS destinations on other issuance modes do not affect automated renewal. Specifically, these destinations support automated renewal with client-side generated keys and CSRs.

PKCS12 Password

The password of the PKCS #12 for delivering the certificate and its private key in the selected **Destinations**.

> This password is encrypted and stored in the application database.

Automating certificate renewal

See below for automating the successive renewals of a certificate.

> As explained in Creating a certificate, you can configure the certificate renewal on certificate creation.

To automate the renewal of a certificate

1. Log in as an administrator with one of the following roles.
   - The <ca>_admin role for the certificate authority that will renew the certificate.
   - A Certificate Role with permission to create certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. In the main grid, click **Select Action > Automate** for the certificate.
4. Configure the following settings.
   - Certificate Authority
   - Certificate Profile
   - Destinations
   - Key Manager
   - Renewal

Certificate Authority

The certificate authority that issues the certificate. See Authorities for how to register certificate authorities.

Certificate Profile

The certificate profile the certificate authority applies to issue the certificate.

⚠ The selected certificate profile must be configured in CA Gateway for the certificate authority.

Destinations

If required by the certificate profile, add one or more Destinations to publish the issued certificate.

⚠ If you selected a Key Manager, ensure the **Allow private key export** option is enabled on this Key Manager to add additional destinations for this certificate.

To add a destination

1. In the **Destinations** list, select a destination previously created as explained in the following sections.
   - Creating a HashiCorp Vault destination
   - Creating a Microsoft IIS web server destination
   - Creating an Apache web server destination
   - Creating an AWS Certificate Manager destination
   - Creating an Azure Key Vault destination
   - Creating an F5 BIG-IP destination
   - Creating an Nginx web server destination
   - Creating an SFTP destination
2. Click **Add** to confirm the selection.

   ⚠ Apache and Nginx destinations do not support adding several destinations or other key managers.
3. If required, configure destination-specific parameters.
   - F5 BIG-IP destination-specific settings
   - Microsoft IIS destination-specific settings

F5 BIG-IP destination-specific settings

Configure the following additional settings when adding a destination of the F5 BIG-IP type.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

ℹ See techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Microsoft IIS destination-specific settings

When adding a destination of the Microsoft IIS type, enter one or more site bindings in the **Site bindings** field. Define each binding with a line in the following syntax.

```
<name>;<host>;<port>
```

Where:

- `<name>` is the website name
- `<host>` is the website hostname or IP address
- `<port>` is the port for connecting to the website.

⚠ Select a certificate profile with "Web Server" or dual usage (key encipherment and digital signature) to deploy the certificate successfully.

Key Manager (auto)

If required by the certificate profile, select the key manager that will generate the key pair.

For the key managers described in Creating a F5 BIG-IP key manager, also configure the settings in the table below.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

ℹ See Key Managers for creating key managers and techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Renewal

If supported by the selected profile, you can check the **Auto Renewal** box and configure the following settings.

- Renewal Period
- PKCS12 Password

Renewal Period

The day the certificate must be renewed, as a number of days before the certificate expiry. For a certificate that expires in E days and a **Renewal Period** set to P, the renewal starts in E-P days. At 12:00 AM UTC every day, a background process collects the certificates that:

- Must be renewed the same day because E-P=0
- Failed a previous renewal because E-P<0

For example, to force a certificate renewal the next day, set a P value equal to E-1 before 12:00 AM UTC. At 12:00 AM UTC, E-P will equal 0, and the certificate will be included in the renewal queue for that day.

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.

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

ℹ See Key Managers for creating key managers and techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Destinations

If required by the certificate profile, add one or more Destinations to publish the issued certificate.

⚠ If you selected a Key Manager, ensure the **Allow private key export** option is enabled on this Key Manager to add additional destinations for this certificate.

To add a destination

1. In the **Destinations** list, select a destination previously created as explained in the following sections.
   - Creating a HashiCorp Vault destination
   - Creating a Microsoft IIS web server destination
   - Creating an Apache web server destination
   - Creating an AWS Certificate Manager destination
   - Creating an Azure Key Vault destination

- Creating an F5 BIG-IP destination
- Creating an Nginx web server destination
- Creating an SFTP destination

2. Click **Add** to confirm the selection.

> ⚠ Apache and Nginx destinations do not support adding several destinations or other key managers.

3. If required, configure destination-specific parameters.
   - F5 BIG-IP destination-specific settings
   - Microsoft IIS destination-specific settings

F5 BIG-IP destination-specific settings

Configure the following additional settings when adding a destination of the F5 BIG-IP type.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

> ℹ See techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Microsoft IIS destination-specific settings

When adding a destination of the Microsoft IIS type, enter one or more site bindings in the **Site bindings** field. Define each binding with a line in the following syntax.

```
<name>;<host>;<port>
```

Where:

- `<name>` is the website name
- `<host>` is the website hostname or IP address
- `<port>` is the port for connecting to the website.

> ⚠ Select a certificate profile with "Web Server" or dual usage (key encipherment and digital signature) to deploy the certificate successfully.

Profile Options

Configure the following settings in the **Profile Options** form of the **Renew** wizard.

- Certificate Signing Request (CSR)
- Password
- Subject DN for CSR
- Subject Variable Requirements
- Subject Alternative Names

Certificate Signing Request (CSR)

The PEM or Base64 encoding of a CSR (Certificate Signing Request).

This field is only present when the selected certificate profile issues certificates from CSR. In this issuance mode:

- The user generates the key pair and the CSR.
- The CA processes the CSR and issues the certificate.
- The user downloads the certificate.

> 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.

> 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.

Requesting a certificate renewal

See below for requesting the renewal of a certificate.

To request the renewal of a certificate

1. Log in as an administrator with one of the following roles.
   - The <ca>_admin role for the certificate authority that will renew the certificate.
   - A Certificate Role with request permission for the same certificate authority and selected certificate profile.
2. Go to **Control > Certificates**.
3. In the main grid, click **Select Action > Request Renew** for a certificate.
4. Fill in the following forms of the **Renew** wizard.
   - General
   - Destinations
   - Profile options
   - Automate Options
5. Click **Create** to create the certificate renewal request.
6. Browse the request status as explained in Browsing my certificate requests and Browsing pending requests.

General

Configure the following settings in the **General** form of the **Renewal** wizard.

- Owner
- Description
- <custom>
- Access Tags
- Certificate Authority
- Certificate Profile
- Use a key manager (KMS) to generate the key pair

Owner

The email address of the person responsible for the certificate – for example, the Web server operator.

Description

A brief description of the certificate purpose.

<custom>

Business-specific Custom Fields defined by your organization.

Access Tags

One or several Certificate Access Tags.

> Certificate Roles with any of these tags will grant permissions on the certificate.

Certificate Authority

The certificate authority that issues the certificate. See Authorities for how to register certificate authorities.

Certificate Profile

The certificate profile the certificate authority applies to issue the certificate. For certificates to be published in Destinations, consider the following profile limitations.

Destination	Limitations
Apache	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).
Azure	Does not support issuing certificates from a CSR.
Nginx	Requires a certificate profile with "Web Server" or dual usage (key encipherment and digital signature).

> The selected certificate profile must be configured in CA Gateway for the Certificate Authority.

Use a key manager (KMS) to generate the key pair

To generate the certificate key pair with a key manager, check this box and select a key manager from the **Key Manager** list.

For the key managers described in Creating a F5 BIG-IP key manager, also configure the settings in the table below.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

> See Key Managers for creating key managers and techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Destinations

If required by the certificate profile, add one or more Destinations to publish the issued certificate.

> ⚠ If you selected a Key Manager, ensure the **Allow private key export** option is enabled on this Key Manager to add additional destinations for this certificate.

To add a destination

1. In the **Destinations** list, select a destination previously created as explained in the following sections.
   - Creating a HashiCorp Vault destination
   - Creating a Microsoft IIS web server destination
   - Creating an Apache web server destination
   - Creating an AWS Certificate Manager destination
   - Creating an Azure Key Vault destination
   - Creating an F5 BIG-IP destination
   - Creating an Nginx web server destination
   - Creating an SFTP destination
2. Click **Add** to confirm the selection.

   > ⚠ Apache and Nginx destinations do not support adding several destinations or other key managers.
3. If required, configure destination-specific parameters.
   - F5 BIG-IP destination-specific settings
   - Microsoft IIS destination-specific settings

F5 BIG-IP destination-specific settings

Configure the following additional settings when adding a destination of the F5 BIG-IP type.

Setting	Value
Client SSL Profile	A BIG-IP Client SSL profile
Server SSL Profile	A BIG-IP Server SSL profile

> ℹ See techdocs.f5.com for a reference of the supported BIG-IP Client SSL profiles.

Microsoft IIS destination-specific settings

When adding a destination of the Microsoft IIS type, enter one or more site bindings in the **Site bindings** field. Define each binding with a line in the following syntax.

```
<name>;<host>;<port>
```

Where:

- `<name>` is the website name
- `<host>` is the website hostname or IP address

- `<port>` is the port for connecting to the website.

⚠ Select a certificate profile with "Web Server" or dual usage (key encipherment and digital signature) to deploy the certificate successfully.

Profile Options

Configure the following settings in the **Profile Options** form of the **Renewal** wizard.

- Certificate Signing Request (CSR)
- Password
- Subject Variable Requirements
- Subject Alternative Names

Certificate Signing Request (CSR)

The PEM or Base64 encoding of a CSR (Certificate Signing Request).

This field is only present when the selected certificate profile issues certificates from CSR. In this issuance mode:

- The user generates the key pair and the CSR.
- The CA processes the CSR and issues the certificate.
- The user downloads the certificate.

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.

Renewal

If supported by the selected profile, you can check the **Auto Renewal** box and configure the following settings.

- Renewal Period
- PKCS12 Password

Renewal Period

The day the certificate must be renewed, as a number of days before the certificate expiry. For a certificate that expires in E days and a **Renewal Period** set to P, the renewal starts in E-P days. At 12:00 AM UTC every day, a background process collects the certificates that:

- Must be renewed the same day because E-P=0
- Failed a previous renewal because E-P<0

For example, to force a certificate renewal the next day, set a P value equal to E-1 before 12:00 AM UTC. At 12:00 AM UTC, E-P will equal 0, and the certificate will be included in the renewal queue for that day.

> The restrictions imposed by Apache, Nginx, or Microsoft IIS destinations on other issuance modes do not affect automated renewal. Specifically, these destinations support automated renewal with client-side generated keys and CSRs.

PKCS12 Password

The password of the PKCS #12 for delivering the certificate and its private key in the selected **Destinations**.

> This password is encrypted and stored in the application database.

Editing a single certificate

See below for editing the settings of a single certificate.

To edit a single certificate

1. Log in as an administrator with one of the following roles.
   - The global_admin role.
   - The <ca>_admin role for the certificate authority that issued the certificate.
   - A Certificate Role with permission to edit certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. In the main grid, click **Select Action > Edit** for one of the listed certificates.
4. Update the value of the following editable certificate settings.
   - Owner
   - Description
   - Access Tags
   - <custom>

Owner

The email address of the person responsible for the certificate – for example, the Web server operator.

Description

A brief description of the certificate purpose.

Access Tags

One or several Certificate Access Tags.

Certificate Roles with any of these tags will grant permissions on the certificate.

<custom>

Business-specific Custom Fields defined by your organization.

Editing certificates in bulk

See below for editing certificate settings in bulk.

To edit certificates in bulk

1. Log in as an administrator with one of the following roles.
   - The global_admin role.
   - The <ca>_admin role for the certificate authority that issued the certificates.
   - A Certificate Role with permission to edit certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. Click **Bulk Actions**.
4. In the **Select bulk actions** drop-down list, select **Edit**.
5. Configure a filter for the certificates you want to edit. Use the filter options to combine several filters.
6. In the **Select field** drop-down list, select the name of an editable field.
   - Owner
   - Description
   - Access Tags
   - <custom>
7. In the **Value** drop-down list, type a new value for the selected field.
8. Click **Add**. You can optionally select and add more fields to modify.
9. Click **Save** to add all the certificates matching the filter to the edit background task.

   An `INFO` log will indicate the number of updated certificates upon task completion.

Owner

The email address of the person responsible for the certificate – for example, the Web server operator.

Description

A brief description of the certificate purpose.

Access Tags

One or several Certificate Access Tags.

Certificate Roles with any of these tags will grant permissions on the certificate.

<custom>

Business-specific Custom Fields defined by your organization.

Revoking a certificate

See below for revoking the validity of a certificate before the certificate expiration date.

To revoke a certificate

1. Log in as an administrator with one of the following roles:
   - The global_admin role.
   - The <ca>_admin role for the certificate authority that issued the certificate.
   - A Certificate Role with permission to revoke certificates for the same certificate authority and certificate profile.
2. Go to **Control > Certificates**.
3. In the main grid, slick **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.

   ℹ 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.

ℹ 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, slick **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.

> ℹ Any file may include the certificate chain in the same file.

<custom>

Business-specific Custom Fields defined by your organization.

> ℹ When importing many certificate files, the selected custom fields will apply to all the imported certificates.

Access Tags

One or several Certificate Access Tags.

> ℹ Certificate Roles with any of these tags will grant permissions on the certificate.

Archiving certificates

See below for archiving a certificate.

> 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.

   > 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:
    - Theglobal_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.

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 certificxate source to Certificate Manager.

- Creating a CA Gateway source
- Creating a F5 BIG-IP source
- Creating an Azure Key Vault source

Creating a CA Gateway source

See below for creating a source that connects Certificate Manager with the CAs managed by an Entrust CA Gateway instance.

If the CA you want to connect is an Entrust Certificate Authority initialized in a pre-8.4.10 release, please run the backfill script before creating the source to correct any missing or incorrect certificate event.

To create a CA Gateway source

1. Log in as an administrator with either:
   - The global_admin role.
   - A <user_defined> role with permission to create sources.
2. Go to **Automate > Sources**.
3. Click **Create** to configure the following settings.
   - Label
   - Owner
   - Description
   - Authorization Tags
   - Select Source Type
   - CA Gateway URL
   - Verify server certificate
   - Required PKCS#12 File
   - Required PKCS#12 Password
   - Optional PKCS#12 Truststore File
   - Optional Truststore Password
4. Click **Verify** for Certificate Manager to verify all the settings. Some plugins might ask for additional configuration settings after verification.

Label

A descriptive name of the source.

Mandatory: Yes

Owner

The username of the source owner. The user who creates the source is automatically made the owner of both the source and the source certificates.

You can later edit this field and assign ownership to someone else.

Description

A description of the source purpose.

Mandatory: No

Authorization Tags

A list of authorization tags. The Custom Roles with any of these tags will grant permissions on the source.

Mandatory: No

Select Source Type

Select **CAGW-Source-Plugin**.

Mandatory: Yes

CA Gateway URL

The URL of the CA Gateway host.

> For Entrust Managed PKI systems, your Entrust contact will provide the URL.

Mandatory: Yes

Verify server certificate

Check this box to verify the CA Gateway server certificate.

Required PKCS#12 File

The PKCS#12 file containing the keys and the certificate that Certificate Manager must present to the CA Gateway instance for accessing the CAs. This PKCS#12 file is either:

- Generated when configuring your CA Gateway instance,
- Provided by Entrust for API access to your Entrust Managed PKI service.

Mandatory: Yes

Required PKCS#12 Password

The password of the PKCS#12 file.

Mandatory: Yes

Optional PKCS#12 Truststore File

A truststore that will override the built-in truststore when using a private CA.

Mandatory: No

Optional Truststore Password

The password of the optional PKCS#12 truststore.

Mandatory: When selecting an **Optional PKCS#12 Truststore File**.

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

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 CA Gateway source
   - Creating a F5 BIG-IP source
   - Creating an Azure Key Vault 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.

5. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
6. 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.

```
Hashicorp-Vault-Destination-Plugin
```

Vault URL

The URL of the vault instance.

Vault SSL CA Bundle (PEM)

The certification chain of the Vault's SSL certificate, as a bundle in PEM format.

Vault KV API Version

The version of the Vault KV mount point.

Authentication Method

The authentication method. Only the token method is supported.

Token

A Vault authentication token with "Vault Mount" write privileges.

Vault Mount

The path of the Vault KV secrets engine. For example, a certificate with this distinguished name:

```
"C=CA,S=Ontario,L=Kanata,O=Entrust,OU=Sales,CN=vaultcert"
```

Is stored with the corresponding private key in this path:

```
dev/vaultcert/Sales/Entrust/Ontario/Kanata/CA/
vaultcert_Sales_Entrust_Ontario_Kanata_CA
```

When setting the following configuration.

Setting	Value
Vault Mount	dev
Vault Path	"{CN}/{OU}/{O}/{S}/{L}/{C}"
Object Name	"{CN}*{OU}*{O}*{S}*{L}_{C}"

Vault Path

A template for generating certificate paths from the following fields of the certificate distinguished names: CN, OU, O, S, L, C.

Object Name

A template for generating certificate entries from the following fields of the certificate distinguished names: CN, OU, O, S, L, C.

Bundle Chain

The storage format for the private key, the certificate, and the certificate chain. See below for a description of each supported format.

Nginx

```
crt: <certificate> + "\n" + <cert_chain>
key: <private_key>
```

Apache

```
crt: <certificate>
chain: <cert_chain>
key: <private_key>
```

PEM

```
pem: <certificate>+ "\n" + <cert_chain> + "\n" + <private_key>
```

No chain

```
crt: <certificate>
key: <private_key>
```

SAN Filter

A regular expression to filter out certificates by subject alternative name (SAN). Certificate Manager will discard a certificate when the certificate SAN does not match this regular expression.

Creating a Microsoft IIS web server destination

Create this destination to install the issued certificates as the server TLS certificate of a Microsoft IIS web server.

> On certificate issuance, Certificate Manager ignores any user-provided CSR and uses instead a CSR generated at the destination along with the key pair.

To create a Microsoft IIS web server destination in Certificate Manager

1. Configure a Microsoft IIS web server as explained in Microsoft IIS web server prerequisites.
2. Log into Certificate Manager as an administrator with one of the following roles:
   - The global_admin role.
   - A <user_defined> role with permission to create destinations.
3. Go to **Automate > Destinations**.
4. Click **Create** and set the Microsoft IIS web destination settings.
5. Click **Verify** to check the connection with the destination.
6. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
7. Click **Create** to confirm the destination creation.

Microsoft IIS web server prerequisites

Perform the following operations in the Microsoft IIS web server.

- Checking basic authentication support
- Configuring HTTPS for WinRM

Checking basic authentication support

Ensure the Microsoft Windows Remote Management WinRM service supports basic authentication, which is the only authentication the IIS plugin for Certificate Manager supports.

> Future releases will support other authentication methods.

To check if the WinRM service supports basic authentication

1. Launch PowerShell in the Microsoft Windows server.
2. Run the following command.

   ```
   winrm get winrm/config/client/auth
   ```

3. Check the command output includes the "Basic = true" line. For example:

```
Auth
    Basic = true
    Digest = true
    Kerberos = true
    Negotiate = true
    Certificate = true
    CredSSP = false
```

Configuring HTTPS for WinRM

Run the following command to check if HTTPS is enabled for the WinRM (Windows Remote Management) protocol.

```
winrm get winrm/config/Listener?Address=*+Transport=HTTPS
```

If the command raises an error, configure HTTPS for WinRM as explained below.

To configure HTTPS for WinRM

1. Issue a certificate for WinRM.

   ⚠ Self-signed certificates will work for testing purposes but will fail certificate validation.

2. Launch PowerShell in the Microsoft Windows server.
3. Import a `.pfx` or PKCS#12 file containing the issued new certificate, the certificate chain, and the private key for WinRM. For example:

   ```
   Import-PfxCertificate -FilePath "C:\Path\To\winrm.pfx" -CertStoreLocation Cert:
   \LocalMachine\My
   ```

4. Delete the existing configuration, if any.

   ```
   winrm delete winrm/config/Listener?Address=*+Transport=HTTPS
   ```

5. Set the WinRM new certificate. For example:

   ```
   winrm create winrm/config/Listener?Address=*+Transport=HTTPS
   '@{Hostname="examplehost";
   CertificateThumbprint="d6013136de9f9d18244ac3bca392ce206d57fe38"}'
   ```

Microsoft IIS web destination settings

In the Certificate Manager web console, configure the following settings of a Microsoft IIS web server destination.

- Label
- Owner
- Description
- Authorization Tags
- Select Destination Type
- Host

- User
- Password
- Validate Windows Remote Management (WinRM) Certificate
- CA Certificate

Label

A descriptive name of the destination.

Owner

The username of the destination owner.

> The user who adds the destination is automatically made the owner. You can later edit this field and assign ownership to someone else.

Description

A description of the destination purpose.

Authorization Tags

A list of authorization tags. The Custom Roles with any of these tags will grant permissions on the source.

Select Destination Type

Select the following value.

```
IIS-Server-Plugin
```

Host

The hostname or IP address of the Microsoft IIS web server.

User

The name of a user with permission to use the Microsoft IIS web server.

Password

The password of the selected user.

Validate Windows Remote Management (WinRM) Certificate

Check this box to validate the certificate of the Windows Remote Management (WinRM) service, Certificate Manager will use this service to install the issued certificate.

CA Certificate

The PEM encoding of the CA certificate chain for validating the WinRM certificate. This value is only mandatory when checking the **Validate Windows Remote Management (WinRM) Certificate** box.

Creating an Apache web server destination

Create this destination to install the issued certificates as the server TLS certificate of an Apache web server. Note that:

- On certificate issuance, Certificate Manager ignores any user-provided CSR and uses instead a CSR generated at the destination along with the key pair.
- On renewal, the operating system timestamp may remain the same, but the contents of the certificate are always updated.

See below for how to create an Apache web server destination.

To create an Apache web server destination in Certificate Manager

1. If not already installed, install Python 3.9 or newer on the Nginx web server.
2. Log in as an administrator with one of the following roles:
    - The global_admin role.
    - A <user_defined> role with permission to create destinations.
3. Go to **Automate > Destinations**.
4. Click **Create** to configure the following settings.
    - Label
    - Owner
    - Description
    - Authorization Tags
    - Select Destination Type
    - Host
    - User
    - Password
    - Private Key File
    - Private Key Password
    - Certificate Destination
    - 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. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
7. 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.

> ℹ 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.

> ℹ 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).

> ℹ 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.
6. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
7. Click **Create** to confirm the destination creation.

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.
6. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
7. Click **Create** to confirm the destination creation.

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 alphanumerical 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.
5. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
6. 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.

```
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. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
7. 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.

ℹ 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.

ℹ 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.
5. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
6. 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.

```
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.
6. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
7. Click **Save** to confirm the changes.

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



See Email for instructions on how to modify the default layout of the notification emails.

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 Address Book of Certificate Manager.
Address Book entry in Custom Field	All the email addresses in an address book set as Custom Field.
Email in Custom Field	The email address in a Custom Field.
Certificate Owner	The email address configured in the **Owner** field of the certificate.

Mandatory: Yes

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 Address Book of Certificate Manager.
Address Book entry in Custom Field	All the email addresses in an address book set as Custom Field.
Email in Custom Field	The email address in a Custom Field.
Certificate Owner	The email address configured in the **Owner** field of the certificate.

Mandatory: Yes

Deleting rules and actions

See below for deleting rules and actions.

To delete rules and actions

1. Log in as an administrator with one of the following roles.
   - The global_admin role.
   - A <user_defined> role with permission to delete destinations.
2. Go to **Automate > Rules & Actions**.
3. In the main grid, select one or more rules.
4. Click **Delete** to remove the selected rules.

Report

Certificate Manager includes extensive reporting capabilities optimized for the automated production and dissemination of management notifications and reports. Click **Report** in the sidebar and select the following options.

- Launch

- Designer
- Report Schedules
- History

Launch

Go to **Report > Launch** to view the control insights page. You can:

- Click the corresponding link to manage:
  - The report Designer
  - The Report Schedules
  - The report History
- Click the tags under **Related Topics** to learn about different topics.

Designer

You can design the reports Certificate Manager periodically generates with updated information on the managed certificates. Report design and scheduling are separated to use one design for multiple reports.

- Browsing reports
- Creating a report
- Editing a report
- Designing a report
- Updating a report design
- Deleting reports

Browsing reports

See below for browsing reports.

To browse reports

1. Log in as an administrator with either:
   - The global_admin role.
   - A Custom Role with permission to view reports.
2. Go to **Report > Designer**.
3. Define report views.
   - Unfold the **Columns** list to select the properties you want to display as columns.
   - Click **Show Filter Options** to display a filtering form below each column name.
   - Select **Show Filter Options / Remove all filters** to remove all filters.
   - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
   - Click **Show Filter Options** to hide the filtering options and keep the filters.
   - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
   - Click **Reset layout** to remove all the column and filter customizations.
   - Click the refresh icon to rerun the query with the current filters.

   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 now 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.

> ℹ 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 now 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 global_admin must add the required roles.

Browsing administrators

See below for browsing the Certificate Manager administrators.

To browse Certificate Manager administrators

1. Log in as an administrator with the global_admin role.
2. Go to **Administer** > **Administrators.**
3. Select **Show Insights** at the top-right and click **View Accounts** for each predefined filter:
   - New Accounts
   - Deactivated Accounts
   - Idle Accounts.
4. Define grid views.
   - Unfold the **Columns** list to select the properties you want to display as columns.
   - Click **Show Filter Options** to display a filtering form below each column name.
   - Select **Show Filter Options / Remove all filters** to remove all filters.
   - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
   - Click **Show Filter Options** to hide the filtering options and keep the filters.
   - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
   - Click **Reset layout** to remove all the column and filter customizations.
   - Click the refresh icon to rerun the query with the current filters.

   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 Browsing and updating users how to force a password change for 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 Browsing and updating users how to force a password change for 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.

Address Type	Contents
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.

   > ℹ 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_1114	Events retention period set to `<retention_period>` days
AUDIT_1115	Reports settings updated. Retention period: `<retention_period>`, Copyright text `<copyright_text>`
AUDIT_1116	Plugin `<plugin_name>` updated. State set to `<plugin_active_state>`
AUDIT_1117	Public Enrollment Forms `<general_setting_enabled/disabled>`
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 Code	Log
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 `<auth_provider_name>` registered
AUDIT_1011	Auth provider `<auth_provider_name>` updated
AUDIT_1012	LDAP login failed for user: `<username>`
AUDIT_1013	LDAP login failed as user: `<username>` is not in the required group: `<auth_provider_registration_group_name>`, dn: `<email>`
AUDIT_1017	API token created for user `<username>`

Audit Code	Log
AUDIT_1018	API token deleted for user `<username>`
AUDIT_1023	Roles updated for user `<username>`
AUDIT_1030	API token deleted for user `<username>`
AUDIT_1031	API token updated for user `<username>`
AUDIT_1032	All API tokens deleted for user `<username>`
AUDIT_1033	All API tokens deactivated for user `<username>`
AUDIT_1036	Created initial user with username: `<username>`.
AUDIT_1037	Created user with username: `<username>`.
AUDIT_1039	Created LDAP user with username: `<username>`.
AUDIT_1040	Created external user username: `<username>`.
AUDIT_1041	Deleted user: `<username>`.
AUDIT_1042	Updated user: `<username>`.
AUDIT_1043	Updated LDAP user: `<username>`.

Audit Code	Log
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_1060	Login denied. Tenant id not found for user `<username>`
AUDIT_1061	Global role created: `<role_name>`
AUDIT_1062	Custom role created: `<role_name>`
AUDIT_1063	Custom role updated: `<role_name>`
AUDIT_1064	Authority role created: `<role_name>`
AUDIT_1065	Composite role created: `<role_name>`

Audit Code	Log
AUDIT_1066	Role deleted: `<role_name>`
AUDIT_1067	Role updated: `<role_name>`
AUDIT_1068	Role `<role_name>` assigned to user `<username>`.
AUDIT_1069	Role `<role_name>` unassigned from user `<username>`.
AUDIT_1070	Certificate role created: `<role_name>`
AUDIT_1071	Certificate role updated: `<role_name>`
AUDIT_1092	Failed login attempt for user: `<username>`. User is not active.
AUDIT_1093	Failed login attempt. User does not exist.

Automation logs

The following logs record rule and report events.

Audit Code	Log
AUDIT_1201	`<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 Code	Log
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 `<cert_name>` (Serial Number: `<cert_sn>`) archived
AUDIT_1435	Certificate `<cert_name>` (Serial Number: `<cert_sn>`) unarchived
AUDIT_1436	Certificate `<cert_name>` (Serial Number: `<cert_sn>`) revoked
AUDIT_1437	Certificate `<cert_name>` (Serial Number: `<cert_sn>`) released from hold
AUDIT_1472	Custom Field created: `<custom_field_name>` .
AUDIT_1473	Custom Field deleted: `<custom_field_name>` .
AUDIT_1474	Custom Field updated: `<custom_field_name>` .

Audit Code	Log
AUDIT_1480	Certificate exported: Common Name `<cert_name>`, Serial Number `<decimal_cert_sn>`, export type: `<export_type>`
AUDIT_1491	<n `umber_of_updated_certs>` certificates queued for bulk update.
AUDIT_1492	New certificate issued by authority: <a `uth_name>`. (Common Name: `<cert_name>`, Serial Number: `<cert_sn >`)
AUDIT_1493	Certificate `<cert_name>` (Serial Number: `<cert_sn >`) updated
AUDIT_1494	Certificate `<cert_name>` (Serial Number: `<decimal_cert_sn >`) imported
AUDIT_1498	Certificate view `<view_name>` created.
AUDIT_1499	Certificate view `<view_name>` updated.
AUDIT_1500	Certificate view `<view_name>` deleted.

Certificate policy logs

The following logs record Access Tags events.

Audit Code	Log
AUDIT_1481	Certificate Access Tag `<access_tag_name>` created.
AUDIT_1482	Certificate Access Tag `<access_tag_name>` updated.
AUDIT_1483	Certificate Access Tag `<access_tag_name>` deleted.

Control logs

The following logs record events on authorities, key managers, and discovery scanners.

Audit Code	Log
AUDIT_1301	CA Gateway added: `<cagw_name>`
AUDIT_1302	CA Gateway updated: `<cagw_name>`
AUDIT_1303	CA Gateway deleted: `<cagw_name>`
AUDIT_1304	Authority added: `<auth_name>`
AUDIT_1305	Authority updated: `<auth_name>`
AUDIT_1306	Authority deleted: `<auth_name>`
AUDIT_1371	Successfully uploaded certificate with Private key Id: `<priv_key_id>` and Public key Id: `<pub_key_id>` to KMS using plugin: `<plugin_name>`
AUDIT_1375	Key pair deactivated at Key Manager `<plugin_name>`, Private key id: `<priv_key_id>`, Public key id: `<pub_key_id>`
AUDIT_1376	Verification request submitted for domain `<domain_name>` to authority `<auth_name>`
AUDIT_1377	Key manager with plugin `<plugin_name>` created: `<key_manager_name>`
AUDIT_1378	Key manager updated: `<key_manager_name>`
AUDIT_1379	Key manager deleted: `<key_manager_name>`
AUDIT_1382	Status updated for domain `<Domain name>` from authority `<auth_name>`

Audit Code	Log
AUDIT_1383	Re-verify request submitted for domain `<domain_name>` to authority `<auth_name>`
AUDIT_1384	Discovery scanner added: `<disco_agent_name>`
AUDIT_1385	Discovery scanner updated: `<disco_agent_name>`
AUDIT_1386	Discovery scanner deleted: `<disco_agent_name>`
AUDIT_1387	`<num_of_disco_agent_scans>` Scan configurations updated for discovery scanner `<disco_agent_name>`
AUDIT_1388	Discovery scanner < `disco_agent_name>` policy updated, new polling frequency: `<disco_agent_poll_freq>` seconds

Destination logs

The following logs record destination events.

Audit Code	Log
AUDIT_1495	Destination `<dest_name>` created.
AUDIT_1496	Destination `<dest_name>` updated.
AUDIT_1497	Destination `<dest_name>` deleted.

Public form logs

The following logs record Public Enrollment Form events.

Audit Code	Log
AUDIT_1504	Public form `<pub_form_name>` created.

Audit Code	Log
AUDIT_1505	Public form `<pub_form_name>` updated.
AUDIT_1506	Public form `<pub_form_name>` deleted.
AUDIT_1507	Certificate request (ID: `<cert_request_id>`) of requester `<requester>` (IP: `<remote_ip>`) is rejected.
AUDIT_1508	Certificate request (ID: `<cert_request_id>`) of requester `<requester>` (IP: `<remote_ip>`) is approved.
AUDIT_1509	Certificate request (ID: `<cert_request_id>`) of requester `<requester>` (IP: `<remote_ip>`) is already approved.
AUDIT_1510	Certificate request (ID: `<cert_request_id>`) of requester `<requester>` (IP: `<remote_ip>`) is already rejected.
AUDIT_1511	Error rejecting certificate request (ID: `<cert_request_id>`) of requester `<requester>` (IP: `<remote_ip>`).
AUDIT_1512	Error approving certificate request (ID: `<cert_request_id>`) of requester `<requester>` (IP: `<remote_ip>`) .
AUDIT_1513	New Certificate request created.
AUDIT_1514	Certificate request (ID: `<cert_request_id>`) of requester `<requester>` (IP: `<remote_ip>`) is cancelled.
AUDIT_1515	New Certificate request created with key algorithm `<key_alg>` , key size `<Key size>` (IP: `<remote_ip>`)
AUDIT_1516	New Certificate request created key algorithm `<key_alg>` , (IP: `<remote_ip>`)

Audit Code	Log
AUDIT_1517	New Certificate request created with key algorithm `<key_alg>`, OID `<pub_key_info_alg>` (IP: `<remote_ip>`).
AUDIT_1518	Deleted `<num_cert_requests_deleted>` certificate requests last modified `<cert_request_retention>` days ago.
AUDIT_1519	Certificate request (ID: `<cert_request_id>`) of requester `<requester>` (IP: `<remote_ip>`) with CA side key generation (profile: `<profile_id>` is marked approved.
AUDIT_1520	Certificate request (ID: `<cert_request_id>`) of requester `<requester>` (IP: `<remote_ip>`) is already issued.
AUDIT_1521	Pkcs12 for Certificate Request (ID: `<cert_request_id>`) of requester `<requester>` (IP: `<remote_ip>`) with CA side key generation (profile: `<profile_id>` is issued.

Source logs

The following logs record source events.

Audit Code	Log
AUDIT_1501	Source deleted: `<source_name>`
AUDIT_1502	Source with plugin `<plugin_name>` created: `<source_name>`
AUDIT_1503	Source updated: `<source_name>`

API Tokens

With API tokens, you can programmatically interface to the Certificate Manager API.

- Browsing API tokens
- Creating an API token
- Deleting API tokens

Each API token is associated with the user who created that token. Therefore, all actions taken through the API are associated with that person and inherit the person's roles.

Browsing API tokens

See below for browsing API tokens.

To browse API tokens

1. Log in as an administrator with the global_admin role.
2. Go to **Administer > API Tokens.**
3. Define API token views.
   - Unfold the **Columns** list to select the properties you want to display as columns.
   - Click **Show Filter Options** to display a filtering form below each column name.
   - Select **Show Filter Options / Remove all filters** to remove all filters.
   - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
   - Click **Show Filter Options** to hide the filtering options and keep the filters.
   - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
   - Click **Reset layout** to remove all the column and filter customizations.
   - Click the refresh icon to rerun the query with the current filters.

   > 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	<ca>_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	The `<ca>` authority only.
	Adding authorities	❌
	Editing an authority	The `<ca>` authority only.
	Deleting authorities	The `<ca>` authority only.
Key Managers	Browsing key managers	Only own-created.
	Creating a key manager	✅
	Editing a key manager	Only own-created.
	Deleting key managers	Only own-created.
Custom Fields	Browsing custom fields	❌
	Creating a custom field	❌
	Editing a custom field	❌

Menu option	Operation	<ca>_admin permissions
	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.
	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.

Menu option	Operation	<ca>_admin permissions
	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	✗

Menu option	Operation	<ca>_admin permissions
	Deleting sources	✗
Destinations	Browsing destinations	✗
	Creating a destination	✗
	Editing a destination	✗
	Deleting destinations	✗
Rules and Actions	Browsing rules	Only rules for certificates issued by the `<ca>` authority.
	Creating a rule	Only rules for certificates issued by the `<ca>` authority.
	Editing a rule	Only rules for certificates issued by the `<ca>` authority.
	Deleting rules and actions	Only rules for certificates issued by the `<ca>` authority.

Report permissions

Administrators with the `<ca>_admin` role have the following permissions on the menu options under Report.

Menu option	Operation	<ca>_admin permissions
Designer	Browsing reports	Only reports on certificates issued by the `<ca>` authority.
	Creating a report	✗
	Editing a report	Only reports on certificates issued by the `<ca>` authority.
	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.

Menu option	Operation	<ca>_admin permissions
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	❌
Address Book	Browsing the address book	✅
	Creating an address	❌
	Importing addresses	❌
	Editing an address	❌

Menu option	Operation	<ca>_admin permissions
	Deleting addresses	✗
Audit Log	Browsing Logs	✗
API Tokens	Browsing API tokens	Only own-created.
	Creating an API token	✓
	Deleting API tokens	Only own-created.
Certificate Access Tags	Browsing certificate access tags	✓
	Creating a certificate access tag	✓
	Editing a certificate access tag	✓
	Deleting Certificate Access Tags	✓
Roles	Browsing roles	Only Certificate Roles for issuing certificates with the `<ca>` authority.
	Creating a role	Only a Certificate Role for issuing certificates with the `<ca>` authority.
	Editing a role	Only Certificate Roles for issuing certificates with the `<ca>` authority.
	Deleting roles	Only Certificate Roles for issuing certificates with the `<ca>` authority.
Settings	General	✗
	Identity Provider	✗
	Reports	✗
	License	✗

Menu option	Operation	<ca>_admin permissions
	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	✓

Menu option	Operation	global_admin permissions
	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	✗
	Editing a public enrollment form	✗
	Deleting public enrollment forms	✗
Requests For Approval	Browsing pending requests	✗

Menu option	Operation	global_admin permissions
	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	✓
Certificate History	Browsing the certificate history	✓
	Restoring archived certificates	✓
Domains	Browsing domains	✓

Menu option	Operation	global_admin permissions
	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	✓
	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	✓

Menu option	Operation	global_admin permissions
	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	✓
	Editing a role	✓
	Deleting roles	✓
Settings	General	✓

Menu option	Operation	global_admin permissions
	Identity Provider	✓
	Reports	✓
	License	✓
	Plugins	✓

Operator Role

This role for backward compatibility maintains the previous permissions of existing users. See below for the permissions granted by this role.

- Find permissions
- Control permissions
- Automate permissions
- Report permissions
- Administer permissions

> You can edit or delete this role after the upgrade.

Find permissions

Administrators with the Operator Role have no permission to use the Find menu.

Control permissions

Administrators with the Operator Role the following permissions on the menu options under Control.

Menu option	Operation	Operator permissions
CA Gateways	Browsing CA Gateway instances	✗
	Adding a CA Gateway instance	✗
	Editing a CA Gateway instance	✗
	Deleting a CA Gateway instance	✗
Authorities	Browsing authorities	✗
	Adding authorities	✗

Menu option	Operation	Operator permissions
	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	✗
	Rejecting a pending certificate request	✗
My Certificate Requests	Browsing my certificate requests	✗
	Making a certificate request	✗

Menu option	Operation	Operator permissions
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	✗
	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	✓

Menu option	Operation	Operator permissions
	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	❌
Address Book	Browsing the address book	✅
	Creating an address	❌
	Importing addresses	❌
	Editing an address	❌
	Deleting addresses	❌

Menu option	Operation	Operator permissions
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	✗
	License	✗
	Plugins	✗

renewal_daemon

This system role for automated certificate renewals cannot be assigned to administrators.

Creating a role

See below for creating a Certificate Role or a Custom Role in Certificate Manager.

To create a role

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 Certificates.
Requestor	Create certificate requests as explained in Making a certificate request.
Approver	Approve certificate requests as explained in Approving a pending certificate request, or manage public forms as explained in Creating a public enrollment form.

Authority

The certificate authority that issued, or will issue, the certificates. Select one of the Certificate Manager-managed Authorities for granting permissions to:

- Issue, edit, revoke, or unhold certificates issued by that certificate authority.
- Manage public forms for the end-users to request certificates from this certificate authority.
- Approve or create certificate requests for this certificate authority.

If this optional field is omitted, the role permissions will be limited to unmanaged certificates – that is, certificates issued by certificate authorities not managed by Certificate Manager.

Profiles

The certificate profiles the **Authority** will use for issuing new certificates. This setting does not affect existing certificates.

The **All Profiles Enabled** default option grants role permissions on all the certificate profiles issued by the **Authority**.

Certificate Access Tag

The Certificate Access Tag assigned to the certificates.

Permissions

The permissions granted by the role on certificates:

- Issued by the **Authority** using the selected **Profiles**.
- Labeled with the **Certificate Access Tag**.

Custom Role

A custom role is a user-defined role covering access to:

- Key Managers
- Destinations
- Sources
- Rules and Actions

When selecting this role type, configure the following settings.

Authorization Tag

The name of a new authorization tag.

Permissions

The permissions granted by the role on the entities with the **Authorization tag**.

Editing a role

See below for how to edit an administrator role in Certificate Manager.

To edit a role

1. Log in as an administrator with:
   - The global_admin role, to edit the Operator Role, a Certificate Role, or a Custom Role.
   - The <ca>_admin role, to edit a Certificate Role.
2. Go to **Administer > Roles**.
3. Define role views.
   - Unfold the **Columns** list to select the properties you want to display as columns.
   - Click **Show Filter Options** to display a filtering form below each column name.
   - Select **Show Filter Options / Remove all filters** to remove all filters.
   - Select **Show Filter Options / <column>** to remove the filters on the <column> column.
   - Click **Show Filter Options** to hide the filtering options and keep the filters.
   - Click **Items per page** at the bottom of the page, select the number of items to view per page: 10, 25, 50, or 100.
   - Click **Reset layout** to remove all the column and filter customizations.
   - Click the refresh icon to rerun the query with the current filters.

   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.
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.

Email

Use the **Email header** and **Email footer** fields to modify the default layout of the notification emails.

Reports

Customize the corporate branding of the reports previously configured with the designer.

To customize the report branding

1. Log in as an administrator with the global_admin role.
2. Go to **Administer > Settings > REPORTS**.
3. Configure the following settings.
   - Retention period field
   - Logo
   - Footer Text
   - Header Color
4. Click **Save** to save the report settings.
5. Click **Preview Report** to generate a sample report with the selected branding.
6. In the **Report Name** dropdown list of the **Preview Report** dialog, select the name of the report design.
7. In the **Format** dropdown list of the **Preview Report** dialog, select the file format for the generated preview: CSV, PDF, Microsoft Excel, or Microsoft Word.
8. Click **Preview** to generate and download the report preview.

Retention period field

The number of days for which Certificate Manager will keep the generated reports.

> By default, Certificate Manager removes generated reports exceeding 365 days.

Logo

The corporate logo for the generated reports. Check the current logo in the **Current image** field (if any).

Footer Text

The footer text for the generated reports.

Header Color

The header color for the generated reports.

License

After a new Certificate Manager installation or an upgrade from 2.1.1, Certificate Manager only provides Administer options. To run the other options, you must import a license.

- Importing a license
- Checking the imported license

Importing a license

Import a license for the Certificate Manager application and the installed plugins.

> You can upload updated licenses for the same order number. Licenses with new order numbers require a new Certificate Manager installation.

To import a license

1. Log in as an administrator with the global_admin role.
2. Go to **Administer > Settings > LICENSE**.
3. Click **Select Files**… and select the license file for your Certificate Manager installation. When importing a zipped license, you must type the **Password** you received by email along with the license file.
4. Click **Save**. The application will display the license details described in the next section Checking the imported license.

Checking the imported license

To check the imported license, you can either:

- Go to **Administer > Settings > LICENSE**.
- Select **About** in the top-right **<username>** menu.

See below for a description of each license field.

Field	Application license	Plugin license
Order Number	The license order number.	The license order number.
Product License	The license name.	The license name.
Summary	The licensed capabilities.	The licensed capabilities.
License Validity	The license validity period.	The license validity period.
Quantity	The number of certificates Certificate Manager is allowed to manage. For non-capped licenses, the value of this field is "Unlimited".	The number of licensed plugins.

Plugins

Manage the installed plugins.

To manage an installed plugin

1. Log in as an administrator with the global_admin role.
2. Select a plugin.
3. Click **Edit**.
4. Manage the following settings.
    - Name
    - Version
    - Active

- Title
- Description
- Group
- Plugin type

5. In grid view, click the plus button to display the global settings of a plugin (if any).

Name

The plugin identifier.

Version

The plugin version.

Active

Yes if the plugin is active, **No** otherwise.

> Activating a plugin requires installing the corresponding License, and you cannot deactivate a plugin in use.

Title

The name of the plugin.

Description

Additional information about the plugin.

Group

The internal identifier of the plugin.

Plugin type

The intended use of the plugin.

Plugin Type	Use
Destination	Integrate certificate publication destinations, as explained in Creating a destination.
Key Management	Integrate key managers, as explained in Creating a key manager.
Notification	Send notifications triggered by Rules and Actions, Report Schedules and certificate requests.
Source	Integrate certificate sources, as explained in Creating a source.

Menu options

Select the following options in the top-right menu.

- Search for help on...
- Notifications
- User menu

Search for help on...

Enter a search term to quickly find information across all UI pages, the user guide, and related content.

Notifications

Check a list of the received notifications (if any).

> Notifications on issued certificates include a download link.

User menu

Click your user name and select:

- **Help** to browse this guide in HTML format.
- **API Help** to browse the Certificate Manager API documentation.
- **Language** to change the interface language.
- **Profile Account** to display user details such as:
  - The number of managed CA Gateways.
  - The number of managed Authorities.
  - The total number of issued Certificates, including details on the number of certificates expiring in 7 days and the number of scheduled renewals.
  - The time and date of the last login.
  - The granted Roles.
  - The managed Certificate Access Tags.
  - The number of managed Discovery Agents.
  - The number of requested workflows.
- **Change Password** to change the user password.
- **Settings** to manage the Certificate Manager Settings.
- **About** to check:
  - The time and date when the Certificate Manager API was last updated.
  - The Certificate Manager API current version.
  - The License details.
- **Logout** to terminate the user session.

Certificate Manager API

Certificate Manager provides an API for programmatic access to:

- Query certificates on their associated metadata (owner, description, and custom fields).
- Import new certificates into Certificate Manager.
- Update the metadata of custom fields.

> As explained in API Tokens, the available API operations depend on the permissions of the API token holder.

Open the following URL in your browser to access the Swagger interactive documentation for the Certificate Manager API.

```
https://<cm>/api
```

Where `<cm>` is the URL or IP address of your Certificate Manager installation.

Certificate Manager error reference

When executed, Certificate Hub can print the following errors.

> See Browsing logs with Grafana for how to browse Certificate Manager logs.

Authentication and authorization errors

The application throws the following authentication and authorization errors.

Code	Message
ERR_1006	Failed to hash the password for user: `<Username>`
ERR_1010	`hasPermission` unexpectedly invoked for `<Permission>`
ERR_1011	The util command must have a `--cmd` argument.
ERR_1012	Unknown command `<Command>`
ERR_1013	`--username`, `--password`, and `--email` must be supplied to the `createUser` command.
ERR_1014	Unexpected crypto error:
ERR_1015	Error creating default cert expiry rule for initial user:
ERR_1016	`--username` and `--role` must be provided.
ERR_1017	Unexpected crypto exception:

Code	Message
ERR_1040	Unexpected parsing error while loading auth request:
ERR_1041	Unexpected parsing error while saving auth request:
ERR_1042	Unexpected parsing error while removing auth request:
ERR_1046	Could not find password auth provider entry.
ERR_1047	Failed to hash the password for user: `<Username>`
ERR_1048	Cannot update non-existent user. User must have existing id.
ERR_1049	Login denied. Tenant id not found for user `<Username>`.
ERR_1056	More than one LDAP auth provider registration found (`<Number of registrations>`). Unexpected behavior may result!
ERR_1057	More than one PASSWORD auth provider registration found (`<Number of registrations>`). Unexpected behavior may result!
ERR_1076	Unable to create keystore: `<CA>`
ERR_1077	Cryptography issue when creating user.
ERR_1078	Cryptographic error processing password.
ERR_1079	Unable to initialize SSLContext for LDAPS

Code	Message
ERR_1080	More that one LDAP auth provider registration present. Unexpected results may occur.
ERR_1081	LDAP authentication error.
ERR_1082	Unexpected exception during LDAP lookup.
ERR_1083	Error closing LDAP context.
ERR_1084	Could not find Active Directory user.
ERR_1085	Error creating the daemon user:
ERR_1086	Error creating the initial user:

Administration errors

The application throws the following administration errors.

Code	Message
ERR_1100	Internal error occurred
ERR_1101	Error parsing license : `<Error message>`
ERR_1102	Error parsing license: Epm client could not parse license
ERR_1103	Error parsing license : `<Error message>`
ERR_1104	Error parsing license: Epm client could not parse license

Code	Message
ERR_11105	Order Number of `<Order number>` uploaded license doesn't match the existing license `<Customer contact reference>`
ERR_11106	License revision `<Revision>` already uploaded.
ERR_11107	Uploaded license revision `<Uploaded revision>` is outdated. Current license revision : `<Current revision>`.
ERR_11108	Failed to create the license expiry schedule
ERR_11109	Failed to send email for license consumption
ERR_11110	Failed to send email for license expiry
ERR_11111	Failed to check the license expiry schedule
ERR_11112	Failed to delete existing license expiry schedule
ERR_11113	Failed to create the license expiry schedule
ERR_11114	Invalid plugin name: `<Plugin name>`
ERR_11115	Error executing plugin options for plugin: `<Plugin name>`
ERR_11116	Error loading plugin jar `<JAR file name>`. Plugin will not be loaded!
ERR_11117	Error loading plugin classloader.

Code	Message
ERR_1118	Plugin `<Canonical name>` is missing a language bundle. Plugin will not be loaded!
ERR_1119	Plugin `<Canonical name>` has invalid language bundle. No messages section found. Plugin will not be loaded!
ERR_1120	Plugin `<Canonical name>` has invalid language bundle. No languages found. Plugin will not be loaded!
ERR_1121	Plugin `<Canonical name>` has an invalid language bundle. Language `<Key>` is an invalid map. Plugin will not be loaded!
ERR_1122	Plugin `<Canonical name>` has an invalid language bundle. Language `<Name>`, key `<Key>` is invalid (`<Value>`). Plugin will not be loaded!
ERR_1123	Error initializing plugins! No `<Plugin class name>` plugins will be loaded until invalid plugin is removed!
ERR_1124	updatePlugin: Error converting global options to Json string from list
ERR_1125	validatePluginStateUpdate : cannot deactivate plugins that don't require license
ERR_1126	validatePluginStateUpdate : cannot deactivate plugin `<Name>` as its in use by destination : `<Label>`
ERR_1127	validatePluginStateUpdate : cannot deactivate plugin `<Name>` as its in use by source : `<Label>`
ERR_1128	addPlugin: Error converting global options to Json string from list
ERR_1129	Error converting global options to list from `Json byte[]`
ERR_1130	addPlugin: Error converting global options to list from `Json byte[]`

Code	Message
ERR_1131	Error fetching language bundle, Plugin `<Plugin name>` not found
ERR_1132	Failed to add an entry to the keystore: `<TBU>`
ERR_1133	Plugin update failed, plugin ID `<Plugin ID>`
ERR_1149	Failed importing multiple addresses.
ERR_1150	Failed importing single addresses.
ERR_1153	Failed to check the events retention schedule: `<Error>`
ERR_1154	Failed to create the events retention schedule: `<Error>`
ERR_1199	Unhandled exception caught

Automation errors

The application throws the following automation errors.

Code	Message
ERR_1207	Failed to mapping existing source plugin options.
ERR_1208	Failed to process existing source plugin options.
ERR_1209	Failed to migrate existing source plugin options.
ERR_1214	Failed to send email for report `<Report name>`, schedule id: `<Schedule ID>`. Error:

Code	Message
ERR_1215	Failed to generate missing report: `<Report ID>`
ERR_1216	Failed to generate missing schedule: `<Schedule ID>`
ERR_1217	Failed to return report: `<Report ID>` . Error: `<Error>`
ERR_1218	Error while retrieving report data:
ERR_1219	Error while generating report:
ERR_1220	User `<Username>` does not have permission to edit or delete report `<Report name>`
ERR_1221	Error while generating report: `<Error>`
ERR_1222	User `<Username>` does not have permission to access artifact `<Artifact ID>`
ERR_1223	User `<Username>` does not have permission to access execution `<Execution ID>`
ERR_1224	Failed to check the reports retention schedule: `<Error>`
ERR_1225	Failed to create the reports retention schedule: `<Error>`
ERR_1230	Field ' `<Name>` ' value ' `<Value>` ' cannot be parsed as `<Type>` . Field will be treated as a String.
ERR_1231	Unexpected exception while processing rule. RULE WILL BE SKIPPED!

Code	Message
ERR_1232	Expiry notification is dropped for certificate `<Certificate name>`. The address field `<Address field>` is empty.
ERR_1233	Expiry notification is dropped for certificate `<Certificate name>`. The address field `<Address field>` is not referring to a text custom field.
ERR_1234	Action plugins not currently supported. THIS ACTION WILL BE SKIPPED!
ERR_1235	Exception while executing rule. RULE WILL BE SKIPPED!
ERR_1236	Error running rules engine for certificate renewal rule.
ERR_1237	Execution of action failed.
ERR_1238	FAILED processing conditions. RULE WILL BE SKIPPED!
ERR_1239	I/O issue while parsing conditions. RULE WILL BE SKIPPED!
ERR_1240	Error running rules engine for event.
ERR_1241	Could not parse plugin config, ACTION WILL BE SKIPPED: `<Plugin config>`
ERR_1242	FAILED to create the expiration rules schedule! Expiry notifications will not be sent!
ERR_1243	Error while processing event rule conditions. RULE WILL BE SKIPPED!
ERR_1244	Only NOTIFICATION actions are supported! ACTION WILL BE SKIPPED!

Code	Message
ERR_1254	Unexpected IOException while formatting the certificate. Error:
ERR_1255	Unexpected IOException while formatting the certificate chain. Error:
ERR_1256	Unexpected IOException while formatting the certificate. Error:
ERR_1260	FAILED to create the key manager scan schedule! Key managers will not be scanned!
ERR_1261	Error encountered while scanning key manager.
ERR_1262	Error encountered while scanning source.
ERR_1271	User `<User ID>` does not have permission to view, edit or delete destination `<Label>`
ERR_1272	Error verifying destination config `<Label>`
ERR_1273	Error verifying destination config for plugin `<Plugin name>`
ERR_1274	Error while generating report.
ERR_1275	Failed to retrieve schedule runtimes for `<Schedule name>`
ERR_1276	Failed to parse schedule runtimes for `<Schedule name>`
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!

Code	Message
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 `<Certificate name>`. The address field `<Address field>` is empty.
ERR_1290	Error running rules engine for certificate renewal rule.
ERR_1291	Failed processing rule. RULE WILL BE SKIPPED!
ERR_1292	I/O issue while running rule. RULE WILL BE SKIPPED!
ERR_1293	Expiry notification is dropped for certificate `<Certificate name>`. The custom field `<Custom field>` is empty.
ERR_1294	Expiry notification is dropped for certificate `<Certificate name>`. The address field `<Address field>` is not referring to a text custom field.
ERR_1295	Expiry notification is dropped for certificate `<Certificate name>`. The address field `<Address field>` is empty.
ERR_1296	Error running rules engine for certificate renewal rule.
ERR_1299	Execution of rule action failed.

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: `<Error>` : \n `<Response body>`
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

Code	Message
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>`
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>`

Code	Message
ERR_1377	Internal error contacting CAGW.
ERR_1378	Internal error contacting CAGW.
ERR_1379	Internal error contacting CAGW while responding to an authority request.
ERR_1380	Failed to create the authority domain sync schedule for authority `<Authority ID>`
ERR_1381	Failed to delete the authority domain sync schedule for authority `<Authority ID>`
ERR_1382	Certificate Authority `<Authority ID>` not found
ERR_1383	Unable to parse plugin options for authority `<Authority ID>` :
ERR_1384	Error response from CAGW while getting domain: `<Domain name>`
ERR_1385	Failed to get domain. Error from CAGW: `<Error>`
ERR_1386	Failed to submit domain, Error from CAGW: `<Error>`
ERR_1387	Unable to fetch whois record from server `<Server name>` . Error:
ERR_1388	Unable to close whois client connection with server `<Server name>` . Error:
ERR_1389	Unable to fetch whois record from default host. Error:
ERR_1390	Unable to close whois client connection with default server. Error:
ERR_1392	Error on DNS lookup : `<Error>`
ERR_1394	Failed to submit domain, Error from CAGW: `<Error>`
ERR_1397	Certificate Authority `<Authority ID>` not found
ERR_1398	Unable to parse plugin options for authority `<Authority ID>`

Code	Message
ERR_1399	Unable to import/update domain id `<Domain ID>` due to Json parsing error from authority `<Authority ID>`

Certificate errors

The application throws the following certificate errors.

Code	Message
ERR_1426	Renewal failed. Missing certificate id.
ERR_1427	Failed auto renewal for certificate `<Certificate ID>`.
ERR_1428	Automated renewal failed for certificate `<Certificate ID>` due to certificate processing error
ERR_1430	Automated renewal failed for certificate `<Certificate ID>` due to destination errors: `<List of errors>`
ERR_1431	Failed to find the renewal daemon user for auto renewal
ERR_1432	Failed to create the renewal schedule for cert `<Certificate serial>` : `<Error>`
ERR_1433	Failed to check the renewal schedule `<Error>`
ERR_1434	Failed to create the renewal schedule `<Error>`
ERR_1435	Adding definition for custom field with duplicate display order : `<Label>` of type `<Type>` at position `<Display order>`
ERR_1436	Deleting definition for custom field with Id : `<Metadata ID>` failed as it is in use by `<Certificates using metadata>` certificates

Code	Message
ERR_1437	Updating definition for custom field with duplicate display order : `<Label>` of type `<Type>` at position `<Display order>`
ERR_1438	Updating definition for custom field with Id : `<Metadata ID>` failed as it is in use by `<Certificates using metadata>` certificates
ERR_1439	Updating definition for custom field with duplicate display order : `<Metadata values>`
ERR_1440	Other certificate custom field definitions exists with same display order `<List>`
ERR_1441	Updating definition for custom field with Id : `<Metadata ID>` failed as one of its value `<List>` is in use by `<Certificates>` certificates
ERR_1442	Error parsing the value `<Value>` for custom field `<Metadata ID>`
ERR_1443	Unsupported Operator `<Operator>` for custom field Id: `<Metadata ID>`
ERR_1450	Could not unarchive certificate because entitlement limit reached.
ERR_1452	Error response from CAGW `<Error>`
ERR_1453	Error exporting a certificate: `<Error>`
ERR_1454	Failed to parse certificate `<Certificate name>` stored in DB. Error: `<Error>`
ERR_1455	Certificate Chain is not available for export
ERR_1456	Error while exporting certificate: `<Error>`

Code	Message
ERR_1457	Error saving chain to keystore for export of : `<Certificate name>`
ERR_1458	Error adding P12 to response stream
ERR_1459	Unable to parse response from CAGW to export certificate for : `<Certificate name>` . Error: `<Error>`
ERR_1460	Certificate can not be exported since the issuing Authority is not known
ERR_1461	Certificate Authority not found
ERR_1462	Error adding P12 to response stream
ERR_1463	Unexpected response received from CAGW when exporting a certificate
ERR_1464	Internal error contacting CAGW
ERR_1465	Failed to export certificate for `<Certificate name>` . Error from CAGW: `<Error>`
ERR_1466	Failed to export certificate for `<Certificate name>` with serial number `<Certificate serial number>` . Certificate key is not backed up.
ERR_1467	Unable to parse response from CAGW to export certificate for : `<Certificate name>` . Error: `<Error>`
ERR_1468	Export private key is not supported for export type `<Type>` You can uncheck \\\"Include Private Key\\\" and try again, however, your exported certificate will not have the private key
ERR_1469	Export certificate chain is not supported for export type `<Type>` You can uncheck \\\"Include Certificate Chain\\\" and try again, however, your exported certificate will not have certificate chain

Code	Message
ERR_1470	Public certificate must be requested for export type `<Type>`
ERR_1471	At least one of public certificate, certificate chain or private key must be requested for export type `<Type>`
ERR_1472	At least one of public certificate, certificate chain or private key must be requested for export type `<Type>`
ERR_1473	Unable to revoke the authority `<Authority name>`
ERR_1474	Unable to unhold the authority `<Authority name>`
ERR_1477	Error building certificate query with filter : `<Filter>` . Error `<Error>`
ERR_1478	Error fetching certificates with predicate : `<Predicate>` . Error `<Error>`
ERR_1479	Certificate Bulk Edit Error: 'certificatesFilter' missing from request body
ERR_1480	Certificate Bulk Edit Error: If 'clearOutAccessTags' is set, 'accessTags' must be empty.
ERR_1481	Certificate Bulk Edit Error: No updated values provided
ERR_1482	Certificate Bulk Edit Error building certificate query with filter : `<Filter>` , Error : `<Error>` .
ERR_1483	Certificate Bulk Edit Error building certificate query with filter : `<Filter>` , Error : `<Error>` .
ERR_1484	Certificate Bulk Edit Error updating certificates with filter : `<Filter>` , Error : `<Error>`

Code	Message
ERR_1486	Certificate unhold error : Could not find certificate with id: `<Certificate ID>` .
ERR_1487	Certificate unhold error : No Authority Id associated with this certificate: `<Certificate ID>` .
ERR_1488	Certificate unhold error : Cannot unhold certificate `<Certificate ID>` . Authority is not active : `<Authority ID>` .
ERR_1489	Certificate unhold error : Cannot unhold certificate `<Certificate ID>` . No external id found.
ERR_1490	Issue certificate error : Subject DN is required for CSR.
ERR_1491	Issue certificate error : CAGW failed to create certificate for authority `<Authority ID>`
ERR_1492	Issue certificate error : CAGW Failed to create certificate: `<Key manager ID>` .
ERR_1493	Issue certificate error : Subject DN is required for CSR.
ERR_1494	Issue certificate error : Subject DN is required for CSR.
ERR_1495	Issue certificate error : Subject DN is required for CSR.
ERR_1496	Issue certificate error : Subject DN is required for CSR.
ERR_1497	Failed to save certificate: `<Error>`
ERR_1498	Failed to upload certificate to the key manager `<Key manager ID>` . Error `<Error>`

Code	Message
ERR_1499	Certificate revoke error : No Authority Id associated with this certificate. `<Certificate ID>`
ERR_1500	Certificate revoke error : Cannot revoke certificate `<Certificate ID>`. Authority `<Authority ID>` is not active.
ERR_1501	Certificate revoke error : Cannot revoke certificate `<Certificate ID>`. No external id found.
ERR_1502	Failed to apply service-level filters on query `<Filter>`
ERR_1503	Failed to apply service-level filters on query `<Filter>`
ERR_1504	Failed to apply service-level filters on query `<Filter>`
ERR_1505	Could not find certificate with id `<Certificate ID>`
ERR_1506	Could not find certificate with id `<Certificate ID>`
ERR_1508	Failed to issue a certificate from authority `<Authority name>`. Error `<Error>`
ERR_1509	Failed to parse the X509 certificate `<Certificate body>` \n Message: `<Error>`
ERR_1510	Unable to find certificate `<Certificate ID>`
ERR_1511	Failed to process the certificate `<Certificate import request body>` \n Message: `<Error>`
ERR_1512	Failed to process the certificate `<Certificate body>` \n External ID: `<Certificate External ID>` \n Message: `<Error>`

Code	Message
ERR_1513	Failed to apply service-level filters on query `<Filter>`
ERR_1514	Failed to run the certificate count query: `<Error>`
ERR_1521	Error verifying source config `<Source Label>`
ERR_1522	Error verifying source config for plugin `<Plugin name>`
ERR_1523	addOrUpdateSource: Error converting plugin options to Json string from list
ERR_1524	Error scheduling source sync, sources will not ne scanned!
ERR_1525	Error creating certificate from certficate request
ERR_1526	Failed to send new external certificate request notification to approver(s). Error : `<Notification message>`
ERR_1527	Failed to send external certificate request cancellation notification to requestor. Error : `<Notification message>`
ERR_1528	Failed to send certificate request approval notification to requestor. Error : `<Notification message>`
ERR_1529	Failed to send certificate request rejection notification to requestor. Error : `<Notification message>`
ERR_1530	Failed to send new certificate request notification to internal requestor. Error : `<Notification message>`
ERR_1531	Failed to send new internal certificate request notification to approver(s). Error : `<Notification message>`

Code	Message
ERR_1533	Failed to send new certificate request notification to external requestor. Error: `<Notification message>`
ERR_1534	CSR key algorithm `<CSR key algorithm>` does not match the required key algorithm `<Allowed key algorithm>`
ERR_1536	CSR key algorithm keysize `<CSR key size>` does not meet minimum public key size required : `<Allowed key size>`
ERR_1537	Invalid certificate signing request provided
ERR_1540	Failed to send new certificate request notification to external requestor. SMTP Notification Plugin not found
ERR_1541	Failed to send certificate request cancellation notification to external requestor. SMTP Notification Plugin not found
ERR_1542	Failed to send new external certificate request notification to approver(s). SMTP Notification Plugin not found
ERR_1543	Failed to send new certificate request notification to admin. SMTP Notification Plugin not found
ERR_1544	Failed to send new internal certificate request notification to approver(s). SMTP Notification Plugin not found
ERR_1545	Failed to send notification for certificate request cancellation. SMTP Notification Plugin not found
ERR_1546	Failed to send notification for certificate request approval. SMTP Notification Plugin not found
ERR_2010	Found invalid certificate with name `<Certificate name>`.
ERR_2011	Unexpected exception while processing certificate.

Code	Message
ERR_2012	Error processing certificate.
ERR_2013	Error creating certificate factory.
ERR_2015	Failed to parse certificate `<Certificate name>` stored in DB. Error: `<Error message>`

Migrating Certificate Manager database to an external host

Only Certificate Manager installations migrated from older versions support an internal database—that is, a database running on the same host as the application. See below for switching from an internal database to an external one.

- Exporting the database contents
- Restoring the database contents
- Applying the database changes to Certificate Manager

⚠ Run the steps below in the same version of Certificate Manager that will use the database.

Exporting the database contents

On any Cryptographic Security Platform installation node, open an SSH session and set the following environment variables.

Variable	Value
KUBECTL	`kubectl`
NAMESPACE	`certhub`
POSTGRES_DB	`certhub`
POSTGRES_PWD	The value of the **Database User Password** configuration parameter described in Configuring and deploying Certificate Manager.
POSTGRES_USER	The value of the **Database User Name** configuration parameter described in Configuring and deploying Certificate Manager.

Run the following commands

```
now=$(date +"%m_%d_%Y")
```

```
$KUBECTL exec deployment/postgres -n "$NAMESPACE" -- bash -c "export
PGPASSWORD=$POSTGRES_PWD; pg_dump -d $POSTGRES_DB -U $POSTGRES_USER"  > "db-backup-
$now.sql"
```

Restoring the database contents

Perform the following steps on an external host to restore the database contents.

To restore the database contents on an external host

1. Install the PostgreSQL version described in Database requirements.
2. Copy the `db-backup-<date>.sql` backup file generated when Exporting the database contents.
3. Set the following environment variables to the values described in Exporting the database contents.
    - POSTGRES_DB
    - POSTGRES_PWD
    - POSTGRES_USER
4. Run the following command.

```
export PGPASSWORD=$POSTGRES_PWD; psql -d $POSTGRES_DB -U $POSTGRES_USER -f db-
backup-<date>.sql
```

Applying the database changes to Certificate Manager

Complete database migration by performing the following operations on Cryptographic Security Platform.

To apply the database changes to Certificate Manager

1. Log in to the Management Console.
2. Update the database configuration parameters described in Configuring and deploying Certificate Manager to match the new external database.
3. Redeploy Certificate Manager to make the changes effective.
4. Wait while the redeployment with the external database is complete.
5. Open an SSH session as an administrator.
6. Manually remove the PostgreSQL pod.

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
- Generating a timestamping key pair and certificate
- Configuring and deploying Timestamping Authority
- Testing the timestamping service

> ⚠ As explained in Manually 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.

> ℹ Skip this step if you use software cryptography (not recommended).

HSM	Command	Additional steps
Entrust nShield HSM	tsactl import-nshield	See Administrating nShield HSM integration
Thales HSM	tsactl import-thales	—

Generating a timestamping key pair and certificate

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-----
MIICqDCCAZACAQAwMzExMC8GA1UEAxMoNGEwMGE0NjE3ZDFhZmQ1YWQ2MjY5NTUx
…
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 timestamping certificate

Use your CA to process the CSR obtained in Generating a timestamping key pair and issue a certificate with the following extension values.

Extension	Value
Key Usage	digitalSignature
Extended Key Usage	timeStamping

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:

```
{
  "csr": "MIIDVzCCAb8...",
  "profileId": "wstep-digital-signature",
  "requiredFormat": {
    "format": "X509"
  },
  "optionalCertificateRequestDetails": {
    "extensions": [
      {
        "oid": "2.5.29.37",
        "critical": true,
        "value": "1.3.6.1.5.5.7.3.8"
      }
    ],
    "validity_period": "2024-11-06T13:00Z/2026-07-06T13:00:00Z"
  }
}
```

See below for the values required by each request field.

Field	Line	Value
csr	2	The base64-encoded Certificate Signing Request previously generated in Generating a timestamping key pair as a single line.
extensions	8	The same fields and values as in the above example (to select the timestamping extended key usage).
validity_period	15	The validity period for the issued certificate. The expiry date in this period cannot exceed the expiry date of the issuing CA certificate.

Processing the timestamping certificate request

See below for processing the timestamping certificate request and obtaining the issued certificate.

To process the timestamping certificate request

1. Use a REST client to process the request as explained in Issuing certificates with a REST client.
2. Edit the REST response and copy the base64-encoded string in the `body` field.
3. Save the string in a file with the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters – for example:

```
-----BEGIN CERTIFICATE-----
MIIIcDCCBligAwIBAgITMwEf/Fvr7NDwanyeRAAAAR/8WzANBgkqhkiG9w0BAQwF
ADBdMQswCQYDVQQGEwJVUzEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9u
...
UdO85g==
```

```
-----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>:8443/management-console
   ```

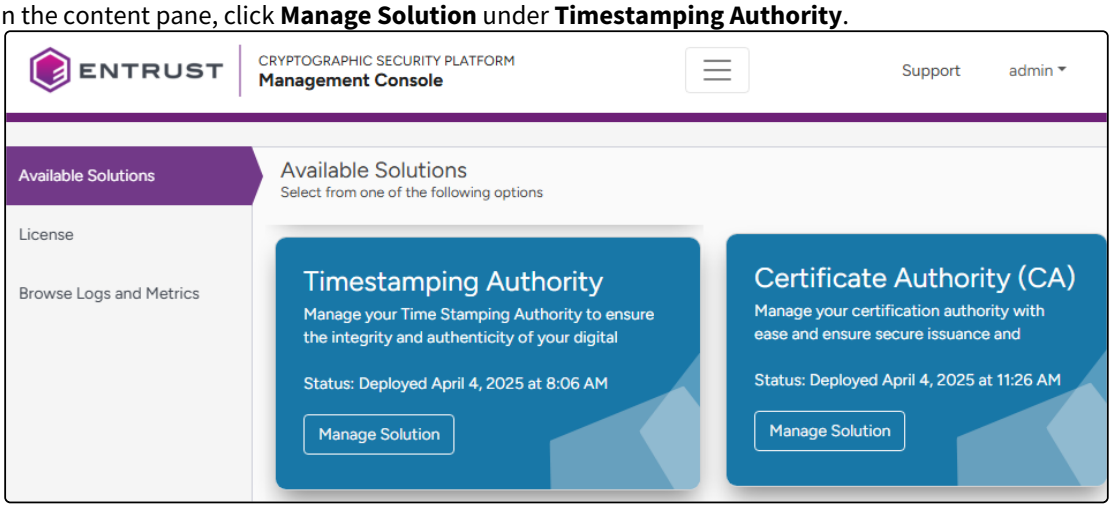
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

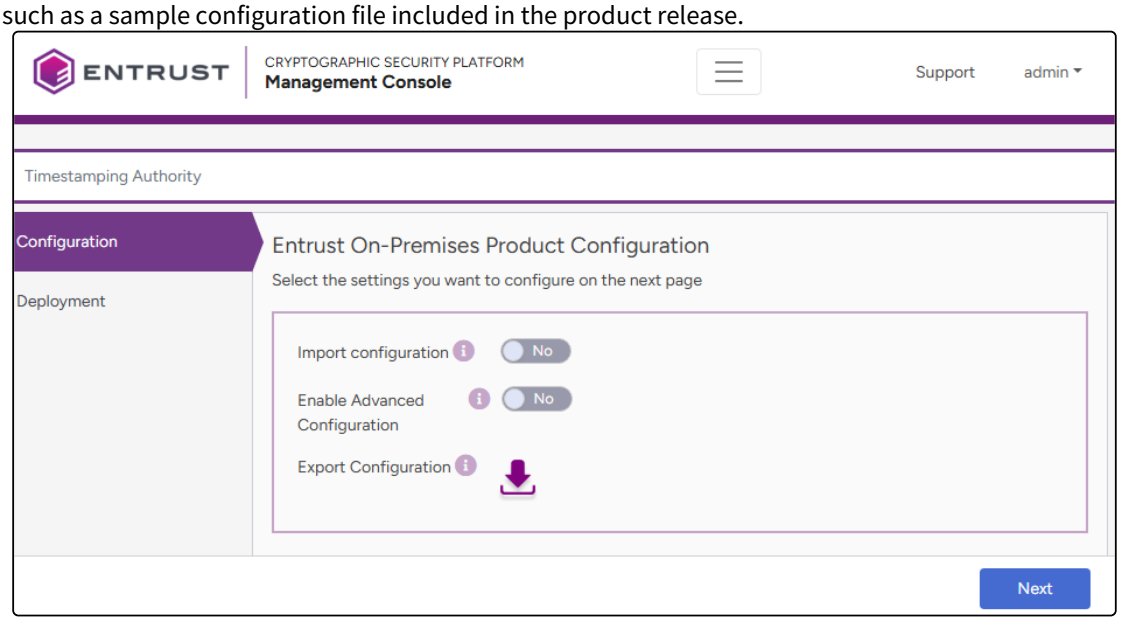
2. Log in to the Management Console as a user belonging to a role with Timestamping Authority management permissions – for example, the initial `admin` administrator user.

   > ℹ See Managing identities 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 HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: Yes.

Token Label

The label of the 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.

ℹ 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 `crony` 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 key pair and 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.

CA chain

Clic **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
- Use RSA-PSS

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.

Use RSA-PSS

Check this box to enable RSA-PSS for the selected **Signature digest algorithm**.

RSA-PSS is an RSA-based probabilistic signature scheme that enhances the security of RSA signatures.

Mandatory: No.

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 `<file>` file.
-sha256	Use the SHA256 algorithm to hash the data.
-cert	Add to the response the certificate described in Issuing a timestamping certificate.
-out <file>	Save the generated request in the `<file>` 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 Entrut 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 administrating the Validation Authority solution.

- Validation Authority overview
- Loading the HSM configuration on Validation Authority
- Initializing the Validation Authority database
- Configuring a certificate information source
- Generating a VA certificate and key pair
- Configuring and deploying 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

> 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.

> 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.

> Skip this step if you use software cryptography (not recommended).

HSM	Command	Additional steps
Entrust nShield HSM	evactl import-nshield	See Administrating nShield HSM integration
Thales HSM	evactl import-thales	Contact the Thales support team if you experience issues with Thales TCT on high availability

Initializing the Validation Authority database

Create an external database meeting the Database requirements, and initialize this database as explained in the following sections.

- Downloading the Validation Authority database scripts
- Setting the variables of the Validation Authority database scripts
- Running the Validation Authority database scripts

Downloading the Validation Authority database scripts

See below for instructions on downloading the Validation Authority database scripts.

To download the Validation Authority database scripts

1. Log in to the secure trustedcare.entrust.com portal with your customer credentials.
2. Select the **PRODUCTS** tab.
3. Click **Cryptographic Security Platform**.
4. Select the product version.
5. In the **SOFTWARE DOWNLOADS** tab**,** download the compressed file containing the database scripts.
6. Extract the contents of the compressed file. In Linux operating system, run:

```
tar -xvf eva-database-scripts.tar.gz
```

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.

Variable	Value
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.

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

> 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
```

Configuring a certificate information source

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 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.

> ℹ 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.

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 an OCSP certificate request
- Processing the OCSP 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 an OCSP certificate request

Create a CA Gateway certificate enrollment request – for example:

```
{
  "csr": "MIIDVzCCAb8...",
  "profileId": "wstep-digital-signature",
  "requiredFormat": {
    "format": "X509"
  },
  "optionalCertificateRequestDetails": {
    "extensions": [
      {
        "oid": "2.5.29.37",
        "critical": true,
        "value": "1.3.6.1.5.5.7.3.9"
      }
    ],
    "validity_period": "2024-11-06T13:00Z/2026-07-06T13:00:00Z"
  }
}
```

See below for the values required by each request field.

Field	Line	Value
csr	2	The base64-encoded Certificate Signing Request previously generated in Generating a VA key pair as a single line.
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 OCSP certificate request

See below for processing the OCSP certificate request and obtaining the issued certificate.

To process the OCSP 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
```

```
ADBdMQswCQYDVQQGEwJVUzEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9u
...
UdO85g==
-----END CERTIFICATE-----
```

4. Use this certificate file as the VA certificate when configuring the OCSP Responder settings.

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.

Configuring and deploying 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>:8443/management-console
```

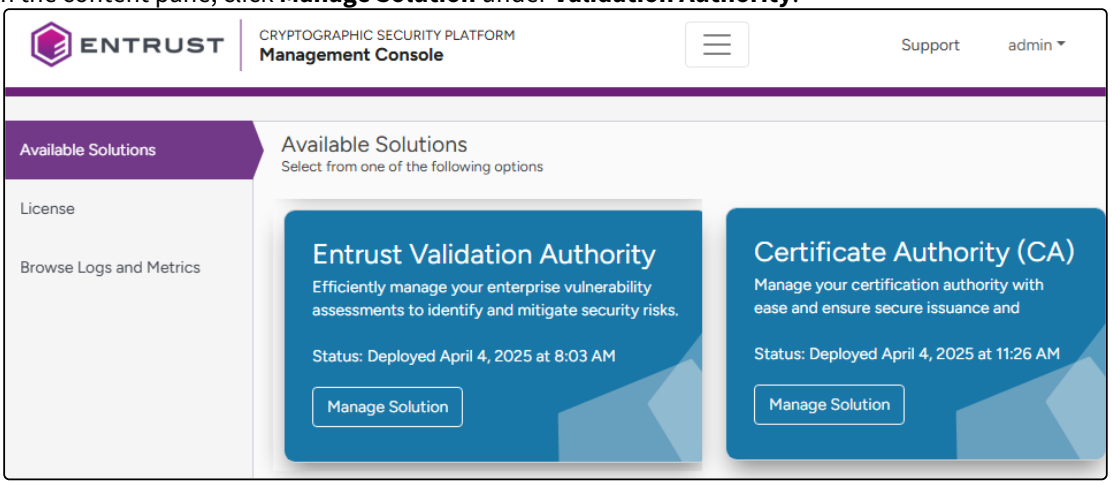
Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

> ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

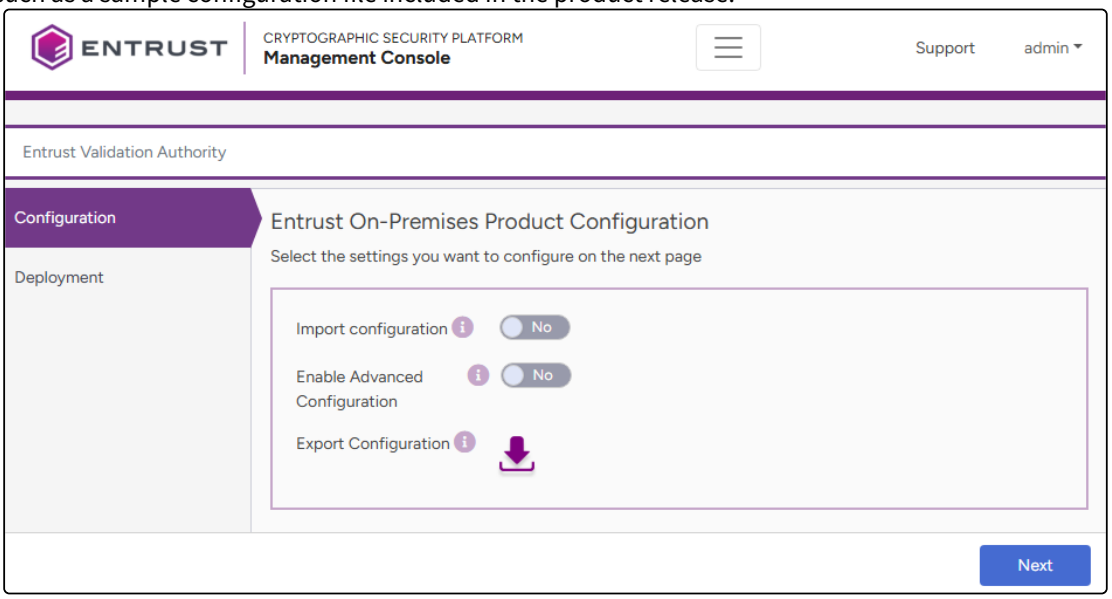
2. Log in to the Management Console as a user belonging to a role with Validation Authority management permissions – for example, the initial `admin` administrator user.

> ℹ See Managing identities 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	✗	✗	✗	✓
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 **Select Files** to import a file containing this certificate in PEM format and Base64 encoding.
oracle	enabled	Use the Oracle utilities to set this certificate.
sqlserver	enabled	Click **Select Files** to import a file containing this certificate in PEM format and Base64 encoding.

Hsm

Select the **Hsm** tab of the **Configuration** page to configure the connection wit the HSM (Hardware Security Module).

- Vendor
- Token label
- HSM PIN
- Number of sessions

Mandatory: Yes.

Vendor

The vendor of the security module.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: Yes.

Token label

The label of the token that contains the private keys of the OCSP server certificate.

ℹ 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.

> ℹ 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		✅
revoked	✅	✅
unknown		

Mandatory: Yes.

CRL Host Server

The type of server hosting the CRL.

- HTTP
- LDAP

Mandatory: Yes.

CRL warning time

The period during which to enable the expiration warning for the last processed CRL. When the time remaining before the CRL expiration is shorter than this parameter value, the `CRLExpirationWarning` metric is set to 1.

Mandatory: No. This optional value defaults to 4 hours.

Wait on error duration

The waiting time before retrying a failed connection with the CRL server, the Status Feeder internal service or the serial number list server.

Mandatory: No. This optional value defaults to "5s".

Wait to pull certs duration

The period between:

- The last upload of the CRL data into the database.
- The next request to the CRL server.

When **Use SN Lists** is ✔, Validation Authority will pull the CRL and the serial number list.

> ⚠ When enabling the **Retry Unknown Certificates** setting in the OCSP Responder-Server tab, this value must be less than or equal to `15s`.

Mandatory: Yes.

Certificate Revocation List in HTTP server

Configuration parameters of the HTTP server hosting the CRL.

- Connection timeout
- CRL HTTP URL

Mandatory: When CRL Host Server is **HTTP**.

Connection timeout

The timeout for connections with the CRL server. When the connection attempt exceeds this value:

1. The request fails.
2. Validation Authority tries another connection after the **Wait on error duration** period selected in CSP CA Gateway.

Mandatory: No. This optional value defaults to 5 seconds.

CRL HTTP URL

The URL of a CRL hosted in an HTTP server – for example:

```
http://127.0.0.1/crl.crl
```

Mandatory: Yes.

Certificate Revocation list in LDAP server

Configuration parameters of the LDAP server hosting the CRL.

- CRL Attribute Name
- CRL Entry Distinguished Name
- Connection timeout
- LDAP Server ID

Mandatory: When CRL Host Server is **LDAP**.

CRL Attribute Name

The name of the attribute that contains the CRL in the corresponding entry of the LDAP server.

Mandatory: No. This optional parameter defaults to:

```
certificateRevocationList;binary
```

CRL Entry Distinguished Name

The Distinguished Name of the entry that contains the CRL in the LDAP server.

Mandatory: Yes.

Connection timeout

The timeout for connections with the CRL server. When the connection attempt exceeds this value:

1. The request fails.
2. Validation Authority tries another connection after the **Wait on error duration** period selected in CSP CA Gateway.

Mandatory: No. This optional value defaults to 5 seconds.

LDAP Server ID

The identifier of the LDAP server.

Mandatory: Yes.

Serial number list HTTP

The configuration settings of the certificate serial number list hosted in an HTTP server.

- Connection timeout
- Serial Number list URL

Connection timeout

The timeout for connections with the HTTP server that hosts a list containing the serial numbers of all certificates issued by the CA. When the connection attempt exceeds this value:

1. The request fails.
2. Validation Authority tries another connection after the **Wait on error duration** period selected in CSP CA Gateway.

Mandatory: No. This optional value defaults to 5 seconds.

Serial Number list URL

The URL of a file containing the serial numbers of all certificates issued by the CA.

```
http://<host>[:<port>]/<file>
```

Where:

- `<host>` is the IP address or domain name of an HTTP server host.
- `<port>` is the port where the HTTP server listens in the host. Defaults to 80.
- `<file>` is the server path to a plain text file containing serial numbers, separated with newlines – such as:

```
00B289EFB35CB7DB0DD62F298BEF422DC1
00B28A0F6293B6F436845E2CE0B62D6E73
00B28A28E5E48BDC06C16737CF8648D2FF
00B28A3A7BB7DF5D8D1B1F61BCD612892F
00B28A3AC06981CD9B74474E1C5CC814B9
00B28A50BD25A8FAA1504F3C9C51467575
00B28A6D799142C3FAA4753E6B00B86EE6
00B28A7564BE6D8750E4685C3C9D0C4CF9
00B28AA8422EBE753C1C21424CDF3C36C6
00B28AA9C68891199600518FE18F7E1610
00B28ABEDD9190DDA89088BF2F227CE51F
00B28ADD33D8BC98BC8BBFACBC0001ACBF
00B28AE8334C44358CBF5856945AE8C26C
```

For example:

```
http://myhost:8080/certs/snlist.txt
```

Mandatory: Yes.

OCSP Responder

Configure the following parameters of the OCSP responder service provided by the Certification Authority.

- Profile ID
- Response Hash Algorithm
- CA certificate
- VA certificate
- Use RSA-PSS

Profile ID

The identifier of the profile for processing the certificate status before generating an OCSP response. See below for the response settings defined by each profile.

Profile identifier	nextUpdate	id-pkix-ocsp-archive-cutoff	Status if unknown	Revocation date
basic	—	—	revoked	Jan 1 00:00:00 1970 GMT
archiveCutOff	—	notBefore date of the CA certificate	revoked	Jan 1 00:00:00 1970 GMT
nextUpdate	thisUpdate + 8 hours	—	revoked	Jan 1 00:00:00 1970 GMT
archiveCutOffWithNextUpdate	thisUpdate + 8 hours	notBefore date of the CA certificate	revoked	Jan 1 00:00:00 1970 GMT
CRLProfile	—	—	good	—
CRLProfileWithArchiveCutOff	—	notBefore date of the CA certificate	good	—
SNListProfile	—	—	unknown	—
SNListProfileWithArchiveCutOff	—	notBefore date of the CA certificate	unknown	—

See the below for the Certificates Source and Use SN Lists values supported by each profile.

Profile identifier	Certificates Source	Use SN Lists
basic	CAGW	—
archiveCutOff	CAGW	—
nextUpdate	CAGW	—
archiveCutOffWithNextUpdate	CAGW	—
CRLProfile	CRL	False
CRLProfileWithArchiveCutOff	CRL	False
SNListProfile	CRL	True

Profile identifier	Certificates Source	Use SN Lists
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.

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.

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.

> RSA-PSS is an RSA-based probabilistic signature scheme that enhances the security of RSA signatures.

Use RSA-PSS

Check this box to enable RSA-PSS for the selected **Response Hash Algorithm**.

> RSA-PSS is an RSA-based probabilistic signature scheme that enhances the security of RSA signatures.

Mandatory: No.

Testing the OCSP Responder

After deploying Validation Authority, you can test the OCSP Responder service as follows.

- Testing the OCSP Responder with openssl
- Testing the OCSP Responder with the health check endpoint

Testing the OCSP Responder with openssl

Run the following `openssl` command to test the OCSP Responder service.

```
openssl ocsp -issuer <ca_cert> -serial <sn> -url <url> -VAfile <va_cert>
```

For example:

```
$ openssl ocsp -issuer issuer.pem -serial 0x000000002439fa8f5fe6370bb20ccb2556da6991
-url http://10.1.141.37/eva -VAfile ./VAFile.pem
Response verify OK
0x000000002439fa8f5fe6370bb20ccb2556da6991: good
        This Update: Nov  7 18:52:34 2022 GMT
        Next Update: Nov  8 02:41:13 2022 GMT
```

See below for a description of each command option.

- -issuer <ca_cert>
- -serial <sn>
- -url <url>
- -VAfile <va_cert>

> ⚠ The OCSP Responder service reboots when losing connection with the HSM. Run the evactl check all command to check the HSM connection and other settings.

-issuer <ca_cert>

Validate the status of a certificate issued by the `<ca_cert>` CA. Where `<ca_cert>` is the file path of the CA certificate.

-serial <sn>

Validate the status of the certificate with the `<sn>` serial number.

-url <url>

Connect to the `<url>` Validation Authority service. Where `<url>` is an URL in the following format.

```
http://<host>/eva
```

Where `<host>` is the IP address or hostname of the host running Validation Authority.

-VAfile <va_cert>

Validate the response with the `<va_cert>` certificate. Where `<va_cert>` is the file path of the certificate:

- Generated as explained in Generating a VA certificate and key pair.
- Selected as VA certificate when configuring the OCSP Responder settings.

Testing the OCSP Responder with the health check endpoint

Entrust Validation Authority exposes the following endpoint to check the health of the database and HSM connections.

```
http://<host>/eva/health
```

This endpoint returns an HTTP 503 response when the health check fails.

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>:8443/management-console
   ```

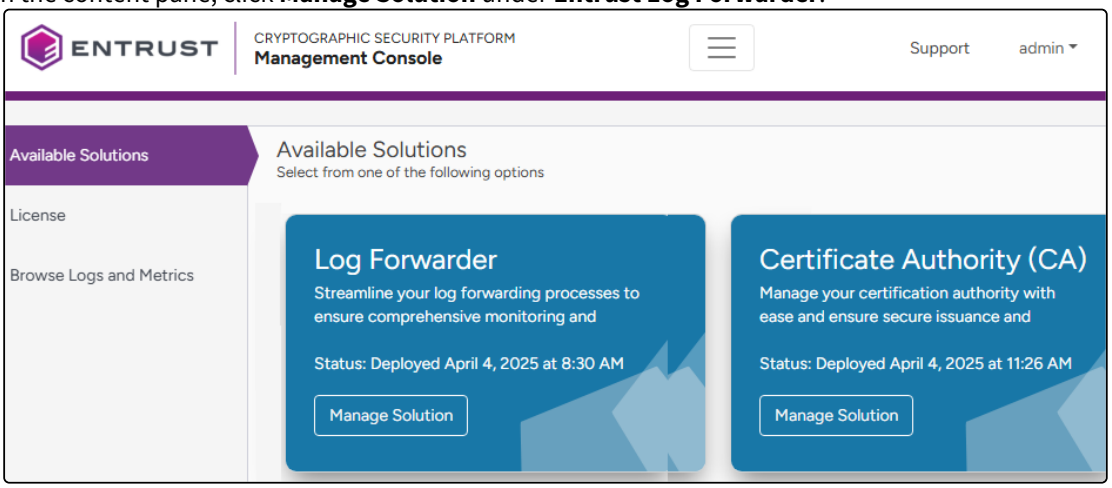
   Where `<machine>` is the IP address or domain name of the machine hosting Cryptographic Security Platform.

   > ⚠ This release changes the URL port to 8443. Update your bookmarks accordingly.

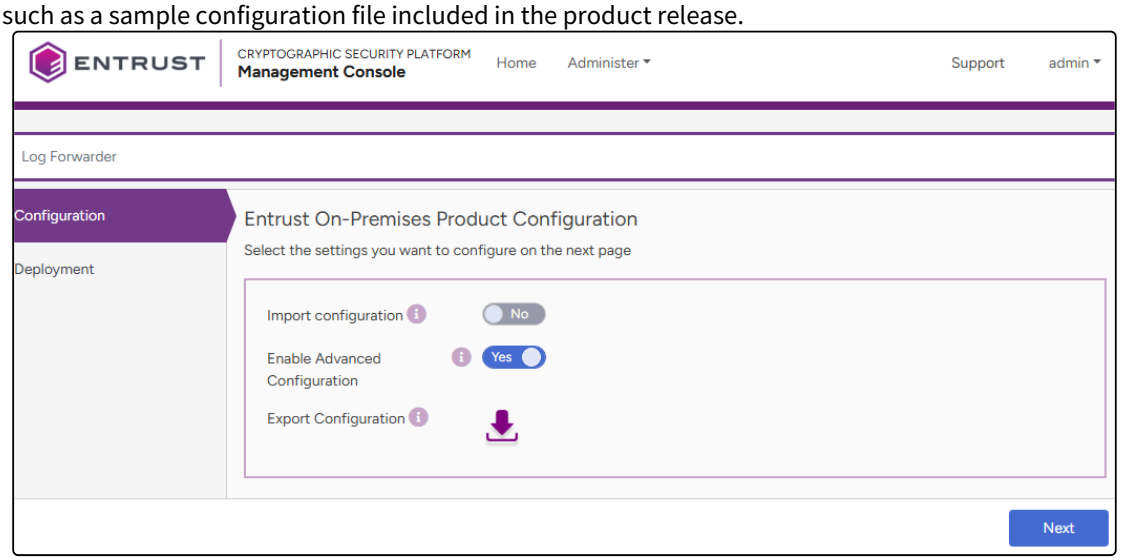
2. Log in to the Management Console as a user belonging to a role with Log Forwarder management permissions – for example, the initial `admin` administrator user.

   > ℹ See Managing identities 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

Type	SIEM 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

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 Administrating

Cryptographic Security Platform supports the administration operations described below.

- Administrating nShield HSM integration
- Checking the node health
- Checking the persistent volume disk usage
- Managing 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 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.

Managing the etcd database

See below for managing the etcd database integrated into Cryptographic Security Platform.

- Checking the etcd database size
- Defragmenting the etcd database

Checking the etcd database size

Check whether the etcd database needs to be defragmented.

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 requires defragmentation, or the etcd used space is approaching 100%, defragment the database as explained in the following section.

Defragmenting the etcd database

Repeat the procedure sequentially in all the nodes to defragment the `etcd` database.

> ⚠ 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 the cluster, only `prod-mode` installations support disaster recovery.

Recovering single-node installations

When a single-node installation crashes, recover the Cryptographic Security Platform and the deployed solutions from a backup as explained in Restoring the state.

Recovering multi-node installations with a quorum

When your multi-node installation retains the quorum described in Required number of nodes, you must simply remove, restore and add the crashed nodes.

To recover a crashed node.

1. Mark the node as unschedulable.

```
sudo kubectl cordon <node-to-delete>
```

2. Drain the pods from the node to delete.

```
sudo kubectl drain <node-to-delete> --delete-emptydir-data --disable-eviction
--force --ignore-daemonsets --timeout=600s
```

3. Delete the node from the cluster.

```
sudo kubectl delete node <node-to-delete> --timeout=600s
```

4. Restore the node and add it again to the cluster, as explained in Adding nodes.

Recovering multi-node installations without a quorum

When your multi-node installation does not retain the quorum described in Load balancing requirements, follow the steps below for recovery.

To recover a multi-node deployment without a quorum

1. Run clusterctl uninstall in all the nodes to uninstall Cryptographic Security Platform.
2. Recover the Cryptographic Security Platform and the deployed solutions from a backup as explained in Restoring the state.

Restarting the nodes

Some Cryptographic Security Platform upgrades may require restarting the system. In prod-mode installations, restart the nodes:

- One by one.
- At least 15 minutes apart.

Otherwise, you might encounter system problems and risk losing the quorum described in Required number of nodes.

After restarting a node, run the following command to force the start of the `chrony` service.

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

Updating DNS resolution

To update DNS resolution after installing Cryptographic Security Platform, repeat the following instructions on each node.

As explained in DNS requirements, Cryptographic Security Platform does not support accessing a DNS server through a proxy.

Platform	Instructions
VMware vSphere or Nutanix	See the Configuring the connection of an ISO installation section of this guide.

Platform	Instructions
Amazon Web Services	Refer to the docs.aws.amazon.com product documentation.
Azure	Refer to the learn.microsoft.com/azure product documentation.

When completing the DNS update, run the following command to restart the `coredns` service.

```
sudo kubectl rollout restart deployment coredns -n kube-system
```

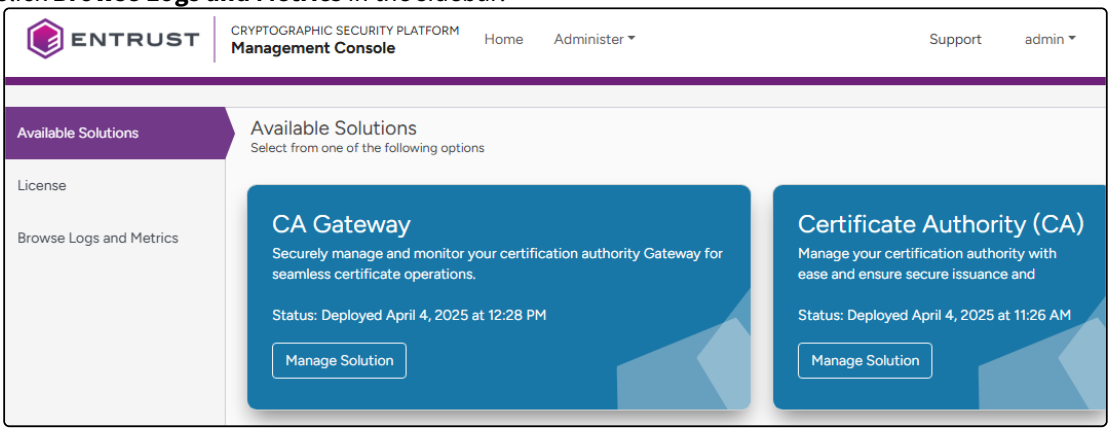
15 Browsing logs with Grafana

Cryptographic Security Platform provides a Grafana portal to browse logs and metrics on the internal services and the installed Entrust solutions.

> 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

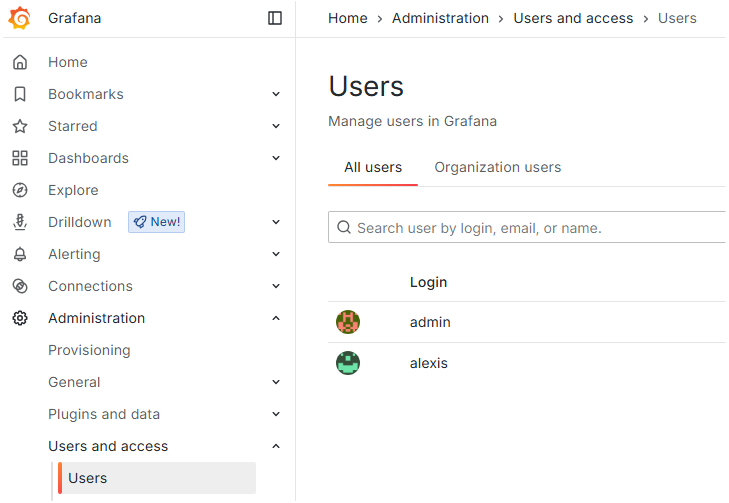
> The process described in Backing up does not include any Grafana configuration.

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:

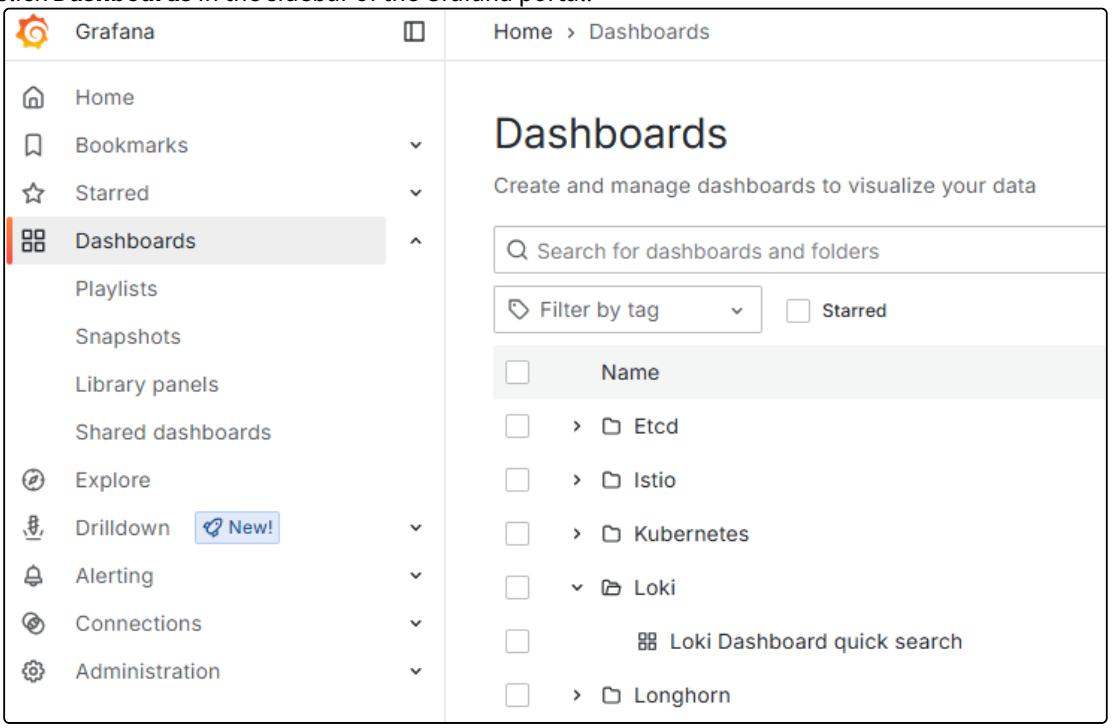
- **Delete user** to delete this initial administrator.
- **Disable user** to disable it.

Browsing and exporting logs with the Grafana Loki Dashboard

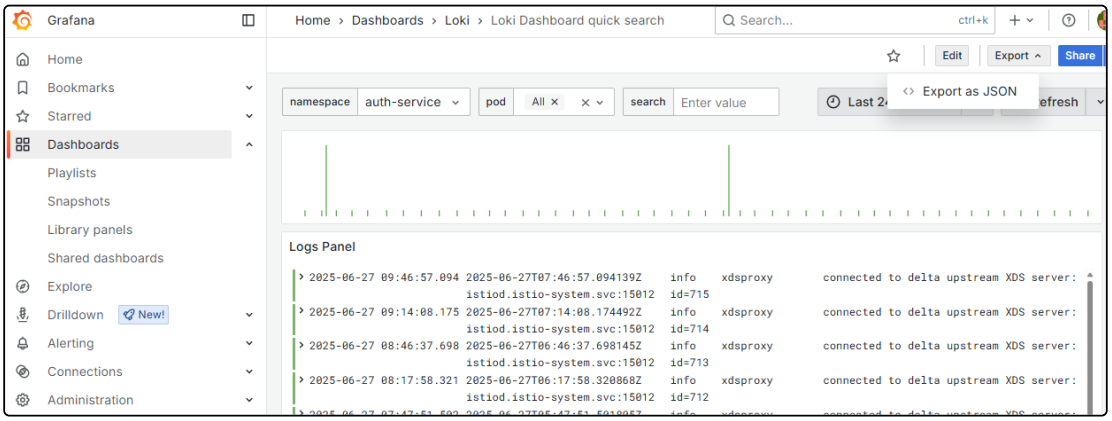
With the Grafana Loki Dashboard, users can browse and export logs of the Cryptographic Security Platform system and the deployed solutions.

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

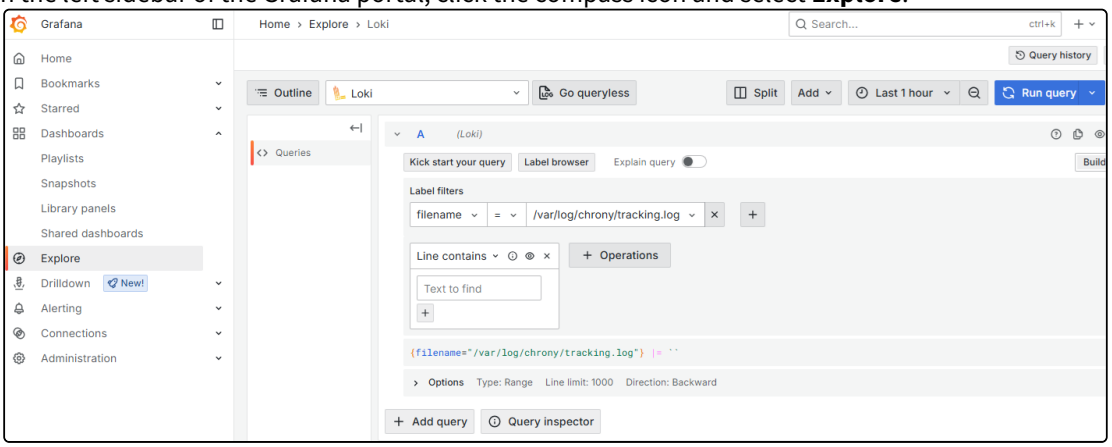
Click the clock icon in the top right menu and select the time range for querying logs.

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 `evactl` 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 `tsactl` commands

Checking the clock status

Add the following filters under **Label filters** to query clock status service logs.

Select label	Select value	Query output
namespace	tsa	Timestamping Authority logs.
app	clockstatus	Logs of the clock status service.

Use the **Line contains** field to filter time checking logs.

Line contains	Query output
"GetClockData.	Logs for time checking operations.

Querying timestamping request logs

Add the following filters under **Label filters** to query timestamping request logs.

Select label	Select value	Query output
namespace	tsa	Timestamping Authority logs.
app	tsa	Logs of the timestamping service.

Use the **Line contains** fields to add filters like the following.

Line contains	Query output
"ProcessTimeStampRequest.	Logs for all timestamping requests.
"ProcessTimeStampRequest.Failed"	Logs for failed timestamping requests.
"endpoint":"<issuerID>"	Logs for timestamping requests received by the `<issuerID>` timestamp issuer, where `<issuerID>` is the value of the Issuer ID configuration value.

16 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 the cluster, 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. Back up the Cryptographic Security Platform and solution databases 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.

   > ℹ 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 wit 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. Back up the Cryptographic Security Platform and solution databases 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 the cluster, 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.

   > ℹ 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. Restore the Cryptographic Security Platform and solution databases according to the instructions of the DBMS vendor.
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.

   > ℹ 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. Restore the Cryptographic Security Platform and solution databases according to the instructions of the DBMS vendor.
4. Import the license as explained in Setting 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**.

17 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 ╢▌▌▌
```

18 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 database info
- clusterctl database set
- clusterctl help
- clusterctl install
- clusterctl license import
- clusterctl node add
- clusterctl node info
- clusterctl node join-token
- clusterctl node user create
- clusterctl node user delete
- clusterctl node user info
- clusterctl node user modify
- 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 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
- tsactl check clock
- tsactl check hsm
- tsactl create-csr
- tsactl create-key
- tsactl delete-key
- tsactl export-nshield
- tsactl import-nshield
- tsactl import-thales
- tsactl list-keys
- tsactl stop

clusterctl backup create

Executed when: Backing up the state.

Saves the state of Cryptographic Security Platform and the installed Entrust solutions.

```
clusterctl backup create --file <file> [--password <pwd>]
```

See below for a description of each parameter.

- -f, --file <file>
- -p, --password <pwd>

For example:

```
$ sudo clusterctl backup create --path /home/sysadmin/edm20230307.bkp
Password:
Re-enter password:
Backing up config  done ╢▌▌▌
```

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
- ECDSA curve NIST P-384
- ECDSA curve NIST P-521

⚠ Password-protected keys are not currently supported.

Mandatory: Yes.

clusterctl database info

Prints the configuration set with the clusterctl install or clusterctl database set commands,

```
clusterctl db info
```

For example:

```
Host:                   dbhost
Port:                   5432
Name:                   dpsdb
Username:               dbadmin
Password:               ****
TLS enabled:            yes
TLS server cert:
 MIIDXTCCAkWgAwIBAgIJALa3alTAnU0+MA0GCSqGSIb3DQEBCwUAMEUxCzAJBgNV...
```

clusterctl database set

Modifies the database configuration.

```
clusterctl database set --host <host> --port <port> --name <name> --username
<username> [--password <password>] [--ca-certificate <ca-certificate>]
```

See below for a description of each parameter.

- --host <host>
- --port <port>
- --name <name>
- --username <username>
- --password <password>
- --tls-enabled <yes|no>
- --ca-certificate <ca-certificate>

--host <host>

Select the DBMS with the `<host>` domain name or IP address.

Mandatory: Yes.

--port <port>

Connect to the DBMS using the `<port>` port.

Mandatory: Yes.

--name <name>

Select the database with the `<name>` name.

Mandatory: Yes.

--username <username>

Authenticate in the database as the basic auth user with the `<username>` username.

Mandatory: Yes.

--password <password>

Authenticate in the database with the `<password>` user password.

Mandatory: No. This value is prompted to the user when omitted.

--tls-enabled <yes|no>

`yes` to enable TLS security in the connections with the database; `no` otherwise.

Mandatory: Yes.

--ca-certificate <ca-certificate>

Validate the TLS certificate of the DBMS using `<ca-certificate>`, where `<ca-certificate>` is the path to a PEM-encoded certificate file.

Mandatory: When enabling TLS.

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 the image.

Installs Cryptographic Security Platform.

```
clusterctl install --db-host <db-host> --db-port <db-port> --db-name <db-name> --db-
username <db-username> [--db-password <db-password>] [--db-tls-enabled <yes|no>] [--
db-ca-certificate <db-ca-certificate>] [--mode <mode>]
```

Omit `--db-password` to interactively enter the database password. For example:

```
[sysadmin@edm00 ~]$ sudo clusterctl install --db-host 10.10.10.10 --db-port 3333 --
db-name test --db-username test --db-tls-enabled no
Database password:

Installing  ⁝ ╢▒▒▒
```

Mandatory: Yes.

--db-name <db-name>

Select the database with the `<name>` name.

Mandatory: Yes.

--db-username <db-username>

Authenticate in the database as the basic auth user with the `<username>` username.

Mandatory: Yes.

--db-password <db-password>

Authenticate in the database with the `<password>` user password.

Mandatory: No. This value is prompted to the user when omitted.

--db-tls-enabled <yes|no>

`yes` to enable TLS security in the connections with the database; `no` otherwise.

Mandatory: Yes.

--db-ca-certificate <db-ca-certificate>

Validate the TLS certificate of the DBMS using `<ca-certificate>`, where `<ca-certificate>` is the path to a PEM-encoded certificate file.

Mandatory: When enabling TLS.

--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 Machine requirements. Specifically, fsync latency is not an issue in this mode.	All the Requirements.

Setting	demo-mode	prod-mode
Supported number of nodes	One	One or more. See Required number of nodes for details.
Supported operations	You cannot perform the operations described in Joining nodes, Backing up the state, Recovering from disaster, or Restoring the state.	All
Supported updates	You cannot upgrade to a newer version or migrate to a prod-mode installation.	All

Mandatory: No. This optional value defaults to `prod-mode`.

clusterctl license import

Executed when: Setting 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 10.1.141.38
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 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 the cluster.
- 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 the cluster.
- 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
LKBJxit1xwSHd7bHNHi3krGpkeDOkzT5P4BDYBlJlek=
                    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	`yes` if the user is enabled; `no` otherwise	On all types of users
SSH password auth	`yes` if the user has a password for SSH authentication; `no` otherwise	Only for users created with the clusterctl node user create 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.

<ssh-password-authentication>	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.

<enable>	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.

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 --protocol <protocol> option only supports the `https` 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.

ℹ Run the clusterctl solution info command to get the identifiers of the installed Entrust solutions.

Mandatory: Yes.

-f, --path <dir_path>

Import all configuration files that are included in the folder with the `<dir_path>` path and have filenames matching the following regular expression.

```
^[a-zA-Z0-9/\\._-]{3,64}$
```

✖ The command removes from the solution any other configuration file. Therefore, always run the clusterctl solution config import command beforehand to ensure you have the complete set of configuration files.

Mandatory: Yes.

clusterctl solution deploy

Deploys an Entrust solution or redeploys an already deployed Entrust solution to make configuration changes effective.

```
clusterctl solution deploy --solution-id <solution_id>
```

-i ,--solution-id <solution_id>

Deploy the solution with the `<solution_id>` identifier.

> Run the clusterctl solution info command to get the identifiers of the installed Entrust solutions.

Mandatory: Yes.

clusterctl solution info

Prints the main settings of each deployed Entrust solution.

```
clusterctl solution info
```

For example:

```
$ sudo clusterctl solution info
SOLUTION ID     DEPLOYED
ceg             1.4 at 2022-04-18T23:45:10.000Z (success)
cm              1.1 at 2022-07-11T10:49:31.000Z (success)
eva             1.0 at 2022-06-11T13:40:57.000Z
cagw            processing
```

See below for a description of each column.

- SOLUTION ID
- DEPLOYED

SOLUTION ID

The solution identifier. See the following table for these supported values.

Solution identifier	Solution
cagw	CA Gateway
cm	Certificate Manager
ceg	Certificate Enrollment Gateway
eva	Validation Authority

Solution identifier	Solution
Log Forwarder	Log Forwarder
pkihub-v<YYYYMMDDhhmm>	Certificate Authority, version `<YYYYMMDDhhmm>`.
tsa	Timestaping Authority

DEPLOYED

The date and status of the last deployment, in the following format.

```
<date> <status>
```

See the following table for the supported values.

Deployment status	<date>	<status>
Not deployed	—	Not deployed yet
In progress	The UTC date when the deployment started.	(deploying)
Successfully completed	The UTC date when the deployment ended.	(success)
Failed	The UTC date when the deployment started.	(failure)

clusterctl solution secret set

Sets the value of a secret.

```
clusterctl solution secret set --solution-id <solution_id> [--from-literal
<secret_id>=<secret_value> | --from-file <secret_id>=<secret_path>]
```

See below for a description of each parameter.

- -i ,--solution-id <solution_id>
- --from-literal <secret_id>=<secret_value>
- --from-file <secret_id>=<secret_path>

For example:

```
$ sudo clusterctl solution secret set --solution-id ceg --from-literal password='S!
B\*d$zDsb='
```

If already deployed, redeploy the solution with the clusterctl solution deploy command to make changes effective.

-i ,--solution-id <solution_id>

Set the secret in the solution with the `<solution_id>` identifier.

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
<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_value>	The value of the secret	Cannot exceed 128KB. Must be enclosed in quotes to escape special characters (such as `$`, `\`, `*`, `=`, and `!`) with a backlash (`\`) as in the above example.

Mandatory: No.

--from-file <secret_id>=<secret_path>

Set the secret value from a file.

This option is mutually exclusive with `--from-literal`. When omitting both options, the command assumes the `--from-literal` option and prompts the user for `<secret_id>` and `<secret_value>`.

Parameter	Value	Format restrictions
<secret_id>	The identifier of the secret	3-128 characters in length, start with a letter, and contain only alphanumeric characters, underscores, and hyphens.

Parameter	Value	Format restrictions
<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 backlash (`\`) as in the above example.

Mandatory: No.

clusterctl solution upload

Execute this command only when instructed by customer support to apply solution hotfixes.

Uploads a solution to the solution manager endpoint.

```
clusterctl solution upload --solution-id <solution_id> --file <sln>
```

See below for a description of each parameter.

- -i, --solution-id <solution_id>
- -f, --file <sln>

For example:

```
$ sudo clusterctl solution upload -i cm -f /home/sysadmin/cm.sln
Preparing  done ╢████████████████████████████████╟ 100 %
Uploading  done ╢████████████████████████████████╟ 100 %
Processing  done ╢███████████████████████████████╟ 100 %
Certificate Manager: version 4.1 uploaded
```

-i, --solution-id <solution_id>

Upload the solution with the `<solution_id>` the solution identifier.

Run the clusterctl solution info command to get the identifiers of the installed Entrust solutions.

Mandatory: Yes.

-f, --file <sln>

Upload the `<sln>` solution setup file, where `<sln>` is the path of the Entrust solution setup file with `sln` extension.

Login to trustedcare.entrust.com for downloading this file.

Mandatory: Yes.

clusterctl uninstall

Uninstalls Cryptographic Security Platform along with all the deployed Entrust solutions.

```
clusterctl uninstall [-y]
```

When prompted, confirm the uninstall process.

```
$ sudo clusterctl uninstall
The cluster and the deployed solutions are going to be uninstalled
Are you sure you want to uninstall the cluster? [Y/n]:
```

-y, --yes

Skip the confirmation prompt.

clusterctl version

Prints the Cryptographic Security Platform version.

```
clusterctl version
```

For example, after installing or upgrading Cryptographic Security Platform to version 1.3.0.

```
$ sudo clusterctl version
Cryptographic Security Platform release 1.3.0
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 1.3.0
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 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 SO (PED) Signing With
Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         FM Ready


        Current Slot Id: 0

Passing HSM checks...                       Done

=============================================
CHECKING DB
=============================================
Starting Configurator...                    Done
Checking DB user privileges...              Done
```

```
Checking DB tables...                          Done

================================================
CHECKING CAGW
================================================

CAID: intminions~subordinate
  Checking CAGW is reachable...                Done
  Checking configured CA...                    Done

================================================

Tests passed successfully
```

See below for a description of each parameter.

- -c <tls_ca_path>
- -i <cert_id>
- -l <level>
- -p <pin>
- -v <vendor>
- -t <token>

-c <tls_ca_path>

Validate the TLS server certificate of CA Gateway with `<tls_ca_path>`. Where `<tls_ca_path>` is the path of a CA file in PEM format.

Mandatory: No. When omitting this option, the command uses the CA configured in CSP CA Gateway.

-i <cert_id>

Authenticate in CA Gateway with the `<cert_id>` certificate, where `<cert_id>` is the identifier of the certificate described in CA Gateway for Validation Authority.

Mandatory: No. This optional parameter defaults to the latest client certificate imported with the evactl import-p12 command.

> Run the evactl list-certs command to list the available certificates and the latest one imported.

-l <level>

Debug the nShield HSM with the `<level>` level, where `<level>` is a `CKNFAST_DEBUG` variable level. When not using a nShield HSM, the command ignores this option.

> See the nShield documentation for details on the `CKNFAST_DEBUG` configuration parameter.

Mandatory: No. This optional parameter defaults to 0.

-p <pin>

Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-v <vendor>

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

⊗ The command will raise an error if you omit this option and the configuration is not loaded.

-t <token>

Select the HSM token with the `<token>` label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

⊗ The command will raise an error if you omit this option and the configuration is not loaded.

evactl check cert-source

Checks the certificate sources for every configured CA.

```
evactl check cert-source [-c <tls_ca_path>] [-i <cert_id>]
```

For example:

```
$ sudo evactl check cert-source
Starting Configurator...                    Done
```

```
CAID: ca~subordinate
  Checking CAGW is reachable...            Done
  Checking configured CA...                Done

Tests passed successfully
```

See below for a description of each option.

- -c <tls_ca_path>
- -i <cert_id>

-c <tls_ca_path>

Validate the TLS server certificate of CA Gateway with `<tls_ca_path>`. Where `<tls_ca_path>` is the path of a CA file in PEM format.

Mandatory: No. When omitting this option, the command uses the CA configured in CSP CA Gateway.

-i <cert_id>

Authenticate in CA Gateway with the `<cert_id>` certificate, where `<cert_id>` is the identifier of the certificate described in CA Gateway for Validation Authority.

Mandatory: No. This optional parameter defaults to the latest client certificate imported with the evactl import-p12 command.

> Run the evactl list-certs command to list the available certificates and the latest one imported.

evactl check db

Checks the database connectivity, required users, user privileges, and tables.

```
evactl check db
```

For example:

```
$ sudo evactl check db
Starting Configurator...                   Done
Checking DB user privileges...             Done
Checking DB tables...                      Done
```

evactl check hsm

Checks the HSM connectivity.

```
evactl check hsm [-l <level>] [-p <pin>] [-v <vendor>] [-t <token>]
```

For example:

```
$ sudo evactl check hsm
Starting PKCS #11 Manager...                Done

        Slot Id ->              0
        Label ->                pking203
        Serial Number ->        1433959427612
        Model ->                LunaSA 7.2.0
        Firmware Version ->     7.0.3
        Configuration ->        Luna User Partition With SO (PED) Signing With
Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         FM Ready

        Slot Id ->              1
        Label ->                pking202
        Serial Number ->        1433964084224
        Model ->                LunaSA 7.2.0
        Firmware Version ->     7.0.3
        Configuration ->        Luna User Partition With SO (PED) Signing With
Cloning Mode
        Slot Description ->     Net Token Slot
        FM HW Status ->         FM Ready


        Current Slot Id: 0

Passing HSM checks...                       Done
```

See below for a description of each option.

- -l <level>
- -p <pin>
- -v <vendor>
- -t <token>

-l <level>

Debug the nShield HSM with the `<level>` level, where `<level>` is a `CKNFAST_DEBUG` variable level. When not using a nShield HSM, the command ignores this option.

> See the nShield documentation for details on the `CKNFAST_DEBUG` configuration parameter.

Mandatory: No. This optional parameter defaults to 0.

-p <pin>

Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-v <vendor>

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

⊗ The command will raise an error if you omit this option and the configuration is not loaded.

-t <token>

Select the HSM token with the `<token>` label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

⊗ The command will raise an error if you omit this option and the configuration is not loaded.

evactl create-csr

Generates a new certificate signing request (CSR) for a key pair previously generated with the evactl create-key command.

```
evactl create-csr -k <key_id> [-s <subject>] [-o <csr>] [-p <pin>] [-t <token>] [-v
<vendor>] [-y]
```

For example:

```
$ sudo evactl create-csr -k 7ce798c13a411bc1da4a9f983ed6d44fb4d7ed1a -s "CN=97357462,
O=Entrust, C=ES"
Starting PKCS #11 resource… Done
Using token with label mytoken
CSR:
----BEGIN CERTIFICATE REQUEST----
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 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 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 HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

⛔ The command will raise an error if you omit this option and the configuration is not loaded.

-y

Skip the confirmation prompt.

evactl create-key

Generates the key pair and the certificate signing request (CSR) of the certificate for signing OCSP responses.

```
evactl create-key -k <key_type> [-s <subject>] [-o <csr>] [-p <pin>] [-t <token>] [-v
<vendor>] [-y]
```

For example:

```
$ sudo evactl create-key -k RSA2048 -s "CN=97357462, O=Entrust, C=ES"
Starting PKCS #11 pod...          Done
Using token with label mytoken
Created key with id 4a00a4617d1afd5ad626955132dd0d396a69ed24
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIICqDCCAZACAQAwMzExMC8GA1UEAxMoNGEwMGE0NjE3ZDFhZmQ1YWQ2MjY5NTUx
…
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, --yes

-k <key_type>

Create a key of the `<key_type>` type, where `<key_type>` is one of the following.

<key_type>	Description	Post-quantum
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	✗
ML-DSA-44	Module-Lattice-Based Digital Signature Algorithm 44-bit	✓

<key_type>	Description	Post-quantum
ML-DSA-65	Module-Lattice-Based Digital Signature Algorithm 65-bit	✅
ML-DSA-87	Module-Lattice-Based Digital Signature Algorithm 87-bit	✅

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 HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

> It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

> The command will raise an error if you omit this option and the configuration is not loaded.

-y, --yes

Skip the confirmation prompt.

evactl delete-key

Deletes a key.

```
evactl delete-key -k <key-id> [-p <pin>] [-t <token>] [-v <vendor>] [-y]
```

For example:

```
$ sudo evactl delete-key -k c403e0abae421c73625666dcff26dacf184eddd4 -y
Starting PKCS #11 Manager...                Done
Using token with label pking203
Deleted public key with id c403e0abae421c73625666dcff26dacf184eddd4
```

```
Deleted private key with id c403e0abae421c73625666dcff26dacf184eddd4
```

See below for a description of each option.

- -k <key_id>
- -p <pin>
- -t <token>
- -v <vendor>
- -y

-k <key_id>

Select the key with the `<key_id>` identifier.

> Run the evactl list-keys command to get the key identifiers.

Mandatory: Yes.

-p <pin>

Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-t <token>

Select the HSM token with the `<token>` label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

> The command will raise an error if you omit this option and the configuration is not loaded.

-v <vendor>

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

> It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

The command will raise an error if you omit this option and the configuration is not loaded.

-y

Skip the confirmation prompt.

evactl enroll

Generates the certificate for authenticating in CA Gateway.

```
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>
- -c <tls_ca_path>
- -l <ca_label>
- -r <ref_number>
- -u <url>

-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 -o <kmdata_dir> [-t]
```

For example:

```
$ sudo evactl export-nshield -f /opt/nfast/copy-kmdata
```

See below for a description of each option.

- -o <kmdata_dir>
- -t

-o <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.

> ℹ See Loading the HSM configuration for considerations on this configuration.

Mandatory: Yes.

-y

Skip the confirmation prompt.

evactl import-p12

Sets the PKCS #12 described in CA Gateway for Validation Authority.

```
evactl import-p12 -f <p12> [-p <pwd>]
```

For example:

```
$ sudo evactl import-p12 -f eva-cagw.p12 -p password
Starting Configurator...                    Done
Importing P12...                            Done
```

See below for a description of each option.

- -f <p12>
- -p <pwd>

> ⚠ Changes will be effective when deploying (or redeploying) the solution with Management Console or the clusterctl solution deploy command.

-f <p12>

The path of the PKCS #12 file containing the key and the certificate for authenticating in CA Gateway.

Mandatory: Yes.

-p <pwd>

The password of the PKCS #12.

Mandatory: No. When omitting this option, the command prompts for the password.

evactl import-thales

Imports the configuration of a Thales HSM. Use the following syntax to import this configuration from a ZIP file.

```
evactl import-thales -d <package_path> [-y]
```

Use the following syntax to import this configuration from a Chrystoki file.

```
evactl import-thales -c <cert_dir> -k <chrystoki> [-y]
```

For example:

```
$ sudo evactl import-thales -c ./eva-thales-config/cert -k ./eva-thales-config/
Chrystoki.conf -y
Saving Thales configuration...              Done
Warning: EVA is already deployed! To apply the changes, EVA needs to be redeployed
using the evactl deploy command.
```

See below for a description of each option.

- -c <cert_dir>
- -d <package_path>
- -k <chrystoki>
- -y, --yes

> ⚠ Changes will be effective when deploying (or redeploying) the solution with Management Console or the clusterctl solution deploy command.

-c <cert_dir>

Import the client and server certificates for the Luna Network or DPoD authentication. Where `<cert_dir>` is the path of a `cert` directory with the following contents.

```
└──cert
    ├──client
    │       <clientKey>.pem
    │       <clientCert>.pem
    │
    └──server
            <caCert>.pem
```

See below for a description of each field.

Value	Description
<clientKey>	The file name of a PEM file containing the client's private key.
<clientCert>	The file name of a PEM file containing the client's certificate.
<caCert>	The file name of a PEM file containing the CA certificate for validating the server's certificate.

After running the command, verify the `Chrystoki.conf` file includes the following configuration.

```
ClientPrivKeyFile = /usr/safenet/lunaclient/cert/client/<clientKey>.pem;
ClientCertFile = /usr/safenet/lunaclient/cert/client/<clientCert>.pem;
ServerCAFile = /usr/safenet/lunaclient/cert/server/<caCert>.pem;
```

⚠ Do not modify any other path in the `Chrystoki.conf` file.

Mandatory: Yes.

-d <package_path>

Use the `<package_path>` DPoD configuration package, where `<package_path>` is the path of the ZIP package file.

Mandatory: Yes.

-k <chrystoki>

Import the `<chrystoki>` configuration of the Luna Network or DPoD client, where `<chrystoki>` is the path of the `Christoky.conf` file.

Mandatory: Yes.

-y, --yes

Skip the confirmation prompt.

evactl list-certs

Shows the list of certificates for authenticating in CA Gateway and their identifier.

```
evactl list-certs
```

For example:

```
$ sudo evactl list-certs
Starting Configurator...                    Done
[
  {
    "ID": 1,
    "Cert": "MIIEojCCA4qgAwIBAgIQYsON4k8fvI/
4oBjC2PXMrTANBgkqhkiG9w0BAQsFADBtMQswCQYDVQQGEwJFUzEcMBoGA1UEChMTRW50cnVzdCBDb3Jwb3Jh
dGlvbjEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRob3JpdGllczEcMBoGA1UEAxMTSW50ZXJuYWwgQ0EgR
2F0ZXdheTAeFw0yMjAxMzExMjAwMjhaFw0yNTAxMzExMjAwMjhaMFcxEzARBgNVBAoTCmludGNhZ3dpZHAxDT
ALBgNVBAsTBENBR1cxMTAvBgNVBAUTKDk5NzllYzE0NTRmZThkYzcwYTc4Yzc3YTFhMWU3OGI2Y2ZhZmRlNzc
wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDBN+5oV4wCZaIzjr7YVzbsBhyCqetGiJWwc4+x9P3K
KNMt9N2HxP3r3KDbHxx+pTtwEYUdJdNKGkP9JLSwPeT7KWS9LepeC86UBeGCdOiC8Sq2Swe1P27DAWcXdhtv6
bvhenv15NPumCL4mbEQNds96ghb+5N1CNyCKMo7zsMRy7WV5sW13Zjd6cvszFLXIc+7sUEntvn6pLyQ6CCxAp
jeOrmUf40QokBd56lFJXFOJ/
NhLfVrBe0QjJTShvI+WuLqHTjyGZqjpkJWtAkQAhFK9D4DXacutWs71CEQ4Gt87athz+H7pYLmPCzsZFAwF6j
rqG7tv0mvpw/
HMxtY9X47AgMBAAGjggFSMIIBTjAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBR1mxLvF1G4laYl/
UDjhQs5tro4hTAfBgNVHSMEGDAWgBQ4XuxK8LobB2x+dGs0jaqQoOBHwzBLBggrBgEFBQcBAQQ/
MD0wOwYIKwYBBQUHMAGGL2h0dHA6Ly9vY3NwLmRldi5wa2lodWIuY29tL29jc3AvZW50cnVzdC9pbnRjYWd3M
EYGA1UdHwQ/
MD0wO6A5oDeGNWh0dHA6Ly9jcmwuZGV2LnBraWh1Yi5jb20vY3JsL2VudHJ1c3QvaW50Y2Fndy9jcmwuY3JsM
EQGA1UdEQQ9MDuGOWlkcDovL2ludGNhZ3dpZHAvOTk3OWVjMTQ1NGZlOGRjNzBhNzhjNzdhMWExZTc4YjZjZm
FmZGU3NzAOBgNVHQ8BAf8EBAMCB4AwEwYDVR0lBAwwCgYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggEBADT
Wv5ii6/jJ2cqpif6zZ/
iRcx8I4Oha3oSn8j25ZSr8oU+wq7BWtQLQVNOZazGttnsf3mNDlqimIidO9tbNCt1vNTSB23NJ6V4B5ar/
vtO1FRnqNHUl/01GJtzvRM2cVIdjPJ+o9fp0Cttr2+zd/
8S4U3W5hoLBDVrod8ke4eVrc3bBktfhnr9VB59eT+dztSTTMm0WTOAeB+DivOeIPQjxE4A4qtCyw6MFhxqZer
z8Piy88Qz0CXQEFeDNIbvFESl1BQWAYVYcfomNurfTvimkJFeyoTPvqSnbmK2SO0bPMCVGiW5zl7w/
LDs6zLhdHpqXwaPzHeycx2HnZBWSOIg=",
    "SN": "62:C3:8D:E2:4F:1F:BC:8F:F8:A0:18:C2:D8:F5:CC:AD",
    "DN": "subject=O = intcagwidp, OU = CAGW, serialNumber =
9979ec1454fe8dc70a78c77a1a1e78b6cfafde77"
  },
  {
    "ID": 2,
    "Cert":
"MIIEojCCA4qgAwIBAgIQMVr8yW7+GCBCa3lyRBSt3jANBgkqhkiG9w0BAQsFADBtMQswCQYDVQQGEwJFUzEc
MBoGA1UEChMTRW50cnVzdCBDb3Jwb3JhdGlvbjEiMCAGA1UECxMZQ2VydGlmaWNhdGlvbiBBdXRob3JpdGllc
zEcMBoGA1UEAxMTSW50ZXJuYWwgQ0EgR2F0ZXdheTAeFw0yMjA5MjMxNjU3MzBaFw0yNTA5MjMxNjU3MjlaMF
cxEzARBgNVBAoTCmludGNhZ3dpZHAxDTALBgNVBAsTBENBR1cxMTAvBgNVBAUTKDA3NzYyZWM1MzdjYWJhYmY
1MGRiNTI3ODNhN2NmMzU0N2EzYmYyYjMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvtsMW84yx
E5Ln6XMprAE6rvIApr0fevYqoaBI89gOdTyf6LSer0eSigVGr4TMyW6yhmfyzQKvBevP/
rK4pCB6mBoAiUTr5QF7HwBUJ0z4xbmiIxwhXIFcVNvXKnCekg3eHVS9DShdjy4U/
```

```
Vt6tXSZmHkI1rZ1uEJweBWVlGp8MHHU6Rot0mZFZ0ourxihmRcD3siDHXu6hADp54wHjGDET7V2WVPMKVcVAW
e+TgzAJcVpYBwO7fj4kqER2UmloT0PfjRtddTC9swxl30aC+UfmleAoBrSjWB+O6lw6Obp5oL1gPgIUD9R5fZ
osqPNbVfS5gs6/
Vo5BqfFcGIGMxVTAgMBAAGjggFSMIIBTjAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBSk2b3+ZE3ZyIe4bTi3ph
Adv6jB0zAfBgNVHSMEGDAWgBQ4XuxK8LobB2x+dGs0jaqQoOBHwzBLBggrBgEFBQcBAQQ/
MD0wOwYIKwYBBQUHMAGGL2h0dHA6Ly9vY3NwLmRldi5wa2lodWIuY29tL29jc3AvZW50cnVzdC9pbnRjYWd3M
EYGA1UdHwQ/
MD0wO6A5oDeGNWh0dHA6Ly9jcmwuZGV2LnBraWh1Yi5jb20vY3JsL2VudHJ1c3QvaW50Y2Fndy9jcmwuY3JsM
EQGA1UdEQQ9MDuGOWlkcDovL2ludGNhZ3dpZHAvMDc3NjJlYzUzN2NhYmFiZjUwZGI1Mjc4M2E3Y2YzNTQ3YT
NiZjJiMzAOBgNVHQ8BAf8EBAMCB4AwEwYDVR0lBAwwCgYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggEBAFy
o2+QcxN4gN8XxhnErYQ3ET9kk5hrXUa+RGGCtLiegiNKX/
fxlG0V51QglvP4rFd12bnYCMqSQulq0HO8mOE3U7wmKZem4OMlOIfjp94RyDHaMnpOWv9e4C6I6Q6nv4CX6nr
9TDmpIKG32c0kKu7veSZaLDBVA/Wg+W2ox6yf3W8PbPpUbf6Ld6UC/
guOhzBMLqw8H+lq4WQs9KWcFFF5+XMm4y1Q38HIL0bODBVpeibOQOno41mc9+7w/
0W3ix+DDcuLIJEMaKg0ynXujl9Ga0wfm7qZdC+eJ1z0N3m2HBVfZWFEWaKZ8lm2ZqkuZNzCyKJ430qgP2X2WF
axav+c=",
    "SN": "31:5A:FC:C9:6E:FE:18:20:42:6B:79:72:44:14:AD:DE",
    "DN": "subject=O = intcagwidp, OU = CAGW, serialNumber =
07762ec537cababf50db52783a7cf3547a3bf2b3"
  }
]
```

evactl list-keys

Lists the keys in the PKCS #11 token.

```
evactl list-keys [-p <pin>] [-t <token>] [-v <vendor>]
```

For example:

```
$ sudo evactl list-keys
Starting PKCS #11 Manager...                Done
Using token with label pking203
Public Key Object; RSA 2048 bits
  Label:      305ecd78340acc3d906be370a01e7884
  ID:         03b1dac1e383b8d3adea5a6a2c6200bde58ffb40
  Usage:      verify

Private Key Object; RSA 2048 bits
  Label:      F
  ID:         0f
  Usage:      sign, unwrap

Public Key Object; RSA 2048 bits
  Label:      F
  ID:         0f
  Usage:      verify, wrap

Private Key Object; RSA 2048 bits
  Label:      webserver-root1
```

```
ID:         103d6c94ea10b98ab37186cc1c4977eb
Usage:      sign
```

See below for a description of each option.

- -p <pin>
- -t <token>
- -v <vendor>

-p <pin>

Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-t <token>

Select the HSM token with the `<token>` label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

> The command will raise an error if you omit this option and the configuration is not loaded.

-v <vendor>

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

> It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

> The command will raise an error if you omit this option and the configuration is not loaded.

evactl load-oracle-wallet

Loads the Oracle wallet for validating the TLS server certificate of an Oracle DBMS. Overwrites the wallet previously loaded.

```
evactl load-oracle-wallet -f <wallet-folder> [-y]
```

For example:

```
sudo evactl load-oracle-wallet -f ./oracle-wallet
Loading Oracle Wallet...                          Done
```

See below for a description of each option.

- -f <wallet-folder>
- -y

> ⚠ 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.

> ℹ 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>

-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 <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.

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 7.2.1.4
        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 7.2.1.4
        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
```

```
        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, --yes

-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 HSM requirements for the supported models.

Vendor	Security module
thales	Thales HSM. See HSM requirements for the supported models.

It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

The command will raise an error if you omit this option and the configuration is not loaded.

-y, --yes

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-----
MIICqDCCAZACAQAwMzExMC8GA1UEAxMoNGEwMGE0NjE3ZDFhZmQ1YWQ2MjY5NTUx
…
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, --yes

-k <key_type>

Create a key of the `<key_type>` type, where `<key_type>` is one of the following.

<key_type>	Description	Post-quantum
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	✗
ML-DSA-44	Module-Lattice-Based Digital Signature Algorithm 44-bit	✓
ML-DSA-65	Module-Lattice-Based Digital Signature Algorithm 65-bit	✓
ML-DSA-87	Module-Lattice-Based Digital Signature Algorithm 87-bit	✓

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 HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

> ⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

The command will raise an error if you omit this option and the configuration is not loaded.

-y, --yes

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, --yes

-k <key_id>

Select the key with the `<key_id>` identifier.

Run the tsactl list-keys command to get the key identifiers.

Mandatory: Yes.

-p <pin>

Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-t <token>

Select the HSM token with the `<token>` label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

The command will raise an error if you omit this option and the configuration is not loaded.

-v <vendor>

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

The command will raise an error if you omit this option and the configuration is not loaded.

-y, --yes

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.

ℹ See Loading the HSM configuration for considerations on this configuration.

Mandatory: Yes.

-y, --yes

Skip the confirmation prompt.

tsactl import-thales

Imports the configuration of a Thales HSM. Use the following syntax to import this configuration from a ZIP file.

```
tsactl import-thales -d <package_path> [-y]
```

Use the following syntax to import this configuration from a Chrystoki file.

```
tsactl import-thales -c <cert_dir> -k <chrystoki> [-y]
```

For example:

```
$ sudo tsactl import-thales -c ./tsa-thales-config/cert -k ./tsa-thales-config/
Chrystoki.conf -y
Saving Thales configuration...              Done
Warning: tsa is already deployed! To apply the changes, tsa needs to be redeployed
using the tsactl deploy command.
```

See below for a description of each option.

- -c <cert_dir>
- -d <package_path>
- -k <chrystoki>
- -y, --yes

> ⚠ Changes will be effective when deploying (or redeploying) the solution with Management Console or the clusterctl solution deploy command.

-c <cert_dir>

Import the client and server certificates for the Luna Network or DPoD authentication. Where `<cert_dir>` is the path of a `cert` directory with the following contents.

```
└──cert
    ├──client
    │       <clientKey>.pem
    │       <clientCert>.pem
    │
    └──server
            <caCert>.pem
```

See below for a description of each field.

Value	Description
<clientKey>	The file name of a PEM file containing the client's private key.
<clientCert>	The file name of a PEM file containing the client's certificate.
<caCert>	The file name of a PEM file containing the CA certificate for validating the server's certificate.

After running the command, verify the `Chrystoki.conf` file includes the following configuration.

```
ClientPrivKeyFile = /usr/safenet/lunaclient/cert/client/<clientKey>.pem;
ClientCertFile = /usr/safenet/lunaclient/cert/client/<clientCert>.pem;
ServerCAFile = /usr/safenet/lunaclient/cert/server/<caCert>.pem;
```

⚠ Do not modify any other path in the `Chrystoki.conf` file.

Mandatory: Yes.

-d <package_path>

Use the `<package_path>` DPoD configuration package, where `<package_path>` is the path of the ZIP package file.

Mandatory: Yes.

-k <chrystoki>

Import the `<chrystoki>` configuration of the Luna Network or DPoD client, where `<chrystoki>` is the path of the `Christoky.conf` file.

Mandatory: Yes.

-y, --yes

Skip the confirmation prompt.

tsactl list-keys

Lists the keys in the PKCS #11 token.

```
tsactl list-keys [-p <pin>] [-t <token>] [-v <vendor>]
```

For example:

```
$ sudo tsactl list-keys
```

```
Obtaining loaded secrets and configuration... Done
Starting PKCS #11 Manager...                  Done
Using token with label pking203
Public Key Object; RSA 2048 bits
  Label:      305ecd78340acc3d906be370a01e7884
  ID:         03b1dac1e383b8d3adea5a6a2c6200bde58ffb40
  Usage:      verify

Private Key Object; RSA 2048 bits
  Label:      F
  ID:         0f
  Usage:      sign, unwrap

Public Key Object; RSA 2048 bits
  Label:      F
  ID:         0f
  Usage:      verify, wrap

Private Key Object; RSA 2048 bits
  Label:      webserver-root1
  ID:         103d6c94ea10b98ab37186cc1c4977eb
  Usage:      sign
```

See below for a description of each option.

- -p <pin>
- -t <token>
- -v <vendor>

-p <pin>

Authenticate in the HSM with the `<pin>` PIN.

Mandatory: No. When omitting this option, the command looks for the PIN in the application secrets. If not found, prompts the user for the PIN.

-t <token>

Select the HSM token with the `<token>` label.

Mandatory: No. When omitting this option, the command uses the value of the **Token label** configuration parameter.

> The command will raise an error if you omit this option and the configuration is not loaded.

-v <vendor>

Use the `<vendor>` security module. See the following table for the supported values.

Vendor	Security module
none	Built-in software PKCS #11 module.
nshield	nShield HSM. See HSM requirements for the supported models.
thales	Thales HSM. See HSM requirements for the supported models.

⚠ It is recommended to select a Hardware Security Module (HSM).

Mandatory: No. When omitting this option, the command assumes the value of the **Vendor** configuration parameter.

✖ The command will raise an error if you omit this option and the configuration is not loaded.

tsactl stop

Stops a deployed Timestamping Authority solution.

```
tsactl stop
```

For example:

```
$ sudo tsactl stop
Stopping Virtual Services...                Done
Stopping Services...                        Done
Stopping Deployments...                     Done
Stopping Stateful Sets...                   Done
Stopping Pods...                            Done
```

ℹ To restart Timestamping Authority, redeploy the solution as explained in Configuring and deploying Timestamping Authority.

19 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 v1.3.0" recommendations for the "Level 1—Server" profile. Specifically, this operating system meets all recommendations except those marked ✗ in the following table.

ℹ The **ISO**, **Raw**, and **VHD** columns refer to the available file formats for Installing the image.

CIS recommendation	Description	ISO	Raw	VHD
1.1.3.1	Ensure `/tmp` is a separate partition	✓	✗	✗
1.1.3.2	Ensure `nodev` option set on `/tmp` partition	✓	✗	✗
1.1.3.3	Ensure `noexec` option set on `/tmp` partition	✓	✗	✗
1.1.3.4	Ensure `nosuid` option set on `/tmp` partition	✓	✗	✗
1.1.3.2	Ensure `nodev` option set on `/var` partition	✓	✗	✗
1.1.3.3	Ensure `noexec` option set on `/var` partition	✗	✗	✗
1.1.3.4	Ensure `nosuid` option set on `/var` partition	✓	✗	✗
1.1.4.2	Ensure `nodev` option set on `/var/tmp` partition	✓	✗	✗
1.1.4.3	Ensure `noexec` option set on `/var/tmp` partition	✓	✗	✗
1.1.4.4	Ensure `nosuid` option set on `/var/tmp` partition	✓	✗	✗
1.1.5.2	Ensure `nodev` option set on `/var/log` partition	✓	✗	✗

CIS recommendation	Description	ISO	Raw	VHD
1.1.5.3	Ensure `noexec` option set on `/var/log` partition	✓	✗	✗
1.1.5.4	Ensure `nosuid` option set on `/var/log` partition	✓	✗	✗
1.1.6.2	Ensure `nodev` option set on `/var/log/audit` partition	✓	✗	✗
1.1.6.3	Ensure `noexec` option set on `/var/log/audit` partition	✓	✗	✗
1.1.6.4	Ensure `nosuid` option set on `/var/log/audit` partition	✓	✗	✗
1.1.7.2	Ensure `nodev` option set on `/home` partition	✓	✗	✗
1.1.7.3	Ensure `nosuid` option set on `/home` 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	✗	✗	✗
2.1.14	Ensure package net-snmp is not installed	✗	✗	✗
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 `firewalld` default zone is set	✓	✗	✗
3.4.3.3.3	Ensure ip6tables firewall rules exist for all open ports	✗	✗	✗

CIS recommendation	Description	ISO	Raw	VHD
5.5.1	Ensure password creation requirements are configured - minlen	✗	✗	✗
6.1.3	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 v1.3.0" 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
Password history retention	8 previous passwords

Setting	Value
Maximum number of failed login attempts before the user account is locked	3 attempts
User account lockout threshold reset counter	24 hours
User lockout duration	24 hours

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	✅
1.1.3	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	✅

CIS recommendation	Description	Compliance
1.1.10	Ensure that the Container Network Interface file ownership is set to root:root	✔
1.1.11	Ensure that the etcd data directory permissions are set to 700 or more restrictive if etcd is used	✔
1.1.12	Ensure that the etcd data directory ownership is set to etcd:etcd if etcd is used	✔
1.1.13	Ensure that the admin.kubeconfig file permissions are set to 644 or more restrictive	✔
1.1.14	Ensure that the admin.kubeconfig file ownership is set to root:root	✔
1.1.15	Ensure that the scheduler.kubeconfig file permissions are set to 644 or more restrictive	✔
1.1.16	Ensure that the scheduler.kubeconfig file ownership is set to root:root	✔
1.1.17	Ensure that the cloud-controller.kubeconfig file permissions are set to 644 or more restrictive	✔
1.1.18	Ensure that the /var/lib/rancher/k3s/server/cred/cloud-controller.kubeconfig file ownership is set to root:root	✔
1.1.19	Ensure that the Kubernetes PKI directory and file ownership is set to root:root	✔
1.1.30	Ensure that the Kubernetes PKI certificate file permissions are set to 644 or more restrictive	✔
1.1.31	Ensure that the Kubernetes PKI key file permissions are set to 600	✔
1.3.1	Ensure that the --anonymous-auth argument is set to false	✔
1.3.2	Ensure that the --basic-auth-file argument is not set	✔
1.3.3	Ensure that the --token-auth-file parameter is not set	✔
1.3.4	Ensure that the --kubelet-https argument is set to true	✔

CIS recommendation	Description	Compliance
1.3.5	Ensure that the --kubelet-client-certificate and --kubelet-client-key arguments are set as appropriate	✓
1.3.6	Ensure that the --kubelet-certificate-authority argument is set as appropriate	✓
1.3.7	Ensure that the --authorization-mode argument is not set to AlwaysAllow	✓
1.3.8	Ensure that the --authorization-mode argument includes Node	✓
1.3.9	Ensure that the --authorization-mode argument includes RBAC	✓
1.3.10	Ensure that the admission control plugin EventRateLimit is set	✗
1.3.11	Ensure that the admission control plugin AlwaysAdmit is not set	✓
1.3.12	Ensure that the admission control plugin AlwaysPullImages is set	✗
1.3.13	Ensure that the admission control plugin SecurityContextDeny is set if PodSecurityPolicy is not used	✓
1.3.14	Ensure that the admission control plugin ServiceAccount is set	✗
1.3.15	Ensure that the admission control plugin NamespaceLifecycle is set	✓
1.3.16	Ensure that the admission control plugin PodSecurityPolicy is set	✓
1.3.17	Ensure that the admission control plugin NodeRestriction is set	✓
1.3.18	Ensure that the --insecure-bind-address argument is not set	✓
1.3.19	Ensure that the --insecure-port argument is set to 0	✗
1.3.20	Ensure that the --secure-port argument is not set to 0	✓
1.3.21	Ensure that the --profiling argument is set to false	✓
1.3.22	Ensure that the --audit-log-path argument is set	✓

CIS recommendation	Description	Compliance
1.3.23	Ensure that the --audit-log-maxage argument is set to 30 or as appropriate	✅
1.3.24	Ensure that the --audit-log-maxbackup argument is set to 10 or as appropriate	✅
1.3.25	Ensure that the --audit-log-maxsize argument is set to 100 or as appropriate	✅
1.3.26	Ensure that the --request-timeout argument is set as appropriate	✅
1.3.27	Ensure that the --service-account-lookup argument is set to true	❌
1.3.28	Ensure that the --service-account-key-file argument is set as appropriate	✅
1.3.29	Ensure that the --etcd-certfile and --etcd-keyfile arguments are set as appropriate	✅
1.3.30	Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate	✅
1.3.31	Ensure that the --client-ca-file argument is set as appropriate	✅
1.3.32	Ensure that the --etcd-cafile argument is set as appropriate	✅
1.3.33	Ensure that the --encryption-provider-config argument is set as appropriate	✅
1.3.34	Ensure that encryption providers are appropriately configured	❌
1.3.35	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	✅

CIS recommendation	Description	Compliance
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	✅
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	✅
4.1.3	Ensure that the kubelet service file ownership is set to root:root	✅

CIS recommendation	Description	Compliance
4.1.3	If proxy kubeproxy.kubeconfig file exists ensure permissions are set to 644 or more restrictive	✓
4.1.4	Ensure that the proxy kubeconfig file ownership is set to root:root	✓
4.1.5	Ensure that the --kubeconfig kubelet.conf file permissions are set to 644 or more restrictive	✓
4.1.6	Ensure that the --kubeconfig kubelet.conf file ownership is set to root:root	✓
4.1.7	Ensure that the certificate authorities file permissions are set to 644 or more restrictive	✓
4.1.8	Ensure that the client certificate authorities file ownership is set to root:root	✓
4.1.9	Ensure that the kubelet --config configuration file has permissions set to 644 or more restrictive	✓
4.1.10	Ensure that the kubelet --config configuration file ownership is set to root:root	✓
4.2.1	Ensure that the anonymous-auth argument is set to false	✓
4.2.2	Ensure that the --authorization-mode argument is not set to AlwaysAllow	✓
4.2.3	Ensure that the --client-ca-file argument is set as appropriate	✓
4.2.4	Ensure that the --read-only-port argument is set to 0	✓
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	✓

CIS recommendation	Description	Compliance
4.2.9	Ensure that the --event-qps argument is set to 0 or a level which ensures appropriate event capture	✗
4.2.10	Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate	✓
4.2.11	Ensure that the --rotate-certificates argument is not set to false	✓
4.2.12	Verify that the RotateKubeletServerCertificate argument is set to true	✓
4.2.13	Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers	✗
5.1.1	Ensure that the cluster-admin role is only used where required	✓
5.1.3	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	✓

CIS recommendation	Description	Compliance
5.2.7	Minimize the admission of containers with the NET_RAW capability	✓
5.2.8	Minimize the admission of containers with added capabilities	✓
5.2.9	Minimize the admission of containers with capabilities assigned	✓
5.3.1	Ensure that the CNI in use supports Network Policies	✓
5.3.2	Ensure that all Namespaces have Network Policies defined	✗
5.4.1	Prefer using secrets as files over secrets as environment variables	✓
5.4.2	Consider external secret storage	✗
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	✓

20 Troubleshooting and technical assistance

See below for how to troubleshoot issues, generate reports and obtain technical assistance.

- Generating technical assistance reports
- Troubleshooting CA Gateway
- Troubleshooting Certificate Enrollment Gateway
- Troubleshooting state restore issues
- Troubleshooting Timestamping Authority
- Troubleshooting Validation Authority

Generating technical assistance reports

To contact customer support, email the following information to support@entrust.com.

- Your contact information
- A description of the problem
- The conditions under which the error occurred
- The troubleshooting activities already performed

Attach to this email a diagnostic report file for each installation node.

- Report file generation
- Report file path

Report file generation

On each installation node, run the following command to generate a diagnostic report.

```
sudo diagnostic-report.sh [--password <pwd>] [--logs-since <hours>]
```

For example:

```
$ sudo diagnostic-report.sh
Gathering system information. This process could take a few minutes...
Packaging the report...

Randomly generated password:
^zuD,h|o`3!>q

Success. This file is meant for incidence analysis at the Support department's
request.
The file resulting from this execution must be sent to the aforementioned department.
```

See below for the supported options.

Option	Description	Mandatory
-p, --password <pwd>	Encrypt the generated diagnostics file with the `<pwd>` password.	No, When omitting this option, the script ciphers the file with a random password containing 13 OWAS special characters and prints the password in the execution console.

Option	Description	Mandatory
-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.
--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.

Troubleshooting CA Gateway

See below for troubleshooting CA Gateway issues related to EJBCA enrollment.

- EJBCA authentication failures
- EJBCA SSL/TLS Connection Failures
- EJBCA certificate issuance failures

EJBCA authentication failures

If you see authentication errors when enrolling certificates with an EJBCA certificate authority:

1. Verify the client certificate was issued by ManagementCA.
2. Verify the administrator was added as a member of the role with the correct match criteria.
3. Check that the role has access to the required CAs and End Entity Profiles.

See Configuring and issuing the EJBCA client certificate for details on each operation.

EJBCA SSL/TLS Connection Failures

If you see SSL/TLS connection errors when enrolling certificates with an EJBCA certificate authority:

1. Verify the trust store file path is correct.
2. Verify the EJBCA hostname matches the SSL certificate.
3. Check that the trust store contains the correct CA certificates.
4. For password-less JKS files, ensure `trust-store-password` is empty or omitted.

See EJBCA Profile Properties for details on the configuration parameters.

EJBCA certificate issuance failures

If certificates fail to issue with an EJBCA certificate authority:

1. Verify the End Entity Profile has access to the requested certificate profile.
2. Verify the certificate profile is configured for the desired key usage and extensions.
3. Check that Subject Alternative Names (SANs) are enabled in the End Entity Profile (if using SANs).
4. Review EJBCA logs for detailed error messages.

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 state restore issues

The clusterctl backup restore command throws an error when restoring the state of a Cryptographic Security Platform installation with Certificate Enrollment Gateway. As explained in Platform 1.3.0 known issues, you must:

1. Contact Entrust support for a new version of the `csf-backup-restore.sh` script
2. Open a user session in any of the Cryptographic Security Platform installation nodes.
3. Run the following commands to install the script.

```
sudo cp --force csf-backup-restore.sh /opt/entrust/scripts/rhel/
sudo chmod 550 /opt/entrust/scripts/rhel/csf-backup-restore.sh
sudo chown sysadmin:edm /opt/entrust/scripts/rhel/csf-backup-restore.sh
```

4. Follow the steps described in Restoring the state to restore the state.

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.

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.

21 Licensing

See below for the Cryptographic Security Platform licenses.

- Customer license
- Third-party license acknowledgments

Customer license

This section defines the licensing model and permitted uses of the Entrust Cryptographic Security Platform (CSP) software solution.

- Authorized Use
- License
- Allocation of Standard and Enhanced Objects Entitlements
- Consumption
- Deployment
- Plugins
- External Dependencies
- Trade Compliance
- Standard Compliance Packs Limitations
- Support and Record-Keeping

Authorized Use

In this Licensing Model section, the term “Customer” means an Entrust customer who has purchased one or more CSP software licenses, or an individual authorized by that customer to access components or features of the CSP software (“Users”).

CSP software is licensed for internal Customer use (i.e. use for the Customer’s own business purposes). Customer may also grant access to Users who are employees of external contractors, but only to the extent that such Users are using CSP software on Customer’s behalf in the operation or management of the Customer’s business and Customer’s own cryptographic assets. In addition, the Customer is permitted to provide digital certificates, keys or secrets to Users who are outside of the Customer’s organization solely to enable resource access between the Customer and that User.

> ⚠ Except as may be otherwise specified in an express license agreement signed by Entrust, neither Customer nor any User may use CSP software to set up or provide its own cryptographic management, analysis or reporting service for other companies (e.g. provision of CSP software functionality as a “Managed Service Provider” or “Systems Integrator”).

License

The CSP software solution 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
Cryptographic Security Platform • CSP Compliance Manager • CSP Public Key Infrastructure • CSP Certificate Manager (Discovery & Control) • CSP Key & Secrets Management	✓	✓	✓
Enhanced PKI Services • CSP Certificate Enrollment Gateway • CSP CA Gateway • CSP Timestamping • CSP Validation Authority		✓	✓
Advanced Automation • CSP Certificate Manager (Automation)			✓
Number of Certificates that can be issued by CSP PKI	50	200	1000
Number of Vault Appliances	2	1	1
Number of Vault Clusters to be assessed for Compliance	2	1	1
Number of Compliance Manager Appliances	1	1	1
Number of Standard Objects	300	50	50
Number of Enhanced Objects	100	25	25
Number of Third Party Objects	300	100	100
Agentless File Encryption – protected data amount in gigabytes (GB)	10	10	10

Allocation of Standard and Enhanced Objects Entitlements

The total number of Standard Objects and Enhanced Objects in each package may be allocated in any way the Customer wishes, as long as the total number of Standard and Enhanced Objects does not exceed the total number for the entitlement for the applicable package.

The default allocation of Standard Objects is shown below.

Standard objects	Standard	Pro	Enterprise
Number of KMIP Keys	100	16	16
Number of Cloud Keys	100	16	16
Number of Secrets	100	18	18

The default allocation of Enhanced Objects is shown below.

Enhanced Objects	Standard	Pro	Enterprise
Number of Application Security Keys	33	8	8
Number of TDE Databases	33	8	8
Number of Virtual Machines	34	9	9
– protected data amount in gigabytes (GB)	10	10	10

Consumption

The Customer will receive one or more license keys (“licenses”) to enable CSP software features and the associated volumes of certificates, standard objects, enhanced objects, and third-party objects based on what the Customer has purchased. These licenses are subject to the following terms:

- Once a digital certificate is issued, it is deemed consumed.
- Once a standard or enhanced object is created, it is deemed consumed.
- Once a third-party object is created, it is deemed consumed.
- The Customer may not alter the license key or attempt to circumvent the licensing mechanism.
- The Customer may only use a valid license key provided by Entrust with the corresponding CSP software component.
- Upon request by Entrust, Customer will provide a report showing its consumption. If Customer’s consumption exceeds the licensed entitlements that it has purchased, Entrust may invoice Customer an overage fee in arrears for its actual consumption.
- The CSP Agentless File Encryption freemium version that comes with the Standard, Pro, and Enterprise packages includes 10 GB in protected data; in order to exceed this protected data limit the Customer must purchase a production subscription (on a per terabyte basis). The calculation to determine whether the 10 GB protected data limit has been reached is based on the original data size and excludes any overhead (added data size) resulting from the encryption.

Deployment

CSP software may be deployed on the Customer’s own infrastructure and/or commercial cloud environments. Entrust strongly recommends keeping all deployments up to date with the latest product release.

Each CSP software 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 software 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 software 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.

Plugins

CSP CA Gateway functionality can be extended, through plugins, to connect to additional CA types. The Customer is permitted to run plugins. These plugins may be:

- Developed by Entrust (sold separately), or
- Developed by the Customer or a third party, under a valid CSP CA Gateway SDK License, and recognized by Entrust (via digital signing).

Plugins are out-of-scope for the product warranty and Entrust support for CSP software.

External Dependencies

CSP software 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 software 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>.
- 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.

22 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.

- Certificate fields
- Certificate critical extensions
- Certificate non-critical extensions

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

Extension	basic-ca-root	basic-ca-subord	basic-ocsp
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 Distributio n Points	Never present (not applicable)	Always present	Always present
OCSP	Never present	Never present	No check
Subject Key Identifier	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

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.

- Certificate fields
- Certificate critical extensions
- Certificate non-critical extensions

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
Subject Key Identifier	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

External subordinate CA certificate profiles

Entrust root Certificate Authorities support the following external subordinate Certificate Authority certificate profiles.

Profile set	Profiles
Azure Firewall Intermediate CA certificate profiles	azure-firewall-ca-subord
TLS Proxy CA certificate profiles	tlsproxy-ca-subord

Azure Firewall Intermediate CA certificate profiles

The Azure Firewall Intermediate CA service provides a `azure-firewall-ca-subord` profile for root Certificate Authorities.

- Azure Firewall Subordinate CA signing use cases
- Azure Firewall Subordinate CA request extensions
- Azure Firewall Subordinate CA certificate fields
- Azure Firewall Subordinate CA certificate extensions
- Azure Firewall Subordinate CA 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.

Field	Value
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 RFC 7093 section 2

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

Alias	OID
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2

Alias	OID
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

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 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

Extension	Critical	Value
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 RFC 7093 section 2

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
'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

Subscriber certificate profiles

Entrust provides the following certificate policies for end-entity subscribers.

Profile set	Profiles
Active Directory (WSTEP) certificate profiles	wstep-digital-signature wstep-digital-signature-key-encipherment wstep-key-encipherment wstep-non-repudiation wstep-non-repudiation-key-encipherment
S_MIME certificate profiles	smime-digital-signature-key-encipherment smime-key-encipherment smime-non-repudiation
Intune certificate profiles	intune-digital-signature intune-digital-signature-key-encipherment intune-digital-signature-key-encipherment-clientauth intune-key-encipherment intune-non-repudiation
Multiuse certificate 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

Profile set	Profiles
	multiuse-p12-key-encipherment-non-repudiation-custom multiuse-p12-key-encipherment-non-repudiation-server multiuse-p12-key-encipherment-server multiuse-p12-non-repudiation-client multiuse-p12-non-repudiation-client-server multiuse-p12-non-repudiation-custom multiuse-p12-non-repudiation-server multiuse-p12-server
Smartcard certificate profiles	smartcard-card-authentication smartcard-digital-signature smartcard-domain-controller smartcard-key-management smartcard-piv-authentication smartcard-piv-content-signing
Mobile device certificate profile	mobile-device-p12-digital-signature-client-authentication
SCEP certificate profiles	scep-digital-signature scep-digital-signature-key-encipherment scep-key-encipherment scep-non-repudiation
V2G certificate profiles	v2g-supply-equipment v2g-user-identity
Code signing certificate profile	codesigning-digital-signature
MDMWS certificate profiles	mdmws-digital-signature mdmws-digital-signature-key-encipherment mdmws-digital-signature-key-encipherment-clientauth mdmws-key-encipherment mdmws-non-repudiation mdmws-p12-digital-signature mdmws-p12-digital-signature-key-encipherment mdmws-p12-digital-signature-key-encipherment-clientauth mdmws-p12-key-encipherment mdmws-p12-non-repudiation
EST certificate profiles	est-digital-signature est-digital-signature-key-encipherment est-key-encipherment est-non-repudiation

Profile set	Profiles
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
CMPv2 certificate profiles	cmp-digital-signature cmp-digital-signature-key-encipherment cmp-key-encipherment cmp-non-repudiation

Active Directory (WSTEP) certificate profiles

Entrust provides the following Active Directory (WSTEP) certificate profiles.

- wstep-digital-signature
- wstep-digital-signature-key-encipherment
- wstep-key-encipherment
- wstep-non-repudiation
- wstep-non-repudiation-key-encipherment

These profiles support the following features.

- WSTEP use cases
- WSTEP key usages
- WSTEP request extensions
- WSTEP certificate fields
- WSTEP certificate extensions
- WSTEP 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

Profile	Key Usage
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.

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.

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 RFC 7093 section 2

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

Alias	OID
'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
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2

Alias	OID
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

CMPv2 certificate profiles

Entrust provides the following CMPv2 certificate profiles.

- cmp-digital-signature
- cmp-digital-signature-key-encipherment
- cmp-key-encipherment
- cmp-non-repudiation

These profiles support the following features.

- CMPv2 use cases
- CMPv2 key usages
- CMPv2 request extensions
- CMPv2 certificate fields
- CMPv2 certificate extensions
- CMPv2 distinguished names

CMPv2 use cases

All CMPv2 profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

CMPv2 key usages

See below the Key Usage extension values supported by each CMPv2 profile.

Profile	Key Usage
cmp-digital-signature	Digital Signature
cmp-digital-signature-key-encipherment	Digital Signature, Key Encipherment
cmp-key-encipherment	Key Encipherment
cmp-non-repudiation	Digital Signature, Non-Repudiation

CMPv2 request extensions

All CMPv2 profiles support the following non-critical extensions in request.

Extension name	Extension OID
Certificate Policies	2.5.29.32
Extended Key Usage	2.5.29.37
Application Policies	1.3.6.1.4.1.311.21.10
Smime Capabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

CMPv2 certificate fields

All CMPv2 profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.

Field	Value
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

CMPv2 certificate extensions

All CMPv2 profiles set the following certificate extension.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Extended Key Usage	No	No constraints
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

CMPv2 distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5

Alias	OID
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2

Alias	OID
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

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 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
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

Code signing 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

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 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.

Field	Value
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 RFC 7093 section 2

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

Alias	OID
'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
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2

Alias	OID
'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 signing distinguished names

EST signing use cases

All EST profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

EST key usages

See below the Key Usage extension values each EST profile supports.

Profile	Key Usage
est-digital-signature	Digital Signature
est-digital-signature-key-encipherment	Digital Signature, Key Encipherment
est-key-encipherment	Key Encipherment
est-non-repudiation	Digital Signature, Non-Repudiation

EST request extensions

All EST profiles support the following non-critical extensions in request.

Extension name	Extension OID
Certificate Policies	2.5.29.32
Extended Key Usage	2.5.29.37
Application Policies	1.3.6.1.4.1.311.21.10
Smime Capabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

EST certificate fields

All EST profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.

Field	Value
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

EST certificate extensions

All EST profiles set the following certificate extension values.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Extended Key Usage	No	No constraints
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

EST 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

Alias	OID
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2

Alias	OID
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

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 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-emailprotection-clientauth	Digital Signature, Key Encipherment	E-mail Protection (with OID 1.3.6.1.5.5.7.3.4), TLS client authentication (with OID 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	Support
Application Policies	1.3.6.1.4.1.311.21.10	All Intune profiles

Extension name	Extension OID	Support
Certificate Policies	2.5.29.32	All Intune profiles
ExtendedKeyUsage	2.5.29.37	All Intune profiles except for `intune-digital-signature-key-encipherment-clientauth` & `intune-emailprotection-clientauth`
MSTemplateName	1.3.6.1.4.1.311.20.2	All Intune profiles
MSTemplateOID	1.3.6.1.4.1.311.21.7	All Intune profiles
Smime Capabilities	1.2.840.113549.1.9.15	All Intune profiles
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2	All Intune profiles

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

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 RFC 7093 section 2

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

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

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 distinguished names

MDMWS use cases

All MDMWS profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API
- Entrust-hosted Enrollment Gateway
- On-prem Enrollment Gateway

MDMWS issuance modes and key usages

MDMWS profiles support the following issuance modes:

- Issue the certificate from a CSR.

- Issue the certificate and an RSA2048 private key in a P12 file.

See below the issuance mode, Key Usage, and Extended Key Usage (EKU) values each MDMWSprofile supports.

Profile	CSR	P12	Key Usage	Extended Key Usage	Allows Extended Key Usage in request
mdmws-digital-signature	✓	✗	Digital Signature	No constraints	✓
mdmws-digital-signature-key-encipherment	✓	✗	Digital Signature, Key Encipherment	No constraints	✓
mdmws-digital-signature-key-encipherment-clientauth	✓	✗	Digital Signature, Key Encipherment	TLS client authentication (1.3.6.1.5.5.7.3.2)	✗
mdmws-key-encipherment	✓	✗	Key Encipherment	No constraints	✓
mdmws-non-repudiation	✓	✗	Digital Signature, Non-Repudiation	No constraints	✓
mdmws-p12-digital-signature	✓	✓	Digital Signature	No constraints	✓
mdmws-p12-digital-signature-key-encipherment	✓	✓	Digital Signature, Key Encipherment	No constraints	✓
mdmws-p12-digital-signature-key-encipherment-clientauth	✓	✓	Digital Signature, Key Encipherment	TLS client authentication (1.3.6.1.5.5.7.3.2)	✗
mdmws-p12-key-encipherment	✓	✓	Key Encipherment	No constraints	✓
mdmws-p12-non-repudiation	✓	✓	Digital Signature, Non-Repudiation	No constraints	✓

MDMWS request extensions

All MDMWS profiles support the following non-critical extensions in request.

Extension name	Extension OID
Certificate Policies	2.5.29.32
Application Policies	1.3.6.1.4.1.311.21.10
Smime Capabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

MDMWS certificate fields

All MDMWS profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

MDMWS certificate extensions

All MDMWS profiles set the following certificate extension values.

Extension	OID
CertificatePolicies	2.5.29.32
ApplicationPolicies	1.3.6.1.4.1.311.21.10
SmimeCapabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7

Extension	OID
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

MDMWS 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

Alias	OID
'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
'StatuteCitation'	1.3.6.1.4.1.53087.3.5

Alias	OID
'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 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
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

Mobile 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

Alias	OID
'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
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2

Alias	OID
'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 distinguished names

Multiuse use cases

All multiuse profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

Multiuse issuance modes

All multiuse profiles support the following issuance modes:

- Issue the certificate from a CSR.
- Issue the certificate and an RSA2048 private key in a P12 file.

Multiuse key usages

See below the Key Usage and Extended Key Usage (EKU) extension values each multiuse profile supports.

Profile Name	Key Usage	Extended Key Usage	Allows Extended Key Usage in request
multiuse-p12-client	Digital Signature, Key Agreement	TLS client Authentication (1.3.6.1.5.5.7.3.2)	✗
multiuse-p12-client-server	Digital Signature, Key Agreement	TLS client Authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)	✗
multiuse-p12-custom	Digital Signature, Key Agreement	No constraints	✓
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)	✗

Profile Name	Key Usage	Extended Key Usage	Allows Extended Key Usage in request
multiuse-p12-key-data-encipherment-non-repudiation-client-server	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment	TLS client Authentication (1.3.6.1.5.5.7.3.2)	✗
multiuse-p12-key-encipherment-client	Digital Signature, Key Agreement, Key Encipherment	TLS client Authentication (1.3.6.1.5.5.7.3.2)	✗
multiuse-p12-key-encipherment-client-server	Digital Signature, Key Agreement, Key Encipherment	TLS client Authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)	✗
multiuse-p12-key-encipherment-custom	Digital Signature, Key Agreement, Key Encipherment	No constraints	✓
multiuse-p12-key-encipherment-non-repudiation-client	Digital Signature, Key Agreement, Key Encipherment, Non-Repudation	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-Repudation	TLS client Authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)	✗
multiuse-p12-key-encipherment-non-repudiation-custom	Digital Signature, Key Agreement, Key Encipherment, Non-Repudation	No constraints	✓
multiuse-p12-key-encipherment-non-repudiation-server	Digital Signature, Key Agreement, Key Encipherment, Non-Repudation	TLS server authentication (1.3.6.1.5.5.7.3.1)	✗
multiuse-p12-key-encipherment-server	Digital Signature, Key Agreement, Key Encipherment	TLS server authentication (1.3.6.1.5.5.7.3.1)	✗

Profile Name	Key Usage	Extended Key Usage	Allows Extended Key Usage in request
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) 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.

Field	Value
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

Multiuse certificate extensions

All multiuse profiles set the following certificate extensions.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Key Usage	Yes	Digital Signature, Key Encipherment
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

Multiuse distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5

Alias	OID
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2

Alias	OID
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

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 distinguished names

Private SSL use cases

All private SSL profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

Private SSL key usages

See below the Key Usage and Extended Key Usage (EKU) extension values each private SSL profile supports.

Profile	Key Usage	Extended Key Usage
privatessl-tls-client	Digital Signature	TLS client authentication (1.3.6.1.5.5.7.3.2)
privatessl-tls-client-server	Digital Signature	TLS client authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)
privatessl-tls-client-server-data-encipherment	Digital Signature, Data Encipherment	TLS client authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)
privatessl-tls-client-server-supply-san	Digital Signature	TLS client authentication (1.3.6.1.5.5.7.3.2) TLS server authentication (1.3.6.1.5.5.7.3.1)
privatessl-tls-server	Digital Signature	TLS server authentication (1.3.6.1.5.5.7.3.1)
privatessl-tls-server-supply-san	Digital Signature	TLS server authentication (1.3.6.1.5.5.7.3.1)

Private SSL fill_san_dns_with_cn

When the `fill_san_dns_with_cn` parameter is `True`, the profile copies in the `SubjectAltname` extension all the `CN` fields:

- included in the `Subject` extension, and
- not already in the `SubjectAltname` extension (to avoid duplicated entries).

See below the value of this parameter in each profile.

Profile	fill_san_dns_with_cn
privatessl-tls-client	False
privatessl-tls-client-server	False
privatessl-tls-client-server-data-encipherment	False
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
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

Private SSL 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

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 distinguished names

S/MIME use cases

All S/MIME Secure Email profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

S/MIME key usages

See below the Key Usage and Extended Key Usage (EKU) extension values each profile supports.

Profile	Key Usage	Extended Key Usage
smime-digital-signature-key-encipherment	Digital Signature, Key Encipherment	TLS client authentication (1.3.6.1.5.5.7.3.2) Email Protection (1.3.6.1.5.5.7.3.4)

Profile	Key Usage	Extended Key Usage
smime-key-encipherment	Key Encipherment	Email Protection (1.3.6.1.5.5.7.3.4)
smime-non-repudiation	Digital Signature, Non-Repudiation	Email Protection (1.3.6.1.5.5.7.3.4)

S/MIME certificate fields

All S/MIME Secure Email profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

S/MIME certificate extensions

All S/MIME Secure Email profiles set the following certificate extensions.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

S/MIME distinguished names

Entrust has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
'CN' 'CommonName'	2.5.4.3
'SN' 'SurName'	2.5.4.4
'SERIALNUMBER' 'DeviceSerialNumber'	2.5.4.5
'C' 'Country'	2.5.4.6
'L' 'Locality'	2.5.4.7
'ST' 'S' 'State'	2.5.4.8
'STREET' 'StreetAddress'	2.5.4.9
'O' 'Org' 'Organization'	2.5.4.10
'OU' 'OrganizationalUnit' 'OrganizationUnit' 'OrgUnit'	2.5.4.11
'T' 'Title'	2.5.4.12
'BUSINESSCATEGORY'	2.5.4.15
'POSTALCODE'	2.5.4.17
'givenName' 'G'	2.5.4.42
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97
'UID'	0.9.2342.19200300.100.1.1
'DC' 'DomainComponent'	0.9.2342.19200300.100.1.25
'Email' 'E'	1.2.840.113549.1.9.1

Alias	OID
'unstructuredName'	1.2.840.113549.1.9.2
'unstructuredAddress'	1.2.840.113549.1.9.8
'JurisdictionOfIncorporationLocalityName'	1.3.6.1.4.1.311.60.2.1.1
'JurisdictionOfIncorporationStateOrProvinceName'	1.3.6.1.4.1.311.60.2.1.2
'JurisdictionOfIncorporationCountryName'	1.3.6.1.4.1.311.60.2.1.3
'TrademarkOfficeName'	1.3.6.1.4.1.53087.1.2
'TrademarkCountryOrRegionName'	1.3.6.1.4.1.53087.1.3
'TrademarkRegistration'	1.3.6.1.4.1.53087.1.4
'LegalEntityIdentifier'	1.3.6.1.4.1.53087.1.5
'WordMark'	1.3.6.1.4.1.53087.1.6
'MarkType'	1.3.6.1.4.1.53087.1.13
'StatuteCountryName'	1.3.6.1.4.1.53087.3.2
'StatuteStateOrProvinceName'	1.3.6.1.4.1.53087.3.3
'StatuteLocalityName'	1.3.6.1.4.1.53087.3.4
'StatuteCitation'	1.3.6.1.4.1.53087.3.5
'StatuteURL'	1.3.6.1.4.1.53087.3.6

SCEP certificate profiles

Entrust provides the following SCEP (Simple Certificate Enrollment Protocol) certificate profiles.

- scep-digital-signature
- scep-digital-signature-key-encipherment
- scep-key-encipherment
- scep-non-repudiation

These profiles support the following features.

- SCEP use cases
- SCEP key usages
- SCEP request extensions
- SCEP certificate fields
- SCEP certificate extensions
- SCEP distinguished names

SCEP use cases

All SCEP profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

SCEP key usages

See below the Key Usage extension values each profile supports.

Profile	Key Usage
scep-digital-signature	Digital Signature
scep-digital-signature-key-encipherment	Digital Signature, Key Encipherment
scep-key-encipherment	Key Encipherment
scep-non-repudiation	Digital Signature, Non-Repudiation

SCEP request extensions

All SCEP profiles support the following non-critical extensions in request.

Extension name	Extension OID
Certificate Policies	2.5.29.32
Extended Key Usage	2.5.29.37
Application Policies	1.3.6.1.4.1.311.21.10
Smime Capabilities	1.2.840.113549.1.9.15
MSTemplateOID	1.3.6.1.4.1.311.21.7

Extension name	Extension OID
MSTemplateName	1.3.6.1.4.1.311.20.2
szOID_NTDS_CA_SECURITY_EXT	1.3.6.1.4.1.311.25.2

SCEP certificate fields

All SCEP profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
Validity period	Less than or equal to the expiry of the issuing CA. Defaults to 1 year if not specified in the request.

SCEP certificate extensions

All SCEP profiles set the following certificate extensions.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Extended Key Usage	No	No constraints
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

SCEP 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

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 distinguished names

Smartcard use cases

All smartcard profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

Smartcard key usages and request extensions

See below the Key Usage and Extended Key Usage (EKU) extension values each smartcard profile supports.

Profile	Key Usage	Extended Key Usage	Allowed in request
smartcard-card-authentication	Digital Signature	No constraints	PIV Interim Indicator (2.16.840.1.101.3.6.9.1) Security ID (1.3.6.1.4.1.311.25.2)
smartcard-digital-signature	Digital Signature, Non-Repudiation	No constraints	PIV Interim Indicator (2.16.840.1.101.3.6.9.1) Security ID (1.3.6.1.4.1.311.25.2)
smartcard-domain-controller	Digital Signature, Key Encipherment	TLS server authentication (1.3.6.1.5.5.7.3.1) TLS client authentication (1.3.6.1.5.5.7.3.2)	—
smartcard-key-management	Key Encipherment	No constraints	PIV Interim Indicator (2.16.840.1.101.3.6.9.1) Security ID (1.3.6.1.4.1.311.25.2)

Profile	Key Usage	Extended Key Usage	Allowed in request
smartcard-piv-authentication	Digital Signature	Any Extended Key Usage (2.5.29.37.0) Microsoft Smart Card Login (1.3.6.1.4.1.311.20.2.2) TLS client authentication (1.3.6.1.5.5.7.3.2)	PIV Interim Indicator (2.16.840.1.101.3.6.9.1) Security ID (1.3.6.1.4.1.311.25.2)
smartcard-piv-content-signing	Digital Signature, Non-Repudiation	No constraints	—

Smartcard certificate fields

All smartcard profiles set the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint.
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

Extension	Critical	Value
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

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
'I' 'Initials'	2.5.4.43
'ORGANIZATIONIDENTIFIER'	2.5.4.97

Alias	OID
'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
'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 distinguished names

V2G use cases

All V2G profiles support the following use cases.

- ECS Enterprise UI
- CA Gateway API

V2G key usages and validity periods

See below the Key Usage, Extended Key Usage (EKU), and certificate validity period each profile supports.

Profile	Key Usage	Extended Key Usage	Validity period
v2g-supply-equipment	Digital Signature, Key Agreement	TLS server authentication (1.3.6.1.5.5.7.3.1)	1 year
v2g-user-identity	Digital Signature, Non-Repudiation	—	2 year

V2G certificate fields

All V2G profiles set the following certificate fields.

Field	Value
Issuer	The customer's subordinate issuing-CA
Subject	No constraint

V2G certificate extensions

All V2G profiles set the following certificate extensions.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Basic Constraints	Yes	cA =False
CRL Distribution Points	No	Always present
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKey» as described in RFC 7093 section 2

V2G 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

23 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 (2.16.840.1.114027.80.8.1.34)
  - MLDSA44-RSA2048-PKCS15 (2.16.840.1.114027.80.8.1.32)
  - MLDSA65-ECDSA-P384 (2.16.840.1.114027.80.8.1.38)
  - MLDSA65-RSA3072-PKCS15 (2.16.840.1.114027.80.8.1.37)
  - 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-----
MIJDWTCBhwIBADBRMRAwDgYDVQQKEwdFbnRydXN0MQ8wDQYDVQQLEwZQS0lIdWIx
LDAqBgNVBAMTI1NQSElOQ1NQbHVzLVNIQTItMTI4Zi1zaW1wbGUgU2FtcGxlMC0w
CAYGK84PBgQNAyEAO6644sgf45+BYFEyuQLej72GY8YWNQ2sHEKTYz515v+gADAI
BgYrzg8GBA0DgkLBAB4lW9O8lqet6lCcYHVkj+5JmKPPMaoY3DNTgt3Vn5CIgrAB
rxKraRX3TEbWJv/n2tMmvHSGzF9nucBjsEuof+sySt M3j8f1hbcoh8Bnq3tJCDNx
NuX8JnuXP3EywE+sDiyBQ5LcoEKCwnr3XNv1XZ2ZfOMy7DxcYxLRpRBbIIc5RQMX
cQlRrVXnz8t4gJg1NmJNXfyFxb16kpeOmT4kl9ECMXlWjJEmgN1Fcz0nIqK43cHB
nWVLzEhKQyRkTHNqnFEUqJHmr1XR/CyMwwk8uVHrSkTyoX2PWdVu6Epk7f7Hj51L
QbqyJW3GycDr3pEJr36Dg8OS3JUW6Td9/7aoGeLmVi+ZQVe+DAEtGADvyM/2HRC2
so3M9zKJDufIwDexUqJ4UyYw9LHkBtkaC3E5LetOlgKr888b3tgkR5Uhz1C//Pq7
7cTaYioY4fBp1V7dC3MwYZ1Oo02DZbxY76/2xZpU2DbuLQ6AzCbX2OoLu9mKjLbl
Zht3VEYKtKT9Yf5+Hdei8uEx+SBzV9dHNNuexHZd30ig/DAgwdHS96C3Q6RtNCFB
TWQT2SAAfhVG4qpGVrUspm6aSf7GyaET5L0l6uZ0JODtus5+IpOtP/gonuR64B/m
6DUXqwtZPHKCJm49EjEz40HbcsOIWexrLAS0/CIzZkv12MLXY7H2FpX22hXebMg5
DWFiPkGvCHCqYd4cG8QevvtUq8/5SVH/pOoBMRQnBNcIIBvVTI4VfFDVEa5Uqmmk
1B0DQg/KAo0tMRD/5DtODu9HYdRLaFVgT6uawrKDhtbP2y5H99X2Gd37XtyUf9LN
Sk2jbGBvpAbeSpVZ1m32tfHw8ydQAFIz7dyMPGBASEVsneEb/5KaYjktVTlirvj3
n32IC3EqAhEQMYV8qjV+edc+x0BSwyIYV9nJqWQSPMdQMBV7eTpdqT4UfGcssG9J
TOAyA6gOpVVJUxtsaSF/t8S+BZ56wx1GZZSFYzU8NJcl/ffRVV3zYrYJFCKuZxVh
z92eqOdTWp38k3BXcwaNar8zd77cesqdKOFj/xsX2PO/z5fPxnfiVnLCNfStz6KJ
0XfBhS2lllfJ9o7CsmQ/6lkkOrel3jOIxLGrCeumN/829JpgZyJvudciMHyAqYGn
eMMN2uM/3edY3mX5+BzTqqt6GX5SpAf4rZ/FWQYkkzzyqg85Nx4GnhK7liUOeZXP
AB/uWgU3MYpwQuS/TSzF2qOe2y7Ll88x07uVadtQ1+hodRJyNN3QFzRbCGAsU1SB
EzUcWoXZQWDdXxF/Ab9bLNil+KC/aJsRvV2gW2VOgtLBJEU4dZGhAVs6MEJjf6Y5
sntcX+7Ga7FFlJk336EFXDdgUC12JeFhhuV8jIV+s26NT3A6H928hrfiWD8oTUr5
jb5mijsVHR4dSY2fjmR1n9tvQ8AwXgzl4oa08UmlO0ZYEn/WBIjx5JRFiXifecep
We68hTkCgq943Cei9BnDREYLLTJAz55BcJut8LiCj8emzzAopbBAaH0JyQbaaBb+
w0FbFA5Lf+8N0GRnz9sJhvTOH+pv36MsP3O7CM4yDpKM38lHxQ1/CCjMQJ37ABtT
HuMbVTLjgIrec36dRzF0Jxb3/jVMCjmbw5f9El2O78E0XzWvBslLfYKqqDqIJbJi
N0BUMwDO1rURM6g8sH9j5dHGowUCLxWI3PJGsBVrZDbgbfTafEQPmphzElUXRhez
5+X91+PZHcIZ/sc7TVwCl4EPdp6BLCP/XhvMyuaOIT+5HtGTDTAR38H3hRrZwz6b
eYsouM2JPbIQB7ttRajl67gbDDtwNaoO0bERa/3BxvoY6Zk4d47J8JRHR2m+jnou
liXs58mjNhZC9jAq7dVAoW3MX2hdBlBl3HwS+Gdc2133Je05E/NLYENz2X7qctXM
jmaACzAaVzVSMeLOnpYHVPjRgFmI/MDD8YKbMeyqt2x8NTIGlQQeHQzcQxTIv3fs
UX/9j258lyXtw63N5i6RFYfFAXAhXWV6BOcFqie63XKVBbiHTsAhLXTYs24A0aHZ
Bju+eciFmzUSyTQKEW4pokIjPfMzhbpJAQ0DA/CKS64ow0uJpk+ciPZbTWs6FXsH
dxv2esFPl8cnboH1t5LIMIPiaa/1grVZ5VFv6noZLBnPBbhfcc0OMWrXZI+C++iE
wC79AUxPAM6JiWuzaVVADpVNgTB1po43n37TwLHBD9eCcaKwtJIAatqyLB5mskYE
LqRP1V22PtO/MDZvQL6GYnF5ck3RSEmulLmEFpD4Tf8G8D8jff8+BEw48nT851Nh
X+2ddOnxuZGB4Yc5vOpX7ZVbpvwKeQtvFu+hCfcaMx6H1DYy8fh2OBZQYLWeoyiY
EG87MAVPAQamFDyqWTToyIkdHqJcYzu8lz0pSXTVT8FpEmTC16pw64ZCjJh0hqGP
wOUqb57VqMXsR5luY/cPQlyWPrgsgeEixVmapRKzEUa5dyqMFP23dMS8obARTdVU
r2xCAtlzhlW2Rc/nYoqWSVTnfJAPvMjAan3GalDV9mvde+yjA1EFH2YBmTWWdjHk
TcCCTxyzqRb1N/QPVeUhpPY4o1M2mDHtNSnPzEraS8uuTgKV6cTx9aayNKSrTJeb
zh4r4C/yyshoMSd6HryOCKQTEllk64yO0vLga6SN2ZsDYUy37CZtUmDsP2IiocVZ
qT2Q22cqbcm0eRZ/S2lxsuRxr0f5YH9ROCYgpAFm2+WoYIN4+/CNYIAhwguKoX3r
azlsT8ZvB+dtUA9hLqs27bWz497fXsE/PLiXuchqMlirBB3DxV0DbRnDTaRLmuLz
l5Ziw0ab/XdrJ4jW6opaMi2zLRo0iszX1qs9OdpTQ7R+vuj9SDWQG1PP5sgYkq2a
DcQG7kBZztiXblMnAYlhRF6ctgMFlFyXzjt3+oIM9WdByIz2eOG0uOnGqE+QNB29
NawOrLzwR1Dts3ZHOE8opR9S/5INzw+VKsXSWEsZ+u5IxU5LkW4Im1f3Yu6z5y6p
o3qWyZDlPgXTsLtGdOgKLWlWeiPnJ87XuxR7RYn4q7J+oHrICfu7zU0xi44OjHEH
```

```
DgjO1qUHOrzF/a0986mXUxHcEcT307kvPLxmWxAUjGcnZ3AdgGbqpUPmwGJCuBCP
8oWK4FilUfwp+SehaK0nZfqKg4aGpRvoZpYP4sPsBkthDWKDS5Zt+fOZjPqunMT+
chl1dHqBuMdWsbUNE8alYzDO/Y+1mWoEO2NvAY3ByJfxBjiTP+jsPqyTo8t6aVpm
q2W8ruqtCRNFiWP0cA+HacAwlZt79fF9bx9/QBTCvkDDW+QZQQnYXhDnwXQHIwVO
deDvbqAxXqMnrmLHiJthRMogyUAym1qDx5iYOUlfNCSDMDG5qZ1U6AVE6wKzOED2
PAFSBPBorYWya5TUh7qQWiRkrPPSGxGn55JllMoZfyAPSkJoKbX1DlYdtDmgcw5f
7LE3mK0b6fRtpr7S/rvoKJACt/eXCV4qMBxYcA4Edoicys39NoN7dJ+OFHv+bzkM
0UThmvL76zlSEQZEFHH/jxQSzR0kUxsgshZNofMzjWMpR1qji0kbwb6sIA3uP76i
a8q87RmV1clI8IeKlczxg96mEXHlQT8kyGdoCIRWvKygkDbVrLOnpAUqVE6fq3at
sfH2WXRBWnUqQNu02cPBUCqWhcjsUBLLe8ZwM+WOn5FnIM0rV6lA7/TlvPGWEwgH
+W8G221HFmHGcIVrzBOBmucp5oS/H0cfESnu9DuAuG2fhtxzoE2HX3aq/0oNpId+
xygN4xZb74680gLpdlkf1td5ik0fyjB/Kni7VSzTrFFuX1/wvlhZ9hN3K/86o+UD
/pJcnRPNiSL0crDQkKfhDXexByxDdeAAxpa4bTuN7fzY817KuDoPcEaaj7HOghkB
qzIr4l/7ScGnFBjM7vUKipYbdPDZI3jrhXa/lqzSDgeSZ/nzKryUvanEqm5VH1ud
uj0IIVBvk2c/gFndzaNT66TlIpj4ARnLlA/KRWNwbyFJdBeVsdrpZpEMeclOMOi3
a8Knz4aOzdzD8wxP2oZQz7fBVliIRerZoLG8UP4vZfeOhebYRNgxbgup6cbrcKKl
ykVfTbEzPe9J4VZOroZf5xqgdDlT24aa0ezokSlDLaN900ffGQmdcMQvua9Oy2sO
oeDZ2cZD3AaB5QVcgjS92UnlP4URYDXhZ0qKfaMnVIBz/itKFqvdicy6qTRTlJD2
GtMxgmOBPEjUDyYoEj7Orm8aeQRWdOopC0DH1/LZs2FaLvLCSCPTSewnyY7S2AN5
idPPuOwW2+ts/QfeW7+PI29eXb6CUmTYqgvgyoJtXcBKW3nvP00OB2CKqjFAC5Ek
/LgangtvZi2sBy2351XIHGsBX3LWeHcCHjz06wfNw07dedJ6Ykj4bXlOZjUHHTnv
EwkyqEkwX2Fs3UrWFmBLUlf1HMlaQfgrYgoGXh+nDMHPM5MvMUzNMOo8JL1lhoy5
PNZA4jVdHN4X4pvI6KPgfziUj7Ms9KH7MSjNPNTMISi37hzZ53SePl2Xo0ICyqDk
/UBmIh6mpoKJ+sw459X1SS4aLV8L3UqUUd9gfnTp0uwajKwq9l6VQsUj3OrHTKTC
FXAW+qa3AhjiqaR+tm01c35z+Zlp4ofdmy4x3cv6f1AR+hrxrUt8x2gOYNFcShMT
UQK87eer+hRj0WpAL26dLhFq9ktw6NdsHJ0JzkVw7VhLSBCby2miljhBg8B9U1WZ
i/tU84ettO9s/DqM+SvHo0C99DInYEFjpY9+wGux1S3aLpyco/TgzInxVzhNrDyq
78Z3umjlxXShD5C/s+B5qXkHUady24G6Z6NuiLf7jJxwVS4UJxE/jGuITAhzSlb5
E0PRwNZoFb52zgOekOrR8V2jlDFkSavuUyyPxtOS5xWztxgM4IUNhd5pQtxMdvJ5
8vdHOADCOQ3MJ/NUkq0a0lzW2d15lPWtdtkWn67ErV9E0t4meeWYjzyH2Ek3ERNc
v8vmBGD9n8Pw7PKbBLHZjueFF6S1tg7sC3XeonaMV+3Iec+uQKzbOmO66fq+5ffM
mgv0M0gWl/BTD1KVDN6Xp4x3/41UzcPcPa1R6B40jt7tDzRY2XR5PtrLkORXJD72
NvT6G1T/kZ3XnXw4L1o78KSkdxnht/9pwMXAtb8vrT98rTVEMIMUZFKqTqP7aLDk
W2OswEh8ruC+MDhwAJlWqM3DrkuKERBoevvMAQLftFGQia3nhjcprr/qX1W2OzMK
o94K2qs1TVwqxSYy/GwbOz9rNB1AzEMZm7VqmVYgfbbFnAnISGbpLXotru/khM8c
073+NV436xlAbrIRudyvlbiTwqq9jXnNrpvHqpB3upGY7okUXlzPdDnlaXWQbsQc
m4+QYAGYzB8YRyAIezTlcULH5+TfYWO2xB8keSEtUrbGwY36IwIDpVGz6dD9mSVZ
nEFmYQxCmZObSEbg1Et4pCJSPdJnS7dMuIj9MM8+M9L/pTmodJQ/KJ0AMXmtwbx8
GdlfPJ3P5dePb6bNGgHaqhuyMPLSHEwrMH2+leR9ZyCvGX9Mu9RVYoTEx1FLVWkS
OFRDclW2cGj19cPUd6O9gHeb0aY8TaGqhK/KbtsVpP0Cl2CE61CfJ7Y3FPh6HJKq
dKLXuqDk6UF/i0egtQRUp5mywHDhMqGtPF8FRvFsOtp5URhYm/f2dlult3zEwfhe
MeZGedSRgCzYF76JJThzdJpAijQ3/hgI5c5mJv0gj6fAme3rtIzkpXrtbIQcpAhX
pm0XnkhXt8V7EcDrREGTZjN87tTH/WN6d3JTZt5m/acKErMf1zhjgFI6ez7s3L3a
64aw6SHA/qJ/VkOcthpA6gtWmM7AgL7zh0m5Ib0vH3HRMbsnZ6JJKgbtBAS9qLbp
oxw1eLOrdrtLh1MCEMb/ese01m4uU8qbYFU+nDDVEO8DJeKM6jmuAgfW1gMii+B8
Y5sx5UJNYEe1D/44lI2Xd6XZCgsigF2cI5L5+gNemg3J5s4pwPIT9OSvbFnaZDqu
uzLHTwLQXhxGj6kN2FKSE9agaHzEUaEUDWQXo3B35IEJx371m0fZgpbQ6UXpyIG1
x4qWc2F0qOp7v1UfKP63iNjZGpodtz9mmi4Dnv+PXWlqBzc/oyI/B4GMy2EX1kal
uELXUEHytxBVlwTztHWNvzVfYTGLbvePh3k+CB5dO1rakM+0i1e4VHHE96OzsZTy
pTAHI005AVCmvCodojHB3af7C/mLUKZCJv0G0ZDmUx66/jcowbmoLm+KMfmSPYTt
9V4VXTTNheH6N7bI0esFx7ab7p9zf//1xk9quwBsKwnr40AoXG5mBE/sQz4Y1geV
+NArFiwtbxfYiISPFqf82KhVnFbnczML1OEJxnkfqSJAQHeHtFg86MaQVT6kN35l
YwmI5PP3/zREhsTmT//sCWiA1unJLcenPWlrGLSAB3LkTt06cs/+CQ5Lx/7RFTq6
```

1QrnQ3MdA9Q53zea1yh0KUwECP2P3LvzoOAabamZeTujNn0VNJ+cekCIFTshXOBu
o539M5kaFf1twT+Iu3Jw/WKFnE8ZwASY19ZcYxppTwMw9HpJNYiTnJU0A2mMem9u
S2fo8KYCazJYVsSo6lCupoglivnLeAmthjLnyeB4/ozIsTw6AVH4G8ctITSaqQCG
Lg5PDOJXWWSwmM04ZQ7xNEt+LEX08jEuGHFXrDEwbBcdKzJPDHztj7Mw3BUTgU6n
nXp9QgueJ+mZbWYRR33UZK9QWA2vUn1JxEjBDJ7vKemLXvm22mNJDIQ+yTKKCEgZ
aL/MCq2yGN+pnVXtYsxw9R2Nan2CC37ZmuSDNTnv6ECMXRWad04KdmoOlo/xuAfu
pd7gQB/vaIgM7yHKwTymQ121iA4mllrxu0ml6JmeyWtwWliSjFm3BJmPM0OiIahV
zIMCIF9Oe+64wmeuznx7YWdIuGx3PXUMmbq1uPBCcMRowokjNX0+I27Ig0zn0WvY
PnHwolJk2nA+mBAmSVgGkIUg+ygW2diS0UdOj+iiJgIQ0/pARhOlvgVULYhxNNgE
hAi3nHx/XV8IaW5+f8QGuIOl0VBKyOJEk+EfP6lhZ3UVwK5HYV7fJCbF4rP4u1KG
bS2AhcKHtxZ5INJIRonVQ6hmkr9jhgxV/E0V5nhZuA9HS9roZA4gSQKC421WkmJl
kHTznM4s8qhYJsY+GYtkWQ/u2qWU+BNh1baeQnBhxhGtDjhGLBAiIEU7mckeP/O6
8ji+JIFrYwAGDc/cMbKG0yrxppf8t/aS1SypbSO4hmVGqV1zZar5QXlTJ4r0wL8p
Rb+0T5BOaVvAEbnoNsnuk7Gs4Eu+AYJp4PieydFlsWgfY+Afx7tju//SfUo63uQq
vu0wWHZA7U7bgdiTsWlYGPaRtTjIXnXx8FtoyEUnwAB/PhJBJaZk5SgncRq+I+EU
fgCpDG90p3e6M/m39rv43VRvjgWzmfAytmE1d0TkvlXtciolyCSzJ6YOYqcx7h0a
n/CpXiiTqquB6CDJgM2BpLp0VpgtYPRmO+gHmjuJp8X0Uoe9MMk5U+y1zkF35Saz
PzoCSi5hoICnWjYSfb+VFUMDEk8KEl/wznI09KTUZHhnlHX14suIKLesL/lszAPk
xwqZeCISgUuX9Ts5v5I9J6kYD0PLmoem91qo8FklY7ty1raTvlwR8ttzcAbNYngF
e+ap6xgL29sayTKPgqTimpyWPrtrnK/lFch/HxSpg0ajyOBKcIDjluwLnsTtR7Qf
cvBFa62RqxJ5EqCSHj1a4Mvkx9db78s9qa6+vnc5E8Gk7CyETVcMng5MoFEQdMpu
Wq+saOeO75ejNdyAFrdtqThgvL+iGRDcVvd/EIU0gbkvObQSPrEjxJ6wTyII+w/P
euBRH8kqgm+GMt/SWh0EQE+430mE1dE8AUcUqBtHO5KsBZe7FM84EZGBR8cfILAm
1W4YWBI9y2D8PgzZaMePQ6JJft3GLdf++ayy3eDJVoGZfnh47myijqMmOJtvvFND
FZiOq0nYMYL8+l48RLp+dHxgQ0BNoMMYUws0pJFuNaP8H/CIndhC3wtHdqrFgXrk
yb3tmGs57Oue592wgTwA/GYTqZZwHPZCXnihvMzyGgvcZapxwP5o/5uwsKwmRlG3
cvPBVs8HdVhjAEgXO7dTnZ/fjRK+zl8TBjYqgWydP37zxwdmJNQcZKq4dbjXYZs9
MLHRM6Mu4klTpPTvvNdGnF90qOGBZeY7pXyHBnS5gKsGwDz4ESM6lAx9Gvs52ZLa
PIke7D76yBXhvaYc4dGUMrIcTyABT99UWXtpMGqt5TaPJXJuGdZOv3eNvyJg0j+Z
hDMtW2bBH133pxwwEu7/QMkJO03iib0m5wCMp9b8lBPv8e2sH2zn5S1922iswAQT
5k+QV/bY9XV2k7wFuq77GOmGt1c5pYWf7FVUR3BIU7Vtk0+fgvGWy6FwXQlXG62p
gMfbFop12TeQuY9+Zvuvw1m70Dp6uZzSkHKUydOeFYL/DOFSCEKB1T6DlKUGnL4Z
8CfufWRJ2ReejUmCBq4hpTZu6QLJHP1xNb59KxqnLnwuFE5u+kpo1q4u7hvqQ5bT
9jv8sKqddF9/pabWWrlB0p5ipFVv4os/bAROXL45I/jdHK867iq6X75ZWtlv8LyN
Sdx2ek0MFTld499m0KgrY8asya3JodTzbvMbTVRY2NW9Gxb+0LmG+a5u2JZ1gPPY
XdxYW5/3wfGgP/n/J6tpVfu+UwLFmr5kqqElwAMa2Ss6v0GA6Zhu4GBKYNzl6K7u
VE+7jxPYwwu0lbSATJD6sJgMHPsGgt01EGyTKzcuHKuMsiG2q9rqd86V/qYYr6t7
1kBq102ip17NAooLVbyxH7tpcuJVeaXPOUjOZjVTHsFCEmipPPKUqgae4x5jWsr+
9LuKS8lMuranGvmy1jky79N33HaT1zhGtgbBZbrG/9645m51+ay4Iuy9qDFeBjYS
pP9/ULNIf103peM8SePKeHPBQ1M9mLtuQiHSBHvR7Orqrg90hKjtL9ylA12TCX/+
rJA1daW8EkGvCv/fqhzHFUf61c+fEUAbwfLjlh+kXRG8RsBiKZrbmrEwRMh54NX3
tXVeIAJcjNglca9gAhJCWNxHLHgRssyLojJ+um+wqfAto+6FyBsBVo25d9icYOGx
YExnAhZmb6TeeFJK6pSTAuTFxuGI45snuV18CkuDQw8vikf5W6oQW8nF/scTIqFa
JJp+XxxgULuIZiUbWjtiw1+uhcNURdfdyOur3s4OnM3Ul/vC3KNOWZx/1x/Ixy18
NGBDtVV081K/CDM6bHwrD0kL8ofs/dmCjqe6BvttzreghfsUGzWUtUEvoqSSRq3v
9wHUFeEeb9InUy+8py3NZ8MkncHYxo8MrRJV9e8PuCwn7X7sdtUWX48O/xgkPMFH
wPsfGQCozHXWctiTEcI4RGk18FU5HJNroSXBUkl41JZOGyQRvTVjt+/nZNSR+l7l
82u2zIehBrHeuu+L4jgHR4LxEr8uYWeAMP26nSkny1vOcQNFXjFg6eyjEc4Xw2Gf
Z7yGmFusINumJFfS1NbfK63r+MePv+w933tB5ALIuswdUK6/J6x3Of9eImNquKi5
obPUcLg+GivgRMU7wEu+Zn8azh/l6iLikSat3Qb/zniUsy9QuS9dBpVtTJ/7jscu
EntAhg9TYkFPxzSfmsFWx+Xj0Cw4ZlbSEZRtb4889JJNHUzjYkD4ZIC07TLmQ8dU
zn56HLwr35ekPlZl39VLFsr0rc6CVUAdUOGkb45AF1cKyCgON+ZLroyxFEYQk16t
b6b5sz8qzJ5e9egbmEhLBnFcF6W9i/rDsBXdX79wFw3HEaQFLg+lnmZbOd6h+y9X

```
GnoKp54r/qpesHGb1nvcYLPhS66OSNAdtrtlQ4nd4CFGC2/NvUMEmwG9c9UlTizQ
cinfGzF4zwaJ01G+Bcg3hIGzTeGD4orgi3Qrjq3F2TRE3MOVlFScbm8Rd02ZxJFf
QF1tquVad3zFaEMAeI1alzxAv2YYL4dfz2sVogLpsAMETUZBN3TfMHQARZ6aLm+j
d/YsHh4Nh85LkDAm9nKSXQ9dmifZmZNmXqg/jUWn4VPzd+2wCojB3VYyHsJH/o5y
1HOX9Q7NH1Z1SVRXiXcms962JRf3SqD+hpt6JE9lVdAly4HiO0FrwvvmchAWBCr1
rEXjdmPy8dnuJgkwcbZ29A7deT6gjRRKi28lsNKhbf7HAV0xTuNMsBPo+l0QvRBn
fujyQT0t2ReZCSmSkWW8VeA/48/wNQZWcEMwGn8syku/RqeFPbL4uZ+s6n8cpGr3
GqBGfKkFkL28quqYNR4YTVU9YieZ9hJvlQVaOpWAYyGLD+N9l8sl06rGBFesOPDi
buPKF3UyximNUf5gLiK3R1oIUFKY90+WUFD8iHkjpVpI0v4VSc0m/cjEJb+vMJ6d
vGMbCX1coNpOVDD17U8nZqftIBe13qEzixquLDjY1mKAPzV2cLgqpWxcPcISaFLd
q6CsokUPnKgSCQzJz8rbGtndG9ZwvJ3Q/47/BplFg0sq27YOtlAWc5JYQZ58Lc6Y
mbWfewIhV7lqWdztQHd0y1NPjcdXtdYEwY6rQIpxiIAc7ztSU2VRKZwGaQDU4B4D
V76PF2/qJER0hMJYgU6/Hn8ZViV4UNSAGZ+Ps/ZL7pNoWkq4d1SlNZcCWbSR6yGB
iysohv4B0IjYz46Ffqo3tOypAvVQh8fdXPIp62Kv2Je9TJu4Sy+kL3yrLnWOmyTe
qqC05TDtARAX6ygg6lLS5g0dk7NQbOGx4XwiPXbpfxDW52Dopd97xtxMb950gy2f
ldsn6kkKnry7eUka91T+QB2Zrds51wUYbBfUJQkdk+MSWRgjhGl0BZ6mvEbn74yd
CralklyxgtiHsWqcS3Ze6bO0L/QPfkmcR+JdBo54yQoKW3lcw7K0BR0FWSykHfwp
7KqzrzcTwyNU+IiQDKbo7hQV7nVr1EM22pCW+fKo7lpxygx14xBKRvo7IuPMybcd
w8lapKmpFS5mN3Y2jbdwGzcJX+bkVDxfyeL4gKog8Vg35tOXSvmPrunu5FV5QMV+
n69uqFM3VXX/oZY4rOYMC3hmd2sW0VvFCfJxpUq9CdV3sBLnC7X0N27aBFRg6aXD
bG6Ypbyiy3ejJOd04LJxlasoQYbTVtiIgvARbpeLWtB3qq5WJcxhghXywu03X9CW
esGiyfkZ2kl9eVkUxgO2iER+50wo6PHJ0KErlWD3iVVH4LqVuNtZpLI+2Rlh8sNw
oZ7dgmZqcyhDtfOO0TkADjBalMEOZ7ah13KEgJeSysTt86lLoQli4W1HOcTWJ/SV
Kj16OeohSK9DPns1o6EWwdRjh+IvB+Ord3jWNvnmLc2E97PnsLE7XNFfHq0oYhMo
V0bUUwPIhWA9Pg+n4lyRCj+DO4wZJFOUQv8MirUR8+RyOwiylBmvEKdKzxMIe+iq
PV668dV3RKi/HQ61LYHg2KnZl7UsmOMcB5PQG5vS71zH7jbQSf1jheQ0Otpy6Uxf
20qp1ZO6NS49QeH8Yh2/OqvcfDBYDlNA0V0TzsOY6o4RAKmkoUmzRAE5bUjq0Rz+
1gF1rKfW4+EXiz85GveUN1BWeWrnrcb/Yl9XdOaogDoAhaz/X2ZDW2ALgLiOQIJV
uZmYEQQ5bjnKE/7lkY20pTmAahYKT7/jhJXEYsKBYwtFs/C90u2d9L3qKN3p0Akz
2pZGDZ/2NOGEn2kMrweD4g55Xk18wwWpMqC62dydullfcrL35K//9xuuFDemkCF3
pp6fWtmbZQmT889+B4DNLdPpo6mxCo8ELCOAzeLLh+rkzwUwS5nqkvVMgohw7zS7
/b4OS0gt1ed5PqJF9lOWrZJc59oUd2LzkTaL36G7hp1GksH21Ed3G8rrMUWBtItX
n7p+oBF0YWhjuz69qHfBA468sdHvVON2k0w3TQveSVL1vDeWGEklQ2Hk6SU4OI6s
4eyf5R9p1ipEii8aoC8a8p/yaPsHlEWrM9oIPNIWOq/1N98vNHQ7hoDypb0U4nv5
cpxCwzZawwskUFPLDMQTUsPonVwJTFGqHKCo4v6XrKeM7eD2+gjVoDRAmvlRWEGR
8DIfYVnIQKdzP+BPKlx8deuLTZg9ss3ggqzew6lnVuAs0v1BOmx/tbjLPg9syjZD
pbTExSOlHKmOynzEiLoaqjUY7yJ1oG51R5LAk1ADfRwuw0TomWJjTl/0FSqAAvQI
/El6wcK3iq/B8dZTaSEWdjd7daey974vywQaN0ZG15z6D4QB9SV0oWGh8aiaPPpx
cMFEu/6z7n5iXlLHp0zhFe4mRtFvF0vMuYI1qJLyoTyG5yJE47y3uw67ccA2Ftah
NSyaPZ95Z3KHUanGSTxBPNds7jfjnNTs+9A1XlyX58aNjiwQ8sYfoGlPGr8n/qYj
mpWY5GRB2S7/QrxvNMdoeHv/2ud4SEYmSzYxmT68RjybdLSKzA3nnXZiN33T+JGL
YFCnS4Fy5TaryM9wByq+KfIS0CkloHc1fqalJm02xAul9qwQ3kxc2sjdgrIRKrrb
4Jj5Jt1TWSxNmUGl3B8IAdNbOXpsmAE0/YCeD7Q/g3GCTShzBQ05BGkpKb4YM8hO
eE8v3qnJLAtuvYfFAnJL3Pf9qbXyOQAeF8xaoyQybnq5JyJLUvaamy0tPucvzzfJ
Fbloj1B2xreplpfqBLXavxbS8JZTT4MbEWMo0U9CgISeS9UeP0rySCiDvVz3cH96
5/QBCOxZLHU91+D5e7yollp0WGOlf4qzhyIneM4FJ8Z9Q49xylkqISs2tS9EDttG
bZH/E97aHiKubXc/4/uPnnBQO7Asn3ULrzcp8udMMD0Li2dOsmtCw2svTT5nEt7i
uiEU0AwpEppN0SLxV+4au4eCImjWnPCVcLwLDqYXhzbiRECmvQXWgaELHAAxWSdv
c7VNcyKVjkiOYs5/eqnO4aIozg+yicDncbSaDyWv4gCXATnvK1Farjky/CHx9Ohh
u7HDwrUevUpTAhej1bSFSZwNCAPxy2wYjSZUWTy7sHQiLCu2BS7BPFWkplJx3AaB
+fRmXmSp1f/O1FoZopoGK+X1JNK/PNmRTphxUTlioSrOiT+sFT1iMfebVgeBe80K
0Fejd5/l+ObIcar81hljGfz+iYh2hmgbI6Nov2FSbAWUNOKmJFMGGvAfdYf1TBud
xNGFMujqUShq3KMd5Kj00EEh0UIM/4zl0W/IjwGWjyVSdJDpKhLszYGSuDTvzv0B
```

```
gbxa3fVkrT8Hvhx7L5TOZkHe2fWm0ESYSgkcU7YbqpPlc4kYTn21CNjmDt5Gv7MY
90TNqEsFn+CefJBmBsHfM6Qc8f39eGEbl0W71/hsIINwINEqlCnOZZWBcPB1gC86
XJxCIEOtbd+7V7vxMFtm2vxpV67EXwPBcPRpYziBfMJR7HQ1S6SC02iZA/st0sxM
TmAwuDOcDlplEylsDP1b5VTe1Kw3K4/wyZzUDGOBiX5NEsNsxbUbAlpapoT4vr/K
rnpHBYazsko/4SNI5tSVba6bBGq10gNI/P+1Z3J6i8n42OhYE+kiuuVZlOJRdnvl
fZngAhdXdP+txjp8x+wJ0H06ECF8weegefByciOu+IUhXZhhbRcln8cD1+X28pRi
Iu0D72BtaQtFBAiRUwJ5vvNNbP+93PpyOtaztZ+OALA8uwSfFIxTzJAzSrhJpQUw
7u5egWZm0q2UYbL5FygB7MNFvSy8X8wulnGzYR1D18L7zVYXXRxlzqm+Dt0ZR6yt
tvdgWdJDCnjmuvMr4D5sooEnnTAoV5IFgPunrkKEPhfLEa96dK4frICYF8+sI716
4BxEuX6Lyvw0N2kVKSNBOIG0g7j0qovm8VL6WD2c5MrgLFkzrdEz5pMwdQezORPJ
6of6JgxUBQVGyqa7wMNTFkw5dsFePax38VbctwMq+EI0ZYyQDTF0ue1Cpboo9EEj
jcC2fCV0TOYMPNjT2rJnZlSJyVSoqlUqz3MimbWhujdhCA98X6Ge7pI8bWSHC08t
OxV4D/VtednzBEZzmNFBTlQ5YJOnia+b02qYX8HxF4l6OiyI9BnFScDnLNvKlLyi
UuLpLtU7v61dWEL8VWn4LmQohH7KqKqJfi6/MhZFLcwUgprG+kUCyFH7nt88+TSb
in6JfjuRwuygd0XEDufklT+IOlaJWe6d/598WVPs3ceevuvvSF/Z1X7E0uqJ+mg3
4GS2+mrg2Wg1y48r/oV9Grf695xPqqS3eC2KKejJkUBZ1GTL43Nm20e9QvFrJKaC
uklxxrgtVYEQ4UNjXpisHkRsoEqy0myFKTCTbYJ++rT+l4eQipdP8A14fNZ7sP3Q
SlQV8f7Lm/s0gbcu7wJeGDJbDTtEq1SvHVQGRXve64kwU2ugdNix/ftCR1XpUR5T
fNoU7J+gxMS/O86qyb8kTLVpw9WkYQ6nRiAn7D/WtCo3e2pXnfvpafyTr1xmQRZ0
BbxPAnCkNSdDrvAzu2VBkXv2tqpaS22ePDh/d0hzZtLJs51+hXkWebtmqCAR28f7
L5sAWlXfL02eYecUSwLaSZKGbQYYC8pKgFRTWH2sBc3VJ83yO2BC5HiEXb6KyR5/
Mdz0o+61XYIgGDY1cPJb2nZNdhiDxDtLssDW+rIiC8poCyDh+SWKS58H2dyrzDJS
eM/mhIN42j3nxfsZWL9xjlqAr59hBGT00ZoDJNXq1UwPAUPQg/bHBjtdlmmxDgUG
FmjYVSc5hKTX1DjUqFEuyK4USZSoM3OzjYeVYT7bmo2APIp2xyAKYq6fl8GQCiOS
DJQV6AuSQHRLGjpdIc7cc6KrLnt3AIXZPT5z5o3Y5vAL0rDO2AnZ43Yl7CXK+tYE
oUc7nRaHfVLqqlzJTINC4Mh70LmA+7sToMOZpdj0g7hUFsUI/GfhE3cgvyY7T4iE
0VhLgHZo2VkTevDjwlyH5Tg5C4nqSI7oE8u3UMgbwe8Igu+PHjf1to0o8DNAE6Dc
TkArqNPWCG6jfYntPsdMnS5FJ/FzcOVHs1ExZ4e5pbn3Ssn+qvsxo6pdPNUDf9ij
uuXZE+SMkoj6B2fWYFP1VlV8D/FRF6BcboNTy8lR55zg6Pff8GDVE6MUlDTuLq/c
RjkiufMtoCezd+gwWyyQqilGcp9Jwxx+AD2vwmAQWgYSLq3HmEyAUZeqbi8IEcFt
lZpNx92ufTfburbSiOSnfPCaugNT+3oS4pQ0siNt+O+4YuEOlI5Ug81XIY9qePqH
f1SJrxJWddd1G7u05zkAcKFSPvH6kWIB5rt9nk2NhOHIy9H5tDTa5Ku+KldSdUrG
3+4hOUpIirZeBrnF4SrzK9X39IPLuk410+AbudRvB4MCaINFDZyFD+JN+hpa6+43
SoXDsdr6Q2U+RVrdLEYcUfhJo2ruSck7PmyRRIwh/P7tUfKHkUPXpx6eBds08Udj
L+ewktAqbHlhdyr40MhL4rBD8g+x1dqf/UBy61t/P0p5yaFttqroueXnq+XBh0Li
1oxlaHH0cm2KFYON55sfHHMSAyIsP/PW5igV2RtiQPpf4Ogqsk7GgUkM9UX+34TM
hvT8JE8OY7SKODEtoMQS4nAHPwRY1eqa5uBpJr6JxHZefjFvEyfkXgivxG8UE5qe
p05POypV8Up9N95MuaAvJ49Np2XH9rmsgerHujb4/8cSIA2Yanp1j3EvKaOl6HoW
isfBi0n55b37YH5cDjSo/J1SL3/ILfCt+tsWPY9gqQfHLY+sK/BeXGKuXwIkSAot
fteHLSnRVKd6G3K396c2JkTdAZnvCSg1G8C6rF5yW2fbYzqiwk/zNSpU1fBcWBm7
a/ghDmcJrVdhei5Vut9ujMyqjmU2HUdrUHaQplvjW66BKOgdDRmZXgQRpU/QN1OD
uUUF8Mocp9PJ3OujSW4im6C8616E0e5A+yBbjbKmg6f+6z9zyWbH+BlHjG8IcrHA
3ys0J5PMgsCZkYD8Fk+Bhdof3ZzUykrysNBCf4N7VXLXSHWoWsDxx7YL/aHLaN5c
hO5H/scsK/gNHQWRBvb8bRxLlBFlphLmNh/sqrbbUFhFcD/7qkiMbM9/OBIyBq/w
+57+z92bxTjnX2B5nVhl7wks00uk9o+9ZhsHG2wwbqh111TCnMt6898nOHzpMNFl
ySve4w0Bcr/j9uO1SCoyTP8ypi7RXJkiPdHlDAdd1D1cX/5MMWHOCUDMHTDYxyTV
QCBx1ScaOZzJHKZdj66orSkzvZCxorOQrFaCZS70rlR+OeBtzS7rlJ9mnkCQYdJI
uAKVpVMTr8cS/cHxo36zSz6BB4xOb1DAP1X3nXJA0uvl7JrBt+H3iRzXBrHzwvlY
dxxd9lxOtJ+BbBOzA6FUQAUjpWx9B+a+t3N6zYr3OAhwRha2n69TPZrciNch4ELE
yMdIiqoSgph4w3Pxxrgsr CkbrsFkCCq0IY/XKfFZDV7ijIQkTjsh0Fak4kvOKZf3
KyYUhAX5uv0N6r8HWIjW5acyM2xg82r1yWU2CvI+fcNCulw1AVBNyElfH5LUTN+m
vp6wZabhZy7geOJgUuuf0s3j7GnlVVl7Um+A3q+l9+jiJFXesmbqjhCdPWZ0fI57
oLthQ+2sCBl+MIvwOc1GLODsAwPApShxI2LaUXo0OX2tKxZhTVcAUfX5Z1iK343j
```

```
YFJakkvefQ6k6iS3RczcvebjJBFZkeDh4+PN51xTqkF79fS/2qBpzi8gTaoPKP90
mT0gkrHRRhyfF8QESsR+jnoZ5IvrolEWpAdih/Ynlz3lyRqBr1XuUzHAoTalP9C2
otlRFkreAcHXl0XZPNjUZDfRno7HgjswdyBbatiFKJkQK9PlKrZZEutfrKj0sg+A
JuO9DaEVIYXQE5yLj39uOQ10m0xwOobJ7PetqVoF9DhxiU/MzmXCPnW0RYAy2fhO
q5uF8/3t46ud8Dv5Sdn59IGw+aWidc0+JNJXv9KJHYAU3wync8FO51S+m6tc1IKb
JdFow74R0Gy9O383q4vGU1ZBmxV6p2e70WQqX7dCG8pybSL6o7GAtvXo2BLXRASF
yQh86aOgTlJZHppJ6oQTRfL3/9duM8S3t8KHpytPkAaC9LfQMyg6EN6WDsNcecGw
c9+xTDZEy1tSjw69CouHiDdIHeORB14inoMXlXyRhyqJkYzkIRn4yAgdZ6RvOr0r
KHf4bWZNTJ6VUtYxYTj8CWTla5pxOmsLMHct3fQdF9S+xXmduT8nD1J6X6wnfa2J
Hq5zXFLOFdY94XF/pC9lZHgFl0XCpu0eyF1ZnkYl9wWwNm0NEWBUgHRyxMBG4cS2
hoRRzniil7Sh3eLuwG71RUEff+uEzjx6MnVNfroBayMPJ2Oa4YQMBXsdfLV8f+UG
CZ4s04k7dK+/OaqgHp9AEKta6ciRzXsSGdlS0pLzu2typjabD3zjHxpko3FPrfm+
KgjGpRDPOOjKPHOnXbC4afBkbLqnQESQ/uFPtdHLP8JxRbejhtOCgs+kFHPt1JCa
6oxW83+y4/tzN/dDWDmud5Jv/kgmQODTLb317mSNnB1r9ntiXhSFfLmKdgriuxXL
wjqDbG3TqXQlLEBbxllBRNpCX2bavKsd3XR+at3csbzB5COMDZ/VbeTurvX7Jd1n
T4YJulKbw9bj1vOq4MLPBdt/YKf5e1MhwXmf9JnNgzcqGwplrQvs5IrYcEIgZmUt
znDCP8bfSKmPx+pER6mzK664tkLQQehZIm722hlT9IN2P0zjcDOChWk+g0hV/Mam
tn0ssxkWAIVHD3/KVlo0jZYOPr6sM63Ic7ekRPShpxNOzpRfcnJXoYXAQNG48gUX
XC2lS6OgdyIHlIh4I5LqQ1LpWnQyCPV8w9qen8LkWlJe/WE7eGR45PGJcEJeoQ2+
tLx7U/Jdz6aifuLPUovalEmpupdlc/QVEoI+npiCbfz5ksSSZ10SYPyShGVdWw0p
cKE2DGR+K8MEt4+FvAn9RPBUzFt0mqCpvK+dfX53+J5sWl4jxdrGLTx3UnlUAAue
snAg+QIqno0qvYLUctn4WDALkrG4gvkZ/P1O/bHzjh26IGOyr9IJzADENVfZhnb4
n3N9Cv8nHYY6Tx60FCJ6wpCtONTY/XTPJG4HkrERTguouzN2sRbB61IhS5ioVJjT
HN3T1nA4wPXEEf3qoFRT/qcZzAe/SDF2kmpG8ExdT3A0kDY1TSN++UWHWEWEr4O6
4y+L0E+dY/aLulmr+iI25GHAqUa7nQg6iL2UE5VQ3fDer+MVaILopyTce8q11NvP
f6HLJvfy77B8rRIJgLv9dGDUTzmP2Y/2v3fS5nqWV2NGJpn29U3HlFgHbYgPh0w0
GtlFAkQkEiYTawB6FeZ02XABv4xX5bG0uPEAGK+7zbg4GqTbcxxBl5xVvO5JG0Wv
AdOeEM+YoXxhSMHIfEGcK4pszRYa9q2RNSuru3p3KF4b8Y5cfXp7MLsI0Shlqbkw
w7nZwfDtwdsDuWx3jABATrck3N5ifQ7Eb6HNEiZLJOAncCvr3CEsOZH2WKI+CuKB
thsj/uCKhr2L8k2gmwTzp589LLapDXIgrGy1CzSSz6CDQMhWtenqRoqNzwXVXsBw
osBC1vUyktMe0R1V6TQl6bIUK8xNOloJkp4ps/+d7f6Kc6r2XnE/PTzP3HwSRv53
tuB+U/JtmnnzaWioFC3ZmLvme1hKtDAOQBmBAsihGjmahO0lw/iPOf0zOT9+Dwun
SUsceS09kOK/CbFNpmJsOcTDzXD2hpP9oSkoXidmYCfylL+fxH6XMPvQ7K7pKgf+
YK1YbrfBqH9qnEn4+21Z1FFcKDqLd1cJvabG8K7LZduOKffrsLUygI1zROb5Ch3q
0gGPv/Bn2h2/yAV6moYsK+7XCoM2sez1PvX0WkfK1jE5K6gffXxJb6bs6mOMpIIP
p29p1evt8SURK1hMO+Cvqnzub9q8r/oYrLF0UOTt7I386R2RZLKdqGNi2JR76i6V
2lBOU0WhlXtC6QvCD/5E2dhi6/3s7o63SadWGuW5CUcXKPjuytmR+jFMARpT0zMc
Va0qAC9I90NAeJ13eTLFmNWJ+o0MY5Xj4ONXT4iGICetcv75iZujmPs9ThrIQU/k
+Ct+VWnQYXSTzO+Gx5zMtqiwY7nSgkHxdHdaRLtkrxI8MkF2EeOhPIGdrm5RuC5k
LTD0ANv0uuwvA9erNG699JQR3Km5d9kfz62a1lmmIAo5hStSclbRqK9Dt36fQgCJ
CrugEo+SkpMyC5VjzS/FvaqutzlDyeND0+l1fXL5KgOaytBtAyIX7ndtxuoy8r9f
DhjVb1UnKLFBVIiMyGenIkTcdghoxQprWZvRIKIO7BKiUV0fR2t6gZuoLerc1wCb
MULE9R5ty8RwgJ1mwvIw6Klpnwk0p/ZrBNCA2H251ZMdKngHGP8IOP8i0p5DFOEk
DTAw3f5+5r/pC/3cpD4wxa49c1U8DCLJyjEJO/8olc0oqTdH58N8/t1ynLxQUhHA
41hqCKQ3xqfzj+QBQ1myp0MocfgHCwoLy+8r8ikNk9HXhYB15fr38/zFBfQ1QQka
YajusDSGMVbLPiYjTYDedqDrbzCr0qIlsF9GNmXRF2hfEZZppl/AJ83Jh/02/FvO
cuvO9TAjS5dYY5rUgokyhFAEpDjS5/Ikn1AXPl4CH1iD0941AAt/c6CK8leJrLd1
IrU5AV0zQ3M6QNExjNpOtfOYd3DUMRHX5tbaXIdRfEZX8kM1c0BxKfif6z+7ZL6e
uOVdRYMkPPOKDOhyPFk+UNdhVFPzVpVP5AwPWdN8sBCTM9QCJQhgf+5RccK0aB7Z
LI1eR09iqnNIEeUNhAjtRG7HUe3P+HUDGxIWZkBq8CAoLY98AXh1IM/5V1j8JMtL
00+keTi4RZBe/st+hGOHf5dLGiCA5GyHC8bu9PgYLPcu6/BZvEOHPTWbQV7I5PWu
D7mLRTxDl8/Z9t660TDVC5Y0fnN+3FkL1wWJLWKvq4h2qj4V6VaFe6wi2n9E9ir5
GKFXwXrppNtaFFL07/8JpohOL4AoSWvuGOJNBMAdUWdvwgO+DNbWBqAAIdO3WJDf
```

```
wTbcucZr88UjSWoc1xZipSmLnrjOdw/2cBOry9XPYkL3YSJhrADRCCnbSfn9478F
7P1XZtXvD5XGmNx3bbYuiOz4cFt6tsMc0CppRjnkEbc3yEV0r6HVj5OzYMBHWd1l
8XRHKJr01yVpmMqdHt4V789OubaRcRtraE6KXwtjCZDkQQA3rjc6LmkaX3CLpJ2v
e3gAtWNoHI+r7j37iBBAstpvmfwXGwX9v/TpH34hiI0eB2WdPIIoLugbZic0qrQQ
WkfxqmpBUse2teBo4bAJlF2WtbB1sXbqdL5bJ7j1PKOwl6GDIUs65K21EJLHKxuB
WRFL2x6PMG3eBJNGdC/e6pDqjRBueCA/R+WoxET4EJhCsUwEzjoxhI5qrF2l8kPz
zFl8ocqrxOFB0Ye0bPPnu/sKDw/Y8rJJ3ttRlaQ9qzeJ9U8mv2Lk+X86a2Gbd5HD
oSzkt7LNsB/43deK3uE9GYzHIprZoL6XGhk1NRU9MddFAzOCMIXO/pvWgNpwHOq2
9/gjJkV0TJDYdMYzJw2G92729ocYVzW7WJEliuVMXvsfYog2kRcQ5iRid6ehiMFP
dP/ANWv1eJnyGepkK9sU1WWFu2MTJ8uVbWfhgerOtdKTHcbl0kB8D/rLJAXp4A78
sM2mTIHE/bzeC1sHstrGOT/V7r7iZzIP1Fa69MD7UVyjPAwbiAIRsFixA/BLHS0/
RwhvPoRUZSPE/5qNa/Yk5Ah1osdoo9pVNJ25ef4AIVT4zwhrSinfbwCerrsNPo7T
awzQ8XM3838t5wCzzd2VdPhMWXD4EWnVRxYNcVqvWfWwyZKDJ1iAfDScpDrknFXJ
uEMhlKCGFBOplU2C2WB1iGO97uxdWaYI61VOnCIkloYB2KtIMYPeRs3ANmHelTzc
70an8hGkJR6rsOnWXg2tORQWW/rrTs1CE4+dqsxwccYiCQqxsV+fBhFAOwoJKo9B
LeFKfE6JE72s6CHfxwsRFlJVjK2jNGG5DOvqHhRpljSsyAiMwq0hyUyNA+JmnaPs
DGUEEyqcDszpTy4SyiGk2Yn1Tkebqx91LEQMVx9HsGa4m9dqlrYFL0e5vOwuJn9v
u7j+NWqk09rHxBzfEB5wtCR3Whvr21jLuuyfIQReeAQcEFWClq4fs9KhXM9BmaWF
iojvcktGL1dXPcjBvZ8pFyykm4Ae6J5hfvvkRq1vVlXnkm6TRq/fFjlBxI1aB+yk
0vuBTUBnyvaW/ZJ0HoE5fpL1Pb3AxubYSf1h5Ll8zNFVnISfpEEE0CcBsR1a7bjg
KYq7arS4Oy3HBex8SEIUPPQVJzXFbMI2kBUnSHZto172My9xAcjXVh6xA/xlyIuB
BDf3tHUGEgcvyJSEFVjwmAdOHFoMMNj/quDYutosct/Sx4+f2dwexM4OBjACG5Ig
ph3uI8LEN+yHJNLhvavdl9yJvdTLuQmcNJse2b9TMnOe2Ra1BGMWVOY0zurtT7WT
HA4YcdHAYEcumedBkLUC8btkDs4/kX9lDuocsSYV92Bm7DrIOqk3UKxv4fha9aNB
aaxCeri9FCzLwsf9jas5ek4+jzi3nFQpO5LxPT0mYJJ1HVTcOuZxhDGAIPoWhC7R
BOf5hCD5CgOmZUnh7Z06LIHLSOZHBQHr4+Uf/E5JpypcF7MO9Tn9scYyOcqaDG9o
3vwhsPVE4xpxKOGD6OECR5JMA+GgfXOTW6fgdIoaFDO6BdIPwcc4c0oBxj7ebQoy
tAu5XCJpuJLHOUtkT86fBTGD76JrVxU072Mrz/hLNI4nHc1gkSF9brfaAqWDMCdy
wxvgtaiR4v6Zl6otCde549GCTaU1KNqnYXuLWlgu/B6Pf6nNwE5JzZDHy+9upcmg
DrPlwinb+rdvNC8veGI7gWDfQG/YZfAN77hM5rfd2XQIsu/bKSYgnMOqhd4+drU9
HtFmeAjsonKmc0OoOw0Ex8fvEIF8QiW3OjJzixsVqvyd7n0rTjoS6fd1K0AIETbD
ThFEg7kEf5hK7Q67WlryQVE71bMpVb3Nt7jROg7yXIaWZGD2rZxluaK+C1L7ZUlC
TR+j2HmSu+r7fjC3LcLyMWBhSPTaprO2sQOjVMXdeWZuK3VhuB5eOpe8v5+suEuF
Dy2PBGF7fYTPslRW7zv2ZhnFeNYJ/mW1PQRIe583qQQ6PxtkwLfOpF76kksMCJrC
Tx1hCBrfVaILU1rOkIYMhjgYL1SSZdV/KW1xWfkgcD1JC0HIvC8jdo3S9D6Blc/s
ETi4HDwDDbH240i4WwtsNxnyE0w8K6Z/zb77WEVUOmKQiH5qSycjrqDqKyKUhxvM
RRNbWCbhoDnhWd5Iws2g9+dSD/vFJ9RuEh5cmqagiMVYmyUWhJU+33aBAUcFbZ+g
Otg9K9mRFE13vDnYzTD3Ja5UwMMtSDyE28fXXvmgbiijffaiJZ5FmeAsZ9HIkUNU
akK+FII+lNZs7RfuQl2TboCHex12ZjLtvBioy5skPfwuCRX47g6D9oGpejEO71+2
mqkzCBSf9PbQV95j41h/yhwFT1BOemYpcI+hzVJaMOKcXptNyDQ6XP+ZhD7rlcQD
FwwJLr17ELZ03U9iHdub1dP0DU/E2oFwEJ844RvNVl7RbE+KBCHD9+W1GhvuAh04
AbsnEw68CdMhsA5Jfgt+A1VHdMjgziA/cvpVEhKqdWtReUS/2PQ9S0icuBwh87Ts
tAjsRMq/Oqyl0LSmdi01yBtDfaVa08J9ydVjB26jNslk+qpV55Q6I+NMx7oZLDjf
vo845OyxW0zB7xQuog==
-----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-----
```

```
MC0wCAYGK84PBgQNAyEAO6644sgf45+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
AqR7O6644sgf45+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 theSPHINCS+-SHA2-128s-simple post-quantum algorithm
- Sample public key to test theSPHINCS+-SHA2-128s-simple post-quantum algorithm
- Sample private key to test theSPHINCS+-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
LDAqBgNVBAMTI1NQSElOQ1NQbHVzLVNIQTItMTI4cy1zaW1wbGUgU2FtcGxlMC0w
CAYGK84PBgQQAyEAXndonwKmchFMOuQUWLz2ib7+RmWyKljkb4Em6J2pnN2gADAI
BgYrzg8GBBADgh6xAAIf/u7Qv+W6YN2b4HIj4Zwf4uYhaob7DcTv1xG/1lIcMXuI
o/vxDIfUAaSuo9wzXViWbK7a+RRcB6BdDnQ3VQdVkr/wTalJdv0PGquja6gBamRp
75TyDaD5dQ4EMkWBSf3NsRHKtnri+47w3Sg6kQUp3Zd7vwE+qKESAXPFVUetUIPQ
7EYlHg/tt+Hv2Yw34SJIC1GBkzDTv1teatkKi3IYtrcNfn4WdKbYhQgWBu5p5F5O
mJ1rVGUxARkUdIbL0Z7PaXMqM2v2A5XatbIYq0OMnwUUgittZQ9N8k8hhpKx0CU3
mpsUChcXvFyt7l3MVCUFtALYxndUNuRRebDOOHM98wCttIo4/jxB+uWkCZBMWvxe
G95WsVjPh6dfeKWjU3oUHl+YSe2dyjTjOYVd/HAFb0/A1WdV5g3f1Qre1XS7+UJO
NZxRFT+UjiS7jaRjVdiISSTA6kgAz0S6PznG96fpVpkO6tIzCqmxJbJnt0aXS+z+
Qpjq4QD/wta8rpUx7nTGA1HDZrXjjorgTdDGVAXriqYX83wRJOMPwAYp5fFX1nff
AYQznUJWGfNzsSPlzLEVXWz1GCDaUDTbd043u7GtYCXpNjsQkgMeydcWCchl1sLA
cqpYpYaQ8xlwzvOeOKB7vQKdMQKXPGr5qfDYz+rQfoUlx2239qoCJZIhxWJKzmbs
OrDPqWmT+q3draHiMmCtO9tASkd1zEOFtAqpGKlkjtqQPMIHYu0Os20AEVUM7XOp
CDBFHalLy9fd9pDxxTEBJlKnYvUBnDejE9Hy/kl8+vHzqrR064Kr2ivMIoYrj0wz
yLmWbo4GGoruD+LXwphKkCEQIAPo76QFO/iPG5iH1xkfQFUXA2BgeXFbYB66QujL
k09VUTwT5BFS1sCFI0lpMyz8bCsQQi8QAYlGgOooCd3p/muk5MYjk/85PiDE6E5E
uBIeqX4Kf+x+eiV8LdRZCJOSjFtyfWNHPtQxjyfJ4WLwLm9fKuCcQrEEYy2dCuJd
5Mx+grf/t4FsrEGNFrabdpd50JwIwNX7vi1oev3kSXNlHPaMns/026rYih9DUc4U
nPFVMSn39DW6AI8CPnDlhPVALL6aKbq0rIvt9Gx9z9Vy0c2PFyGIR/1nHZMlunGc
+8RjXrm0fp8Vp53sPl1VhKLirclMd3qAa9bsxxAMedzetrVZt8fTU3676oEAaiZt
```

```
3WbEupO3LhL3zyDnmvr0wBKJDwA3/1RJshCnWaPQb9RN+bkDvy/13Wtgi8FKXExX
GTwgINbxYDNyxAg6I/siSoLuvmZZL6L3BN+ghexPznCraUvhE9YoSTROQDruTTqY
76bpnjzv0/SkojarptmmYsltKsB9NF6DEWpfEJ9IVMv4oMbI8UpqzYGgLP1WB7V5
tOGLaXTZfSy3sFDTog+gEvKFVHJL4rWkWT5bZ0iNsMYshicrq90qqMR3Lwu/MgO2
pTOyiRlCCSTofkObcSmdCwp2jg+7fjWTCWLz13G7NeElkbtttjkp+27OAefTD57M
+IcV260sIww1fnF91yzZxMoHDKRy1h0CVBSFKhHQ0hjp4ffdgJtyzCdgI3pVCSxA
xza8xvuKzA/F44zhlWLjRxF85UTz02AyI7N7pGtYgp/hugbULmi1CE3aYmS/Ztrl
W44rXJcSL+Ztw0gjgAqjL2ZYi6UWtUbHizq19WPAq+l7YM7AU8KU05VJjmduRl4O
MLUX/MaY7Vuh8y9FKfPHQq6wK2eSxIH2N1mh1XfwY3nCzpztuQi3i/VWoY2wNL2V
B9rpuFY4a44q3lbVt6yefvciJuNYWvMrOVJekVBPzZqlWQ/1jKH8Oj3QzdHYujNT
ySR0lJQq88add9oEglgiWTIcmmHwb0olfZ0WwaocE1Zy4K0RHCPf5jwaSGI0cLaa
g5hT2QD1QG+PzgzN6wjn306d6XnNTHD07+f/yS6znf3L5YVN8Ik4LWFKHbI8bycx
oiUVQIBhhbkoFVkboucGPVz0OiWzA0bRGiJBImdMCMErbY1SpieaqPVJbHS62th9
82ldfQ0iFVmuFif0fvZgarogPS5lgkMe2uEQImS9Ev/pixpFL1pwij0CG4ADldkN
yu4+YeYmUjkZBFsTB4mFRTWU/8GrT9EhElmOcAMOIgPBGwbJJWLzw8Y2JKnIhWqE
YY3948TW5nKXCV7OVbjoaKDZZtRDsMQPI39NmbIz5pwbJapxEYRrmDt3R/gwBo4L
KMdycn753XQ+Rehy4cpwXMNPVpfnpZxnbteeaTHwpHZn7JCmnCNo1uUrQd+gtzJv
HTc/Apx4y01ZqFKzMuS02Uj6swGQJmdXLXtI+chULKTEgYJKk2F75Sfg0wECgH05
1LTzjB5hXe1THRQNq23rsNYpCBpUrUzhnqI2yVLzmgjiSMQ9Kx53pUHd99eQ+1c1
TJnUq2hyyKWqjeEW43beqqk7YQudmSglPBb/6mc/jyXI6dF5Y/Iu7Pr4jfVG2HRB
+rkaNN0ruORTDM0O1sCW5ZEmudf/Jn21RFkzMw5jqLZceRGvrtjnhNrFrXir5VVn
t2CY+SK5n8QrWGb+CsPh2rQ/h46InGavNfNi2Cjj8zwSs3EHCEStpdjryA01HrGt
P3oEhWr51GEnozLbMb9/myL+uArJ1J67Cazl2C+hEvP50/0X4JQTqxGxbzqVnqvx
6uRlFHarmNiLjOZyT5Q0dJkR4wD3BemtevjbPvgHjjXQHtyiutkFjeI464y2cjJ5
XywddfAw60PdB8W2ToE9iqrgAdkfJUzAlFm1K3sgKgGFOHwyxe4igQUGhlzoZzpd
BQDLtS7CNA3DY6Nl4XQ8ZKbDvGl0HCghgjgz0wWc/yTK59K6JHixe+JK/qdJUXYw
ADr+FxIkFuzK+zipoHm9UsViSGOElrWUuD9yNGUo7A5P1u47sUs9ykaiQfD0icMv
2gR+w5Y0bmz/DFIml23J7d7PQD/rh8vHzkAKM1SxIYFICJCMvEo/F4CqhMtzt3mX
/sx7Td5Lq2oLCbmK23dfSPXxI7JSu5p/XyWJWe7SoUonK8eX+r0bplalRl6IirrW
6vDjuehuakyPi8mbslQabOzri6FhZjNvM+8MmxI+U5EHRXg2lHnKvoia+gIXRXmD
TgVtkzKyrotRetcHCWevJVxYK1CDeCN0TZRkuJuo4CoSTfp3Vo3AAhsC14OsMKCh
78YeTvlCwtUKu0biNMOP/L8x3URfadea5EYOq0nmrb1jA7tl4gTVRUBTdU7dOz3q
M57wpkL8RlgZQgTNo+Rt+4arYk8MK5PdMP8XFDR41Xyjq15rlJppHjdzuK+SrH8M
FRVs6evkaom6Yzj/FQ27Et+Y2uXPNqQFt3uVIufAacCfaUSTi5RcqX+bCwqFZtA1
kqLTjciyHSVBC5kbWp3D8e6LCPxJ2szV6CdQYVMTYdIH3tVkZ03nxksy8jVAx6GN
lh+hGgzhl9X0RTKUk9jh6jE8ursS9OXkVMLwQr2Grsqa/k42D75U9rw7fVdtEG5S
1yZEhUADhXpRfezf4Og8cEgw6u6Ouxh2akI7+EXITdiyS63yBqNiSIAH81CvutXx
N7PDwBuufI5ziSK/PyD69Eq2Y94K2hzlaCKstaTnNroaXmRETMdT/AZhHGDjdQ7o
RT8kslWBelTZ0ppBkFCcYcI2I80+LQu/U2YkaBr8M6o2a3LMyZTUSbvXZ1GCQye6
6Hc1zCPI4QRjmbm5LnNHo87nAYpjbS1dQ9jITYNARyYRIhTG5D2S/zt70NdnPDGi
QMa/6vCwCLKn5QXgBowUVH/xoTMpiOW7fWsf+suxXqqSId0jVChURcgE/VBuhu6l
A4safMy+k6ZRbSVJ0Fh4y2lXVM/zYhXA+LgSz2DQlMuxhbYP2U+2N9o259Ckhw5p
ruysIuOZHTG1hMkg8GuN52hDzBKMCtIZOd71lGMdzBql/nqn/37czJeY1mMunB9Y
ccx0MLDN6txWAa8/JABQsLVh2pPiEoYvC7FjMKtTK7YQX2K5ghuL4BiQ7q+q6Hk6
8maba+FpxWI321D/dQeBKPiq3KHFiVd17567mpquspDwT8gHwkhapA58o2ORMbV3
DQu4AAEW8AAoxSU9tqvV0VMauwjcd2CBYBy13WvTMQ8duOVnLZiIztSz8wAW14aL
3Xu5yGTlwoaPqrfK86y21jfnn83e0tgNtKe9FvVq0yGbPS6V+bE/MgxyhtVYtwYx
YasNlL1Cwx/DrH/U5WcQ1mC2Q6Ls5XsbbLdP/7gImNKJDOfjGOTV/9KrQpKRkJ2T
XRiT2RG6ba7dOCy8jq88VRxR3gyvHLm6jb7SaaDS49mYG91aF/lEjj7EnEeKo0Xp
5Xx1KnVm/PncNgXgw77sYS75sdPMxMTVFud0RoGb495JyCZbru427xYrQiXRHtYd
fPT2EuAYr1m18H2xJWX7ipKrLhNaMyjIWwc5G62gRWcNuKVFD5bLiURVz82mdfop
N7AcN+n2dQfuHy5fGEk8r9ep+B3Wte2L9KS8Oqpn9k2Mu/rKnnqp9dPDzl7P0vn6
7IhOk5A9uE7m3fJtAaUWLpCqsnxysTTkV4sVC8mJABiqHLZEijT0vHcSwq8N1maA
```

```
JbxXVALXmVLPH8a44zggYZ29AQpgIq5cvpphMywzTdT38HhxYwOYrTqOSL9gfpqA
Yq/SVb55S3SADjX8QOqSwur5ssDCtv1vRZ5CsABpekcaF7rdGznrgjpkx7x38pig
/7ONlmhnFvMtupIIYLOZLcTghoJkT7nAl2Osz89RJ2HgUHIeKO94xK/vr1m1/054
+s6F4QavUaJjoYDyVyONSJiCqT9NbJzGwMKRtw9kQMkRad8wWhuenhMpXBjGthj7
ImdkFPhJ28vViOFU0GToY4MEJChs0GPkE8wLyzYxDhBq8i4eW7FuFu/WPF0AmnT+
uXqA5KIO+1NjtWoyFEms2Ckz4NeEmS4WXfz669pq62AsDdNywqGH1e1Qfz61OnpK
a4zntScNDlld1PTmyVoQIm41x0bqPh0pLnagLGjR/PE/5dRCDlROitzRaXHYALed
OgcFnfOV/oI+MVSYHyQmtEDX+/HXR0sZ1utYtfqUBmJMCltruyDt8za9A8W2Inbs
SMkh7KPnOEbn5dx3ejuhLDga/Pp59NZlzf1cUmMLZQLjEAEGVqjuUXoUZkO0zymQ
i/3HQqctXkZsgDTa6aywPHpuxG9uyhprXXLxlzMJwrJifelppKZpnLzFnhTWXjaH
cTkfS0vHWGjyw6lsWOT2wXkter+3w90yACyAYVWkYCDoNMG5LiIrxik9iFCnYaxY
gxqqCkB0GVaHJEZh/V/Z4n7C9CgaXeI1hc8/ROzffujDtw43+Sk3hpS96+f4sgXx
XsBX900LO3ZIItnSFrKiUvZvGusZ3VP9+roUUJk625h/h/O3oAEj2oaML2F+O3KD
u2SQUusJ5Ag6bp4qN1hWbJmMfC4bGsax6MIXNALhIpnWhQAsjqqZH6I17EtwUjkp
1o3EjUD3BTV9a8O51k0IquuqFNufiLe1RHTrlrAd5Mxt507s1c20rOERNRqrqwGI
PMPsKpLUuvPyowCNWKvIXj8+ZGAumVQ9nqwF5nZovAcwuArn7o/lhuUN7rjShUD/
2Qfnh8nCJX9FjDtQCIoYmoVXn/nsRGPnU4kj860rd8Ne974Dpv+jHlm7z5ivNGqh
PRqOkvEBB4HQ+SjLxf9fxfLe7M9A10hKIZEhHjmqPfD3ACTgLdKKs0PMhjz8iOSW
oV00NY6fM9e736C5Zf01E010U4ckGp1q9cqjmQ9rWHiV8KLme/XTo2QRR5QEXvFo
Ii3Ek/UcrmoR0sv2wLCVU1xYX9PXHrE+/AXuVF842uOVeKVFT7/GJ1fgSueTSD7Y
ID9ynTVhL23cYbLpcifICvRzNxEmah/9U8tYwLGh7HxU3C+sD30syUVc/hnGP6G7
+TR6C7c1MKKKmYW6ZzKYySIFW5eyfgI6+WMRufdMkvHr19VELCEZleGaT4X7NKWt
oWMQfFWCYugP7yHq4PPvvNR/H+NjYlE/yXUtM5GBnDZD77XnQH+n/U2hPowtm5Yp
4VnBI9/Vpr1uxW3RETEhPF0TlMquutVaSRQAcdy5lx6/P+zkIpnFrjMRImqezhTe
Hbkif0CKbgxGws/hEncp9Tt+kLXMf2QovU7SLD5/GTWo7EqWYbqTqZ8tYwSZFAhy
kO9hDRGFSwLfR1ILEprOrPiP1nafYhH0odZbECkCb2DCp4/jzFBE2BeWMoiEUJmW
X2zCD2Qz/FgaC34MyTCcY2DdIiTbDxRoTpT+6MBW8NFqKYOofHDSn76oy6xamhNk
Oz76vfMSdikzYUZLgVtZurZ4SyXcMyD245jgitX3LTbc0EqiEiJ+S6mxuXmzDVfM
yU3oaggrGrh7BDmboBL1s300ib61pAWuim11lCerbuo181/kFUxXieAFs0EpbO/q
OQob+zzotpuVALlcz7uQsmOhl56iAy7j3WBezrWhJlZHIiXvfvq/bnX2T/XLX7Lo
wC1UHNyKHCbwjTvhYF8c+G3ekVFRBCXHXuCson8la2LIGAfvbUrtdsH2ed4+P6+h
lBaXISvZAkUp+QprctXS1C5SB2a5VYIwt102wxCuJpzhMcqVxalgmgtRiy44gnOK
MGL7UK6TmDjjrJvciNy5P1FBdQLnEmvKQ/5NrRE7W0hMpBqBN0p6FI0GBji+RBAO
MozxITIiVcNUwmoGm6/jMCwRfs9JsAjJfMFmFOtUDfuN927G5Rf+zaIjqM4+m+gw
IoaY5OS/Gv4WbsBY+Kce2DL/c7tEE781v53yP0mKMxR2boJx3NFl6G1XCoHHAt6c
W9Tw2M+O4kt+a8+zIJIoKwLzWj4v+7WzUWQ8405tdaxwismKgaXJV9vGqO0RWXGk
0sLUXSqfu52t4J29iwdrL81JYMeD1x1GwqscoVdD0sXE+1FUCJ703BvCL/20uKDd
ldDSpjH++LmOjneHCTO2bYnTonDvUvBNwwjahN3kPxkk4MztGqX9G4wcmhoGy1Ff
p3SjBiEA59kTMgZpGNa2UVEPSxxHOq0V8uE2NUIdPHz4fBxfTQFQHaGFC6Tl/Pa2
wLmyzM1UREp3LGI8AuAU6IBHwkPDeBNLHW7Et4ovI1skHMBavYqi2trGtRWDzO1J
ndv5xwg19M0jpMYawfMOCyYmGE22PyaDe/55IROXBZB5oAxD9mozn6mTp9thyZLc
aUE6Dj1UmqDEKx8zXN5ND2PGwN4em1b7/YHePvNnxxmPX0hUSWNS5/nM80EqyL/r
Oxaucebel+blbh3rze78cOWLQHm5KOOncq+yBxw5NHYxyNbrgciAfYew0XIPiIom
e6Fq8cg5/X/zQA7EB2T92oTMDKQXd3Q/CkbEzdLAOExXluX3D0BHFeirW8PUkVFL
+R+6Ztua0t3bVqqVmQ+cyb1woStmnMh9txOg/neGkR0SWfw8T9sF+LVlaaqes0lq
OxIbunZat6czCFB7IriBRAbQ4HM9ImUoccUbLCEm+IxImvACQA3jEgY8EkRYzwAy
z5m0G2AAt5+mIpTbN6b9w9iBu5FekEkH7rjDemDseHoFIFYMeLbnHdeTY8BMxSW1
5o29tug4ublBRUexD4/T0slCHXrpAfXBlPVvOXkaCOaiA47Xga4zLbDOefcxvYjy
/SxqHaNUCVSWpdHvpjw+2/quJMyd4iLYyjmQg2lut9GfrHpe1kDDM3BKyhABmv8n
QrQCjEIqY3H5dglpOBD+Q65njB8oIya13Du4DGKeLmQd65dZRERdENG7shvUfp6L
rkfbL8mdkByQhFn2HZrcIUfpoiLhzLxOmUYJs5FyR4ii8QDtsroysYvOXgYRGTFc
cQDQwImyGuKlRwpshIIIvUwQ1iINkF1Sa0u87+3+GVe4RCEDxmIcSKzS3kt1AsLX
JNBQ4s9i2KQGb1uVEO/wu6PQAxIjxycgx/FvCmw7oxGDgRiFmAiLeoDU4XNZLnVv
```

```
4jOP7e3g9sP09qpOFOTZSAgfhk0kJ3iNWfQ/vY72u7DQ2pdOojDzYPjPMmjRxUom
2It0nSzhn3ZUFXN9jhajCQd3JFaQu/06Yn9vqAceeREipFGz8s/D4V7FH8vb6gWt
fxuSGICqLCOc3faMbPzm03zF6G6djjQMZwX//hqiR+J7Ku2Ma/QX308uxvPZWWgP
NrlCtvlPtPpd1sL0qoiJ6vxPiJGnrMCQ8ABD9Vpbyt1oeUr63j5BaQv62rOW3nWZ
hh1lEA63iPf8p6yezPkU7pCctu/3q9/6baWZhn447wlJ2OHOL+OLza6A2SyxnQid
Ow5Z8+ByK9ll6AOFJ+I52WG1FoocX4THUnztRppF+CwzIjATs3TfT1X6Wi2aY84a
qkdwwut56bqSMI/lqI35sOD4MgIaUJUtTCyRAXO5W49R6y4bYH97X/nQPNUoj2Vt
2iBtET/CYZLnnC1Qt2D3IFXUyyyG7lpBKSqQV5OYJU67bd2O/hdjpNrtyZvMKt0k
RwMYZpItb0L6dSIqXusbLZnJ6zMlaBnYQy8mToIVJxdiaXrQIZNJhrKbs34Nk3Mz
chS1tUS5FqAFNkN785CcZBftSU9cHmGwu1rDD7UWSPTeQ2EIvuyoG+nGVZXugZ92
lbPN1DLK7lKGzDpRzdDsBhkggiIIUqJQkA7aIBwBTm6j1K9i+7+tamdJXhgMgJI7
86lRmRuakTPlz14P/exGkxPnLC5Dvp+dK4nojw68mzT+6oZPwAhL1+DM6E0GJRzS
cBnReY3Oq9aLiwcIdFB1hel1WLKaXACvGCgVScGHRRihZrhQRxv36ZuHQMvjQIdt
R5Fmor6GK6UbXemtvi/WSx/LcixT2qUC0NXeaOQtDiBEhw9N/7UfqLUY7Iolio/8
0H6lpvx7eTdcLvXnKfZh0QHdTh0F19TiLJRLuHzYtDHnzwGsDsC5WAb5DcYMBnk+
DmFR5gn0T3t5DqxXxR5OhNGrZnCgps0k7+LXL7ETZwayF7KlsXaDmB9A2ZoFI2F4
W8VFFVJpFi5ExfZE3EHsvhh4xdAzshQlaIpWwUHeYccSZnZPvTgvDJ2M4KD3kaVc
TaIa3fbT9CiEDLqb/6L5BpT1LVkkMKy6QYm5hxnespY+c+P3J01Vwe2iU94+HG5c
AfDaKt27VTXAmk97LcX/uVavxA6QDfZNyn5ac3DjEd1oJM3VxcEMz36iK0IeB/if
FwObU8aNTrjYbVXNaOfIUJtXFnk/7YuOjmbIwtMDXXXTgsMtBhV8IZJU7nqVf/Uh
u37psbzNzZ7cdezOFvKRK5O+tysbUz6FGxOjoiPFOk7a8hSm4571h4dhxMtvuhjF
K3ymBaci8Gcuu9+oBfMAIpd7w3xObk3aw9oh1VQbYVqVLOVNO+2gZQfda2H6KDkI
PimnA9VxTS9kdVDVY1hLEQP2EGONqOvMi/5+4wUM/0coJ8ktGxBQq1e+PVhFrvwR
8OcDwi9B7JIQZF9zG9dp8mIuJRS0SaEWCteAHtbI/eCTl8hVN47Vbt+/EnE+QccL
7shcoGJCPJ5y2n6gTy3F8AbmkdSZncFXwFZ0bl8KR7sXyAajRYtEzhvEIk1+Ca2p
SvEqzKS71T88726PX8c8WFCdMoPh+K6bY5DSOD/R4ohd4gRNY1saqNey1ZniED19
RF90oDX1OLbttHrupk1+yXjy7t8hLGY6hX3ybkTh4N93dmoN68uytM88ZAN/1ww4
OMxeL1jv6abkDN3PpmshLvTq/ertZddqS4siGEI6TLCiQpTyOCXlwJFagHIoYO07
5GpeS+EJTc2DZSAX1exnBGx4Z9pjVTpet9YlguHymjGB1K2CuNSfFNoa1zubI5mK
55tyD/iYxtf2IcrQV5QI0uE5BoTA5sPjv/N8Mob8I1ekKsuXmyAYr45A53pCLBu8
c5Na3xpcF1geQFOMMeLMsGV4wGYdfQAJl3HbI3CRZrynafoBhjY+JooyuNrVN5EF
od+axkrBWiLJoSJOy3OAXnZM5ecMgriWxQWxKxWP+EdCZbuqumN9wZtnP0eh5+hY
Yl5Kz0u9gfswJPb29RElj0T3PkSx1nkYQz4nM5iesVpQzHJxOg/0IpU6IUtc8N3n
mAQVmo1N9QxbpmLcpl2PJuJidYGehI9hOPfZ4JXRvN/It0TKeFMJEM0Xdr6FYFs+
+CrBMeBoJSw/MWgKo0WmP5vJx4QdQwYRM3cOCjeKcomFsY4flP7qu9Y6Cc9NlxS+
cPOWwmlY209wEu0Sdsl+kC8ngtA8itw7YanGDXW3VtcdQieHGXL8qGAa11+b5/l6
LdvCS82SpVglGnzLeR9+Y63BtHMJggUp8kMwsUUM5giRnfvEIvNzAA9DRTISpezH
SVNaRL8DdaZqNRKd7/4XiJ4W/y2knA4Ui1FGfsPK1dnFiBzGz/ddl9zlRIT5eWS5
HIbPYDAkFUuDqts+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-----
MC0wCAYGK84PBgQQAyEAXndonwKmchFMOuQUWLz2ib7+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
beonXndonwKmchFMOuQUWLz2ib7+RmWyKljkb4Em6J2pnN1ed2ifAqZyEUw65BRY
vPaJvv5GZbIqWORvgSbonamc3Q==
-----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+TCBlwIBADBRMRAwDgYDVQQKEwdFbnRydXN0MQ8wDQYDVQQLEwZQS0lIdWIx
LDAqBgNVBAMTI1NQSElOQ1NQbHVzLVNIQTItMTkyZi1zaW1wbGUgU2FtcGxlMD0w
CAYGK84PBgUKAzEA3C9QKtQNnTZRINo1ueM9SpptZbq/8Y839YR/JhjnSxFVOm1H
HN8ZZC5rfPHvYA/koAAwCAYGK84PBgUKA4KLUQCYa7+cJPCu2c5M6scrS0QVb5i8
Jp9LqC5Q6/+HSCgvFT4X2Vn8K9P2beTKuGN2sVOiTEp+biB1PbPDIc3hhtzUVFvV
ygPoXQ+aHa2dSFBxSIDTNMj8GLryabMUTmtHSyNAcjYNEZ041OkZNkBOqtrKxUG6
KbEa0fEsRXgayO7fh29Wc/YOrLSkzWmuHjyBfozZW63hsOKmLCOe4T6daj7oiD/r
QnGxgvV1/IRDQ5/1NAWnVJ5412zlreuOwilPCNhDu+rmr/of3Ahv8EnGZXuJL5c+
sWu2bLkBMUQbwBrq8yoJ86E0mmPR43qdn2SI8nFdJv/1/TULWVEItEqoxJJAlEa4
ESSaoJVnmOuB7AUfbimNVP78+2ZNuVRoY0IZYq+GFgwPb1u37ErqiqtJh5KSNMRw
XqGsvm4gIUq+4iMm8Ya1PuOcr1q96T7Ug6HE7shTSi+IfSt2ci3274xXG0wIvQR1
vwt9rcYi5NQtNF6hwGeAb+5q8sr+ZhQh5fWQ6IyGb7IuH7BB5YgHOLz4HZmWZMRn
tMd25cytsB6JPd/5gjPtJ44TrOZFOFwo6z2u3TtyyYs0h4vbFUOq3DHCim/eL6za
dk1OrCzaXJLQvhpeykSWqB0LaA8f3p2woIZiJR+cgWkCxgm1shms25NlW1kj3TdG
pR35Q/uE0dePkZvFOq+9/MzBzPt5aObAoJBO0p6ptLLQk/BzZ8qQWLL+LHPoJrew
h7pYrKQcuNIFGn8tfDFqEuzfT9LGBZjKhqtFZCjGbZMZg1IOaAuVbKfHL9qXhZOL
S5S2Ds8IqxbgI1I4YfAfkMcDrX6NQVwOn3Apg9ZLun8USXjHB0XOGCKYEMJ3fR0h
/kgC84T48NSZei+ZNIDaZmMBtg1+UnAkuJPRyj8zBOhKDOWcafELwDPoCD9mMVaU
qF6JUvL4QRu0J7CDh1NzNc2xbv+6I4dPwtisPgE06LH5ltLD9SffXL3SR2PcWlJH
UCKU0NGPXtWVBZM6Lj95Hr033vKUQwEaLRTzgti5l4xhjYM4LiQQBOtRwT9OKXI/
2uiB9OQlqx/ZdIzng4v8juMrAH4p87AU5lMaBLDH7cIn+leKp1YSvRrLnt0wgJmi
VlIqAFr6QfNG1us8o6BMJK1oLKdbbwWu2HEexdRwnYuhdP+aPU68p077tDKvNh40
FH3CyPaVv/DGU0Q2WScoLJ0EEoXhX+3ob8N8xZxWptgJzkplCUPQ9YGIk1heyYTu
xYCiRHtj1ikatPwwDZqPHpWNmlz8VAdTuvNJoXffsKIkLrDI5nvYE9LXvGKt4b0Y
RzOQfp3fuHEa59+LFrzHSmNO2EZq8ehKXjW+UIC/yptpZINTlQE+JSz/NyQ4Q7XA
/a/KU8XRrG3/j8J/JhdLFy4kpGCI3gVhAZmVQs8xlSk88ZEupThZukYiyOzusg1/
YNw8hx8ziRmMJt4UJplxuE5F4OMZXUxmXP5JcYCq+CTebareT3zze8AqAfE2K/1z
```

```
+tbqLdh/GUEhbM4xpBtJLAIvVNDF7s3nYCQGIYGQ3xhggaKhvtc6vNt1WcSnjLzC
miZPScvFP8+SQCEWWQts4vCS5PSwu4iYp3MHhjxMrRRhTGvCTv60f7Wpx0UbX+na
2L/IBCC7ez+9VXMLNx53+NnU4VZqtxuD+CT53ArIxcnmz7n7LnAqfJM5ebKT2ntF
yWOJd2Q3piPzNzDKT5razcpLFLnlwV78KcPx4S5likKV6J4gaTOP2Vu1j8g0ZkJC
2t8zLzA/T3NZs2o6j3x7uMivnLWd68HwMAwxLAVBZwO06SFl11qP/aUCNNy2VLzw
v4OCIReHe417finR+xjn6P24/aknLuBeHJeVUzufpdVkx261hsG/syEIQpMu5zNw
CJqCtaz5jTXJMUKzRDpveY2bgG5AqaDUKWYgWuxBKfAOeizDgmBBRyCyFh5bPUXV
PIK5comNf2f26q1dFQlUYjDFHjdwnzk8Q3f4ZfLn0vP0PBAsfsn3oLJxDS5VHouu
ET88sceoG7yRlgl/wOrAC+8ga+SD8RZMProJKAVvAH9WMpBNxxAFTrGnljvI4f35
2Urb7jA24ioHJde6Z1e1s7tac7cGDYApHxone5RF5sjYy8AohI8ZMGnWLcHHUlxu
Qmzh77CQwUCaga2Y0XmswNDiBe5w8kULfTmezTVesA/SDkbV0RNzSglqgoPZYciB
nmGRaIPL//srzQTtBu4vHbWS3yVffM2rvp54hMD90poMvHEtNP2bQQ1OOq18vu3b
OghUr9jOjdFJ9004icyU/33FGDgdIy5dX/KlYxQqhyH8wRHQRpswJs/f3Nce2dGo
zq27h3BURJkZ/TgKjD51mt29v8YMDWhs5ukkyG3EKT2MEIAivDN1TV7SGEm57Hi3
8tLOvoVV89V2PhpuefKK1TriGMx0upO4zkQpYAThObepzSN+bVx38GFsK8BlYxRx
yYHiSll6JNpI2H83aVAvX6tlywnfMKGajr8uha9OAdUeTvxHXSqVd1ntbykPU/tj
sxIufDXQrTxAYwDro2n/larx/P4Fv9mDV+UxTIvGmHuHm+kB2HK1tyD09TnfpfkR
KjewDsfrn8q7KdTls//G7/cB25RWhVmppyYh4zFVf+H7uNHEbxoPo0ZH100HvaeY
2eqwqSJd716q0bXhRedWuWP/QGfIvSt78xNz5m9QVY4EouMBLV2poRcFbeFKGAg0
nYGxFQ1gzTBKBIDCw0QYe5B30ZP8e3MPsb6K+SdauD5iAlzOfXL1uzLFJ7YVgx2v
hn/QPzKKB2Er7PG4nBxAhlGCYOANaIsrAvEvVhAkwuWqu/fTgyB/LhbtCGvXnIej
yrVfhjfva2iMfXB3QJXKoD9NpLFEf33B4hwQImsA00zzfMpbS16ljztop9wnx25i
Mejl9h7+HjDIa27fql0zUjcy7s3FEqy9vBERgh6rUXjLxrL5KCXUwyGtV2wr70A9
DACxZ9yJNe874KzdnOsjw5S4LCFKxzaTBnwmw8fpo0J4uUIeMymHHqQ0QsR9eICT
Iz+0PSZ2OipAG+O6R9JfxXpdA6Jfz8Q1ZYZI4tDs1qoxQTg/X31VVeWTs9FseCt9
D2CyUknP1vzFJfs4RjWYW4TnrIlTpuOb/njH4N7gTrNhLMwbY0lzN4PDV5/6798/
pPZ6bGkURqmDPo88AI7P+TDX3N34Kpt/N4ygs/2Ua8+9314QqfboLkfGThl1AgpF
0i0bG1Pbea6JiPfXwHf0BBi3RkbZmmHj2YOfkIIVKMihACQVev+whWyVic2FdMeH
Mc1Kwx9d13v/N0pxFWaHt0UrrKDywydxn5Mqxlyom54y46+kKBhFKafJzLuRShI5
YysEZaFKgVAe2E23TsAz0oQ2u12yFuCrW7Xn8MVRTVuYbodGuMpm/8BxduhqU9Rt
IcCMEAMs1UrSp4pYddeDhGrr2ARKQvl+HQXvD2wd1OUXV/0ce+mSy9z4zn78PAc4
kk18SXrl2qGqvdynfuemc2IAPrzByw9Co9vqHn8SHHyvmrbJdHKad36PavoVqv2g
qBwXfxVGNo92jygdtcd5y8k8trouoqViFBdD2Q0BAmn0rC2WFuVtQesXDH/E21ah
s8BHd63gIaqi1HKw0irD+kjGPZveFZrpyEzZmVQnE6ZRTqfb4TbZk14H8qjD4K3R
2yka4XzonQzqnjYqRQCxpJ7UHxtyt1OB1gPcaG+ks4yfjkZHIslWc78NbgpJDgd4
ufHvkYUgobyNOrTcoVRo0c0A7uqf6i2neqbasy+10HwB+uclqpUx/Hv2sb4KPESw
7OjaBOB0uGJCN7KgGNGBXIsTfd2R4/V5XyJyTyEwXKC/oT9lWrurKw9zLwlyIVGJ
u0IyfPMayvWNph7eLqU8wZruQQYCUlyyqTkm43EiomR8WOAlFsq2H3d0yKVmn3Wo
xGOhcy6PykXAEWDUjbrhiEqUy45SpPZyF7nQ2W/xqE+weILSJfhyRon6Ikyvhjt0
rfmnjDjP4ix9DSeHVkR2B6P440mynRXZpCDUCEcOVdcMM/wqp1ZT56gY0AjboboX
gmkVnMncgW5r0raQHjTd31yj9Hg3tH+IsgptlJ8hcO378t8wXdLmvzBB6Be2U0hB
2hqR8bP5jY4ZTaf2aeO0dQler3z7QmPw8/8x/76Wh77dABRJfmbU7iw5yS5LHPjJ
qzmHILZqY8QSbs7dYM8RwHqBRThFwwAlbMSRNp3TloDDt5Q9MOKMPGYbbJya/n8V
eZC0FeEkd3qbfzWMBzPNCodBVI0nBsVRMGZAuW5wP6F+HhO7Cman9CKKtXbmO9ek
cly1HBERmJZh94SGQNkN1aa1vcllfjXAeQ1MUBsYDDKH7N642LHNzEAUpaB9c7T1
cyu8jNM89wPJS5EpqVWX+ny7yTQTo0MK1Py5ZBwHpc0EdJ8EBgDO9yagXhsBdijc
1aw4ZMacQb5AyXymbzEt7MStgWVxdkTTG3nXz4op37GkO337RXzjY72MmvqBmnok
E0JkuTnl7xveeP+WqSeeinqf5OOr3/1QbcdGzfTImGvN8Ey3zIyVyAiKTRhZWXFf
dvCsV9HAv/6tJRuI5Q3EMoCwEjZqZ8ue32DkzWG72aZc/qKM3PT0Ch/YopQf9/V0
zq16jQ3mrbU0T3oQGLYlCl5Na+UEhXF0sirn9adBjeWeVa2TGcwkrL8ZVTuFxlKh
5MAtSFVvuur0n7KmyfDKN0cdvgfqKcLZf32R3N8qNytYYOvX/ACsuyb0yVAPA73g
KFSeviuYAGlGb3bLwLHnv3LpX0OFwM1PVSDIREaX4I1//0GxQ8btIwcZ8btEu/+5
ViUEA+cK24HO+ez5TJxPsVRQ+r8C3suGr9Hb5sYBmNPRj9r4Wclm50CO38liNljn
```

```
T+bbx3QXkiu/E9t3wByEp7j1kW61X1nL28xdXhnG0sAseTeh2fLjaSDAhIIdX8RC
r3Ve1qZipYRruwjek3s+rhl8GYGLea3axwrlDm4ffEGqIBlgT+F9BDSOzuHdAbQu
nAotPOS2jRp5uAV7sOYaxzYfIa5Zp3oFKCzoMeOnLmrbctjaVQLdPnObVqoU/2sw
sJ9tQLu1E05riHb5dvJ52wLbNNcgzBYrduX18aT8UppS0aKFJfoliZC5Km7dGtO4
NrzETXetqRMLBM4aABqoljlgqyYEbwx7D+calkLVgNJzSF1OIOlp0/LM9PZz5G9f
whYPReCbZ+ny6Ohh7IVFF7iGcKeejdZQGbsiVbrhK6w9hBFTT/qpSJ5gf+0y1qc+
2cx4shOh4ET/Cx9gYzGXoOO/lljZdejoo0Orw9ZWXlx625AvrYR/gsGieGxyygos
ssKi11WT6Lvj+0MyKz1ySQX7YTqNP/o83TpdF1Y7Get9McG2HZSy4Vvov2lYqSgk
9wM2HaCBSm7METOvy4H/o+uaVYnyPUldf4yMu0LCxJDQ2O6/lFikHefMPj/52tVq
1NWMj8fzET5X5ZYW9QVs5ewYBORuy39ZUOt2yabIn5+OC3xBN+1wzMcsxQXbv1nc
WiNccvod1JGVBbvUpcu2NCFrm/hcnytbMBEtrAmK1D7GfHJudswWE3t4EzS8zLm2
txmVpPbuKZj6b6t6FYEn9jQEi1eeO/Q99BaYQM/lLFhtWYmwwuB/DdKaRAJfkTXg
akJV1mUrF5OA2jCAoSItJokkKoHoIj4/lxv0CQM6qD7T7yupOK8+VhNSJkg6peNP
ZilnsZcJj1ujYflACbIWnq2roAk6gUmFRw6BsZfTs/BtonwfLwuvpwKyBe0BVbvK
uclXnW8ZM7OmvMAfiy+sEordvZNQsxW9bZJXdoT0yTWsLH51EUdfM6RAtVyuzxqs
p7CaadFuq3j942eq2tQ4+G9GQ21DXZ+ZnSQKXbSR9S1UYT2Op0l/WD5qs6ZNNEP3
uPWgUpVgK8uHtmHIsIg+s/ofPGFeYhHcAoAfjCFfsSKA8qj60BjyzPXctSwrq+/K
yUpBQ4Bl786MkpSAMfRUTBiGC+G67AXpXmkHo/xFivuZT7V2Xzm6sv0BTN30ko+s
le5/koiCURbw3xtJB5/A3h/0fPpyuKpgB5eU/c3nS4urmMzimJE3qMhdI7s4c4ta
95kbVDXlbETHzTGOuS6JoIvfmtTVrDxnVmSkMRFu2jp0fq4MUJn4JPgxTeJQidzH
qTHJygZF69q2eLzPgz290jfZPEd/67g6AHK3QCw3MgUIzex2lhbN+o5PjN/z+BuD
3EDkOU5S3NbDElCZR1IcitW7/7+p+eu5LpMa9/uManVBMrw5YKj3yEdu9DWYF4PG
tuUKi+fjtL0s/BDEcWrrlgZcpss9IY0caVaqR7ZNk+JpUA1vyP3/tMk8PAQ/Ou/i
utPwS+fhneOxgjKUvdJQqZvWCc75niE4XchXLsnuARiP0JzWP3zjvEOZmRJj32iA
ls0dcaHFRbwkGw5ieKwuCj7+CwpH1s49mOm8iEjgInmlCf0Rud9KxIxJ0ZBvvR2R
zawfVWD0ioDy/ULrM1HqPcxxdizwMU1DV6Hw/4SM22KEXqPiYU2ls/xgYv3FUNwi
Bduv4NZ51XXrz9apU1cEBtU1qzaCAE6uSt+4xx3BHMNsViv+X+XSs9/mYS2H9BKz
giqt4BIly84OgbFbSvUH8f2GBEnuv2SCBdVzqSGEVEfpF1/6zbhJ8teqBa6yjmLm
k9XldJZeB3VHBd6XBJZHsvXzuEG0RIjFCqu/QBiycr8fz8fyXRnwG66rGAmN7FNB
uNcArOEJ5VE21kdnocTtdSDN2nd3ew4pMKiTB6m6z413VBG/IJDPqD9npZCacXRp
OO8T2td97a9oRPN7WZ+hQlbhMQJdqibmTwzJ4woFoyzf1ULvgCMc+aMV5289evyk
zzGdAbSUkTVL8P2FrlmkoS0/btsZaMyWYfdDHW6Y8aGtz6A/bTbSA9uWMCtgSaNT
mIO9b8LxfHF0VmgXSPutAkg5fJsqso1ie6SyTWP6Yvy3plbQXpSQAry+0V9j1yDp
he1bHMkSbbUSCnJKmhWHQwVmaGw4OJ4UER2kF7E9FHlS3tB3mGdqZTRpOrEsz34d
jMrfGg1LmEAsWbfq5xtU23G/aTDObJJRY/ZuNGCkVyEraorJTPIy1mRPpAB1uxdC
Jxgg0b+P2XYvqYOyaDsoJodakHpWbsqeENMshLEr3alCLUVKgPGLeguQkuWYScrU
8N69R3rfr784ImT3Zcqxy3+8TJ/zs9s7GYccChXcu+yORdxcRghbnxBYnJcEOZso
K+5VqQlz6NKnSxpNxR9U92WJHwhfDE2XtqIyrFEuBkCiuhnuxe/9AvE4xUUREuDB
L06PtWuXDbp7SR32GL/jvt5vIktFJLYyAQdxT/P4aLAszfDuoRQ4Z6k7jMXIhAtK
nyd8kfkbeKHt8qeanGa9nuntblygGDVlTiwHMbVm9Bjl87M12rE+QZLo34tlv00l
r/GIn1WPPs3m5l/vliWtyeHRbH9fesWOb7jKq/xzQgAJS+xBp8CTD7jqHHM7Ic0S
fB4qDEReHYjL1SzGBRitBxjNG99ZLQTIxS19UHqU63FlJfTWFM6BzzrSvM9HY+JM
iIQX0+UV16N2SW7VkcJ5MjxH51TDIGUIcpTT0Wcq/FbXh4WvBYVdQnoP89H+pnIj
tJgA55FPV9wQLWI4wCOQ1wAR7SiV5wkcwk+3SUMxyN0D8R5aL2p9AboKxTUUInuP
M6wyIKthDpYi82oCdSpzl+YlgyOH6k4ml11bly+Z/4iy4Vf69MufyP+HrXDtala5
oS5hfkhMD0+FBJzC4/YOXS7rjFx2xKn3aArOcD8YJsrkzc3+yKNbbWIce9zSbTam
XVQb4LvVcxHIFOvybbHwfH6FtcPnyqlTqd042yeZDEiAjvJCPS+dJIjF9eE5sOO+
VWGQ8mjNJCP3rfwUUHFzdfqJ/F3m/CB1xruUIUke21ifGM1cio35x6Ggs6S8W3t+
EHat3i7ZVT9v3MP3D/uI0yhx5bqq5Nsjf8k77MOK1Vgb1VA9EiglVZQsSrtcLOk+
Lz6cYMVYlmJ3E14v9z6VmTE0X60S2HVQ/lQJ11g7Q4tv6zdUI3siqwWZ0DPGT+MW
19LoU2frSN0J05THwdGv0CLSjCaMxnHVOZVj/FHmjPQ9tJuzo4mTDUSElqKMyIEW
H40cyrLyfAG1JM+Vd7RBklFIrVCGuD537+EPw0ztIOitFCoY9H15fWmcMHVwvBdS
ax2KGrTTUlflBFwnP9QUpEbAvbDzxFhq40AtfU+ztAW5aSi/4/qwD/6fwSTf7f37
```

```
7+49vNh2G5QHMbClqmT/ueIpgxs5vaEtpcbjASirhDqE9GVReoBh4HWk+0lcHulz
uHxGhkFIfEB8XxIpYC//tf7+jRfWRZr6hrHe/sTB6LVrjXCRmfSX1My1veNWqlbR
LXlF55oLqlYGevDwBWMTVql8y2XC4KIa5sUmqBQhraI8jVzkFRq7f7T1vJvhwNbN
U+t6O+JA+H1recqh+nmkqOc+FGQHAjiwg/w2OolxlFHR/7gusb2MFpDeUz+Tmegw
R1iObwxYyHNDCLhWU3b5Rk9/AHbwnxvdVZgec2owo9ATSJsyyRmRv7/HwQInwQ34
ViEl6kahs0dz1yLCc+7ZAWCow3sia+oaM+1r3kzqOf201qML2vqieUFxswkeP1Os
w4nUTZ0JpU66GsXaKQA94T+MxCZeiv7kltRFZT+eaLQlW8LyTNR9gPO6UjSb+teT
NEiciblMg4qYOam3W+Z21A0z2kwzfiRlPY6Rla5EP5eEdd9gX+Uvzg1TtPutpa0i
6rqarQzYtv8jNs61vvKbCdcQs4YXcYD+DEfNI+gyJI+B7ep6b74Vx2btmBHi7hCq
3IOW5YxtalFkqOI7s7Oo/b+HoZHp4FfaVZQsCgYaCPyR4YwNQju6WC4sbADnWjUH
q5KxvhMsj7Y3REV2LNQjBEr/0P2oF7pOLHc67hJeXGr8qPAsKZUzCVf7xUFKUukd
U4mHSiAl6aIz+7up6qX3P4jlJDYx4PogZwF34BqH32OF9yqbWUwwLaGzxGMIocLY
u1sljE75C9pvDKmh6nkatfrLzXWfDjGYYx8+YDMgveOZf58HNwgl4T7fxdMM77dq
6r7KsrQAZPelQSYiv6A3A/ipAehJlwjJPT08I26x/KXY4y8jOXN3mvB1hXt6g4ls
dGQX0RWS9qGiijwavaxvYF7UFRTpEKobqjU1ocUSGnFZw+j4z7EWQLLoe0dGzLE5
INZ93uzTjzOqLRleg+APSnifgWX42KVETep9FoW6La214az/qY+mN0hK9jbITrJR
frtdxSAq7EMXeamaF/AuNuY4M19innNVbfnKKqvfHZoefeK8tFbhmRA1iVsLW46K
//4E5svpOks6OzSEHWKdSIG8RGZlvwW7U8hVT52BkfWQ85/V5heWXTkZE7hmVry+
uPk15mXLT4i0mLLR190r2SFWskBf5tVG4G4f5yenChKUE2ZM0gPRp0nkO5YyoYkK
34erdiv45ktYVNUPj5p47bnibZYRyW0CXW1p1a4rxQ7JV6sT7n7tVtE91RFG8gDP
R4AxqtGTGTARTef9wdOVVZ+3C6tABN/xoQOwWByPLPv5MlCT4ELXpoyQVpP2Q6vW
qfvY6N5WeJVBBkJRqiacquTwc57pl3Llr5PfPIX+HtF40W0Etxu4lODZyTM0pJuj
65pKO4cfPBQ6tKvfErr+edMk7x80+dQo9UFBgikaiJE0+A27OWNZonPqnvWeQtAt
z20An8BuWFBZbbaKmy2arYVqfuV4BS+jwHHG9bf8xbUO1YFr6lYbCDHwP6hz3g5e
M+vMZ+fet/BkIjXkcMZZfeqMKMkN66+cM/pDJB2NkfXTFZrbpuR+mn7+5+UK1MrI
t35I+pJMdU+NDjGZbBDRoN2wOb2HtB+yhCu1rgRBEX40aNVpwYYtyhucw1PtrJxP
pJiYyPcV/1miKHMdlBAZZ9qawG1Uc+6P3faTDkP1o/rexvQHb4hPGZD84rtREGqu
74rkzlkkU6qhZw8BYKaBWaX/GqFF4oR7tIdliwNz3RcVhvgiIZ2smQMryF1xjHPr
PcngdBc2lu8eWPraU8sPSd0AmQCG/Vm+0cFvBje4aeH+JcOUY/ZJaDuMkyC3b03Z
nlEfckilOb++zfd3OMVlfe2yAufVcIcoHAMtjrY9AUwTpp2WkZOpF6KSY4Jben3K
05Tmiy8Z36tNqGW/wSKD+19yOhXFT9ZbmbGXAi2UMB/DaMeBsI/5aXUuLprl9oBx
7jOFIMvkIFAm055bJcNG2UVRlbQbJqk4jvyZg0gMlJFDCMYh3Pu4jDvGaRnqd1u9
aN0O5r3WIJ0vUkAC+SexvRSCiK9YUUR4LgCDNAc9b1ng3+Axp6gkFVhvMfRgN3TG
csnsXeDDVJI61/+JhlNBa3GWvYtJsHzdIdZ9H5EoitV4pvmuTdfd9xaWfmar1Ltt
xthwoptMHPqhfgpYHARLGedtTntRfjTqHx9F3P1e52xNNp8XUr7nqJa7wQb2ovAS
1VuzfsNa/17OSAXjx72Pk2meiBw9icASwdIzkc0g8GOgsNwIncGkkoUxQqULrmDp
q11fEGYGcUP2bnhjblKNXWEuVxO34UVBrbIWXFMhmnS1cZSLAJSPhGaouB+mB4gz
fs1D9aVltueCJhtIlD48avL71HnKqSiqKForftqBBjAmnlEVptI7t10yXSrUWhsG
+1gy0W0rBZcIqvU2x0/k/4STXoYao/IrW/P4IB20EDi4yo0tIhL3BswPFwX0M3Y/
SXR5FSauKqr7T2cr6t3CkWNPlaZgHxfox3VTNqCLECWJpGevJjG9mEq9DGxQIozN
TGNLwCISX8m3HpLfwxN7j4VeswtJtrDNu/MdhC3oyvOwpdaiOqn8fGF3luEK7YQK
4N9aWT4//M9ruP/aAQv2K6vxtJex0betyK2WuNmTKkyIIM0Mlbcaw3YJ2eyfIceS
LWjsrCx78q70AUcK0f9dhDI9n9kuepkq/igk8sSwijruKJPXXc6ZwbhFdjT/XcBN
Gns5S0EJlmjqI7+UjdqAyRwM+j/K/MtR+xMkDPrmEnq/lTIde/sYrzCLHiv8BD8r
V5IIPUrkgoAxv6Iix98ehUHGdx+JsbZg8eIctpVoQ2CO8oM7ipXOxgpxKz8eKKTL
JApyMMWYp4VZA7WWW4HTQP14IGw/21uwOWKcnQtEhIqjCay+7igAFDagLttCLI8K
V1g56cPB9mbrnMBpN2jvO6HPVw6LgeGh/vHebTAOIGeq+znjKT34FSKBO/Ukz3BA
WefOw0/7VOGiP1nFrDJIbBxA0ssyefpXtsz6BurT+asPGu+V9QI8TVCskB3MZph/
QElQuKph34L6w1tDvztO8iNNQv6F2N8HkRx1Sa/z4mficvD8ylpaPQcqoIKmJyi5
NOII3DAU/OAJCb3Qs3HOADBN4UOKFuY8pMM1elMaILglJ34a0+GvHNs9IF/U1hTY
3OpFTb7+s/d+lm52vj5LMkaST/x1BTy2o5/LenDNbNWpT4TjLDIeSterRPhf8Tjt
vm1lyP2Sxo9nRZXo3I6hZohYsAh5+iXbogxxOGd2BG916z9KdEHrCfrzqN15/fKs
Z/wSTqIy4l2JgkSUzh7h4J4tEuBpDWqew2ew55C/fJ5QUzIwyCRxc1h1OTJIr83V
```

```
EGFdb+rUCsB42MXnDn6LhCsJk4rjWZt8hwQ3z1UqctJTSkNohzxgdzUqyV/y2bAv
93rC+AIi12N6cINVzeJW13Ce5jgEki+MnlXtoMOihdq/hL/DMWw4FSwAibFA/Dt+
BOxm4eKpS3yxSd2IZ/EeTBJAqaUZCn68UQFb6Q5uZDD+74A/ocIAk3wxi1B6W3i8
K2O+ThY9m1/5SiA672/Xnp99HV9jnV3ZMZuGyYPraS/NrwGYLBKYU+LZwHQrJ1iC
oaX8btDSp+lVTIv6q2iM3uOZFRqYl2WVKLqz/0hLGy/sMxVpRZkNy95E/9d74YjL
2RotfE5ZjgXt+x3UdtgzsoADfvS9GyMMQOPgyo5IhdFHHq/5xwJrhvaibdtaowmQ
oTCsam6xAj1t/KiNnDlf7Lw9r/75XJG0ZftrRvm6gk1JlzT3KsZl4WwbN04JN2+6
hOHnbcK5Ko8hxim5wNNkxRObbPGU1E1eAysTjZCT7EI5DhUyb7Q62LWQPd09x2Xa
U8AlNRULcHphavUyD7l4jfs1Lawphf6CaAXbI3AmlqvV0weWNE5NMP2U7SDHP8jW
SycehxczgkrhG/V7/imQU3e7ZJresKp+U/5J5EF39BEg/4/lYOResAzdXqNyYu/j
EO1trlz+VQXD7pVSiwM1EaGCESvddoa0qHbtKWrE60EefMjKSzm8OG9d9WWuAip+
UnrkJNxYLBWP4Zj351Nwujmc0JVGrm5PhK3D+w0RDq0yG+fvUmYK6/n5Eyqjq9V+
t7koJBVeedXbMLGgGBEWYfCjREHiC1tHx7QYesqlSF866ZTL0KlOsw9+gLKuYEsw
F1j+vZDGN43gcufwW4YZI+jbwkHRxcQ9aaPn0mTO+R1Wn1G2mQTy4zGBJCtb69Xu
O208w2A1WW5R7GQ8AYRbnR2ZyPzMyXNjyNwZjoGYWF0GNVDOQRuHOIyORSAh8LFz
s63qI0lkyoXfX+NBYeYLXpyTSZH4E88TbYQG+bl9WW18+eTvIBGbuCkdijMg3kDp
GkDL33grYofvdixrsgXvovjGYMuBZbERqbTguTgqftR+p53XqimK6LWrDEMe+D1g
93ptLN1pX61fvhC6r2efENHeSviNHM2u9Cay5eGXE3NPEjZ+3L1HH6gPmHtFBKQT
KlCBIQuSWsrWT9ClD9Ggl9CRyURyZ6t4wCaSBmK9lkGBtODmCVVgBblijs6JxVRV
/jkvcV/Gi7wDJcWnBZNVpArAXd9xlmbkYLqlxlHf9LNheJokqACBfdEvRkiQhPCR
7myDs2Q2mlJKwOhuV//n6aObVCR9GWEqg2HN5Cvfrii4EkSudcI5Xl1TntWuLnzO
PA7za4rqFSeVGI2I5mOLDXifIAZd7AlCg+WReFlJGNG/GBZBQuOTP+cVtA798aR6
4kLE+gaCNbR/sSO1+RGtaBAds4irl0xRZtGsdJR8D3d5/f926pKRq/RJ4ONF4J+m
zBcURd2iYstXutz9yPkkOifvIvMg0SxZCia2BI85CPiFWt2bb5ezQveIxjIaoqcd
vDUzrVMDT6ewgVKG0EaxjkAmpfZgKx0gXFwHTdV2e9ZKfmWwm1azG0KL89EXDLt1
l2u/td7uHff+pltVZ2MtOlKKex/jbNVJbBMHWZt7TdNjm51ZtUyV/5qvfXC9RajF
jFX9hg1euA93SgeXL3MthhB8GlFIsx66OB/6VgTU7FRuXFEQwPrwz/ya3en+k9AF
fOpyGDkA/gLGwJZUJIcz4ATypVXs4/W2QNpkgLoOzd8ddKogomA516z2SKihp27E
rOhV2jeJofFenSNGTKezQEub0TeIaXjQn6d1gyqrDcr5eZM+9iwag+EIUNRHv5wm
bzcdMMAZpcx3lKJsLnJmS0arDFwI6GDcvN0hJ3Um3dz//tc+7y7ZGi2DHt04fEna
DvlbFtiUNFOWKKNxky9McmnX+9SxLnsbpCIIRIWNeCVkrT+VRvN43ipB9tFzjHa/
0o/7x0j1oiYnBoNCmnNNrhg1IzNA/u12o3zpm40PEEY5VB/FOvDqSjyMbvbWDvKy
65hX2grB03VGYcq41903rC0W0uuoTADz1F7tSWHF/YTCkT8ABcTpH9AzKwssE52n
OQAQ9581RFlGYNSPFVsbx6K/2uV8XNPwTwbknu+0Ddm3YXhl72irA9woXaWvhPzC
+kYBrkVkTHROhpJVBNz6Lr/W4Hhv9QMBtddkRult6TnBHsojV5QKKDXi8WcyGBtn
t7pz2FSJxFXdAi7+WeUOMsIJIA/DXlZ+u3VRuBOhhJ8GniEqW8YgZkz7m97+1XdE
bSsvCjfIWPYf17YX4KEsrrdnWrtuCvurad2YJfIovkLLpQTcghL/EsYDHTqVyHN3
sc0orojQ0qyCq1Razlih493bJIlZKa8sckyt15l7ElvRvhmASxvnGfMr0tmY6qHX
QL/uEbFiRf79m3JJvJBLi1dLj8tPHIWNdKsaluqK9eiYTlnPS7pP/3qFVric2FXz
+v5W/Tc+rg4N7ZXYBc5EAnbKFZoxEWhLJw1j8QSJA1zsn4hIl1poy5zy9ZAxWnbq
dpdXDRay6PTZQZiOaa+3Vt15rEWxOkjrMLZZwBnVaIxTm/mAG5/SssA2N4h1GEl1
emm4m9tDNyv+PRXONEYVT/vITjTlkhMO4z9pg5VOlWumzNYS6hGposIMUOuTj8lX
q+TIrzCZJIDSV0aA1yYePU6xI4uq91dawQusd5b/vky+TIVg3uHiZU+t4HFus+dH
PxC28BGyIYZNrGgb+h8cyBAYTu1f6ejpOJ1StoC/C+23JhtrqYZunKvr8d/mjh0j
eUbjJibfNzPwt397HApiOnUKt3Sz7ArfDmvogcTHOJ9W7Z3a86wSIOuCz9m03gXK
rlKvYuYsGcT4CRKyxpUrNQHWfhygl+4b5KrxevC2PtSX+2dJdzx0lCI5IzBJum0S
z2+KBPNE7S+FV770IAGN0Z/d6Dj0NCi6uE+pcro07eGSH/yJqhsnn0EcwZaOUWYj
15uYaPItL2WLF6AD2ABaPcI5VhXul/sTSf8RUHpZNl7EMqvVZYg2GFUDem329Ju9
4rWtqcMweM6jOvL3g88vRpkFNjHSiaHYze87gdi5PgEpfLoewEVIQKgysQs6HejI
lE5mWHUNTa/EdVh3AK3ooLIadwpHeqrMhBB30+uf8SkgQEdlI1EMeKSMXqs4xvEl
YfFnH3KKuTiuLJGaaJ3pIHne3+NViytJvrLXzRatQl6jCdjq3CyyDmqpe8GyJoM4
X1U0hL9WWEfycBUdtiysn+E3bSKqd+VnpLzbDoWvgU20HY1CUoi3SSH0OAnuVFF6
dzTh8wF8ja8mGd+8u2wlmgic990djP3jGR9qcww/04v9Xf89z9sm2+yi09YvQdxE
```

```
ydVDCdjWXD1F0q5J9ghSiCm8ZjGEV4h+ntL5diRWAD5C/IKoepL9LFIgvzJvNhiO
xOEOpnm0UHfU+0o2xGXaND1kwCwNN5PFkkm/LawkNI3m70UCPkQcRYyL2LBGcgMB
dKC/oYhhw1U8oueRiXFSbIJ7Z25bCIJfa4CSe3DasGdiscqQex9IzEmhMTRwqIeD
PtA1dElX61GyTNI1dl8olWdnZshdg2HaM8sYWEgthF0rb+9ILH3UetHOXTAmYLHr
6m+gdJ0efrNifbj8F8xvOFMoJz/eqUqywkYRM8IyPRClkRszvrHxS/cXiXVdal16
M/vIPsrWOipoCyvVKS7iijPFsloZv6EGyBqMziJCA5jMDrIk6zsHjOQ1VK1jG+2C
kViV874CncpFG12yHXsZKTgbDA4+YEkrur3zBzqH8GMrjALse/dEHibplZYMBZgq
8iuxvmCkxInkwEoJzUI+Ixvzyx6/u5uwekdu0ECMdiVCy29TcV6UPSoMf3zzp32a
u/3LRMGu2lo/yUDvxFnwlcS41V8if9+zJCTm1baP0xH5IQdA2qs8h+U5WkWWAmJx
7lP13IGtA2SDboRWqjrsq9Nq4uEtK6V0dnvcJoZC9dNTe8Bp4dYB+k4zlTTm2G6/
XzeGO98+EO0yoYafkopSMmmqOzroFiMGZVLyBO6dR6z2TCVZkTUxI+VPgmFr1BXu
4LmXPSMH2FK8G/ufsYqdcgsSNrKZrDXAQA+sXjmK83qtnroDufRiN339FQUa7zxS
nxG4YKAWnCseSp1uX7FVgplHgRgT3nyPupMqOSMfnsyaJDBLNWXf54VUJxOGVWsE
DE4vTQhB4wedMbQftgIwnLRGNAl0DezouztH80wYwREOfy80jgtSCasd7ehcXfIM
S8Dc/v67HpZry4u87GU3/X7JgyEmLlxMdVIUXjZXp3rQqrAN211NwZkOUkdKM/YE
Zd6A8qYTutdhmPqmUSsucwAGa4ZPK6UoLHJyHGaW8JWsPjPMAF06HzEHUbob4/yn
saNTt6xeQ/2rDprcHJIAM9CcLklp6C/mSYBby9AjWGYJ85DgmpYq1SSkrD+sY/pS
hiVEzLH2VIKH5k7T0rzyjHn1sGn8BkL5kq259Dz4IHeXl1TJnYatCiV4oyo1zgeD
UlUMX9fSJ+LzIQswkIHBKLDIPU4ePhp+XmuXZKkrleVmqxOC/YC5tuvEbIwdleh9
UAJCfrUuSgEhs59v2Gns8NrNHAgYjNmV6WDfdJSzETdD4qfgQ7fXOTzkO5N0me/H
xNzB7OWPqUf1ll4fZPNTnOvSTKffUTRFlaAuj/4kBoBXF3U4KZtmigc9+2JcMNBD
UYqNZ1i3omEgpdBgZg+F9wmxTA7as4a95j2/tnSUf49PjSpGoPRQU7T2WPFNAHr3
96wCYvUbhS5QAHAkqO9XXK87oyWFawpeR/cqswe6Jli8nvOdAj695XUj9t0AqmRe
AjoTniTBCS1CbYgXUNhRJZMrtLSJbKWz19V0v83UNKmJm9sIH1DyDp/Nj+rHJSF8
NZw8WyGq9GM+XGTWtbR9TBxcMl69OsFT5kfqaxYv+d9VW/M6tqng3KXBbWwmgOym
ZRPINP6UYtr8lvWN/CMo5ULAhDOjA6pJ0Jzcmc7uK0SZom4wxz8TsGAbrNtXH4tM
c5WmoDWbwk37dsqjepBrZdTUvlT7OXCPrgGe4jUqTSul5x5KltQnB8zf+BlK3Ex6
cO8rV0sG+v/fBs4YV8CGMo86OVDZzhS2Or4tTQ/efb0wuv2q+uOVtFHGEEgNqHCv
28JyqK55jS2t+9DNXS2ylmvioEpXDVn+jMKuAjfEV9QPPJ8Y7FLbK08Juf/0X8zW
NHOom3WyjGikbsocak2CvMiRJL6MPRUEX9vrNC+Nmy01deb/BNg49G401hBG3iUY
a+Y8b4fxCmJvJAL/PffKA8DTQG5anSOs6xBWGGs34G51lp1L5mPjww0XoR8viJHi
XhF0rGskkYJiqw79QkILbewvf+N8sVqyt4N8GCaeTeU+fpk9VzBVrE1vi6PMoar6
dMWrZUMIsPu1DbyPwzUjimmcOntvHp2fGuWxDm2aZrGfXqc7ulA/RBIU5tmYa/kt
Vsz6sZMIdjkiB5rLhA83UDNrU/Olk84mW/gMi6SjT9ji9y+SDqB9t0f2uEDQipsH
8nYsjVeS4kPZW4pIDZ0+mP2Q9R1aP587KXh0m5nALVlzUDoAKnwtdbhFII8LVcbB
3MH9K3Ct6oJEBo4QXeEk0raFQQUpYjD+pB2Ms/xtUMolC+/S8zPFetqhTTXpsmwu
1RB0D4Sjw/e/w/b5DECklxPjz4fRwwORvc90RcN0rG4wwMbQStV7QJR2lDTSidO7
i8jOmgA+c5N+6yULc8qf4KVdlOCqml27u/tTZSYuEeWWL0r6iZMA3kte07G5wfSf
naImpEPv5EyVUGAuCIiolaE3Z4QOOegQy+QFKQEXg1fRDzVwLRqie/UsbFymaAsH
y23QpeKFDWVbdDwwsOrPnhvtKG3B0ESXjQ7lS/oS4Bp2ztsF5bOK6PZFbOdgU8CO
qF71ocpZeR1dekwCHu1OXxndNQipLwUWnjQgUfjQxUmLCVSSljE9lv1s1riI/UHD
zqfcUSPf7Wn3Z+SIqSDehR7euHJOSSujdjsrBM7uI2fsRhZxhQU6EV9R0np6zR/d
tAOog8zrjWpt//CeXE36Z3wBtFeKtfGuY/COJ00HL+67+MHhWitaZu9LIiFzfW86
bmJbt6/fa+pdX5hP0OVqAX1wbvbEltyNV8zmPeVz4V9ykL7mhfih0N9t4YCtivMB
1UsSMkj6ZJpg/bEvAIW3fd3qyUXgsWloCtUL0DsJajSZCbjFUCPMKwxOj4ftlc2J
bAQPL01Dy2OvrmKWGucHIr4yEFJLhR7ii+3ZvrKcAreLKfQOpbnL4fzr4ZInVios
KhKIUt4sjV7r7m3kkpGOt2hhgQvX4I/E8tcgu4XnoTfgXRexQWuVTmqpSIca87wW
JVdNenX0qUpb/z4oE71MBkVOKsV5iIS70lDS1/I69CRlAXSsvkF3nTlAlbIe0vhg
+fGeAIuncdg9gaDLwrZBhsOGbZPjI9P2ChB7qng74CWvw598rydaJglSARR9SEIR
vJQyTCrj29IpWVeSeew2qGQ9xV/KLSMZGeR42zFS4Ezi+YEwDTDknyHe+P/lvxzj
QOt0YJek0ojc0ZCK/kDsHC5VG1DhJK8FIEqLq2zz0JGwiJWEKRixyxsBka+/soAL
fjNAcfUQoWgCl/cHoNrIu17x02UKjPNv/KvfNgCOp3qFWDgUHUoiaXbojXwd9IgN
CKzYPMnjqFoOzD08b2urpyu7dybgmvzk3PuSlKNPUucV7/7nJovZw9xLCcPIDDmR
```

```
BBLvUF/tPf7me0sLWzT01uSnp2FALFvnimO9c/O75imHxX8b7uLUtIJcraX8ay8n
1wT7PypT4nYsL2GuMsGCz/xew9ZbZ7GuhtfBkyftHBGGjf9+UMoB6Ep8G/WbVFfn
L0v71oHkTq8XxetePSjIdC6m4LBwwShPIU6kj0qYzPBMZvUz48wbhWLHZGbvbqlL
RdHIwTJRykToc3JxXn+6P5KhyMK3oSJfy0S1qmC0eyhQ24oXE2p4OzCmLiz6RktW
mLPlTpTDksYjgQrQ9LgpCPsV+W6G3LzCIEqjGXAKSJZT/M2wR/KVZz0Y3NUPIudz
6BnaSKu5Rbs1lI8WT1j5QzEVass+YGBpBp35cQ0fbSbNwrnTC3OVNkwtSKVIqE8p
uLbyh3ZaT2ZGAYPMKECYkC7QMplSMI/1PB+/fv96pDZRJIzTWdFONi8JLHP1AoTl
xCzOCxtYUDzKj2GwZRuClZT2SAOM95EpceZJeo8/vmUSHCFSdV4nRJmXc30Hy1nn
rAVM/2tqftkfcE8GqpL6aUsvXUawF4Ncwe3B4crzVWmfR8hdjeFqKhpScSvAnUR4
N2D8G3d+G7UcmzuPVQIzkN9v/9d+qjAzoZIBBkvQmG2Xbx2obGUkR8onxMGPGIhq
8sq8h01ta3Q6yCZvt9JL8w4dMdpDupBlhaEbkVeQm7t8l6m8lViCunyov5faDBiG
G4mgvWwL6fFIRqANzZODMiOCvoavFY0sKgQlE29qFRE0DVC4+ZmTVXLCP3AKB91e
D2vnlkqI3OkuXzSGwp2sAJFelYDnnq+gbOt1kQW43sB8kHhH8K+EHDcWaThVaBGd
tHd0G/n3Ib0z4+ufBXC6pVFbw6/lypGTpmBxJk9c3QrDdyaVxJDpDc4jQVRUkt2h
pMjJEA6rxhPZ0DKY1RQYNw6AP2Cta3pIZP0Z9hXOpM3wVYrrkc686krYkP90E6ad
6+zrkgKxIlj//pOdFvJwBkp/gX4GPq0ACkGxhUDwX0DEZNnQKavTFsIL9TMmwq5t
LBDT6FJNWqOrzT93pXg0s5SahcG9gjg9R0udq+J7uztmQVftOUohN+CTTzvmcFBI
0YbwPB01QrBCWcHshpY0T0fmH3+TmtRO2qm+BL4ydjiJarzI/wwkue1f902xnqZy
r2IGfzZ+kwY8b3gZgRYod6AI3f5vxKE1z2pYthSWQyVOAQQ8RkK72rDxXsSuwx3M
FCY7wDwkE3D8dUPWDUvZlre7fpuI+sKiVC7f3fd88v0ldsPkxztlOkUmvEwImEHn
EpU3flDxcYxWIgyQYzYRZiY9goL6ujQhc6tjLvnDnQw/xIi3LIfBiBSFjj7Lea/I
Whq0gzuyzwXdZS8/akZzPQhdHq79aCM2onXFK6K9aMjYhSoBCAq9gGQpfU3yq417
cuqx7IMRKSJuNpw4L+0H4bbt7ZKkp7nYMNPE3ah07KnCnSu185PlK5+FONITTFXV
LMPy3gostDe1cv/OceBP/101SeBrfOPokTcQaaCFddZuM0Qdfj7OVIt0eAU09yye
/xdJzWKhjovMrp2QgMEkWGNl5ItdmP5a5P+BDZYyrGv8yGlqTaV/FkiS66QF8bVU
zLAwed0Fzvyw9Zq9eVsEjQOOCko16YTAVS3VzavCriP2BYAOni5wtpQQ701xSlLb
D0opKo/auXH9RyWiXkZOkvYTvpqmFLUdzFqrqUJOVu55hlfQwH6fT3fve2k9PYzk
sDg55VFUUQ7LVIJ/DE3hDD4KJEs6gr45gf+U//kIxujxWtCgwBn/qBW99WjuJMKV
jUhK9OuOBxZDSV3pFRf2drvSnuZ3RZbm/nIJ+R9mC5HhjXE2e20IjTlIdbUcrSn9
qd/3LRRuI7ymhOmHaHxCgB2KGqRxyjz5zOk5mMizWe+PpknabIyQ6fHHLUEY+Qa+
OILaJEZvONd2ilbeYAM6oY0SD6Rg7py/NeSn4/ua3UpEDh7fj7jKRy9nFMV0vy6W
b9bcBIp91xKITjpmbxYhmrZqhMyvaUQ1/wbrre4YD/YVx4/EsV3LNnVvcD3kHedZ
vBbLevKhGJYxRacbSYAuD2kQyguMF1azMR5o3dvWNdz1LHe/JTNANCc9P9qSRIrN
XrOq2yVortMFf1YzGtXg2ICw5/pusoN4QnGuMOOPF/tbEXadmlL9CzqHmHR7gaJc
t14jLyj0c90Q1OpBfu7dI5WLXTx0AyLZjvbDhdoOiFVF9KKwztYkr30CZDRx0qj2
AUz4y6NgxRhCf0LFY3gnWkOHKhrLz7IybWEnppm2b8j5tJiaCMazNVFdPl6k7jG/
BUoP3bVB0foN33/B/v4TdeHK0cuaYudd3sCWnE18NVNaVHk4HGLeK2KhtASI5mh0
0DlrTa4WhD31idGqk1LJkFU7wGgKf+3toB6MmOuA6Sw+wD4BYuX40E1xrWnTATNw
8WAVAjSSN9pTlmyrxC6lqyep4MGcGb/vKJvqKurJF4wVLBrp/42qYv2IAqfipsqG
MlA8ddOudFYQFYb0Nds/WHeKZ/4ICFLH2hGPPtzJIU3N9j5yYpV4jAceGzC9/xVj
jx3hT8mVxnxF8ISCZwGS1ODVMHc1fzN+iipWJNzvBtZgqOjRxs2a1dTVRFYd4T1Q
NjtwBKZfjVotqVOLEYSRQ8grFYhcNpOhqp3d5P4ExjJLYQFe7zBfA4xbWdgbzyiU
cK8RRV9v9NT4KbUVsk7MNqBkcy1Sd64cq7peSRTb7w353XvSBeKl7LTalCHk/fhq
DPvWb+/c/gVFtIKBYYIzmeCuI9wh2xkLA64PJHQXPY0QpfMw8WtZkdEjGeKOmbtd
jVoxhsRybOBWc9yVu+Uqy+bHpjwuya/HHcweqnUsiMmh0Qe7MEbbFbsTZNQDXsNL
WLQFXsNE0+ONRolwRQprM/dZcjIO0Fa1atoA92TCjYMiBQqN7vp8D/7t35QYuicc
vMc/pPK5k0WMdtRdf3w+3AHsng3LbICynDMqGsdbM8HXOP6xYj5NmdrGKlX6L7h+
cAw0NVmPhcv3CVHHxYRXtzuyd6ThQdr4mwCXxYglxBMJCH/Xip0wgC76itcrXRPa
0PKPxc4Ci4WFa2STuqWgyqZIWgPOYowRRPIyntFE2jGLcK5j+fW4YMQ0jPJLTB6S
YPuk9Fy+EtssZwe2byBya1zZ8xVu4XUcHSRh5plkb/t++djrcX7/4uAlKI+8lGJp
/hWnAayiex/i0p8ay52dd+RhaQ8QBo4ES8Do3b6H9bzp+27JLR8JQNlFk4EMMu7X
odCXAfN/7iDPvAS/u0dqkK54bg9DRmK14bTsNVjp238hbUohy6wPdXSguR+f5wXr
VyJ2QOE1Uj5Pr7l9HiddaoBBZ5GH8OK4YV1ajprb0XtU0VbAoYaqv3aPlpVWoAnN
```

```
Zni1slrQ5oo1Lfn0CId5P/+hz/d1PWoTbu4p3GvZir3TcNkn4zuWCDut45VQV+zM
m67fLnnRtNfa/YEWosCVEbZFo6A4lABPWV4ESfrUQoJMyBPyy4gDnRBETZF917bl
JevRnhSnn1QMjDrMaDs+02D6ZcCzrNpk2nGYwV2BX/skN3BrBe4za0KD4RSDvox9
C0cuuLhw9jmz6FN6eFVdVR9bqcAXWECuk3QangD/36CD3adCNDI5ZsTmN7w+FYl2
0eeEgXQ0iqSzlq474W5zGVYUP/mFGJAXq5oqoWRzKXFW2Uo5LdQxaoGQ5VXMVvlb
O6xHWyUGqyQQyiqn7ZO2S5bkbP8FFI1M4PPxqa2o/uLBSgsY6CzBeOYlJx3vw3CG
KAjO6VtNr4EB0pkgQa0h76rwbWPizoaEtxR18GiNFCzuskuJFFtixbkHOlNbpmmp
UiEFws0h98N1qGoRCr52IVxN1iheZR7BT1YIgUl1gjeaHZHtQPMU6pGpeKirhzIk
5USGvKszszqZNfXHi/3gOX6qqIfpPPRBIaXaYawQI5q62/lhuPkYCubhTShKRxHw
kcbJDPvdOKND2KTe9F9yto3aWLCN515XYwQHgYQHu4TO9x6npww3FKKjptD6nP6P
pAJ1z+QUHY7MlDd/+HnhGm2ZG2yYoPTA/zJg4+/TunESDveMcGs5Pp7cJ71f+ldL
rEZKDYys+gRn1Bgs8G+oC5gNy/fFy0ZtKsl+trwOV1fe0WShBBNn31GJxcO+9gxd
CroBEoB/QKc7cmUNZukYhP73nRw/Ndm4uX7iuQ4YZ0hPnt8QAQuQ1VzsqLk3bYY9
4wr+kb9vX3T0x3+YPEJ6vQYx/Rcpjjv7BaAE/QR/R0ngw6/5laSxRJiNYk/EuBiI
zFshaVFFy5YsVfMiP3eFFzptJ29l0wv9rCFNV0muH6TYtrLJ1rUZvRJRYxe0EAwy
IDFZwg9d6NDwCs900eeFsPagx4HHloWFeOFI3BwmK1xGHIH9OG2/01dOgKOpR9yZ
zFLyZr/Dvtq6F1ahB/ylXcRyQeLC/wLmKfIPrPre961v9bnxXy5/M6gujiPZ1YDq
moB8Zc5o6VrvXIT/c3Xa627p+v0anzUYIaGsvNSTHvalZXjdEAtfpgG5t4Kn3GdX
VV8t2LlYaK5yQz6PkjoZj+eeTho+rv+nyn0qATLTq+kbHVOHsW1fxF1NxD3FUoNx
XCSvNBUgSrwUpQ32BAsmDW9wurk2n4mG4fU/q2bsfOZNhBXg5+YpIR0PLeBH/VHZ
VCM7j0z69R5V5PBTuARPnOkTEWrUJuRLMUWuO/Ur4kK/YYTUuHsF9P6Jsgwv690R
QuLDbFAfUVWm9IkvuCArubTxG9bL4WhtWSCfCEuxPv/Ccaq341yEJ4RVRehcIw6v
53ZrG5sxHSYSycWVf9B8RwajnedYWMLERlwdBztRmVrxcOMKvLTFMC/QQO9yfsd/
oyN0tOfOR4q8DyXYm5xhsvGTcWH73BKmwrsNuJNIm7D4+TJghnTyDaBmG7OFKpaX
bAVwyuixI9BmgvWc0N0/bLn9MrLQJMVAm1ZGNZV5HPvpYCxDQWcacvr1B5wRMtVQ
N+FsfkxSDPzEiXK7tswz/Y3cfgO8XTrCyDl6qAMQvwwDvJr9OgFjWUf8ozpKejBa
1g7TVjR19kktoxTvRbGsqEEH7nUogq+nyorm7Sdka3VwL+SOoqx6xbfW/v+nOO1Q
XUl/MAVH7xktkDmEz7Mw0e9GdosN3K3IYUy8youKP7HwdiqzQi7oCorc+15cX/6t
J3uEBJRhLw6DFRpHb6Ez0YLMG8k+Ee7DG6ootFAhKPZINMkuOiM9ccJNL0FJB3UV
1QVes4YXvddW9GGBuia2bGMumjE4PKLoTyTi+O7rsCiRMF50fi22Hg+/ykcCP4wN
R0d4ZVz1i5JwZiOCwJK7A51wlncKdGBsgveLOGBZRLA/UMxuAzWRMbrfTE6BjzPo
fC9ByhC7U0DpB8PISjgJicSQV0kVyrq/PiFOUEObZfgcSyORgZbzlj1Q6AC6rZls
caJaMRtt8JcYuiDtrsMLMP+wBsCv7Luwo5H09ezuJyELr53+FNvVzZFKr4DY167A
UN8vK3TxI/nVCw1/GU+QF/LjbCFmGxjC1LFtRhxvuScS5E8Ex1pM9RI0ljCndxul
FZnL7tsQDwxgdNiPqpcWn/sk3QJgHCBh/bNm6ITmE8jHBMQqv389EGZQ9+EaL6Px
Xi1vJuCUvwXf1j4G4l8etETa/GeeR35HN+f1w2D6Ex2qFjFo6zHnZL544zRZZY+a
dE8H7yBN3Yftt0uZdQUaTyQDrEgIvW8msGur7IFA8dR4nwqWf0/46wQDrn7XhacS
z96AGW1WlUyHEHBtx3+JbLx48DEbxRho5yaWKILstLrKHhuLnPK1/K6vvQ1KA0u1
gDr2HR+/clafasivLZpHiSJSElFIPhfv0Bs+JFbGwzHnG3/BmtZkubjLugeJLCHi
0NxbX7/fEe2sHPWQVPn5Ishv7rD1a408lL5xdRDxP5bMW1/25sd+I46gKwmUWy5h
rq0DZfaKyETHYt56xshx4X8F3VrsRhfq+yKndkGiih3gnYvO3COcI0hWyRvfpyzr
yb8ie/+AON4jCJSLmh7c+SjtUrXP+MUULi8HZfXugzVhoIp4JynbBYBuZ9N9N29D
f9XmkCn1MkjOGuz0aLWD4cMu4nk6VEsA+dkdTWXOjqhFuaZanwgGoueMViluKmB2
gb1XL/oB2twsEYhYlwjpCOJrh3zAH3Oqan/MKXU5DeeVn+aAu54TvmEoNI77LEjc
8sq3Ms2mZwXNw+8jwYW4U7Ih5dFwcezofWyPJYXGs2XgCN1zGWHuEZANiOd/S1Vb
sn9LFeN2JNeIpOnK+YFvArtSxOYo5oT1J75QfWipExHjUkvsFQ42Cf1XfvHj08hp
uPltjh1qnRjLm5OEmTOInZ/e5BQju45Il1EJuVnBOKqEec3Hp1+Gq6XOXlrQdYDf
0Ba1CBXr5z0Ul2xBEWAaKg2fAHpJ4uOmTqdY4TZF7QiMoENpjvkZlmkQNwBHOSe1
+eYlx6ML7sQapuo8LrP71cAXpYmWvS1WGw037mfeBVb8/biOP2zpC7QLmp7bIQxJ
Fj0TMbJ56A/MJKzUzZvOMCWSjL/bL8atlAP94rXEZ/K5uidf1l6tAQBbfvdPN0t7
y/WAIA2A86x7fm9X9EW+yOUB9EJAQi/kjLMtj/vfzIVngyhvrBvcf06G7PNCmdz7
t7YOiNLwuVsS8x326HbjF/cSWGJJOw8Z4kKvPZDH3e5LLRN/04jDI12hYJ42D6q1
U55VB4AJOlsJXM4W9aNuu6uB26en1+23t7Z/G05EPKY6LKjNxUwXJ/f7+y1p/64v
```

```
kVF6ZpKYXKSw/RarkCQ32J0SsGgMC9an8JED1f7RBP4VLxL6aiusuWE7qqcHEvpg
e9xZzDm/HKnEGBgR/ZJU53zE7ZdAdRdbtqg86j6E3Y4mGPhlOEp2YelQcngZBDKN
F0v/6HviFalaTLn+xwvZ83UA1iQo7C8XH/nerqlXgoJXOmB7zh80ydQDdkHzwVlN
JSdhZ8M6FFIdcLWEJa8xnXfuEMPelmTqXew2/e1TbwARins5T2q/8cyAlrbx5lLT
SGs5nqOSg/H1Ujh1MIxT1azVYXUpMQIgiGjCteSmSR3a6h9pWzxrirCZmMvxHM9i
D47dsN9NbGc0q/YikS5AnMricLBLOhH0ey9BgVu48r9YLLjC67iB0PXp+eVQ/Od/
7ujYBb+h8uVGbDSr6++jZmsTMkePcdPdOTDY/3broOzhzVzAuAZWxYYrd5FuYoqk
EK5EwC53ZmIyAAYRuCiYA0RutFrm0zndNbNDZ7VPLam9w+TUEnl6bD7jdoQH+5OT
qEbeuH0wL5KlgiQoKIOzn5Mma4MxNTkI7Av5z6Qwt68+uBk65GPQ1FA8Awyfwzw9
/97DfVCyXO57sLMPYchM5pIXYyOpkDvyX3InESdH2VsT4nfGMIFE9LPUtiwwNlzW
mqxqtZ7q+dr4sT8DMaUKmZ3zkC9n5s/F6Xqx33yKus0QlEQvPtC/9rTesTC3U1My
tyX7G66QX+FMmy9a7xXsyKcrbWxMIMhQiVVvibyx3FDznUW9nNdYgKNl9aBJzW1l
sfOXafZ8VCwmAkAphLHSR1akBMGHSSAhT8Mr3878IaUKa2aSsRN/9d/Xy1FqFsmV
nhqjML0orCE6PO9csvBXUJq3dpx6+qGMX//QFpIkimGB0GCtfAk/olNYKkGMQst2
iePNps7Gx+A8LqDeE1Qb7lpQ3aKjIjxAvXKUTtZz4w+sFvAtPYnrKfLRa+DiYdcn
W84YBxHYpSXBqAvlUe9qJUgEDDD2i5tqTmxgmT7K6wNRHvdqi44NUwvHLoHD7BQG
AocOm4fQ57B6D/ItO8sQobTXMqo2lrrPrAko0x8YYdczSYBe7kRwZLlcA6kGZ9/g
YvDUo58ksNtK/Goa2/exZ7gDu99z9butU3xvCZWMUNmrX6PIVsrVonLhr63yBiV/
q0pDpSBahFuHktpLOsJgU0aKdqgLNXFuko9hT/4TQ9HL2pMyd/PXroQuS7Du7X1k
YEXYcGmN1RiEXJuACJJ+lbn0YedDk7MGcAvZ6UPYsfNHY07/4d+3b+c0w23xUIy9
D6Pkj4EiYk48WKKmuDp+jj2ARsS81/HkC/cBOjcm2FFSKaKHFv2BoK1vSs93qw7n
TIUdpNbXNYU05AKzzQp91KFbogDTpxZKnYPvujBlOtJbFEQsPocEM2ZCw6mtmdoP
JJCw2D7RXeRpAUT+JFdXVy7OF0FFT15oGk4ybArCUf+9JzvLZZk3+ddsQvB2MgUP
s9hujNBmwDcUlk5SgZvvBzbSQsjB0zzOpjs4Pcu6CcbFtC9ipdENkmkcdcVMmG+/
Qkz9/wE7UNCE3dfwmjyCpjP653awA+KVVxPXIHthCv9gwn1MuJF2keprLtXFbO6w
KiR20catmAPYCzhnzLcKWwpWQUka74pYaxiri4VF8PYkdJEKAU4gWEY3MbDjnk/g
jwhfrymJappT/t4Fggttzsg3RolJtTsCve9K2G7ihNPgxfEomS8czeDgFqhfIEU9
YBeElKj1rDUDTGqnvbwUVY3ccH3quawNGJ0MftvQ+yxGhXL/PVUCtlzGG+b3B0OT
dcR48N2GSlM6y1cQQEntU+DgzPcQ/Do8v0gsYt1Dvo/BOBj1hkMdC7R726ySxq3Y
r2R03F90BsWtAfKSTL+vBxFOUfr8ksWEBGlcgp5ZHFvlyIub5MSdaZQnuDJMF+3L
3EMWPxCVKkWXkt9qhSn0KKpW6mtxUC5hLwtYOp22hh22aKXXWNfYB4J8SDlvSfIv
V5swEO5QZp1bzyR87K74x0m8sbF3/yU9jRy1AkOoiRHLtKUk9JqhLO8RT7L9mLb1
Piq+AmrydWSLhh6DDPXp2LbHw2DuLlnp6OfDQ+vafms+eWKGxRfzKiUph95Ky44Q
ZqTa+CuvjcmZ9eWgoClt350qRqNtXXnAAM6PhAXoD/D66mMiFDOeAm9ojqgSp9bV
uvVMJ9fZ3S2iz2zHvykhCdkxV0FdCqFREvlw4NHocA8/aSpp4iyE/YqYRN6NOhBb
G0EK2EosGYA46MlPhkICE1a3qdxLq6KvDPIvgt4TN1Csp/sO9VH4RW42WFyJIx5l
tF4S6wdiOLh1+IDBVD1xC7ocA4ym0PWV7PnwZfJEKXUZ3ahBbkHVjkau4Bi1QQN1
Qmu69/D58oFyJOQmMDPEH2cRPU6BE3Oc7VpHY98U+2MktH9X4xtdbl31G8ah5NJy
3dfTqWl/YhVhaEcFVm0UAaSrYgnrvwKPGNvrJeF9rMYu+BOV7pHQW04m6FOU5tkK
I1Hjk7rLDo6PPLLgugIAM094d3Kk28B1QENv2pjcygs3xuCTwy4qpy/FpRGMt4k8
TWCOvramlPBNaoYO+d2vPCjzxJTnHlpkxm0EuNvP/JyG6KD7+we9CavugGBlZ2rw
hOye+RNyKLndtbUrrRuVgIzCEQK5gxZBktp+2IpzITwKiRhWr2rye3W6DvluCuA8
Zb2dulyF1CTs3Ot/NNNfHMUyEL7p1Bfgp+cFxvtdJKajvuZUpoUm+NvF7sL87hx7
6rDsIl/DOIBVOxAjMfQBtlUY439IgNv4SBvbLsDV/96Chi2UTPQ2Y+csTC7rUqdd
ErMKy0gyQklVQp99XsjB4QNKjbLS6RL9OaG1aT7a0AjPVcg4z4O/koBJ6BAdhr4Y
5k/MoCVVLp4F/vS08zmfZlXzYs9H/aJME6xcHGmmVU8gf5zxbkm8F31gLixxt3J8
4QOqtNA1Ih2iVEF/AnH5zViD0C+lkP9cQUiEpCU7Vb9fqkh9UyxrOzpRr65Dr5AT
N07npVfExTWpjUIEFvDpKj5MPcAimOtkugZPVmxa3HtvaZW30Ev3xar4JH8jt8uG
seG1MT2QKFGSUIuYwF/iRbUVyS4FC7T8UNBRHqoFNzF/F+n8rebb5RYUcSFgibHR
T+dIeC8EX7CCW/VyOz2cSPq5dWgsJCHJVXxHBP04IB/IQnjjYxfQQfC/QkArD/xT
xUXwFRcOouM9g+m81QcfzhJ6RvaJTz02WNU/gaRsHjVHxQdmB++B2O89QsCLdyTB
hTn9xr9n4M8l5Vo36SFCFPITuAoI3VtMR1nMRmh0sojyGGyDRs3etWtu7/oeKTOr
QJ6IIsIXc9OHMg0FYMpat50zIM75x6S04iXbd4ve2aYZ2xXVBNLPR6L9lmMl2bci
```

```
ChvLnlH0YhUvk8qtsndwEhLbnfi9tTHOeOqZ1ySjgNvvZhO+v2zk93u2YUOm1J5B
JoHMAuhcFggIkz690z90jdsdn4awrXSG0iB44jDX2j2YwiPKMSZwNZ1Ou13nvbI+
W6eVAiksO48Sp/DLQd5g+k05G7SVziHR39mxXmzkARwfKlMa/tgej4ACK61VDjBp
6qQDeioSCkMfwUc7zdzzRJ5MTPmFjSlTW422GxTPk8FCrVXOfxLtKQJihMXrJs69
4iUIBvRM+t1gSjv2fNf2bHA9vyT95t+17a3K5ww0t+WfewM1yXoFlq5Xf9WTXdqp
JkxCbriYSCNRmc0EAS/zgR+WgvTWdCjw86FFz43UX5TXyEYfwGmk4Aqbo9HUa8wh
0H6NMkyh+Z6peJ/juOx+VVaf88oLd1F8uZOMeiEPYZ0dCUolpd7m0zLu8wX6VBRe
A50ypsxz3RfD/2oBQzk7zWl/BdF2+mhbnx1QVf4qQKtx41eItCZLdoS9II8tcxwr
YJdeDKWh/8p1UjMPLHKsR3d9jLwZhrOAmjTYespAp1xmQE6FXhC8ADFqPmqSCoJG
5x8WsWdcYt6qCPgzNtIWjzosXkMT+JNbpuouT2zcSMd0ZuWLYH0Cgpytyze8HSQm
Lcnu0TpvkqG7eBnENouIECNwTWkm7J08hVJG+a19vkUIQ1C6Ef8Q37dE/HVGJTQ5
RsMYhN16fL7f9pOxvQslXxA6RGNiki8agzdz1NdJiKdWZt07ObFNl6kn6h+/fCPN
WDXWH8CtZXwVRft6ypKgeRAO8dCGNoMZl8YEGlUM92OIVALpq1XBPnGvRG/qZyb6
Ay0Lfy2InxcBlguAG5e7uUctOUdBgTJLf6nvhtLc+2BK6+9X/i8iMY4YJR9jZoxV
pZOjKZJVQs0JWaYruhVle1b1+HplTDbMBZpVtNslTWEqvIPBsM43Gi4SIgn8EnCI
CbE7CHFRIo2WcL4wGPncWjSZ1TjV1zojRNI6hLzMmij2flCZ7VSzLl0ejUZfuo6Y
006iHG2zmfTUGwas7wLhx6cNcBeCmGEALRBfcdd2mvHUuf0NMkKaTd2FIXU586NS
TgDCsitejJVZI1pGwYBgLdrVpZxtAKpOU+z9ZRuvdoOKJKr9qYgbDkKyxCekABpS
CNpRf2UlWvq4+DzeC2hiiv+yKZy1re583SiKfv3mXGmG1U2p0ZqXktv6iZlb1nst
okp0dBREQUofH1zrBnHa3BKJV6TOrsARk+Df1KHR/JJdf0o74JKm7eMYMDvK+XNL
ne2Q+eyIf7FQKlQH6TR2YkjiXWYc7e5nmuiXX4d3IdxtUbsSoJAKdSvP1AixvCMn
1/PbhKGWZMkBEpPXPexFjajPB0ZNv0NTjoKHUC2Jzew6mAPR7jZi6rptTiPW/mGv
LO9fhQhrBrIV+iR3VjrkctMpVvSx5NQU7R1Zj+Y/6KldLSLqbZ0jKgAp56jnDLWA
/kl0Xw1IaQlhKWXxeyL5VLyMg5k6MUuIzpoi2rRpj8zAuOv2Zqt4x/hMfxMt2Ohw
OVQvvVvoT0XwdMnaXTuBX7dWhgsf83xsZc5XoRSL40GiXQMqdiTVfa9wpAbHlDyU
p5tpWayCb6ipXftz7vlHUxyuFHZ9uGaR7q1HXMjYxlcCmSYgcGYSdccKG1rqHHxp
9JLPnJZ2bmO6d8SmoD3axiJirLQYSy7C+4bZ7YwdTeliSzF32jG/vVB/Dzlh92ws
HrjLCvL/T9QHpSqva4WE79+75/5eZeq5rfc7hH9O3qpUmmr1UA0QjxndkADZz4mh
5I/Q30Z4lbxqHRayyVsZrZSKvgOGVxWI3sMmZu1LAyxPI18hHiuQsdeyHgGVJJQH
JzZ6+3cyalqHidCRg4Sxs4wg6zuUtODPheFEdBCpc47v91N6tFwoWc96KYXg4dmH
ZRwOJsTQTEEJD+kwKDtRwka6CE95iu1/ejGFOGpNHRbJcEKiaIekuPbniUw5FERQ
4pohdxQ1QNKtG/ixr1w0Tg6UQ+k4fRZYrKGqUcV5XqlJgKX4HpUPZiqzBsXwNSE+
8pjC32Pe+O6qoM84wUbcH787J++sYT5rAjwQnccTooqOw3XLCeohz9uF6Nuu3fSZ
RhhVUvqsfy++2DhPtvjgSTOEIfEFnkdNfxEhj9bjDOrPzgckjK6oZ8P+F5Zw8AAO
z8DABVAe/WQqq3EuGIKfTG80BpfHm9P4Bv5TvCNTVLN/GZsCRBC4UOqFxWyMK31U
llA3ZTfPKjKHo2e4cNpQSVyBL8gxeUW8qQVx4PpGByX7duM708LrMEisC0kyYy0Z
5grpXYfYa+VLB6rAf6liVcIr5/w+fTK4k67//iTrLuwbjEifQPjA7mAOiPoQnJ3v
ukD6Obb21D5Gzxkf8Hig8/35Be8Xhlwr7SvhWWWEtOaLnIK8dvE7OHRl7CZ+cPHB
sBJIIX0fakiwmnCdh8UL+UWH4YYviMLySfGD93OFiog5dqYv37iwJMiBG778pj1a
1pdmRfvhwGUowuLyZwvAGnyUfU7w6U4wUzNpvEelouvTC68UGO3oNGbRNolweOpw
RPBZe9uD/x+i1nS6imAJ43FlKXjPTV9CGg/YOsHy9uiaNln6t9jHq5Crs7bdpt9E
ycIS8zgI6v8bgx0vo9tA7XPgGB/JMLkkqD33b4r3vLiPpn2hnBn63VUVP20VclDh
9oejg92aGXekhOY+jMQCcNpLT9vPUjJO0XdX05jPe+362C5aC0fVcegVveuvuIbM
nHVah1CqVGOTLbE+NcA/GlCSkPQv9+auaBkOeN4RgQFhKmAVr68haeqKkJWjApBP
JKevmS2412J82Ih4hrp4z56c0xSvzpZ3e+ybsKpO+YuzBQJpkv1OGXUGF8QRC/Lh
GHXJIfKTn9Pt8YOGVdSB4VMjhmoToIyf7Ct02rmDs3et6iFj/+w9rZTM3oYajdpi
TOP8Z25Onbuv7xbaIFLCWnUqpM/XEHhWPUEIk1PWBkUxR7rg4GrQWCxvRu0g6zwB
eJINE4Z11XIBu+/l9xMDy5EPDFytvLoiOmWbfILc0IL lXGDJy1rPk8XAmjabEol2
WD0F7wXwXWIJj0euSZDiP3HX2VPWDnzH7fLZKbgZTFghhEGn//SYewlEnfLUTI5h
fStDAPgavWjNVrzn0Pf4BmjNROxkx2/Jc6nMZTyAVOqmm4aDraE7rqlVKwAii0Nq
l4wrKbLLWQrSotzNKSCQZ9rRdlOQdWwbYJldqI8lrJYYX11EvtcvHyhLWEKssWMo
T2QXhx8XigEChXRQ98tiEAZcly5U/04/Yn16hPBIvVyXLCpjuadnfXl9yRUlQvv2
c6RUAxtcjlCfQ043hTZRZ9wPVvVKZq467bSB1zLx2BLJBRdXGR8YkGUHjp7HZ2Vu
```

```
RSuDA1rUyJOM7Dhw/j8lmHBN2pU1zx04iEpmvCRDmGxoYNZwBAu4GO1BYlXPjr0f
6jagKEK0vAleF7QONITAUVwSB8+tIicTC+iznZm0oIPvuVi8RT8Zpi4nGowcC5MN
+DuLqkRfWsZdgNucdA7PD/J+5BQt5nLwz9+ApfQwLtBAzKBt1joz20hF/685ytuX
1BmtQ/I5cVmbN0nUsLANLqEQbCxg64lYuLwuVfmwYjddNn4pDtONEWWMsmc8RfxK
NVRAZ8xJveSfXxL1xL0I5DhjTHKUnxWbmFwdg/EOWVJZyhQMPrwMxwmnlUZ8+P1s
A7Bz51ebp58em7LoVgKocnRnKtOjrtchNxoz7stu4fImgl0iZHNfgVeHpzoOXG+U
UWZGoJAj1ru8xSfl4AHeEM8J/FwYLVAtIyvkB+Hb3MY+Hp19ZM8F3Z4nPyBSfdeg
u/Bjr5VykBwn8ZrUYOvXPvg1VEtY9NnqmIqb3Yhg7oXpoqJ6A16L9KXxaj+/bjhT
ZYxu9AlnpgTeRoKog4AFibWRnGknnaUqKwDpyMh6QpzusbbmInFqswJlN2KIbH3K
ZWnPt1aGcqsgHjlLJ/nNqvghHlz7ZLi15DycrkHRub7Yy7Z4B7Pq3Y5XU35O1i0S
Thwv/42cdenQCi3zlBHntF/IBHk5jjEbgiwITioh4jZ6p82W49Y7YHcVCSAWfumv
Hqea+5+4GPr/DTFYVcyt1vKcCDsEQrhKjWY01S7QZfz7sG4gktUQVC68245g9l5Z
U72fo17v3eKgF5G2RCs+RnaRDHE0PWyxWe1O30RvoO773TOatY9VJXD/1rPDdPYs
fX5ZVxu+IE5X+Xavd1BjtGMZOEFx5qt9jrIrk98kkyGMAE4Mx97nojJj/uHO+TkI
UaVo0hd5NHtVjUsCElAlyKyU2y9Ey+ZT2G1CQpLZ2VQ652VtNtZowSNdq+1LsPRE
LdRqmEp2hIq2Th17dI9NwDp6lBrSmkJ8/XTYPONIxO8xBV9GEXRgZa+f0R04m0YD
veiVS/wG9NjKWlMZygZCzLRT11M0jSrWc/xlU5QyUwxQIbjFWayUhiwSsXuTkj9K
GLqvDu78TCviD/nWGZDMIMN+B+MsBdiv9Sc7EbSBQus6abn397u4OLGkTjwbPPtr
rF6IRsSZ4EGcnWTQcuXWTdDOugmNbpLT9/CUqVql0r4EIklXHuWKcso7KUalWp11
riLSz2BYzk8WB4FGjLabXJKXjT1FpK6HpoBa3v2Zvr6pMEin1jqFZih4aiIOUOJk
4PLWkTpgDJOw0DnVaFSpAQZpA3lfGhHv/NQVib+GirjUniBhCvvqruOFelbqVb2q
Kok+vdkIufl88kKumtVjUupB2oDd0plnOjeTf2itdsuJUk/JbOpkibAUp/8V0Inl
iqhScEL4u5bPVrYOVHjK1bl9V+0WKweelSGf9y53O4+tcC61HIE57dQWCjqX6e6E
44fPanMZvx03bFOCdouBAxK9duyxIXhSkA3++t2pHm2/REb6YmMWovLcZZxWwS0t
Uvgfw1L6fXzYI5C+oz/STVOCIOxPN9ZukZlKchZ1+wWZTKBj0X6vNK2pla1vzY09
B24dcX5i6AdiIFf1cbzPxjyNfPZrZRLU4hm/R6e3+8OIhXazy1yYmaKGRpzfS+Uu
WIYbIVCBpOo1Vj5vzl+KrH+SbCRHP8DZnSVicCZLnNwWvCiQ8cnwwjLNK9kS+C1y
CmQ3+kTlvCgi8Tr6uw7xyRMNXwTTMKe0po+qXSz93EdauDYGm4stLJNmb3kqhe5Y
e6npPCDhMW0+XdfN9dQdFgFrCvb/qDNYt0GyG0nSWHqHje7KaeLy3ajIRrrfJJGo
J2+sXg7rxyFn8pps3+PQKfTebmn21UGU/f4yIwPORwwLCpTTJ9ZZBhb5Y+nTDHAl
XVgP+tmf1moS1WiCKmEm73RJ2Z2b2agc862uuSoIbG+j3BRDQ9KGUYUxN+X02eLF
l8vOkVfyL+GrSDgVoUG4JJkm1C1WXtrYmUjXjHsF4rfy+YiCaTXttzY5DQScZ90o
WQwQApV0kroX+e6fYIc6xSHlROhayNTOpBXDHDBDo/H+WiM6GASYVIigVdSeVRoe
gzT1aZNuWJ+G7SS54hcz4hFypp0lph8FWeUTjEXVj4dwacvLsYOIQ/9ei3bLLOJV
BsmAobkxA/DGFMtpdsS4IasH0VeM3/GG3nDlZFnVXVv8q1Cus7LCOvxKL4wp3ZLx
MmagxqxYr4hsC6kcj8ZETZ4zijdi85Q8znOpYV7089yqffFdxHZcV2/5wEPozMU3
uzmjbMURNwNy9QUZFdOEQV+BoyBNli45u2JWeMpFStkJJZR+3jJrJHlMJlpvzPNi
EnU65QZTktHq8xbGJYsnMbZBwaQfqT/mEbWw1/FdrDa+dgCbquQjChAAXdBfDQcL
5dEGEcm7uOMvm2zGAnidxXfO2Ix/1QZsKEmWIyyhpGiSy8kbKapAULGO9z6nC1nt
6ZL5q8zS5b3OFBv+OwpuzebDxsIc7iG/zg1cMI5Gz/jDLuzxieUaFai9dJe6s/NH
9AG3qoS2u8lAwKa3nG9DhzT5NYt2Ot0gY1f5mPFuIH6NWMnTavEXnyr5GkD88rvv
RIg5It9rwqy1h/7fvhQBzI6gHc5rzSSEGwoPd5hZKrbmPpVl28UATOaYZ8HcSX2B
UvKvJF3244jOLJzswxJ43FL5c9Uc05aO6S7bPJPq7oKn5QgwJesa/+1KODKZ42NO
boCn+PSXD5tjSx3Oos5goiCrRS2k2YC592UXCqWCh4po5b3Y2KEvSBw1h85XxkZC
sxiODDcHL0IqSRIwttVNK0B5QDFDrTtfY+TDDJ7qC8zmrFQQLNsBYQnAz4QgtIPO
TvFiTOSbh9s/Wo/Ze9UztXUVff+BVsOzfVlDkJ5k653y+T4N851Hu8sXk+SmG/6p
t4SJVM0g0QaqRk7p5lHA0F/UWDqPl31nfwigOfQIjRiLW2+Uva//UfH3BJfMgP91
NJIMz16CJha4L3jIIV6CPJy1u1Z2SWEWQ0Tae5Atd1YfGS3E2/miLtYhquOjERKR
yqX5ZDvjlAgqyqZSMTOPUYkTOwpJ2uzt2dw64bVZG5+Gv21PUT25ysvNGxFd5Ps8
hjTv12NR52GCWQJgEIkBXZIne1IZoJt8Tiu3/6wLJyLMqJ6PSluL4SG4LqbnQZea
jhlE9XoxlL/hLIuC2flUIfcqDOpNJ5Nu7fMTajJ44ebK5fj/yb5RlGjjxdJ2G476
uJjWcyI0aEIqjmRKkak93dx2QkrC+lX4gvhaX1kDH+pkwWY9MIZn1m1RlgFRs/t5
ABvs49OP8Xut1ZPzFiCKpsye78WEzm+kN2l9YdK3hjbQUPaMwxsMV1U/0Bib0+Jo
```

```
qL0irRlv9xrenpskqD7/E3suUvnKIcA5jAjjn1q4Jcu7S0neVSPXMDivpJBQfEQo
FuKwCwhtoXnPjj+XRVcClpS3yj6tfaMYOi8OukhfkKrTgBl5dhVI36o+WFo3MDLV
uvs6yEVYvA81Jy4lgkZIBa7HjUhmqdUzK7NQYxAQxEaw1oNaqxvRpYcxIRsUYDIg
dIvVN0uO+jxkgP6XrSSRgjfbssHg8/peAJkj3IbXyqiQqDVFn7kUftGSLDuIgUqg
ax5yZ6IJFcj+Mwt5cY01u4f9dVmSNEKLFybnPo9C0r4cbosE+tNowrvkU9r8Kvwb
U98jjqbjOc7BIRGLJXSPzT4pSlMpAIOVFoewINLv9QJIyiksE2AixHmCxtUaYvS5
EAgirW5juATgnay5T/V58u3RnNcLvfs2oPwZKGHTZnDEE2PRgHi7Q+HLCG+OhrVB
wSZb9f9dSpwsRWJV+52dX9RCTX9kolBjtiWonlEb3CL6uchJ/FcrJj6IDdT4+zof
V5C7ers6Oj6A6vom0hpDmCPh24fBPDjN+SuJH61bETMoDuSUjRREmj9gMB2oITjE
bEAiLuAp6zN8kljmFKqwMwcFINFphjvFxqVjbj8GW/zvJGHnVo+V6Ap3Wjm7kImd
6oXc1i/gyeT9IF5dMPGbImuTDgQJ2hylMaSjiEv6FIcj2I2N8BKKBhZvohNt5KQK
6qsvWVK4pTwXxJFQOnVPXPy2RoeUgqKj918Kqu4cm5WMMhx9pkc+OI6KINmJAsfq
nrAqoNDAq/usWsJFjv27wGeFu90N5z51NxyKlyyp3sG52x5qmDpWjAQO27LWhf5m
bKw/qnixtYUTv7JaxI55RTjRvXbDH9UGIfUfOjiMmvkDUrgidBoSPDnZnVRQJvFE
ja/fxIYbKoFBrXAqtKQJeVqPXS3MgcJCp4ovqFcWey+BBaC2BlnlLvF2cHO1EvLr
byLfKj0Fr/bHQeJPkc6Usu/TWmTMbzyQXeXPuWdg9eIOx2jtfY5KrWuMoUCCEQcZ
cXD63ccYJ9ZSxopF0u9jbPs6eWKX4qLMNIU9akMT2ePxCTidHECTaIQJhIuOtPn6
KmrwWC610WgIWsWPSKczXqjGhxC39uNZAiejMDXWjzMRJcp+1nxgXQi+ZgTw2Jpk
1bQnHtoBV9uAmx+tx2ipjYNB2uj3A1FxsQBS6/oGgA6pSy7ANVTVlKdiccoA2EVr
EvjH6tYS0k1vlUdyspDAGLYI6ANcYWGfFKqKWHU5gC0RbAs5dTqzywXhKU2ej5HA
23eS8flB2+eVVwObeG0XHmtZuHLa3YiIksKdRajA4DxvSA9ehPS125ZQKgZZP3sT
DeglmnkmkGSJDG6z/HPx/Ksdhsq86+n5YfyLtX93pfvhT006/AW8cY6Oo42jqXbH
GXO/1wc4YwBNZl8Y5OYhdLRQc1H5wgwEpYi7enoeM88NqoEE45SrpYiv5GgC0IFp
+SYuMM66Cd0pJCVSzr9H9+Bzsbwqcwy9NiWVmnoz25OdvRh24qClLza0J6Fu1zkv
YnEOGsnCwKXWuCMooIkMJVbHTUUeYYhsgEWH71TSGlNmGQihQUk7xrb1cLP9oCD8
eLQ6srr4QVMZl4/c+s2gEsyw5+LyQR/jjOs3fqWJlw1bT+7yOqTNk0TOb7RKdezw
8dpeK/T1z6GE2rchNOi56ODDlNzvLiSEwz7II2jPf60q/ePZDfew4xrFROtnUXmh
5GZ4l9W+LJGIIx+aBJT3CHrDdPutqrj5fu54YV/lPMGlNzwv2KQ5Kg+MgUu23Q9g
1kvG6Vr3AAVF5jhTDyEvrgCjIc2HfzP3uGATtC/dQHtd0/WH1BIeVXUA97c0mc8g
z0hlEkOYncx53a0InjzwMkqqR5R1pVWzBU6m2q3ri/O/dzqbnXP6DB+g+F9Twsz4
6rQEECLUlbRMD+LS9Z0mF0t5csjTuJ9Ahvez0FGSkdQ7MLnm8vPXlVV1qtpu/sWa
psrMIoJRRCwlqgR/UYqo7132A/8qsN7HWpQrQaq89ZdAemRqh36ZnJEdTp02Gx7z
VtW8XPHLs37/fzSW9U9A4hr9PuQ9Agv6Ssf9MOdvWKqIiF2kvUtdq9PQ+b6J0zCb
UrTp+qgtq1MPm3fcWCmQzYdHi6BUTrSzEbE/L4m+qEUh72R8aHlWRfTCV5QHAvPP
+A4+aK9uexuMKS27pAObCp+WZJfvlbMxtTifm+i7NQvC1WigfqOOxndraqLyK3PS
ypHc/5+SuJngeAiU2ixykMnVFCmq3FYDUGseuN960E/LvZY4dFfrzLmApKJJuWv5
/LBx4QpP+FffbLSCgT6xLB+kYwdwNt4wc9Qv55CB9uyrb+PFemT7RGacX/mz7z1e
ANTY9UucLc5pTAnLOeVDdcnwqG1C6UIC8LcpyM20V6EfcvUGe9GUDDlQuPHx9m9X
F3qHOAj8Pc3ZAGpIM4RvTxZm3uq/Oef7FBZOovEI940bBB/R+ntUSa5yWyzI16Xy
IZthd5pzDmnA1tY9rintqxprtBWmAfbjThvKprDzlHX0hI9cMrY25CH83AB0dVKG
cJjAsDe0nJ46H+ArkbGSrXNJ2f+l+P8ifbPAmH7ZBb+LaQMuS3ZIcqU4DxnZc2mG
u36O6GTFFYiic0yagxpBhjtPWkbg8wkgIUO5x0iWKbdx5AkSJ4imq1IiPs1l9Co0
MVWLXJ+yb/xZ9Zja9FhYlIDZJ7SL4sOp8JbFBJm4zOwI8ZtTXMLl3wS+L2hJ12zq
kyhUWoWZM1DBBWwjsoeu3ToGuZ2Wd42qNVH83FqG3wkS7Fz0g3i0FZlylnl2+jRm
OpjP46Noe6VoJf7+8ZNJaAa+V35TLXbjV8XRsJjItnBxu7SOHOYaKv5XNYOE4LbB
XugpKtvOWQWDF6WqS9FOOdUdS5+OGhR9HSNXnou66kGm+XVC53NezxFI1D0/SDy+
Mu8nPRJEk6j/piC/sfMVjXc1dlr+C7r4IafRi+xg/j5ChiEFQaYTuzOzWW078fr4
i9a0EzBIswZL1nQj042RHfyBt+VE484P/c2lemFXIxStMXhC/ySoOMYW3h0LUSv+
L/a98cYn5JpQmQFbNwV9bz8pH1L1VrA+zhHKGTS3yLSjez6yR/6wyakzeHdsEZbR
OVl7VMXdQjU2HkpjxRVs9QaxOe6s2QXLr6u5AhSR/ABrjWPs5r/4hfJoqoyxHCPV
inWAL7cF3sHhmBB5hWivBZH9CFXYxAA6fvbGmfEz9pn6IO7CtiRtqzNbCzsBN3oQ
Rjq0alM+SZlEZGhe0RACtLnRhxWz80JcVK9ANVvVvahOx6q4PISHdQALHCiimbnE
sHtxeGBfcfAk6q3ETM0nYX+iDcMSm9eFCwxI+wImjh5Tsr0yUnfyDPWIZkj6JblA
```

```
g7WY2+/AtXRJNYFTKK3cvB9feUQTlA+O/dnSBgvcKb2Xltyw68AyIw1vB7vVhHWS
CxBnGkoBieYzyXofZ560E05Kd0ig0/MscAShRWfS2XtzlX9YlZWvIHr1/W9wk4z9
BKZkF/FplcwygtQO9t34pkez/SQh0wslcBM87NjnvpB2OsZMlhBKAalM8XIJFcEe
328olwA9EhAAJTkt0jnuzEy5TT4JmAiJ6lZG1IG+IimsVrJXdxFx6h16Wqx4hjqk
vf7L8rYfG7cQYsXImI6LjjRh0odnxgtW2z4crWLcSb3oCErGo+LfKWf8RNRLGuyB
fzBNUPeRFZVuG935l7DwoxM02Fw/tb8IluZ1at8UInSfY9DMzJm6XnkSBOifLxDx
F8QkLq/c0Xxpkzm5mJSDTb0DJw0TugF8XqVdX9DdbFKl/De1Jujk9CsFzbpyvH4o
Jloh6T5qNp7P7cA90MZbqa0+0vt3sjFK3ROWlkOGBoY9RhhGCmtug1EA8T958oVQ
2Vaoz+aO+mCjGZ5TMkhU6T1nd/nTygbntjmGzrkj7JluMbqu9ZD1fAX8OhiPmpon
qQxdzuE4asYS1J+NElKCJ/P4w2W8jAtWPm2I1nQmB6AbY1AuNAq2s3a/9B45/Lcy
JIq/FCPF2I07vML2CcEQlQUtxULfIz97N7b1zpz+xjkkWv9VYYeKTix/gFpAjgnp
eI6vrOSPfD4IEyn46OfuJxYYixFfE3AqF/4DwcxUJghNzWVcfGdcyHQ0wwcge6K6
gvc7MF5HBLv6nAgvG0DAwXRqK43ZFBscF/DG6fUqVozehAgcesEnjDgxIEjcQtlH
GfKM7ljbteIjCSKl058GndQ4vIAw4mTny/Am1b5T8wXyzAh/T6zZupOgoz73MeON
G245da2d9KCZ9AaN6E479YdY3q3dmPK2XM1mPbb9qgF2fqPmJJvCT/lPydkh/uTY
vkp2l123atJcR43mvf12u1jS9/lztMPXMO6u3NdAyan+St3+p7E3OdelECr0s4m5
wfNu5r/HmIgj8EYWyzWV3G926UEnk5wQdNKI6FEc35Qx8kQ+M1j0hvLBEIvFknkb
NTG8EMN64oq0ODU6yQ4uX1EPXXb/fXiCJfiyPSCOqIew22wUEmIMLjCfBQ1IKbzB
tBmXTt66wA7+Of2uVtZB0ls5VhPlFV0+OquwLZ2OnVvQfO6Nw9MlAHpHWA6SSu1V
pg7/FT7ah4IOf+9WECoTaoAR5ISEmZBfitIij6I3zmsz5d1zXkvBYfqYoLwY4Qum
qaP8AH15zqMhGOcbv/VqI7kFx/UJHhEYGjTz/2RPmO50oqDFqT++H32nptjjbfa3
HEzf7yLi9G34ilD9AZY4dPFEDE6neBuonI2MFtGV581cPbRh5BxNZcnUuv0qMEzg
OuocwvJZyqjUsZhzt+yBIpkmuRRlwjiJnmnpKQ2HAtuInnNaQjDXpEe2UkQqGcsF
HYhPQvs3Bj23KJCIoERVE+MlEK6VRVr88pWCNFH6pXT40gw2KIydDqbi+AcVhWBZ
YrecEEZP5DmJdHKVxQ4jB2ohLGaE6hV3rF735u+Z+4mxI4BT55L0VjGBzxn/zPmf
9Sn1MnRYZZZqlgKRYb2ZsQBtd8ZCCi50OasW8cqpVU/KmSeXZOO8PUjLBxNEcPrr
PXRbOzHaBq6/jbqpkuN8Q/gazM9euNtEzfP5fY22AxmqFSqa2wv8aquYFX04aIY8
hLsbw/G2iZFlakZRzt+hRiDdGKo0yrmAiKgQH7If6yq9lqbYKRDTnLx/JBkrdEmw
dsUZxVNNIEsTrsLM6xXNFwqpFdpWewEjz9vIliTwN3zRwClqItovhJlbxvVcHtqd
hKq9ayOYoGBCgWNIjex2NE8srtkmTQAMrirr0EHlg/hlWsZk2uYHfFohDRlYkMQg
01UM6XAij/fbzeBBXaHjDkd2mrCOyk/F7Roh6ifxf2OgTxmSO+HWLKu4KThEvGX0
3n4bnxC1dBbIm8u0o5tN4oYvDJyQ08a4q/H3Z+LCfWlRtNLdBztZCbHkWdn3ic0f
c5Ub+ODT7tyoYNMQUuXBiZSM/DRH5bzHpTtLRtmuUOCg1UOTtrKbTJV0LZ3MhfsQ
EhQI82f5uIfF5JbeqmhtbI1QK/5NCCTWskJc+QDUvY8wPEyLDsS5ptuKDxqNp0Ms
Te9riT4gjMC3gxIxMhDN/FNXPbks5hyLtIAi/H0bCepZrcrf65Nezw7r8oVD45gz
7GChSF+dFKqRL/7ormCCySDisjS5XylJJGIrTqesG8QmXhZNr0BcPCyk5MuZVCQw
YhMHWBccZB09aD0Af/SaUZ+KkouolWIv9IED5FjSWK3S1qVrQ8Bpaw4X0aN2TnFG
wwsklORtnagUeJGx1n4rbZbZzlsTN8+NVxZjqKP21RkoX7e2vW6yMrbULDRIX3ZR
thHSs31gRNXozhxKg6NTTxwZQotdy0Ckt2wkvcalQK50ZPaj5bplWBPazGzP3hMb
Vou2nYo1FTXWVx+kf3t26edITEg17is7ZdbaD0hGL246lY4OiIAHOJtdbyACsoa0
IgLUqaVNELyoJ6Ix4Ols+UxeBmCEKFJcskEQv/KZ9YNaFq24nv9Tw1mTNEfONFQi
laqaqKckLmEB8Wa8C3WuHG19Nc1VnA29HMPRGjDo9W3fTI/D5wvh+iZaxqZKpq0V
VtMX3YqjbYSUSJ7AsLD5aNx0ZzPdjhY83lj8qtR2OGF5gSAnx95uxSgzUR2tUFsv
9Xrh3wOdrePMk2tr5BrAP75iUFJXt8eaeYH5P+JeXzm6sH2WzQbbKu58kC8PHJ04
4Cw1fmgNP1OHcnrBrDeOCwBELKwL4CwQ1S6SU2pzUtT+J2MrX1+rAw6as7fnz2MO
TAjNhsF6yjGjU9+/a6GrPHir/dkS8IFBVrOixaOdnXPkCyrg5WdA5GRYQ14FHYn3
YHP2BWf49+kEJPQbh4yhOtdiNJ5DWJ5tdzYRgG+hS/Y7hIwv2l944zwnPT2hExOB
pmfL6mAkECBu3CiLD/0UBc0ABxeWMcEc7yTijrqXC2bDEqPPcNf6gWcR2f860mRu
uE7AeXt3UgB4xqsNfmp6RcM4pQARDo8S/RJzykToodLqdJtLKkMovMoQuzBLFWkh
iJmwESUAFtfBOs8EKtakTmZVFifs9+d5JanfEvOtIXZLv5WTCVDbECOS22pJMGl3
OoTzi+ehg6cHVjRUEQzOn8YZ2NIDAf8xQAiePJr2hqeQaNv9xIVkp3ICeyBaIlXn
rzaW/LeN4yFCF5UTJSHrfFPRtaGvFePtpeIDtxTQopXy94OFIErN3Udv1wf/Hhfy
Kflni75cmOVQfnwoXARbNleNkZRUNuyeJ6cOw7NSibTxfUxXGS3MMtEaOD0ht4Vb
```

```
gTsx0L5QecZRF8qEC08VHGTnxfZEnof1nSsBimUKLkkxUxWoQmnHsLw3FuwqCetF
ks1LAkYp+Pa2aVE4vHSvgSoLVuxlQyyBcZC6t1a4Nf/BPPaNHFSJ6zOTrwj3V03f
vJ2AK4muv95XghnDyy4qsa6ogiXbdBNtA91utPCW7PGeLKpT08tVFA255RKX07wZ
Z3Wx3vZ/CkA8ttsW0fPaBs91wuiexYHhamxIJbigqHaJZOn8hcjeISkMYqCfUbaZ
hYUERl9LlIe3UDS505BvWJ71F1NGQmvLC9qfAoa4pUBDDpRB4j2/Sc38sSTamZfZ
nSuHs1W9v9Qypzndpv0Bgwqax9GeGLcBvsZEw2svScLwqj6vQbgUZMPAinzn01yw
CQc9V3ruXbH2NfMVL1gj9doUR7mQc0Q532f9wJTOYFjY7raIdbBUknajRvin1roZ
AMsAIPbpJ2jo1bREJbeOKUnzdGSzBEn87rZ7QWdVGsw96aUbVpQjTlYBOKD9l2OK
p1Bq9NPExUcK3Y4jzxzBgcMKeWu8BTtlETc07LcSuwnmt/AQvtrYbmeSPvtzWOqT
FiSlVeG6Yft2E57BYwRA4knJQNU7wryyC1/MqPCn0ybZDpIi3m55jMrESi7BiSMd
ojrCPvy0hne2iQw/yhLFVGHRypJS9Vgu7CwTeNi8XZJQ/GvnphhcwgCAo9BVpNlI
EBP+JrFJ1b8cBbBMwC3x9vBDjipQd4q3z8qXJ6rJBzxKRsZwCBEiv3Oq63piSyJl
lJBlWwbXcrrABFwG/Jd05p3Vb9/ZTzhIfIPqUtRdn75VjafGSAoS2+ryS5W74tu/
C7PZzQJESNPm52pac8uvuD/RIGxPTEkAepCCbt2Pw11tiApuXvVg+L79b6hvvXMn
YlqBYn9k/Bghw/Y1lSkBMbkKor5OV2eKDfqJoCppWbhEkpkznipqxV9y7Z3iezQn
UVpdGxorpM0pwoC6w5VgbTFeGvU7XwgNPUAfu6tpr5fmm/a0pl/rGxSpzZiLf++F
1q3eluWLTruMwCo7G13/YbtzErEiZO02ii163XF6akG51fdBMNqjMALVHdmx4OWt
6VnZ9UXdFgZHhwN3PPVGuJDphSmBI2ciHL39uDW5AczPLP1uUFbfHt8bR0TlJuSD
z1+TP6URxJLfLAQCYOJwZob/Tc8CU2tPcptT/mT4Y/Ebc6Md/rjz6R/mCV3r5pb6
XHY3xOwaelhvISQLaEKA+eivetwzL4LvVqQ3oxGiOsYYNsZZ7INC6kUAJqTzfNCT
HGCOYui/KlV5S4CegSPgw9yIp5WxXgwxU7kFyPu86LKjc3c1zUd8DM25+zS6B/63
69scBKFoFZwM7Fq8JPM64psQtghgqRP0pPs7ym0Pjlf+9oaXvN4+hYtraCtIpeGN
J25hxINcC9y7D2Uivp7sjCY3ykJZ5VAbvEPzLVw041upT25z4yMhTD3g/TGMKwXf
vEsxVEIkGY/dVGEoJOOndaqV0Y08Nk3oUurmSLFQlUSfK6t18zqL+Yt1YzEhEblp
TmeKBvNf7mSWb5AZn2/ZAVA4pKoj3B19Lwh6giidSAZvv42a2jbgI+t2cx2PrFVX
3r+46G5BEtTHjrfsUWJRuf8ggLZMNzEQPAsLxpCvQ1YowS7VhPHMrg+rw4w+Mp8Y
7HzR+P2HLv+uT2SX4InH5VDzZCe1ssz7bbrdPKR33wknzJ4weBagpf4JAv+JCwiD
/JmJp9uWzebKzZn9GVHuzKvNA64bcAyTrM0ZJr537mPGN89/3NsRKDTDa1OhdC+X
2A8sbk8V1Qfs54qsVSzkmX8XlTaZ0wEQKWFPxXhPcqE5Z4d3n+i8fL/BzPyPLD7a
vR0utzS4M7J/ozWMgQGo+KrYtYNR5gy9kXUsYaEN6mByjUqVct6vwaVS+cfvlz4C
rrZzKut3uaWuNxxJ/7LVT3UsDTgNSjhegtq0jAiAFiNdXFhHJ8BGMNDCVbdbE6gO
gHwgReWyJbRk/kCUmtPP0iJmCGetWUWsNzlsqsm/TjgoKApUhFX86qkB401Np319
tQtsJuzOPSUfV4KcG1QPEAsVmhQKfCY90R5qEKst12owNmcVDMNTO1RckX/86Reg
PXSfUCd8JfXxPEVXAAXsUSucFZdxE6BWR8w4RrvC4U/y8rDv2l/ww/pmPYmxC4mE
BAt1rxQWdglEzcxbPCEaZzVqsBw14SSmjFQABYgBApD09unQnfxUBmu3+EvM4d7n
n6a8LuaOIjsV7wn9fU8OUqDoig/sJlty+oGSK0IgkA3Rgd/CncOPeCS0+VkZdjPM
FGuJYzKZNcTg7TdltPeFwl0Q7Oyt/qLJK1jGgHlzZgIKY0Ca0YFPTdbCItwNi/ot
RfrRciviCusfIRGdX7T3uPgC/uQlNV4Ep3IDBerqfiudx2bMDhSZ7EuQJdGdsZ6B
xRrWg/JnHh3fYah1Rnw/iuQ2J/KQ6Q3uiQn2ExF/ORw5UsHUsu6buVY7Q2zXX/X6
4A5RfPy8FlMyhFX/U3hkLDennxECiBIM6ZjoFjb0MO0a5YxOaZtrb0UlGW3ApfTH
HPJT1T5bD52BujtZHsHbmT+hKFu02omYfMLWsA1GFRNNdipkaE6fUZdPZCSMTHUQ
ZjGSJBhPL4lZ+hcJ0dAC2adbPk4A4JYX3ZT6QKEL97yZb7NU+zQeW551xtLQt6T3
WQaN9zZ52343wzBFSplJIe495e16/U18YVMFJWTCv9ew6zdTDk7RaTq/EC+sOvhU
06qe6lGagvExvot3NDzj3P/Xn7eUokAHhmPiHM0FwdQFoS/13k/FNpeS+jQLoC0R
+njhMMrb5VCn+BWymk/TCDl5ojmFrlPlbhc/kt0TkPZz6wzqTY/YFP22heyw0u9J
j0C9dQJ99H7XXs7jcosjJJtMVOIJog0+Q30lA2cfBxyI/htC5eEErJXbLgrMUA5U
KI/UNOU0xh6bagnX/aTdPHDAS487CLj61IgMKjOqQXlBecVxZIrDD/XUqt9+eLG2
MZdcW3lengBFs7oJGRWlMyALsHXzkDZmDxYx52nQQbrJZS8S2a74ffxUwIv4Ou1W
l3d06FxL7WB3A8mEh1WZVP+Ndl/zMIVWpdJIS5BL0vuuVScYNXDfU4wgQHOjmtgq
kr6ZXdxkVNQ7tydnsciVW0lsyAWg36S8guBqkYfGv7AdI7wg6hoUiDaxhNicAJqY
UXtF1CbNuZRHV4aExHfVK9TXmNG1/sYvDaf+uWqEUbZVFfy5y9lByLZ7F/otfyQl
TEIMcuOt2wgCgWW4eQQZ7tiuchLIi7bTJBumfhIfhbny8cEjTQnfs9G4i36pfQVj
gy+d442giQRvh6HIDBOAyZZCC7gD+7xiwOTQ4afYrIILvDo6PIklQkdqeoibsgwA
```

```
6L+ga9Xc8Iwcf7Y6aWUAw0pWgdVCt2OsiOcGJPxto0jZbmhBM0SFTK1Qs7qyDiJE
fB53KTIVGgcOFuQJ1kqkXB0vcLm2cEGFhcbvHQkgKJfjXrimAccJc5GuSCt/rAlp
mD7iLDHc1a0unLVM2vGYmXNBKv+m6aIs2yZGmaIetOWRvN04ZnJsF7tOXVXv1LMd
EUB5JFsoumg9OcqVHOQgbcRM4MJr/sA6yjFySg/TzqWZ0R+Jjo5WqA61lwJjZ5zK
9ZhQRjy/w6ptWByridB6Rsazqbz9ea/kLQIzoHtIrY26lCszPCgnpaWKqPKPOzVk
qZQ+mRfYO2KsTIvth9oQKLMCybhOfFOU0x7xPTDKW+5ML+kxbj3O+84dzobInPFx
pl/TySGfFHXv3SQ9F1FFLnEfZf0wjfPD4yH4VSA//a7JUq49Nb3pxewc4hcrQbDx
b2+0VTr+gzxs/k0r4D9MFdeApaGsBMYN/z+mm5NG2pFjMn9uIS+b+/cO7Y602r8C
TyD76DOnC1VGYB2ea0T6G+989PjEahgsYd1fpuBwZCJ7y+hx2+RHqcCUEnbjuC5/
WD4hzzEC6iId5N2WXYJbSgZzeYDPXMwVsKjjDbHraNeZYofozAHoluNFLw7wbLg1
5EMJNPBpe/OHBYLUNuPYM5XIQK42xPS5FliZykTarlWvsqS9j5L5QkK6rh6ft2Rb
C20kxUoSw1o0qktKbwxolJAeZVAgye+BLkKzq2OBLxZAF0NJAak0H/pwIKZKFALn
TGWWD1vFoVN+3KAlV7sAo1VgxJAste4dRrax7DlvJTNmcqART2fMbrWhYPz1IMfd
7wwNgoeQ9iAMx8Bz4BpNLdJyXlMGYkMjdSPFJZ78QDZ9FIQKUw7svyF6wnk/cIWL
IwUzrHCpOlJrfoBK0N4oybjcn6tBXcScvimbhvGMKqQrG2yDQKAqdJiLuAajZI81
y3eu16TxclszFp/nkSkPXBQG8bAv6DzIDbV2bYVM7dGFz4sa5LwLJoOMiDF3GtfW
Yzj2eIeP6PDDcE54wRdkPOlnU8fo2NDEymO3b0TUPVeaIG+fEy9XHhbwI1hirtqr
bPQBJ8txb2Rg4UjoBDLvcPaNHyTpBhZ0a/HLDyofD6eB6qnTmSHyQaeKIOlk+lWq
alw/mURGHAzQXHby9343AcbBqqfxmdXbnZGTtl13Qh2a1sVTgvW1LmBCKUS3dnZB
rOkaY20JSMw87fU2r78hwdtgJI954wv6vNybjdyN53xPAAjyXxtnVtIDrh2b9fjk
Fl1u6SFgF+8/DKvtlwcx2hWkbbJ5qc0U6STYXko38Bp8DpuygTZ2O11Ld+5+tjYt
QTwDUaPOFmiBpkI7f5U3xyOR5EwAbFftuBImfq5qTjEwgAm3Q//vMOQ8JVlk/jtf
5PAGaVf+/hcGewOyItbihmI3sdd6o6hT+mqjnJtfAdLxIJ2iFCLYOyM4M/ssaRCY
b2K9DTxfsoxEjh7tR6KEs3ZDPQ/rJqIwd9pWgVgriBAB87SV80rYrLn3TYQOMc8u
17F8ZQ69icKc+9EnBEz6Rpsfrc6Kgw9ljiRC0a8nIDCsqSqqCp8ROxmwpga6N2Ak
ChFG+Z4GwHq6NA2AqyPGKzYi+YSgXNnDvGJyQKEQF4pHVl91liVrz/NssYbSTPL/
YLWlojyOXVSoWDz6yakwALV1T7NHumfSTU7GcGYyXtfiNIXDxgBnF5jz1TeSisL4
q9sxSVQdlCwME+dJMYfzeOjvTYEsuZTffq7v15uLTUGsL8s1BhFbkVo/q4MN8mwy
woVIDvTt3AYDJ0ijt40ST/wl5+ulXh7hZJJs0DedgKhRejqZ0KiCgxBS+CIzRVsF
pvZtOKUNceZTUGC7HLGWekNxh/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-----
MIGjAgEAMAgGBivODwYFCgSBkwSBkA5u7nnDNrqioeDXfJzlEf88oIaM6XuHhPoT
SBCuL5OWMnKYgufhh4pvxPOPKFbH59wvUCrUDZ02USDaNbnjPUqabWW6v/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-----
MIJACTCBlwIBADBRMRAwDgYDVQQKEwdFbnRydXN0MQ8wDQYDVQQLEwZQS0lIdWIx
LDAqBgNVBAMTI1NQSElOQ1NQbHVzLVNIQTItMTkycy1zaW1wbGUgU2FtcGxlMD0w
CAYGK84PBgUMAzEA5M7gViQs5zFAommoRgvO0d6C0g1dJYIycRl3UNd7SWMifydo
knPaAj6VT9/kYwuPoAAwCAYGK84PBgUMA4I/YQBXEfp/euxg0msmfCiXbnweOC0p
fSGTCYHajyt3VGWmpFott60P3fv8Q4B6UYBxiHFd5IJVdhkiKEA5CMNK1E1/Gueg
+HbAEdxIB86wU7eDNgxPIdaDmTkzwnyks28rTYdwVyEIY9257AphDy7AM1Je59ge
HGzXKonP1Hqhzf6I+rzv7Sy06qvg2N6FvLD7KaKgu+FpbZufkI+fMJWSdg1LQq07
cxGhr7NUQU1YEjtVomGwOI/3otdjnpLQDX+s+99Z7ajgADgE4BhpZlj3BZz0Ln2/
AFy6Vp/7sk1EpFcTMxVAiM3so9nfeVUvGptuAWzdH7MQHaiu6PDY2lkcqhmc/yCy
xFdFjNH0+0fgENGTVFM6hBanOvytZ5pDwpFIX4xbtk8pi7Pxi++fn/PaNFZHoRRZ
OQmX62cqeOyqBgc0VcdEcK4rQRED+5KrsbGVmv15fDqDRfdirIlzkZld6WcwokAM
Swn44Z4KnAxsnYHahSHznQWqixjhjqpS27oYMjycxrdpGV0vQY7+fogiQtS0p9/I
pno0oLzMTymBk3R0fsZauCxdyPfbyyz+aJM9XnMG5i/cfuLuGZBD3w52zc9bxddp
aJbJDuPqyGs60/aZCdKwgUC/GACMrSGO6oaLqpYSU8bLRn/3NsHlu2tRUlj8u3QI
pdt+CSQB9QEfzgBnQHxxuHQaYjL7g15vsBWCuFrYOyrEjANXB3B170fZc6PM82A5
Z+ARkiF/+h9sBh3RnQrtQk2loSjv5a/+t57HfcoWhyQQzi5KDtqVU+BhuIzVWD1U
JVEsniPXtPRpuSIaDM132f2LIOj0fyskwKI3gx0CmjQMg4KsvT7oYb+om4GjDZzc
bDB1waXbEshNGEnMAhVi12XUVNDdFunFawFNFUaZOfuKVU9fLJddRHRcQdZqIoYI
YXu8K11yGjX6gnegcEe4XDlr9VbtPwECOSvz1ahmG9YKSUTA1pml3tf1M4QfGhhn
x5GZWPKMJABnmxmSVsFRTT77IqRGcOBUtuDmVZDRxwNzcsNJo1aNt40wyCuON3M2
RSt0qHV+UV/c3MF1w5IMjZ0Dc2ZWJoEPBkEh41oGNS7w7arx601KpIq9dO5J4aXi
WYAlFJI2Nsmc4sYWD+bBijcHpGY8tJh3yKALYubYtnQRIlMM5i+qFloBHXfAEq4I
fNaXnZZlE+A/Dy0VEspkqC7RhMXALwdbrSYh6ovT+j4oOao2BXowSwQIrx1eBuZR
fvSF7WkRzVs67VNcY8XrilGvvLcf/j0Tyy0zi06H7nNSrBRNknaXzlKUJz0l74fV
1DOMYYDoWL6AZOathE1r5IlSo2T42ACWEEVvBA+gbuDmJIah2MIJddMwofm8pBRe
T8ep0ggd/06A2zh1sHY0KUplRlJ1VMooOiIFcblduY0qCwQyui0T8NGjzQBSJJ7W
RabUMs4a0hCwASrMviJ7hDaR6FEWx+cvi2g3iG4kpkU4X5Qotn/iEDZ6BJht+BKh
MnqoWiopkUQbGoAYSa2f2JrQzNQD4pVAPaDJ4SM4SbjDMHsUOdcWo24nOXqRoBug
Ev7h9Q8tcpgjJTqtksLvY8lYyThEh864+yuY0LnuGId+M1NblsElGIzH11B+BpW0
jKsYReKUFwG6MgNKpK2b1I34rJvRkuSznNkwlRS2Gbnnch2LWGqS4nPyFxtvnt+E
Gp8bJfBlS2cWXefCX54OPeX2DQHuoEevqgVF4eK5LxKy7uZX3wrjPz57xN5RH+Ko
mSdXL7UTB+h49RyW0d/PieyO9TCSx71Ix9AvKhGkv1Ur12caQZbOvAQevujCw3Y6
gL9wLMCzHb0hkxmTge21RQMn0a/6T+tewQwv0SiNmawaB4rnT8nY4BZubGa+eOR0
```

```
hNU+F3uTmsdpeVvQFDQ/fqpL0Ji4qBmYszAmN+HPRvHHrBO3JC8l6jh3LbF/ozTb
SxTmkIF37VVTbtJHvmpqSpBwwMOYAy+nZrOYgpyVFO9RyvWS1d4He7IKJ5MMBz7C
BMVVvHIStyizeJVX/5daFddjEiJFS1bF54Ybm/mlFpD5YkkacwEexgCMCb1mnTo/
DjSCp+zWUDxabBcUNXai3UWnHrUUZl+SuL/ztMM2Sfdx5NST42IpkvMi4efFvBGC
c33KHLCKJuuNC7vHkVJLg/eRjh+8kvTJAc7oel/HhPHXHGWUY1gHgAUYsBJZqUX3
067UTtBowjsXAg3lSUxvfACezygVAZZD69CRuPKBRYXWIsDXNdWG7EShX2WrwmcY
YsrglExexShYUQ6FLqa4XSXFMAn5JnzjRtWLc6D+EA2FUZjc5qPrA9vq/CykNP9O
/gFczf2sT9qPrbkZaOVi8MfDRRDosePHQL7cpjDQ2iYC3vDjsLqLSKIZmz4FogGk
eXmp/vrAiewlcXI5/2q6hUXok8yB8oAnzB9377F7WhSMoeSOE4IEhTY5GFmM7W4G
JeBbtB8fhBsWWtsKxZGkbwGP1MEJ9WZdMUHRdagZ6TjVW/hVFlWjoOTfjZj0F09m
qAenzSQWoYUn7gWMkgFOXDEeiCBGTXfb21KAu17CGJ0VMe50Vxv2D3mEhloU5GCz
b1Zd888taLu36xQNHoMXFrA3rUmD6seAGjB7SmskXJX1CWWVTKJthrtM3OWW81qX
wIagM8deGBXid+ZHy6s/YLqvuFYgmo/NBT0PVT85ZSqi/nF9C2zggA1v0S1VG931
4kOSGWL90IhOfCooRTvxSQ2rnUSZw95C0apGj+any+PUZy48ZUxOX2fTaXPYkUvk
SCY1XzsFAftVYJwAtpnYZN7+pVSv1tMni95RfETmF/OAmqDERPz2cUJH6XLZXAJo
6ScUlXtQ+KoWpzQ1ZNfHU5BUSKdFJUVLQlQjoRJiMLE0FchupP45Nz5+nsmCx++1
Spm9stJTRqNNKwLCXR4DwPIiRTp71E0AEACiIhSF2iIXXEk/GfSIYuS+Hrn15+/Y
riEnnwj+AopxIOLeZEPXL1sANotMi5cDBt0ZoUfhMBeR/gzIa1c2OPvxQMRWQ4Ik
sLnBY9f0v64O1NQl7bdW9c3KSOb9PJ6Ocm+gd4SyGDnn+LO7TFEFDVH2LcRbUmvp
NKmPBa6dteBmyEzjuCTJfH0KjLuLQCdfuqloOT5+JJVNYcfGUZV2ouBITT5jtgVJ
QpW3KaV90lZtzTKDy4GpC9Ay5iT2oa23hlfMHQ/Ybmxc3OCC/eZjR0hRyY7t7/Xt
sdkAyU0OsDa4Mrsgpe33IUipgjAD12kVqBvg1PUsFh2ZQoPFZZ5ga2nl3g2C7RAJ
9UYLPLgxuYg9mejPfNmqG3HphtpFAclMUvgbjrIJkB5+Ho0vITPBQSoAiX/a1K+1
IjjX06YbE9g8PkLkcVbX0+vjyICrOyzUhRi8mGg2zKHsltsYMPUFzaAzTwB9/DEe
L+sBGMWqUJ2a0z7bxrrg6uA022b0aZjJQ7M8M0K8FuvqPsBV0XHI90Ry8OPYRvhk
jCEmh7GZFWsSIcUthIzocvneTKG7JnSWSR62AaOFyCUnQ2/KlQqDDpG8yP1MqrUQ
XzT0tdFBSsSk3foFyBqBzeVyrPgaDztCIIwJzfcxS7/Uk5K7FtpMIVmD88P1KwyT
I+Z1Os/fy0nTWcqTQoEELs9pfPWMiY++HIFxDeN9+AsOrHR2kISXzacDHnfvoE+U
/m2HXyevSGhjNCD5A6sw7E/mawnCnJx/iuhty7HVnAier4EJ9IpZbzBkAkRxAFHf
g/8uUYxl+Kka4L7i3f6TPHricdbig7nC61Vq5PirOZ9zC8ZXjZSusNz384utKeBJ
NTNAoiaGRU3DBIPSoL9EW644AVjItMrZb3C91z1SVunkoGlVnsYGVx8bjScE6t+1
YdyzWCTxjaIVwVnEXh5FISQOkDy3Cv5BRuZt1OmXHCyPQNOmOo+t5gTHf3ocIa+b
MGg0YWIF6mtYpXnRzRNhRUPUjmfCwWwgNn5nfxtDUKEghrBrtspxu6h43TIsyIWT
Xd3CNNRVqcyaYOlJPust4Jbody3z4ELniIL8S4OaDYlZw20ak2njpyCVi3G3zPke
YC8+NMx40025SV3eihYRvlSIwrWwNlhASbD+uiqddI8pNHqclb0Snfk9SeFtWFOU
8JjlB0VdCdYvkkADnFB4tCKVJuPRbYXgtRXiFMJJXw9GJZioYhxx++Me9AX2ndJz
mI2gVhpZaIq7wY3XIk6lBJTCtQbpXqbXhFkqi1gq1ccabMt5JLcoZjGewpN/C2yF
WlXq7Gja8rxK12lUU+tvkNT8pTEEWgB2GAGLvCW0SGNNupbpXOCbztHzbZW04cti
o6qsg6+XV5a1p/2Q27om1UC+WyXT2L+/tgynLw1KsNJ2kO03FYM5HuyRTqIsPXfA
e/CD8pbYtq3ZCS5QBZgzl46sYkIw5pAwMZpk3meYNJH1XnkC1LOiygiP40VMLH1a
L0HRPL+hehVl5wMuy/xufmrUI2i6zEbfxQDAhCnNEXpFQJyZ9zH00sTv6Wlm2ywy
L1rBm3rBZnbskgtK4G0+zp54A2z4u1UKPUC8DZNCC2FNiPDY7gdDar195LHNPf7x
IKis18WvEAM6d23Tp+ud3kPy1WikqfwdjWQvw69U5jOLgEFxXtgIUPbRk71mBasz
l1btpGxU71UqarVKvUx3J/p1+atFXrtO74gHDdydHer/zGQBtSbInYgEjlOPZBiZ
Wa9TsS8Fmzsz986Fn0co67qzXbS7cFOnJqbNdp3ilycV2MHySyjuZWh4XrlWxfNk
K3JDaARxzpPhuAwDjI3lhRC5SdS9BvAXom8rgbybhdGMn2Dumt06xdGZ6XBF5P4t
Kxy4qmV/oyc0M9I+vfLXDDR9tBbvtLsbCjwTw0rXGjusvbZ5DaM5FQSgjSaKZNkL
Avte1Qo+ksT3QQe49mp1LwXIOHBGYA6vFOOYFrbmr4GBICqh+2hLBm4/gMn5XuGa
DoiWMN4ef2eF0MXoPF96fzm+kjUKA66lYI5eoxD7l2lhxvOBNo4fzp2OdjNuKPX9
UmxJ7EwEakZm6gaep6PmvB2YPf0oSAZCi1EKn7LOYf/XgcGTWg1z+CVCuZ0NDpFO
ZiJKS2VR8FdeoGoRwCc4s5Zs02f9wVZukteE+ZzyEaZe3Kdzehra1G5AEMjIPVNk
lzVZb+xy0U0I6XiYyglTcRaYNvztA/Z9+oOMLlUrjIM+AL8GVCq2UlWBUskQZEEI
F3jBPsyIDrUV1+J/pP3FpFP2yhmjalAHCFvZaD2nhsxs1NVYGEY9jw328+wqKE5x
```

```
3XMkQ8KbnzyTXy8p+J9KUOdkHa0lGAxXNKN8qZJ3Tb2NuYbNEbfCUuP5sW8OjMa8
IqwKdBx+pMA5JUcW0fDssu2Xi/3QurTKaws04+T1VCuKD/8cf8c9LJb999zeS7gC
VvruwkgVlc7w6Rd4nZd3U2XjQJB2tgXZkfCR32nXE4a+PINWpgRq94gXv4zjkPu9
feDNgA3QWlqGXiZ914YbuH5bd87C+c6aQjy8yj5HjzTOcBuE4HzgVJ92+TEZ+2na
fbXiDzbGWv5VKu5xkOSROWGLuEtelfDht6ocMmsSIZiLQehF6oxcwHRt7ZZGJpG0
4DrXpi5NRVmRgN34SqbABbeDEDPc1C6RSlxonUqt7Bexar1uqIs5lbBxplvb3mdJ
P5KdgBydnM3Km8KaK8pdHoZrttTnEqO8XLRjmAPj+HZiL5uQFRu5FMeFL9D8LCo5
pMNZCLH4C6FTq2/9pjXUOwsFbyKQ0kK6oR8WfPRRMYGWjDYbQGkF+7WxasEGe7jI
KopJKaokzHrAO9Q1QuvWSICvDqF8y8hMVOZHsOKcjCWmzvKYDAx0fKPgDwx2PqmA
aaC4R0GRsAWH+5tPXzxirFsp5inz2JGD+L3P7WhM9QnT+PN2W9bJbFKi8f/ITHlL
Df9Dk4Sh2Zdf6056x6A1adXbGGL0ABQjldLmKSpLdSbgzuJ3+4uwFsuVCuJeuzCY
NYppAZjx5/bpo2+Xh/USpi4hTCNHDLeB20EsMwLeGGQ8vlrfhFEJLUpWildadaF1
7EzZ1M95EJswF3mrl6IDEuQ/Jxi9y22j4aYuWgRmUIFFNvCvU1fQgmbq0sZFhfLw
uTPVatkVgNv8ziKyckD1mJbgGoEK4tk3mnpXLoEWoBpoxhbibQNgR7Gqtwj66Rke
B7zgjYgfRgtH6SaolHdszlddAg1ZD4jrAHLef222d5I+8eZcQ0rgoIg9OEUcxNwr
lwGKVvRd8za/FrmmSR5JJaafJhU8ZCulHWvKWQpCc0JECxjP7qza7Z0XBBq5An/k
qw5EXSbFELdgP37xR7RvQKaMXbGUkhqDEWMIfxQQc1zE92K3AFJrx1lV6G5b569Y
NB33Ns4yHbiv3h7zRlkLgjyGfsWGwZ/L/11zdLJDP07DXie81jVC6VYs2CmbJnh0
R1uRiytWYC301KjYTOuyER5SEysy9KXrg4//oNN2hIk80z2BFq2ldUtWDj7WFLZj
5w6LBXwDak1iBGJTMeGPfTnBA1bkg7ALTdGnHqlOiRA1ozxAS2AwNPbl7Uvr5AVB
8g9MIYvWyojTSlhsxNLnsgo4fff9FNlPCOcQfzonj0OnialT1nXx2/XduuSGaYpW
2bxnoNyZDjoWDIn33seMdfMlNtVG4HROeMQvchy1CeO8ajdYtmhdaGx24CQ2sq32
CMmqeTYmReJTOvNVOdQAAqS8EfhLsR0e7WuSj2hqU+SbMIG/EuuuB5Asv6Ri1dxC
i/9tu6+gbrymuV60IHVSgMZyaUNVUiojjjY6sUTTfNONZeEciYvc+diw+lgyQNDc
U2Z3IY7SxC0rYAK+b6+ocgc2JgdANeHUIUcHa4ZCQqfjKwq6UfB4gGnncBhgpW5K
D18IJFli5cZYwgXh8pOHkuam6Vpa5ka9f6xGY0YP7REg+U3pS7tMq3hs3SHRs1+K
jnsi4f/Ftw6uwDJOA+8K98piNefv1TNUDftyLrgEeGRNX9yZkXjojQzLIi8c028T
9qDqxpomBit1fh8NlJIWqNYWUB7UbTSylBCdvOEF6MCV6EwhfSsjqd3KjH/fCEzZ
Dq+VCx0WnkV0t1yktvKCJjnFRCkPYAYAsATonq+6BRKohTqNPCDyLdsn8Y1YFpKS
OLGOdBycB5TS4wBgZwaaEmmExPa3F52bRspYpuxNbbiE6dtKnyLGCK3phuywBBV1
DuI2i7CENOCsgxEl5UUgNMYQK2U+5eS0pLhedmx0zs7Htf2Yme4I2Vg/zk0RTv1a
vUWwow6zIV4mJPEBDsgTDdE729DJeejafcRhFrzn91velhIYPyw7E33fap+LfGA2
8N430RgNvghiWCj/F4tne08kFxFeO4fOquD/92aynLcWNHjuuGKXzqXKTPGvyADS
LLIfNuNwrgBiDv9tPcBNcdQL/wTPGRe0WbBcviKcIr22Vz+7LoSqNqjbd7jkNTmF
CkEszQoT88RLnGd+htNVu+NIID2AOJillCJicAJ8qk938pkKnr/h7gcBfIQrmJc5
jX/xb6IVfT0qGItZ9rfZ5Afht19gBWXtoKxnBMMcjqozhir5c+1ZRBFgoBpmc0vb
yBQuOZhN5i7PKmjDPVK3dyXNu3IBEQox2BQMStTNR75NUcEHK9liNiGca3pz28cV
hd4+mMf4KX8TzAVX/j9zoysiSzz+49wtPGJHs0EmlbgwRfxQG8sr9nbT0Bet+Zpa
9eCCzWdC6fSeY8DHUIJA85weJGpr9OKFUGl8nOBk92ld3MFifchGEZ6CNLeZ6JKj
qs8eAXfbKJNFyPAUX31qVr2aDdbyoAThvA/aApOWzNCgkzcEmD2EQ5fLeXVleNtI
aZe2rs7C/z31cAEOC5GrismxnRMmV1GN3sWizoL3MUT7O8xmvFPE9natM54nnEUa
ph6q4/RdSP8ptv2NdYWCOmAf9OMgDVmY+gEUvReOCBmDlS2xt6n4vW7HpDMV5dDz
EMnSPyNVzsWOon0WmbcYcLMFvHgzA9asgaAi7Rr20Sf0D4IF1EtLBDS1lnRdMezM
iHfxqMZrXROdTTOIcUCeH/BIBYUqrFpBwUXu+TYlvKMoij4F0EkTcfpDU5n6aB2E
lIAyDxJ/FJ3BT1mV/SVgsAW6vrF6XPTyI5y8q9U7gIZc90DMP2cgkNMuCYagkhsU
cop6IWC0Xa7zyQJ5WHAA6APiX3gmb03mamcCYt/Nqcqtos437VQvUrlwqItxPXpT
Pz1UuKjMJ2ZZHixU6pvjdsew6Ezp5/znRP4BjhUen6HOb6NEXT8cvpXic0BfmG4P
/sqYCaUS94PQEfthO0LtajfUvbhiD+fNHr0cOUtDHhubDriBw6M99KZpuSaQb8Sv
7S+wf2bdP/2616wSjL8xQCZtOnJ+GE1gjEerV9omEw3d9LSuRLOwpN3dplNxOegL
yy2rUkxfAXqU+TRoCOjG0RlG4AqibDuR0s9lvk6/0dX1y2jP1iPAD2OBp3qufJme
H8jwXRfDjAOAiIRtKaReDiknVjkjFYY0ryd7w1tOC5mhDj/a94D/083ewESu95qn
IW8j6869nmxgj4vBUD6kUx419gT1zo9uhMsgGXpGARGdgwdSXPY6xDFLIRgjyKn/
giqlj5CGuPlnv5iY8GiK/Z6kEKShlqS9lFnIkuxD+a9kJ6hqezeZJRrGNkvCvxWS
```

```
1n8VnWyjGcKKXLPfKFFhUQONiqtVLyBckTbVpQ6E1g8c13htXXoh0+sUHxIwmK/c
oPtKNVxDJRkGokMtQXF72YwQceHoSC4WPM2cKMKcG28QvRuoz3SkiLgqTJEN0OCI
6kJlcBezduH7vuab9hacfmnC8GieG0G2pNQYODrEcfRVieR0nsFEDKbuK/M6fksj
No48V1etDxe4nO21Fv+jdvD8Lc57+3wsDP27nTLkKpSeztmkkCuCYD1YtCThxMaw
DnZftcwwHIcNhsrMmkgcmsVa6J8N5eXFBNwOh1tq0TQMc+/3XgaZEiBAYdjvzeqe
3IiBDheQ7LJIb4AZj+tJq12hGko4nfJjiMRW/zdA8gj6AfBe5QzcfxlXBFLaYsbj
tjt3+F0qXj+DNwbSmM/71g5WKFjNHMrbIqw2K2vishdPqt3cc6KBWfIdTYT0P+aj
agCvgl0TyKOvOot3mcrQkvaFi4Ftjm7Sv3vxdI+uNc2YYPWXIcHcaG7z4V+xQ3g0
ZZUhxS5rRhmc7EVHxe0WX4OmYlDcD/PUcWz4AwN00LSZH5pd++yudIoqCDAPAd3X
qFIPhxxd9RywETMHBee6HYgqWaofhVGeOxrnJ7w65EnLVfM22dcFOT8Qkh84mCN/
Zxp8kowHPqc6AOlg5if901w9acPn9Z9bJZEQDPM2Ay8JmLpQJ75mwgAQ/IyaR2CX
zCwPfEapwUv1OiMrrZdBFBVjDT6DL6Ydsbma1wMta+dzMSj90kLWkAPA9jqedmi0
18uMtC5CCgwaKXRetywKXBQyKRuHUu1UhOhACNSx3CimT3PcGo0Y8izuEELuGkfk
ut3XZVVK8jv4309PRm+xQjr9y2vKL6BbDyImXFHD6+Y1iSrEas11jbGggmBNmE3L
cM7Z8KSbsDKIZdVni9m35MhlCGOy7SAX8IgE90jf7lVlRgRft/oANdTP5vWpCXz+
RRKseKZ+/O0jw7hmRUt90TXAXBSXj7dLiMXygoL7IqDw6+FvcZwRXnKnGVYbOm8a
gkrmYSw9glmMjpg17WoRuMJZvSSpfd1BlUgWnRJAx1xivv4UDaefaDdf+Z/3FAue
puwcC25/Fpj3VsqH1wngcJwm6t0wO9L0GZHU0oP2kB0ads4TzB+6Unb72bfvuWv9
jbJLibgTT1BlaCkuC4Xh0RCC2DrEtkcfqiUsYjmNTYpsk4dc64AtEkV0Di9gJNph
ISMHzboakEmsm4xlyhumU8vAvjh6wP1ajL4D3AhVkiuSn939BuXPUrTgKh2yj1Jr
BsWL1oAWKUspmlL2R9Sv7tHonNS4b1v2gMoVswwUtLhPQ6YtAzHJmT+gQSzbG5XK
aNoVTlrOxqiFBURlv1i5JlPYPH9eOiSTshtPa8iVeoH/7fBCgkHFjhTEd/2v2piZ
kwgdQGQBOYs50XNsn7sUeLECSTXjzQoMTXgfoNdMDlAdZwYBRp0dHJg44qXB5C+2
LCfOd69JBdL+hPMBLt/V3J+hhsvJOYATi1p5Ycl6rQ+PHCzDYfqvIcKPLR92ecUY
Mw+cAi/X1+LOpO+stLrjx0XkaKrziqbgnjqNA4YGJ1heydtmHxohYb5b+oYrcDAT
4+5oKAN50CIwCX0c8QbytoJ5NMEKm71lSX0c5DB0/TniyrylmzEJIhQ9cjjdCVDX
mzYFkCdNkVFlR1QftS3k2Ld0CMPzS+snBYlUdclnJ/8x/xrXEqu4JJ8qaW84A6WO
VxwUF/SLbSVCWC+5Lrcln9eVWH5fA9M81IFwdt5GgSiQf9y9TMtDyTobyQ68IM8t
1pIQWZKfZFy1fdopUIZWICxfGFkvAuF1g5DjAB7PHH+mUDHnyESXa4D329JC3iE5
whAq3d7mdj0byyK4jM5e1LZD30m3RSbQHPsnFpX1NvZb3Rot+BT9E+6S2atIIUgc
3zTlRlTXmv65hSHPnlyzLno6rreB5T0GweH5NPZluzr3t0hat93psOAqkRwrfG8G
isKPzL7B44uFBj2fNaO8YpoRXmRSJ24CLwa0HoWR8NOhVd1MT6A9zznV2irHFasp
JbR9aNximhkBXFvu90uDEM4cBVj/YNmufXLQ9ANcIWmwDMKRwfIvklqO6jakRt2N
pNgT26HEHzxFvUYks2KJ1qwzhUig1gkk98iV6h+uwoPsca83H7IEMXtvZXaflNxO
keJlwAKG1C7GTAi4ePfx3agGrvpM8i0s4uMhpx9vYaSMO1QIOYeGrJLakG+eo4H0
hsMpO+8W7uF3JA2Nu2NjP88x9KFHJXQcvmBHGYUztnaRcuyplevropM7h7Uu9MEA
Qjk6anE42IpfrfRXquyhTRCgVc+5D2nPUd6pAFwX1ujftdCFjSz1JRqjfZJqbitW
+Zf3thHbCHeCD3qQwhR1gCrdxjuD4YrqNJ26ua5oarVQnd1C+riZ0UfwbbaW8joX
uI0/CDBlES5T5qGHFwyeHNhxqdoQB12d2cWEMIRKdRaj9dF9MXkzNx5LQfyYCp4A
+LKKqPENz1NURnl4U3ZiqU5W+ReZfPuPyODp2OGuJUURtrMXp0asFwwgAzplmePs
5Ok6bxd+Q4kfFrvuxM5skh0g1DLhI66ByP91CAb5HQouXQINypr/q/zPLOMGtsf/
9R97V20/vS301Z031nTDMLZoabMvB6zK9umZabAu5VUc8zXgraLu8w4xGvePpKIM
Cy8m9WWcodM6dOWEv01baDzzvz9DfuzNoTU+KIvMCZLFMoOG5Qz5RMqCdVquzAee
uZZH5MDIS+sGb806S/Vkxy5L2J8N+KiPQj+Rtr2LPn/6NZt0RCWaeUNkZH110GrL
Q1mZIB2Wo64hyK2TWR0HldncYyMwUxdANNfTE0Zfk9Xg45VqF+vAfAUZgTHz/K1f
V3E07XkE5vtlXhvUBUiCAEUWheWFf8/zgJ5ci4uj8gIaGFIeZu0h3NRsMPMLP9Nh
IUUvWqiuT6+jrq/P/1zZyGFjTYX0iBOTyuUOotSQ3ghVyuaVptph6MwcCwodu0nj
Vm6Glucuc0C6snzWLvTHt0i+IUsf2dm0p19aMGWe6JeDdY09U0RFTHgq/DF21K9z
OiSnxeAj2GxE7QRmdwdGPExedwficpr1NQS7cHJWA69Xq+Gy97Ayflyz9FDOBMso
78kWpjUKzi/yV9UPBGTCTP61//Eh0ukD7+XeJE6TOp5CkGSdXyfFU2/JQaktunlI
r04dciv93FStY8zLZkJ19S61WMrtrNza5JUQk0dpjO1RJTf4yLjoBNI7TRp5wLTj
mBhxilU786BXuB3VR+G2ZVABFmr3N/M1fyOLWFDDlvRKu0jjaYxH5jCBW8ueblyw
2OK/S+UhgcB4d5INqo9FGc3P8Y/LUMV+1KD1h1wWMYKu+I2wLgD/a2uJ1/swXz9S
```

```
k0e9IZAl8u3gMD4aSPCQJcO8MYbWcohH7Kj0DzuPJUDkrEvTHgpAmxHpPr2SDMdZ
E8udlrH9Jbaxvf1rp+VCyusAFLguWVN/9JuKp9qOcIsBIU5kjKCLE7o+JN8CjGqz
dca9CTNeMnZfMiEJAoz6+Y57V1Nq+FzRnXxlDesp1ks5P2vUuyrEOrfrjYJ8S22o
qPH6dstyK8FY/wRtHb3oaGAZVrn10a2/Gp42d1/WCI+a5eJM+s2EfpLjgDtYFQUA
t/p3L9OvBbkDqBzSQUQBFvo++w/0C0iz2ZzJMQ6HXDaxdLTWsL1xcpV0HC/m1ioX
bSky21HSUEK3D/h6alzaq5rOTEOeXI1NK9UeFwSWwUr+UY6gZl0/CIr7rtSAlokd
FWaTulb5hU4AsSMTljA7LirHrDbHEmGlq0zOgttDUbVKzkdvk+7UO57n+2GpOCjj
rXvF9p+mcthZPwIjkxBaEgCMHHYsfYWiVqKNmn1l7vtRc1bZR+xRWtL2t6RVW8eE
ha5ujQzYwxthxoznktQ2PQ2fuuHGm1/DxNNJgVv/MnqhCQsocGU4wtFG9fxyqQmQ
QO3d4myLfK6Kpa3LoaH0OX6koWpD1sc8Q3QTqxWqF4Zs7jRQExzBNIem8pmxexqs
7eDrojEjrImFXR2KixfBiUJOST/2gb0RVmOByImhLWwWFs67ckRrOdbsQyRusESU
RnMZRvnK1VCjySwIr/dCOVHVT9XNDNUFEaUcIr40WNxYA6sjgqQXmmFxfMKGuRDg
cZWJSk6t7oVpRGlY/8bMmhUyC1qKEpNmSe0pIxE6Azq9e45mpQMfK+OJMez4BWui
QGGJCyKiodO4ATBbFPUXnfk+LR/C1kec77g3aAMKuCPxkCU4gTnbpZY1M2KI8ylQ
j/WM+3YZLRnPz1rQPQEHy3lpTNnYNSlYC+3EvcORobZQJSJsa5QFlWX4/d3LRteR
tScSiXf04Pt7mjZoOY0HfOghmKZisT3PBTt9XKOYdGW3QEzuh/pDFMjzKUSSU3vQ
/LSX5I2gY2csGKeq0lkwR20/oEwZk3QKFfP68/nv+BBs6wo1ncaDTDklr2XLMAd8
xpMW+UBUsVdwoXAa1lvkNeKlJeJuHawN88IkHA8d4p470Ig+zyFZcpk50N8SsVqy
+1YhLlFevkH6bhx7zHoxihCT9oXAPLaqsR1LNLxOUS5RSqestlLC5DZvelXYrHhj
jRRjvuzHuV3pJHyo3ii+Qn/AAFneeVG+e7NOzw/9cW/gAol6pWRqFUb9zWhUYR9k
UlmOS0DGkbYnLL7kTYOmcq4FhVLzNM0QaSGo/FvTGJRQIyNGAFiQvk1xYZP+nSe1
zvFmZJRjuNmsZi8902h9OnFqeIIkofkBcogWhTM5OB0QZPTS5fDDA/nIDQZ1TN+i
FSuB1npjyoAHNCHM35/ugxRr5MwcK/E6YF+Gu3rh/yOlaoFTVr04mwAamgPdRPtg
+kgExx6vy34t0Ex8gDwIctHf4Y7y4pJq12FOvafcMuVnIiEa8+dbPKXEOhKa0XkJ
dy8xuyNFBcyIiMlS28QaSBn/D5s0qgNx/IPRokWF06m4Ry4ANcpP3/vJnDVKbMPm
yJb1pF5hJRnslzYS9yWnIHOZHN+bgnMhIdJ/R845xSrEEGc7HGhyfiwzTGv6tQU3
g0pZCmHvRWKJW3N8y3FBKPx9knzv0Yhr+K5RR4F2aaAJBf9xMXhtKkKWVWBUTFlp
uUADmX0pKSeXg9sfIBxiDaCeZ1ocX9RQ/XbvIV52uJP6wPO/c/eQNZl6VCSpcg9E
t35Ep/j3rid0o5pt7T6GUvT9fLP7AzAPYyt/JkJ6GnLlEU6RO8OQU4p1yYSwvKBl
ZtZ5U6ZKomhRiHa/ioYqg/jK7l72x8TzC61vHe1XxlBEW6CYJ7rYsd4Bwr5T/kau
6Jhd2l02atFDkuyNUiIBHUjVpCMZcpilt1M6I3aiPIcBRY5AO/zSLdU3KrCTVeg9
aFNpT48FUzC0gCqeAVjuQ49pp7Ew0/xJE/ZgClVpZbjFwOG7r4diqPC79neMgqWb
3iArHv7T+p2w5SJp87+0+Jy7U1gMId84eULe03A/YyEJjlREvRFxp9qs5brD60B+
S0X7MTQwxSfMjM+hrxHnPfTqqCK7bgWYWcj+R8qMCbbRQW53qxmy+SwGY/0qGlti
KvFUARj4DrNdBUQOZVenXB9rwb+IKnqD2F5PUqY5/ryY2wofCfnLOaI7N9+ww6PK
y+f6iJCK1pNg7c0GNiYzguG1ZbvTqodmA4DHdnoOH3PBCVYDtC0rpwy3tBEU9oIu
6iezIozgvV1gi7HuPIFprM4ePGM1al7F6SrzeZiv0uvcGM6n0LdPemwwGyC9ktAk
v6hk2iLJnwQ8R4sGAZqLJrtYpQxdDnghzzyWhdeU2nG+gLsEDeAm8FcHX7LXQc/L
x+JRDj8RseywQwku3iAGGxUNBoTvRQoujyR8iOeYRpYFZoD6ic8Wnag1/asAt6wV
95kzEqCnZMVCsh3wy4xRy24F0xw0BlYkXjYFXTsIN5FxzHcBavQxtewMc54RhwT2
k/SL80jFrqYPr0tv86uP7GJpMTRxZ72fLaTJJ4VIsuvcttM2umcN/kAUjUVFyHIE
Ml29PxdVzDyxWrY8FeNVqSX3IWUhX7BlDrqHV4uJ2QkfDBTPvvpTbdScxqdE/WgB
ojT901PCzkEW24z2bL043EaaoQpfoHV8F4r0op3V9tpDLcn19Sagd1ez3v8p7l49
GnpL4kkgA/VETDjttRnTz9FTEYpPGcnFolNm/eZKHX9zv3i/2ard5rTMx7f+HsZx
AHiR5E7eC/qHyXApMOYCTXc8I4NcEX78W4GFVzuzuXgK5eUGrDDrQWLY5B19zy5U
DXw4eUMRbrmyxp3DtZSTMh2Vf62Z9uCMw3XgVwU3CveiBAq5vLRYWsRw5ojzoLQM
GhoTXr9yRf0g2kjj/IyOu1MGMZlrRxtzFh68OeuchnNxZH3VVMlhUtxD5JlPOUNh
5pT4iS6l3NYYPZFoGFfH6NUkfPp/1GmwMHigzGIZvxjhQh7hX0bZK+5BtE1BQbTS
QyB/qxBnfk+MQ1IGHMH03Rlm7S+mMXtuIoWmQvPk1rumLyQIP/MrXijpKGxnGnLu
qArIAOzkmNkI2yr6n45lvwYMXE9gvTdTF5KzlG7EThq1cli9vi0ogu95/dqcBnAo
hDGDeYy9/NXGVeJ/4joR/QnAeyohnHNix+mbSgwBmCLJeoM6tvKNtYodE2rBCa4Q
LR90X04CfodsmJadOMN88oKG6sEyxOYefI1VYD6+6YNN+nRmTnnSJzJXD/k+lgme
uzDDBpyLPhasNTEMTs5Y6LQf+moyY9Fx/M8K5GUBXM7DVLkxYHceJZSwwUvTbM8i
```

```
0vcOtIKdarnZmOayEAEimtd7Pgl29Fuxmv5FjgH8KadfN0eetNlMzEz0UryERwIh
/4RE7u+HSwLdLHD0zDWrtLErN80ujdY8726YvgWJp63VhD/1UKUnAw3J9HLCJUcJ
ja8HgQ1YTz5OJhmbu651+z3MyNbwAty6wTwxKC268oJ/HGNt2QZjp5kYwaI1jq7J
7qoT0amlF0n5W7Env937LDiZEjNzzphTGbdhevM12W1mNbU1uZXz1cPjWqnage9O
K9d2pMmlryoq13baOXulGDik6+yVhjjxXe4qhI7BjWvNgYlOV1yrtUb5mkWq2+PS
RW8+uJP28KqQAo2jqK68KgY1d33ffuid9uPKU6HWBnP33feIAgx+zP6IAJQ/i86O
6tVwn7ng5G55cL6zrddvHXzOy7ZT8e0emhzekdKfpDnS8XswD9/oczq6LFxM37Ts
tw+YdEeKBNRQ7crq3VoupmwwiUiCVrXvtZksQLjDx0AcfQUG8PPCGyZrtUUioGFf
2gvK/by5rfF3zlszSx6/dyzMkGPiufL8GDJUoWIc7aEcQ2DOXfrxjlLXrbPrbxvC
/WoeGX1u986EZsVIbIW4uqeFgdNeAtleq+1Bo4QFR7Uh4zoPaWRqMW56WOlfXf7y
fFwREu+JyEDNLnaUVW5JNYg0QP0hUaiIG2eL72Gss3PCTQ18FqvYU7OqQ5xGP7BD
uERwXy7qdM5yvD3IGEavW4FwezPS7Y7iOP7h7GpWj2Eh/b3PFZGKfq6tYDACQtYs
pZ84X7rwrzMnhesa2cGDN0SAk7dhW8bmsbK0ZB/GuXeCO0I4UnPEymYcSdnkVqCV
HXAn/XillyAMmFRzgA9lUgcCIoIFDnzxMi+tKpuzZQjJD7WySTlyGOTPyrI3KBo+
JeVjF2aZmYCp0t3JrRpk3O2LsR+qFhAy2ZCmid8wPZhbGWiu54pqBq4vfvNDRCaY
MzC6kXLqiMFdRZojQDaFrAiqqC9RqvjbYkBaTEylmyNzRzTzrujEI+nOpDULCVQx
JPOIRtH0QDX6bvqaE7sDHK6fRWIuuFxBY7n1IbM6/PjVJeeasQo+o/g9i2hbfzgq
ulH/KNFHFG5jJ80pR35sk1i2hfYQSpVYr1GL/PKKOEOSkdcrcK/eXDtKFvKIvsYK
i/RzlhN5NUj6nmAVd30mYYBWhxZWTbsn+gBqfqOZOahLx+VHLMQM7Icnt0De0/8Q
Ehj5/ONvshmr2y5LfgmC7D+J5zRadfIOKzPpcYRGgYFPkxYG2bTnVLKcULpInakF
3QoKxrDRqI3O7SYZr+/JyEktelGNyh/nsgsE/S2kz7kMfdUALB5fhEOqI9AS67pY
ZJgKrhGKlas7aQp3D7ZGgGVrs6GiBlUnfD49JHqiFdYdTixr6T7Hgs3ufuQ5rSQZ
eCjt/2br3Q3ttkWTJD43MXHR9PMNGIEBJ/RehN08Gy+NfT0Y2Tb274DdQK/tZqqk
FXH2GOzpmeUSEupOvNP+8yF7MaMuDAkgbio1F4UpycxhJVRs2P8bLJxrMnYfqXla
adSnkFQigcGUHgwfuOQr6pB7Q7zS6Aepyv6rvM95RwC19h2r8/9UEh9cu6NEFHAj
rXxDcPpYqng9AIj2U1OVE90bDAZZtXd3+aS/i9aq6n8Ly6GVNyuv4htd04YWGZdk
HEJ7YzdgxSiLDoTIXKiO172R1ix0OEBBAirv5VJCdj4rCgfxHtxaizRMEyiBw7dl
wymBibj5ssw5dN1haue3WKFa/IaPv3YWjFa5SQKy3ivQq5stNhp5IyUIXseUOczs
y/t1aAuiigxGUs5gj8Q1KqI0AKjvJCfdsiPDjlNnCkxCqy7lgWMDGmPz/hpr+a+S
5Xx4rxbQ2t2k4mb84Fa5BzUFRPgFjWASucSc/ACrdwb2EtoidiwSW4C2MXdR/pOY
JpYS29lP1QqWoLC4AHNs/soNL46DzYBCCn79qruVdBDcYScOuUa3qPavq99950uR
ymVZOyXCgZi1scGqlRDfa4gF/HCqKM8E/7uoNFMHZwSZ9UGjEzizEr8KDS1xoxDi
mXsV7rrovL+ThgD04bywC/XILTvhL1yEGLdIImfzPcnsEig1UUAkuC7WNQMjBHMo
Myxy8Pr33pvLuJ8IE6CmBp3HNPw3gwUWghNvR2lKDANLcYrAQ3RUCWBvSnbsba1G
oDQVP7qNBOd/NDx/FpKY0k3guyizgKZS9z2HTvttTW4qvHY5UGzpep5apDCsC86e
lmIqM03NRDOxnfus8T1Z7bbkbOyKBbX6mjuKmKQVOrvQ/jVlwSiWC+CGtJ7nHbsU
kkBoPw26eGSCWOFMcJZCS+sB+FKX0vSL59AehVm1EE+1rqc2YMCbVSCYfR1mIjIm
O7/AiUva5pLwyOvVHvEgx7Y1+4uBhs11z5SKGSSwykGfHAaY954vT2fmmpmfE5EF
Ozrd5tSzrosW61FYszWFHOUKPg053R7C1nLI5aDgvb+UWYhXSQCOBRQNAPSoPS04
ts4X9Cszp8lCyOApivZqmuDJHJ6zVO2wbHxw4gumvwwr834pziTntpcFPAzl4zZV
e+wRnPr5/wwmd98qrWEdc3fFEv/ETPNQXPk4t+WRGVNtUyrs/Uh0DWv+Anga2Usp
a6v7gPqe86P+d7LL0zsHkjrPpBDwrmdD/Gt8UnFaRFk6yMnE2sbAXTm0U9Dt1UIp
a5RNFjPvKTvnnPF/O7GJAWV1qSRRRjVw1b+Ag+Pk82TooxKdNb70Vjo3ijpa+rmP
sVrW2RnWQKrLmWiqY41w1hOUd9IFaQ7NJYv9YpEle+zcLshRJSMPsfl5iOV7QNhz
kNtfL9sGrED7HhMugOhYlbezMGCrjyyzVIB020DhzflxnXASsu4URRw+Ov5HMpRb
gSRR9Po1p0/CrXlZJKpv+donQbM7YTTA4xDZOsPcN7M+bMG/t7MhrtjjYOGCu7Ym
RaVlaJs/QPl6WtG0r8HqhxJ2tHDcHGoYbIesAfT55mxEaIJpS5XDO1/R+aLpscG+
5bWp5qHfjugUz5dGicWaciJTdW4XePCZ/UIAVbOEocQYuHfYhXJL0N4ZpcA4j0A2
YVOD+dSqdzLDX7twQcFe7Ixma+5s/wgs6tfZWZiJoqn7S0dooHo98hi8dd1ZnC68
URqwpI/HRox18+xjV264L4gLT3PRxF5RmKmcrzIe4QDBOIj7BDJeZEr/jK+KyEwX
X1NhUatmG+ndrMRc2CdU5lMyi0Bx/1egCQjDvVtSigfe01I/dGr4m9Wn6tf0gJTE
YBk0dgo/5DXtOnXMZio9rVFYuRbhKjhhWPJWcUBptg3epzwntiPHwA3U3fiP8Xhs
Mg9HLQ8ppxw8XO/+wfJl4TLZcdkGw8osmy2capjNvjP7QrQrOTtlBvw273B7Dbao
```

```
Ae7ySgN4KV2uCS8thfDbeiL4EDkklnEpvhdcTSvwjZySbptQhj87tpxZnJsPDo/O
X1kJpvyRPnqcIjrHHWgf/mOajNkHsK3I0pCXcz501lRhhjTxVQMmF5abMPngi0Uj
qNbog72ShxedFjdJpD6KsynMTiB+sCmjgJo2Z+aNazVLe7LrAn/wTAo6VgaP7TR8
DnctSfKXQTrpO43uLgkn3DJo3MvJBkNt8JP/6zNaU/FQ+TMPTvt0m2pipvbqQZ6C
vEt7KPU45+ZDSV44ULaGcEPh4WUXLgKNAQ9PGH8VexF6U+v9npVHDM0PUSXwrbsi
G0ZDHMfAmJv9z6vo62yMGqZxYnV0xRvYLtCXrlgr9cSJG9G/ln2hVC0POQyx9NdG
yTmOeDLQ8e1/6ioSYR88/9LxXLNjGZcaY1/o4S05b6zbiP2Y+aag7DX+cbJKYX0X
hBWLX1lEzlAqKbGEUX1lEmyVVzqjPKSeiaVl+izXW93KrrkYeyGuYmy0uyqm6Ykh
UUyf7CEi4GMgWYy4mCjeqyY+4efcfG4lx7uF05MX5AtShY1QRdiIqSeolTWemsqU
rgZowqMVkVdMO3Kk8iQoOpz/+XtlkqpvN+vCg9c/ynX44PLsI/lVb/v4SJ5lkoyJ
0PKPU2Ui3qE018XdXSytAMVFQP2iuROTQPy1+bM4pmfL/N1T+fw5Am0fWRXcvljz
GCkDGOEW00/nZT/J++jJV2EasEj9SxhOZaar9s+j6h91hIGELMRyzGqUyiSLveo+
KQ+oDTfBskO/IfBbvNHM4m/l2vG3o1STMnHxu7Lrn6Aonr3lWbBAfEjW7CGnkoGU
jx5Nw3GFvR7Ks7J/mOGLRfQNDNkXk17enoSA52ifvAzH8C+0AynG+c+luC2T6urK
6o79/ZDH5UTfgveQLjfy0XwofVC7gFrbPaNtIzL/ZffJROONG6iNjGqfVc0Ktw7Q
AuZm/FI1Ief3hN2gz5w0akfcjQZSlLSWQI97Qwm88fD3i9XsPSJOO8XhlpFT0qoc
yXGiYye07ZHS+cHhYepK3Uv0Iq5b8ik86sWwyesSdAfuUkrOmVmYrbDsl4WbrbZU
TOcuULN2X/pbVcIB3CaKfSZZ1bAe8RfNc7gWCY7Y+JV3qgDA8kQtlGDZIE3W8NGm
pL8umQcszXzKcCryEkfCtByAHJRGtZke4J+/C4Vos3TSD86IdSR/XOaR6ngl+HQy
q0rWx8buz1Fq6WePbkVO/fHvzuSdGGOo9Hfa6KgzrRYZawiAa9ItwlcLgoo/CTL3
+gWMTBgxzhNBRBkhgH+S1/wExzSjXryeci+oO8+oxq22avcOzCTdNsolEUIafsZn
F2GXEzP6p4fCWdvcYmN+/VR3/ed+oTxV1m2ql1DZa6VLspiCbPOnd4N1JQ/m6RgQ
PYUuNQmvwpYAs44OqUt9DhfC8MGAIUdQomMLeCkpNGFmECQb7nM1ZjixpEa5UQgy
9r7oB2ZOg43ynPuIt8e7zOTFPtXrEOuWp6wSFoqRLSOYFlpJOD31aH+okuTtnC8c
m/BvnsTr2oKMtbmlzHuV+KfURc76iVKXGCrJ2Vjb5ad7OjFOPX4tSMT1LzTGT22q
Vy/14wHPZlUBbwbTlh5iQfWk1QlSZvLcnVqIUBA/E9QffN9PQ0n1ktR3BfboT0Sp
F48jYYsgyqw/STiZVZSEUyu0bRgjiIA2uAgxUsf7mc3t7rIbGFfNvFWOAt+zVp+O
4MvCKPpKyAqUxqi7nNEQtwuUnYVXaw5wSJlzwnVFLGU7sK0AiAmg5cqBsMf4vUGj
7+Ml+KqcmOUj7XJOOs/T2dPblU5kix932/z5xMFHuhwMdhvHVtHhKw847G0k3GKt
Djdb46LWlOrza7ZaeNpQSAS+TYJK3I/u/OXp3OSZcV77ONJ1CG7xVxnm2kQkCsWv
rMJocxuRG4dzWET9X7L982rG3dcZofNjIHCwHBBmG61mBRfoIiTDPdrlGhJzQLKC
4N4p9NOcDyUhUHJnPp57MUlK46JgQvXKAq4n4djjlEffhySR6UET0SX6emo1sO9h
fFIoHT9W8fxxbYKfvWhxpq4tjk6d7Q79RVZOKKto0lR2hubeCetucuJxFGLzoqgv
PDwjNH45EXfrN0/aeTyQ8NJayXKKeCxBj7/igqTYdX64k880Bawy5ngGTXvEf5J+
PDn5UpWD6Q4IakEp5i+DX5H6t7WAPWOMj8t8dzJWTUyPSvomlhkRLz87w0XkZY8Z
+c0YxgCu0miryEJoa+Wz2pvxguXtigc++g9wURsQxnfxlzdS9mTNEbT3ShplyhPu
ESVLm4MNu72Laf6dr6mH9TVWPQWVAKxE9+TgQp+l6nCa0DLieiul/rkxrs6+AfwS
JkBXUwSpQ9gwG+YHXTsFzDWW1MWiGwIgYfE73FmcGqcR4rWkx/8gBfoznSWYqmCW
xo7eygtBErm+QKQy7ycQYgXEkLDTSmRBvi2lCah92OI9T+ve5sXz+0lFed7abKRQ
iFBgbArJGAV6UN8puwkisIv6PDoB9/X4/08DBPOZF5JwjmZ+aoJel12ovUMIHkCm
mZlemcfiGiRxmdQDH7juZ8BrHIKk0wOtDjPZUNFEjwqUWaOXxjmq/pCc9fPmG1Wd
RWZ8Gm/fvohw8Z7ngJX83Ah88oQK8nIajwkKRFyz/stpHwANqOBsggBblkf9qvLZ
CNLC5ZnhTaMNsxHMZLGIoxV4ZLYXJh+5lLRqPs2UFTDlT/sa0JAZ2ac8OrXhbby9
7NX5Y9OqRwMuryi3DMOFP94PipAjyjg2V2Q80xc=
-----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-----
```

```
MD0wCAYGK84PBgUMAzEA5M7gViQs5zFAommoRgvO0d6C0g1dJYIycRl3UNd7SWMi
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+qOyW8r/2AE0mRroMzeTO4FYkLOcxQKJpqEYLztHegtINXSWCMnEZ
d1DXe0ljIn8naJJz2gI+lU/f5GMLj+TO4FYkLOcxQKJpqEYLztHegtINXSWCMnEZ
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
LDAqBgNVBAMTI1NQSElOQ1NQbHVzLVNIQTItMjU2Zi1zaW1wbGUgU2FtcGxlME0w
CAYGK84PBgYKA0EARx6ql5/SCS1BkE/R6nr2q1a4TrsEJfEQdER277IRvZl3WPPx
y7jSJ+z9XbFCVc7pYvl85Dk1f53xYmhB4371OqAAMAgGBivODwYGCgOCwsEApz76
Z2zpJ7y39dSgHUjW9LFSNBN0J5fAsSjtabIGmUw9/fT58W5xGXqMXaCzgOvzQix5
+m82L8WD9kdFX5bd12ocGTsc4A+sO7JB+O9raxZRv9CCveJupBoLIv0+PM/aF1hG
jFd3r6bY+mJDtMO3yFbAAgJkQUrH/F56D5rBWgxXvtgRxjzubcFbNeYV9ekyZbu9
QBiKM9o3JbuwB3lGlq1iXpWYoiKIuBqZmamLZI6TT61mQB8kWDMJ2tHoqTklnzs+
kxGWqvy3M80MIlJMnl8CbXqp4cbulB1Rs4qd4II93YYENpy9cE6QNZBO74Go/cf/
WrkPCPRCWGsY5kjnx8nutbqvqf7BBA3lUyD7Drb1KQbYVvL6bW+O/d1Bcps7lG9Q
FDeHeHj3sxhv0hFF0PVzqg8Er9Tk44zJ4fFCtlYLc9B1DYyX4q1lS08BGltzkVhX
ng26xerdbbLEky0Xefw8ITQpEFOYXb2JxyUUUeTbehSv+ZmEdSM4dEAPjJEZXq/n
dEvglB2JaalQfXCxx4V52MMaKkdFEsJl8B83QXf5akfyMfsYbYgxaLbD/kilcKX6
5MAfhtd9cKmzyTwvgGU8szJUqaUgPyMVJOEtZum00gfSmK21/Y5XjPkoFAgoNtXq
yt1FfIf+Uc5R4DAKUWKus/BjdJTfI4dxSMKTJVZ6Yyne86PvcUK1mTJxmvwgWHvt
17Vc1xAXgXzZI4vxFB1NIWa0U2sGnhC0DIS+pF7/l0YYzhD3sXNOZiE4CS6Zx3eh
kKtLxK4a9lt0U+JXU7gD9DKnwqIlIMwpEeqbdqOgFaBhpQm/bBmS17G0rfKtZ+2O
N2fOmtXEhhwgZ3OfbwIZRqcL34UStrKxe7qpGRFjh7guQFrp6bUfHgc+cntD/rjT
Atj9eFOKkulOvahBmiWocBqMal5ddoRFX2nwjBDXtCoazv+Y3y3u2DJt+kCNM0vj
WlWnug3+A7ZWbVklpWS730/9kS4A0yFmPMY9GLTZGLq6aMhJ81pvl8cmmb/DKebx
```

```
RqIgBcNa0qI0MXQ0Ko/ZpPZPFafwrFPhcvqrwxWBuwGqv07dEtzPznr+1I4Gae+g
7Gi74/DYxIrW1lfi99pZpLaF3wo30lR44clh/SOcxrw03BsmHub12aOtkFKpqkLX
sR3zgT/yO5cE4QyOqUuARXi+yc5zbkLPpUl1n3KCJun7mjYBzVb+mQpXIZ59W8Ji
Skj0hwGLDrGb8aE9Tn5ZBEfcWCE/K+6NnENtro32PPur4qM/fYgWYaPYVge4fSaR
sm5vFRqw+SfzJUUU/4+oihLJkhZgejQYvjmbfhSNhPopwLzGhD32vA0Zl7xkl8BN
/5RrymCDRqOt/4Cn11soYb+lE0qunLMWMdMRQiXNhejU1ZgxA7e2u6zQE8upMOIJ
zpLNCw5QH9LFX+EgmQRyS9Rz8xUa+5QryHZ73+DFmn+/oHBeiyGCwwaQ0SdtZgAj
l6xjiRDvcKCy1FfsLwCPbdCS4DfoumcTGZW/kumAkVs6lFlcRdeoXwoblihk5H3u
ZtnMi+QN0dUmknzwPf6jW22VJR053ArTgBR9lg7+vpyBVBr7KWwZMk2gbAHE+5Wb
2h7+P+Ud04jd7MEuuCrAT4fCLduLPjOPZTGs5Uq+qVM/VEdasM0vgg9dMtcVaG0C
L7tWvd393hliN1p+A2WJFStOK9LMX+amt/QpiJAvamIJSQj9+X8twG+6OSuH9USS
qjlZTSv7fbkT2FUaTFOzalTdmM5MQbzwdE5COXlxMNP9cuqucT16wcGSs3J9bvx4
7zNyjVbNr4M1KBS/6zhk6Oem6nID8CnstCzagOCRkh/19SSmpSvpvLgKtP0sDaJ8
jhhybU30BuIhOkzbYUu1nDWeEV+werdsFmma9b/JR3MIzmW/XqgUvgAbhVgYn7re
L3UtQH00y9POEUYI0HWR35wb80beP1gYY/mC3rdSC3U4Tw87y1YtYMHKp3S66YAn
f/6Tn3+lync2H0vOY9Nk3LVWdXw3gWHDC5NC+WkZ1r5jyoLwz06JWGo8LATfTdI9
3/wVxhaV+XPgD3V3JzT/WMUq96vU3jCQo9ikSBkX54NfR/ZwBGqLtf/awX2kuO1A
NB+RkNLm5XW5y5J/Hkm32V0jsAyyfIqV7QNoCZWjxavgTZTdu7t9KrszUSxBs34R
wkdJ9Brc9Iiz2NooqBWzDFikvF5ZzOTD3dkiqezjRoW/4L8cr3zvo8VIMrTAF115
/tBeo245hLQSQ67VoWMPH+XSs5PpR6eHOx1Ro1FQTUvp7obXr0Wna3OQ4qycvZPZ
qH4CBriAgjh3rNYl/+DfsvZiKrxwMO5/0YSfo7DGO3I1rAil/pZQZdeNZWgyDrYM
Sh2cDQ79jx85E/FvFPoj5YkfF/u0GDJvXAnajs8lTtDvr4DitH2ZbObWdpYnANhB
baf76Ee+aaIwCKnFXIog0ZGI3yOZhwkrwdc1MoT+zZ0Hih/7nIJFsWy+gd3DmSD1
zF+5hVl3U+6eObKpvMctPEMyt3Rs+Jyf+ddmqQEfGEr1ZLHs2ECRbadE5X8/DtFA
AFHBcXF2Ic2Gh9tqDFBTiVHH8dFZzA7Ys3hQGxmG1M4+g+eHgvz1OnlFmIAFnbgk
50PIk/TA5EZknij1jYjCSIq3YYVT/rVVIKbCFeu+hyRtCFYa/tZ3gZTi7bmvcmoM
9DOStjXc+d8q+FHPYCy6oQGUQ8yDSq3l6mY/VFDXVH3FJ3kGJk4GtfAbRlg7AUli
Zrq0UHWq7C5Bwfp7Yw3rgZi5g/PJAm2p3vn0DJ1Zg/7vMOGjaTFQW8PBanCsCePb
hzcvlP3sSawZ7G8ekIsnhlCBeq7uQbP981o/jFKzapB+vl+0cqZo080QUaneYvuH
oO7gLA1PD6/kUd1eOuDH6oL1HQVxNJERd9vJAVYMg0gcrqprtozBb/71r6K6Bd9q
DSkWHGsOS2S8s8JKLV1QGQ6epzQMsprFzT54IzlzRcu5bsUgNxtHOsdZoCMdFhf4
ILFRjb0AdjG+Ux/SVx0aVhWhYgLvWgH/qQnOKWDIV32cJ/hbFXcUz2hnCKlW9bwO
63PJc+ZBBLdoI6TlvNAKbPrEYWepIi3KGyt5odsctMqf8jEnRBy+8KZLBAOwlF+b
RFu3iCTYYl5fu2rYwZInQWV/UTg1RV0e2geEpRbYRnbk8Kh54o/pzrFvxn1zLbuq
efPqtQRVpjvO0qtxqigqijGvAr72AiW5K21t/4M/OuVcDX0+pc2M76A3i6j4tdjh
uGia4oECnQqWV/NJ0fZ49fDnC/rJu8IHk2RWimUQBV5yl2a8Iems5xyQl1i/Cs2f
o+JRDtCtn7hxdSZjMDs62gIy5v56y63ewUYpP3swfEkJhrWa6jntt+yvVuDsuDVq
GORE8tGkmdXSlaXX+R50ealgGlpScYfs6impPtFzpKr5ckIYAku4yE9abtTXMRrk
du6c15VfGWHGepZV1PAC3RJI6MpBluDXq6h6GFf2sEGlc6eI4Q4v13RMFqce/aVG
82Q6nZQXcF72GMeIL7udlLfllvWDtgjTeOlmkdSsEtyNA0pgKommhx/MjZ8blhM+
abzcOf2An//wwfeboNcgAz5DEfTfYS5A3Q4oHYcth2BSDIcKSDPwBZ9GSix3+nS6
Mrw8XkO5iK3PUcT/getEBWTiqbph8LfBvwvKhVyvGicTl+pB5jLmLOLwVYF9WS/B
al0vVEA0IpKs9RSTxluoGxMHP+8+1Nmq7QvFZBNj7A2d6rJMqfDRSmdYaYeOslBn
8ShYCNLzbaCzzlReOh5wIcweH9CvN8t8op1qGw3ybWmqx8VGH7KnRXnJ4SGm7Owl
TsQGxTLh0i8opk2Wa5B29X1RG4lWsSCVvoRsbZpjH2YhckYC8Ke890vxsYnEVm/d
9eNfEU/brj/LZJOKVSvpMjx6gsuufJJY8XVeBEuIUgNLx0UaX+Vs4mGVtoXr75vf
9lGs8rT1uUse8ezasgPzQDm6a0DrKOkhKJUY6T5Sz5a4gXkRl6gf0n6/uRgApMlR
cm7YxER3nOY858n3ZoGib8SSPvn4RO6WWIXf/96/LRi/b228u0nvZnTxVF7+QO8F
kOFjR22bZE/yIbmWS89rsKPZKIb1axKq+yR6XOP0fqPbu2/o1W6PLobZBT6IjSAp
0KtJVkm+GcpSTTkl1+7V/cEN3G/bx1nqrqDCfTFPaFPO1TLrkjx5DY5Bzs45Zd6n
8G/iiJbXd3TfIOfkFMqk7mIJhCExHrUKdbqhw8Qdf/QlbivnuAPm4nYayIXZvd1c
GpmGDcJu0n/pqZ04Jw46OdjhkEOgcvAACOojFzM6fcma0mj2ZQgUI986q53m/59B
f7CYBZHk4o4kcmlitbBUCHSUcoNGufJdGnpqZ8LjrujOouyDbzIjDqBsg0lQpQpT
```

```
hUscKWx5gZRRwZk5ueiB6AdD9G4T6eSXtltdafS3b7bpYQWrdiQPcTckz334/gIV
NK2K5+IPT9jKj2F/H5fweBtNzCVPRPHMWE0h0sA5pcbMf1rd+w1BEOBSm6fT8upz
13WVJ5hoWUVpm8BYqRfNsJhgCjEZGtrneXTJqPwIaoDPsRGob13mGPTKD/Pxlz8f
QSN6kO/oVKXGkYeh48S39kzxQrQajCIvrhTLxB+DK8/TTNuYf4H/F+uNH5Bi7+O0
4QH9C9M+FHs2BID6MHYpFRw/TFFvw3Ss5FvV7S64L3uPH2w2WwyovkuVx3eZiIYw
H8DcC1MQOJ+VD6ODP9t/afx9pwqOiOfPyy6PMuD0GKeWMAd8Ebg/B3lfCwi9f2w1
21HYoD7HLID3TVmeGKUu6CpyOjMFtKzqL2GxUbfjHIHs+VG6EYxcCbYm0Yk/8unu
LF+P+TR/eNJerOQGTzIOYr3nuawis6dh3M7+kxjBtv+UdOLpnuk6+Pxo63W55puw
wwr25rJangHQIua3WnKyn04JE+RBwcVhPZOrwHuEG6RUpUD9V+Jx5Ano4QV4wSwI
Sjy/fOrtSWb+RFpfY1f1u3QSr/M1JnUgfXfbAVBPmzogmcpqfXyklDg3ayevz7jR
BdZOMXICmcTbRREcChWnFSNTJh7vksVbN/nGXifl4UNzI8PlWVY0R/+ywjTajzdv
jjTmVJl7maQHLC0L4kD2xzhofHZFLFRkacVe+2BZu2K/TEFWwgXLAuySE7FtUZK+
iSQ9gYuMGdWZBPHs17k4s9FNMKbgsoYpKXyWZxPWllGEx4M7e7or26wogSYCy1ka
yC3LEPOULuHQVoccS9t2gGmYwlWQj50P+piRGWti4Up/RqrY8G5oyrcchtQ5p9Pg
Na0ITJ1wRv/PFPg9CQvQ0t0b1kG1pa13yK7LVLSKc4aJ8OqPWe7S+OdxJpu9ktht
LkBZAl80q60cN+oRSZ51gwyCIoob7nj0uby6+YJyUmItwwKXlnPIpLKiBxENQPuN
dgxtbswY5vKP8XZR/tn6P1oTCjeaVLsrujRIdzBfoP2hpJD2iLM2+JTHbqbRqYp1
FjSkwodsJE9NIAZlQEW3Y27H3b8k6P27mXmUIM78EOtMHfv8QpFizvxen+ehuncW
/j9EOav4ssl7yjn4v8VnjiARjmiS+MMKwVcQ8GUmryLX/NmNvrfubZFIDIhBgyP5
HVS/Nkm/qGvY8Q206URPCDH+q6mqB5PjBzXUqWfQC4ZMJs8D5J5tUcKx3MJ1Zabu
Qk6tll88JUm738WLvrswSKU64dlCuvl4l2vJ3XfcM8sAxgLQPkE8GHbSpUUayQab
ER1r47fTKHEdU/XDIpoB2qdlxhEHtZjtsjzRbRta2r8AN+S9UJF5Acsvb+i128bN
IkPfjv2E8DOts6T1ijDqq07PpIiVBGMwh25grFDI4ploRBO2GyddyLD/NfyD+q3o
x8R6JRCxcGaD6jRNsx5/8BaXHzjgYK2W6X5i7r2smNAE6l1dHd+Sfm6D3Kvi5JZs
z2ascKQLBUG8/TfxBVBI79KtRq00kJNSbo99/BURIv8R7/c4f2W1bOQhXdzvvJsf
HKo4oPc5phpXH0HVN+LcV8AqTLunkcUQfutbwrNB/zgh0s9Im5e14ZTKtVmyUOyc
Os4hOTxUoIwNJEmXJ2axj5IcEZAR7hV7VvMm7eF9sbLj3v54oOPrs+oDUUmWNgh+
JAP7FyoZZ4/qq+Ei90lQREa/XbEjkmWf85HLtmgwtHcQ4PufZ0VfzpIMV3Z95s0P
LLVbpUIfb22oCJbVFnQHKj/lf+8avvNDoE9kqvAAfEh0GVBvXBJlDm8EJbuNYMeG
/gzSZnggofg7YgyXlrg2RpWfK/FXlaRhVCHN7pJU9C7l9bptpPAbEF88fJQLiXAo
tH5xZpR8h9wRiv16ADyOHSOpTQjw6rEj/YduUWmGE2gzjz+bEEyA2OzyWYx/NYUQ
Rkw10CdJ/KwBY164bPcZ4a2byHRQPHXRbfRhtnPL7l//09ci+VBAIoR2X1Lp5JR7
ciu4WwlZnTqVXWNXuRogALlDtHh7FroRETqOiVVI2d1eHsuQEEGvLRnj+Qee/LVQ
Lo3itj+ZoE1oGZTE0gjUZWtjcEMcBQdDGsW3akICamMc4DxN2bmEbTBgmhlP2zzh
1zzz2kYzjd4GBXDWH0FIjRcXNlARH++bh55FGENTFh/KtWj5IW7sgDHp7cr8uVLq
wZF9Pq7v7peNRpwjmD0ksN24qT+Q+ckl1qibVw1ZTBe9XAASIq2xHvborMz/RIrY
kVR8HGHaM9s7EDJ/Xm52KiZ9FG4/RA8G0EJLL+YbHJNzb99JS0Z9Ja7vwqkk574e
n7+mAf5WUROVFfswmYHrJAQE6GrnDk2VhGefXvEOV3+IOsEEMtXi9gcPFY6QLCMu
8f0sUzrmtaJqYw3AVj4r7RF5R91vEILTtqCNboDmvI9eOph4WQ9swwanYUa8BS4M
airNYJ2k9A60Fl0bF0s3RRVrBXtL83xJ1nq1wkvLb8bjqmD/aIOlIh+f3irWfp6/
xYc0VEaBxWGoTUvmAGehlzA0wq+G/e+/fDLwfZiy6bn2fO7R052CSVOFok9knlwt
c3UXTEfQwJ5iEGxLOMvXWlYW4xp7xodyUtwgPOG43kYX86DKt9Bb/4tDeGDFHcWc
Q/lkxqI/dfX+ukhKwxsa2398SUgicv0eh1E1InKcvzGlYJsMTXyswuE1sgbFHN/N
WPAsAqOnWHGW3iNiH6Hu+W/X38wl3FoTyPcv7u2WNIf+cLCNd3f6AtFzitDg39lV
RQH46z0UbtcF5Yck7436V+cqKrtc8EAqrhJQgE8Etm5ptkBKlyA99V4zaHGHBQjr
TP5kMoso5SCBXvCg/rDWCDMwSaGzLg8yMdEgjkkMPy9Yiws5IxS49sUILFY1yo7/
hKTQZw4oC5s4c43v7+s+qmtzXsev8XueLyl7Nooytaa7RxVThjk75vXhiQh3cS+Q
Hil1chuoEB1/R4Rb418sgz7rzumhLSz4kIeeYKr8x5xmNR5Zm9io/JrcK8nvZO76
djV8QfRh4vs6MvmFF0bBHtggrQ/da48DtSxC4E36qyYWDqC6vHws7/yIQYLgSPlK
mhMeJK0OlZX7T47I/erjWySCoTVgJAEC1Lyk49bS4LIdAW9PXIeuahC3an3PGrEm
WDx4b+a46Yo8CFc8Mm7Z/SOYYPBO9146RNUfXHs0Y1JEOrFEpbWz0aTOjsyVWcyU
GpCvUiRwq9zO5JoBM588ulO/Z3SMfFfZPG14HGRc2LBE8zmEyriP7JM1hvAlj2u5
5DQznMSmWqh2zJRxjUVw+QEe5Lsz+Iq8f+q80ehtwknghQb85PuN54UZKRDShEAS
```

```
/OOPV0aveDx5RN0J9FHITbZqto6MZz7DF9Yceo7zw7LAvKN658kpmdFI6z10s6yb
GhPTTB0JN8AXcolpjIZftmw3V/PjO3APGGqZM2JX4b0xapTJZeDDYYATFRxYUkR2
ZPaleKIVfR1vfUoKDLxMZVzDX0OGhmnDWKDTgMuO4+EeRD8js5gqCyMXc4PAMP9W
9djKa/jeM4Lcjf+AY7pBeoqpybkVz4jXqd6Og9YdGkUOFScKHieBpyZ0f16JUg/E
RABWMU8XfdJXbxpf8AWgI55WMJlJQvxFuxruw4BrL0nOQRpPmtYJ5DUlf2TC/nvw
uIsrpdbEBRKGurVLIeA2maAPwxlPsNWDvc9H23bfmjJDCz3kx7oOjRFYsfzdFye0
PCOO7ot6tqaoO3qFPnZ6AKL1U+Wa1Dfvsi7ZkfOaVgVE79JixbWofPJbK1y78Z6q
RfLjgUnTGvkfoyA9Uc2K9A0Mekgyi9vSUa5/66Te1U2TSjJh5sgkm0ap6iOpeo5m
9XV0t77NjUI5QpQcAtXAWwQ7Ju77C6A1PLWOlceWavfg6dQbsy4xrbEACPZlhp1I
O3t/ZtOryWDTaczglR3nN3V/AYLdhliBr7PwUy3fNVAr4WpRaCAG2ZwpT9VC/Ls+
9cb90Z8yEFkFv5sYurmvXanpIE8iIvLyD8eFE2woYa/89eYaYQ1uMUg+tFhyUoxd
VLX3jTo79w2mpxw0fQaLiZ3E/jZljjy2qJZ48bMPwPwI7H35w3Jm51ZDMwvUKkeh
fvBwItoHjSlBA47k/MdaVcUYBWqdU9LeH2KqKiZn6uLCYraLOxWCipsTAd6JfwLC
oWm7h5ChTUdMLCe8SBDvztES9Y+Vd3g7GYz9errD6LZF0WFnvMNcIxUXHOl5vlug
oC/V4eyrbug7tcZ/NvYJ+oJyjlkYQq/lsM2NdvP6Z/1HqWZFGwQRo61Jw9dCs7oc
QfdjOH74vCqXb/1LNFxKp5IT/dw2H2D4gqtN3zOpJ7QwBp7kaoe6XCGBoNjmPz9M
2wgYisEGrk61T0IF/zNBIiG2vJHiQf9prbR6LVeuWAXPdizfyWXQrtJHJTBY6mZw
ajQ1zDiQ8EcBsFj1L8KndorPYiQrkflo583MxfUi98YB1SuDxrNbckc5eoEhi0MH
cwnKMMp3aVnvrRvrktqFRS4mJEdTPuBB7dtzlQVMlC8DKcPEnF0rzlwDL0jcalmA
qYsoxS8OFhGVGP7D7FEbWO36/tdt+xORZ+tQPhZW6NiZtrj9g7HBNWjwzcfL72P9
rN32S4ny9y91/TH/dw3t64UKyVntYboWcDhYS+RHoMApiqqhPD1r8xCHZBB2B34P
YfPxTDI4pTfF7dFbZ8YNrACTJp9uaZz424qZYNC43AkrtI8sLz7e1FGJLUpdm0hr
72EPEoD4ObuINbr844LKMcBeEzlNSCllap7qc5X+Ve13ubJ8B+iQOC4FnQamTFSb
LzA0Zie6RLu01rg4WxtSWpJgVYAjh3jFO+Q7TkHTjW1mj4gW22jcAs+3bAkmgzTj
X/uo2uIWBxL3L44R4As8P+Dxy7gThfLsZ91QQ4lXtyWJc132hCUVN/NfZzFmSYbX
EDyI/rn27+96sCDHIsBiDDFE5oOnwoQCrBD3xmAnmrw5W9YinzLUvHBCUrPho0ul
tYTFjpkI4uqOpj7RkSKmp7kWVPrZXdUlmtizGz7Rh1KDpZVtxRhEad4vZK4kOe2U
X3zB1+l1DyCO4H/LkY8HRJTI7w2z9WJOnkSZ+GOTtS2hjS0SUoqqLYUCPKdbRDLT
5cK/TSR56Jp/TZRFAthd/XJ6XSf/xMUSB06LYLcbnZnfW5o1KCs8TcadspEPqY3W
di8q+y/4wkcKqwU3qM+TRkD5iiHiHklY3ZlpIyERjIRhlnnT4MRA2bHInWgirxU7
ElHyCPeabM55omJmf3Qn+50P7xariZClgFV3uRFbhSNedTLhtPyggzBpLLns8nae
ThXHVoRVL+THIGtESuHM4M5WM6JVcMMnsrsUv/CtwRL32L4wvczbjbInvxVt58Lm
CCFrs26o2lSk6bkOVeELLsNVrbCmnyep1MFPqk3nPl+tEwrPAzdlT9DKbrNiwYn5
lERx70OYKQ+xjJSFjlrQMP4oTAn1QaJtlOW8nmiSHTGJnZfKUOXuGRe+JhYimq4y
/mdeN3jFB/yshmLQfYI6BD1sudnBFTRo6XpZxadL8qwJabO+LGq+DKCaimMrDPZK
efCSC7V+HAO25JyXTBuF8EmlUtkRa23zMHdLr2pAIK5959RoyG2rUNyEPDBkkFfS
nOleS8efBwd8OfDDwvg6WSJogzNk5yXNF9W+Y/0H62TF9JD0r1HZejEh5DK/oUjA
vtyhlEraKmvQXr0RWyIezJCmNrwHqxL0+mUlcsTwtIEuk3TnYp+5AmAffzoLYwrE
87AS6JgbpSLTY5NEzPSGSjD93+C9hHRuKVMjwJQkHy+Fum4eFH/P/oW7f+QODRfS
67vJqzBvPDUWKKntHK9Al2zKpIHnoqJz2DlxIPzslAboINeIf51lU+MYkpu/l+1G
xv14VU5UfOkIW1P+XULjYfHX9joKm9LkrrNcjBfwYqEJM21KUqTQ020syCcs4oc8
rOmreCkvnI5EHts4IhR86wCyBXt8I5d9VOV+uwT+Ozqb1xtsd7ZdaGb0qFTHSayF
K4GoaYhEprMenu/lacjEs/FLTf69VCobnZl7fFEqtoLBSi7WSrBPYQ3nYT5QFLIJ
Sqi6RhtdP436XVQkB1o3QMhdFOk5VzqbBYiCUhfn4NVPaD+on7jnPm4Zqg5ZregA
AmV25HmYHU9JTpC6AsKzN9wXriXwGFZ23687cKbRVYJRVuvDsOssiOfsFAsZpjr8
NQCysl3DWLZ8S7u8mRYzPKmr4uLz/bjXQv70Hj1ahebm55h5gmSb/QD3nQcbWQgK
4si4nnZ/LdvtK0CdFkM2+A0fE5gZWOmSq2VkyYuXyDN5iYYEx+zA945le01jW5Ts
8Gc//uaRafKYCIfZ7D/DG5sZyPg/LigLh1uvx67ZrWmJ0993Y6Lq3fxgPGRc1MI7
zpYUYJfHdG8lrJO/f/jvF4v6nNDXRJWONidyNylZsRNzJgMxWe+ggYPmJQgxvAj5
LpE2RWmfSzmDupWVfY4c9MkNUob31gEL21jWGJw4Ri9dhwIeNYORMRyaE+q9BNpS
2kmit9uTvnguJKzyehIr3hW9qZD1s2OLLYYn/DqrgrY4DolsWowML6N+fvvJaZP0
TtsMLMntNNyxi2UvPMv1JgIMVj19aUAkzp7/uDAjsYKi+sTaedVGW9crIWTGXrtE
ys8BVssy5jsKJxvK4pPG/fTgxzUN5cvUM8PZIaU7Mh1g6rb8PkdBczNQtEt5cMFn
```

```
Po/iM3RHZe/81JWwGScjqMhT8MQTg/J+2fLViSWaAQl7pt8p+P15v1JNAanCQ3Kl
LtAxsFJI80PhZ4kghJEEHgunWszUGEvkAEM40Rh/juAOnkU8KAwFcqmAR7zgf5Fw
STjVkVnO0tmg0wclN4s1yhyzUwHGxAZzKsbQ2Ab2alehsZtd9xX0/78sXtVJApXG
voHU3rEgK9KTuCySIZjKvdj9Rl8YT7/8Zmpb/7BqKrLaG/ZkdT5R04IMq1RKrA2y
xbOK/HiGjmIQeoXk5IJW5i7E1v1BSLkAIgXVm3RyAU28KakwmdtMUswT8B6WFf3m
EtRWsoTzX1yPBESQ6TRespi6b0WA04zICWfeBkdqBFfSzKsPZX3u9jK9Yygb6IMY
16pby9B3RocNb16MkgycJMG+Q+fctRLrnN5bOJvZsr+ebu5jNyBs0JaQr9vesOmT
30WS8datNLDKdjpDNeLzRw1DWjEuK+7l4RmOdvRo1q85ynE1JsKjpWJJtqMlaxJt
sFWCoJF3nPIn0qNXo/qxavGHB9j6raW8UUjUQMhtXrwBaaX0texlC1nUH9CPiv2P
4S47wab3awuxmj0rwRL3PJJHC9BD3vILhfWFASAz9KbkBW3dBh8VqpqxTzhXoBgR
Lf5F2+FpKYeMipHoUVuLf1pE9WYTU12XBSZO04IWX8XrO8yhv5a/UfYk9l4wC5Jq
cpGGvLZqLrV3FCdUaDYC0ySW7DtdQ1CNTG10F7ekg8rxYxpBwYCccOuIxlXd+HKM
HjBhm1Sv3f/oKiD4LFnHFO22GwewpXSMxcaDsPsQvuoThp0FzYnUhf/Z8ZRj+TE3
xmjUG0WHnlFOx6qyEy3/AOrokYRhaBF9dnWNGDmPQXi7Z56noZ9kvd9d5EfQiafG
RRlAY/+7B6lZXdLfY3Pv5DAkl6TP1GUtBGL84BlXUU61cgsI+pEzFp0HHQNAZErD
vB/zkK2+bBDR/oMzWqIpr2dsh4MQRoR4tbsZsWl9sfxP0owmqiwHydlzg0sQkb/d
e8SOLo13e8AW0YFchcvLXujhDgkB+6P+WAnjZDEy0Lk6SdFRa/7ieMRcRaq8fWuH
EcCSaxMoXqzvfPVIEnez6fXu8G97/VkKFvkdPT65OqihRjGt0hEnVP1AmQPZLnxO
CicLek09OkYW8FcqyKzE2ygTCBj/AXtxIINm8NJEDXg4+vc7DNcIkIo0qVPGNDzh
dIse8WnjUm+bVGM88ni+w8vsVTP0qCHLEcTDQmJ8CUvwnMa+eNOYWkLnQJjAjIhf
FdLwtupbL68mZ4MAXVe6J7eA7ocwnBoWTFHz/8vxLdsXZJxcnh6rgqE32SMlXYZo
ylTG2DgKdOkk2bcJ3maqV05Xvz2mP1DGnpaaDscHqHG8SEU0Jug+fMNDp5Nt+Fpr
PxgmzOfGxxxdEy4wPSToltg1cJQiPK6hHnDqb02ETouw48NIO0wozXh6xHrHK72r
qk1z/dZGjPM9GMNQiBXo3jFzmvctcYD4DzFShJNEAsqHx9qwE1D5EIObM8V4e39U
tW+PH8F1XTDx4NYrB4IH1e9tTFDuZVNfAEzWvfpIkrw0guRjs8ahYJrYZUZJ1sjq
r+SDY3oNfQMReM6qUYegJBeao9WsCRF0juGlAfzR6IZq49CAZoGLznaGWy3C08rA
lsqFAzYR9Hr4pykjV+57QVlnb72JBFFai+QRg+HsOaaol08lxiT8BhFr/gJ/737j
ABUO/7R9hWz0M8dBSLzQu2UvmXX+/DSfXZMJbLOc3bw5/KoLMag4e95bHxP0tzRT
S4H6r1hpeFxaGh7T/BeslaPdQx1Nze8d2Fu9cX4AgUpsSo36fsW5iLCzPM1e2VHx
YZQjEADlcBqntrKuVvYFiV+POS6CDAFmDh55gewL75Ej2/qIWmaMjiaaTy4lSh6D
yriGZf/OJ/YOXGp8jfwdlFs5mbB9KvflcG8e8YCLatjR4eCKDFAlQbbGuTuAkb+L
TvkpeWEG6Y4iOx4eV3ai2P0t9XENAE2ITAUqH3lsMf8q531wL4WYBbhC31i8e1Id
bhGDcPRNYBwXyf11Yi+EqMWo5/j/2OnOtrWmg/NwbAXwACBphTEgtBAh688yy9Ff
ob2h8mqoD01Cpix3QaflINyu86jTRywTI7Zj0qg0hVR4RrAJkQ/KPhSSjFaJzDDg
hkIFFAi8Bmq7IkatN2PRrv5UeMWhMqkPlX2Ln7JNub8j3S6RKYEg0o1hXVyfNRwc
dLROVqwWe48DuhnirLlZ9K5inrxIoAerELaZItXCMgv5MBRBao17A3jaB67qbNNp
YHriPOCDCx0F+T+Xg7zj+DOSdQ7vRKPkVR4OOnftSuyoEP0GqgUh/jRx2mVReYeZ
8i7gAZFw86ovQN3LAY3i66TgOib3EL3wHJBtMqpegsxWFxLMJLppydpaGd5NioEd
PiFk+KQcnOx7Xz5NF+Iif8i/jM1lXfOxQQHj1PwQ6fmctxt+BhD+yyYKVEhnSDHN
dnIOYMRMFoECmp2snKLZk7B15PA6Qw7Rp6QD0BvdeZQklN99Qn5A5cGEUXUINmMS
J7aWY04x8d1qVnlCFEpfEqXnNIXcPK3fO+k9NHguBAzs6jmuLTJ7EYpzKGjxyA9h
IwxJv0WXcolVbAVgQvqeZ35/EN+40hLfC+u5/+n7kV+8cJssPiNZKNcduLE1UJW2
Tc1Ow8U7HVwuAe9WHgmnw2y2dP6+k2kVOVR65Jc3I/pTgQJoGSrUQR0bkpVJI07Y
6z7eayPZzpUrJNjCDrDKL4/tU5bo30GzH7G40YeRWQAUV7L1ZNSwy0xXm/L8b/6t
0w5/lx771gGSlhHlmsm+iwBUwYqBfqtYnzILpqezpDgaRmYW5x3fcDTY1h7h1n1r
zsSVDFxYwD+v/+qNopCj5DFQjLuIO5dM1eNnJejo3awX1Q3ZSaP7BWe9FxPmeXZ5
zvzPR16cBl0gahk5quYfgdJM1LSpK2+dOfDc67888aKLduIAijgIOPhkTt/EQLpB
tiD+LZpsWtGHoIZNF9cpi2aATw/ALbMO8oB/cblyzHyj97yjCMfD71mR0RQq89Lz
3+zPmU0PdOKZRMCTmn5R8e12S528GkIsNLUqKfk+lrAWzxWQ1b3yr5MY67PI3iBt
6CXHG6KJezaCvCOC9gZCb1Tq3c8InjnByGx28crta89jqnif55ekMYLjRZKRimp4
RzgUhf0FdAEXexK7uvl9zakmQcrpk6OYAwOgC+jSrRMUneUiCuqFI/ftWFucT7Af
BqKR+HluzAdBx28nq72b1g9PcESvel/Xfi2t4GoBYvT3EV0/ajBWdD34AZ4Ihf3J
iF9OURNkFTngBDyHH+cX7LkXQkODyVKO+G4YdSAWzhpCe3ZXL/nQiUwLgafQ5xk3
```

```
YjL5/bdQo3h2XaUu3MG0gCgdSJj1LKolq43oFkwpeIof7ZtFvH/4WyjoG2u5WQWC
j96+iNauscpTUlX2oRRm4UpdOgzg367NMjCeiS39+vU/DiXH3iY3N2VX6I0+5B/u
Cnno3ulwsEHr3vQULUHfJEZ8XwohOqE7vwXQl9WMS+oR8DQrvwVA9G3SMSG4rD0g
fgNk3S9k1ncBqC3tkha3bgCCc1rm8boENRpVUaHt92WBuggUk21GQsWQ8z6UdG1U
wdXsnEMqGCHiO09MJjTzd7xSSW+RjjtbPLjS0+Sv++lYxGPYyMVMNkywpUPBrhBP
ElFWuncbCdj0TH2mZPDQJWeoi24pUJllqp9sObTkFREEAH5K28sO5kozwKXCdtNS
houVV/AoKVNhtyXAzpXb4yB7y8eWRKIPKjImQvRbbEbshE7Hw16MjJcsl7X5++6+
83/i/CfZjaseIE2GHF1vltfjZjGJ1/gAXowHd0S5hCzBIDHLS0obaKiOhIlpXhxD
TcTomNNcwzINQHdaj+pHqX6O80Xi25GwBnaE3ovIOGUJzugZpUY4uyb2n17PIB4P
5HaW3YKgHUt7anyll8O1eNASZRrn0CQul/44aLk8Fyf2pL3IZ0pAdryFEIffI2C0
ELEYHbS6V5ri1uHj9nUiL03PM49MQ3c4x9+e1p8oqP5aNS4xOqJy/UGalO1XgT16
PSc7LsZ6hp9lmodLagHyIQC+mfeQ50RqlgnIUPnKBoaAtoEsQ4Yej5ZcHtZ/RZKV
o1KjoIE5NKJcWa4Uq2hOHrYmzlnYuAWlwiLMnRFOe5dPSMLUDicfGFzwV0wuF1zV
zxmjT2A2drf4FO0HLRkus0auYZWJ5iw8Zd57lZZzkkVXyp1daGNbKtpOZw0ZnmZA
sjMFs2twXmPHJ8ArHrCEi2AfJo4YobwcX3t4w8dXxIyZL/ls+uLntc1x4oSfSvaf
OMKKe8NqDSxF4NaKrtrFqyUycDwOEqodavkw68RVrRuLKTPe7u/Mn0QmmOgAe4WN
NReAjxaYiqa7z+MmjGs58f1izxo/syBJN3QdJbnQUQrtxTa1YcA2fAhg3AsvcuvZ
KxJKEbVGh3PEmMPgQqWnAoH4jsIr05qKMkwYMf4Ffc7H2/OS+RqVm9j3JkNw17X1
SUbCeiLz8eHSlPoq4NDikL9rT4Tn5DUsb+86B1/IlLhuHZDU4bAGAdH+KIvOfRfg
8mWSdzwYcqlyclwC0Rz1H9oDhCT/XYVG4rAEkFDwa9c3vZV+PNGTpmgsPGJXL4ta
5S3IQuK9FtgBqK4REogSDZS8RA1ESU1GrtVajJgjUit97PSf03oo06kKe5sCEBOT
tYt60tJDuQS4rwQ4SToDCb1AT2EpfSIV1qYzp1ofxZzAzQDibmG8/MvDIPquIyz+
cr/8FSTJ5b+tGb1xlMhAgrs+BpznDn3CJUuBuyM6ieIL3B2SAwdmSdQM8z2VrsFW
gsgGjTSi+V+7R3OXihVixEwloy6KoSB3EvbS+Pmd/aWYRr6aKu5HX0jkA6/Y8oBM
WuM6Shbu3ZfGM1cNI42VzRlCf0DIBK3skP4AOZm3BrsQaK+9B+medEP7/QDx5h3D
AZ0WM7HMoisF6f6ODgvGq9stn3ibTwjmt6HlHG8a+77mZFJhIrOVqBYixzR9SiUr
APY+VoecsJWwWWAH81q3bltrb/yq+FyLHjpAjjYiCA1KcYunGk9vDLKK7wDz2Zv
ZGU4cptUhkrWnVtNf5+8IWU4tn0qUfrMi8rtkHmx6JOLgdmzG77cZxILJ8SGnRFg
l5MKT9lltbWmfDYX2sLJcn+DyAHhIXsT2pXkhbLy/oyKZNuaHrOCBaU0rsglXtl5
yntMg/SSjQhbzl+hQQQRDEj5d3qezCh3MEgoS/VoD0ASYp5d61cUwgi88aK8mDXr
jEu/g7zBnHYqDLtfwiWNyB7WRLoydCU9c1VCvtwPCQdh6TuAPYM238EL8Urpv08R
7jXwEZiNF2srQuudJyhpoLp6qPh7A+hmY8NDvWPxIaYC5YGIaAKtUi0YuFGCZChz
rxOO01zd3DYtYQ1MOrZEF7Ivl1/zz5pJ903YFCEz+wW6JBbdRPGPkRq/3dW26q9w
V3FxNI82Pi9Hf5ya9QACfcKIe5SmDUh5kZwLCIfQiGzjJW/t19ma0SY61lMu5pwJ
aePjilykB5BHD0xYLjweZNSWVei/cFOSZgE8IGodfsbNxj8BAXG7CD3dOIJupwna
j4jd7s3EHm7I91jBbvnXFenzZwYqlvdf9fc0HsuHQMICCjCyDBmyhzcSSFHVtaXP
dCXG4zsUIqC1myk5tmSpGdfIV80rQ/JBiRnUVHnLpK/qFoa02DXT7FddOPJbvq5o
l/1y0nhgOQ+n+Uqup8PsQGQcjVMpfClE0S5VKr6YsbgR40ebn40YRvCIhOp0BiLh
6x+UdKQ4DpEqlXOvAABt0vOQgL9eCdrd9AxAHte6HjW8lBYv8RJqwD/SdR6brSe1
OQ3JcMI49igKaqwm62cSq8OKQtD/7hfChzrk5ARQRt99ap47KYqLbniv5EIVzn7Q
WJ3w+x6Bt/jP4QiRlioWHOx9TvB5AYzvIfQPgX/M3Ef2xdwWIusaPj/p7is2pY7K
Ckr2kD8htacM3Ix8GTHf2FGd7/cftXmtv3lyS21vtwny/z9oX4MnJh7xsfmvbPNi
Zm2u35Chw0/1oxR/fFpeOAx75PT9Ocbbm+N5K/grn1ztx5Jvm8NZJLV72RTOHD+O
OY12Exq++DvWsJo3O9BT7sw1ocuAd3YMMOm8HE9yv6Ob5zCx31iOlIVCL5vW6uN2
bGh3/sAk+6dfBwccS5hsYyFDIi0sXmw2opr+3ppn0I7oP4rQOzogLKT8uTRV4xTd
U1hBm44irSbUThTPgQ3wFNzNOu0SdcFdKwGjJuLMOdYKt3lWoF8sh2e+4TvoixC/
afa9SBXyzQP87Mh1KtPCyEhnw5bVGVdUb2542MNUpZoW5/UPNnvYBSBRLUWWC7fd
+oPV4RL7qOj4CK6ChuzOFEgrIOC0nGcNwiZnOQILnslzxUNJgPCoRjDjA86+JXH
R6HAcsgOIMtTEB2tQNGuI2uTX0oYOTa5cNNQfYpSafHeJW3s/MkbNuDFLXRTMZcz
herL5vSKkfRlkkqk/dEbZvc4JyZz+XsW2zmoBsh8xTKPT01ec7ZkyO+AkRhuMmU7
Vi3TJXXiBVcoWb8QKP0hHfD4bh48axYoJ7dWQ7JGSZZ7DRipkrzJsb2GOwfmiTPU
1AkESKkCSUOftxXZCFtwU46naM4Ev0EjYef/DqxtDfml0rhgvvxeqJVjW44/TnAK
gOqwAAHFaJn9e3Cn6mYsobT20Dok7Lnox1Eoc/OgLP7x+zXyam0Nh+3+lulA7V3m
```

```
hdr9SRgAJ2bOGeJH2hYGYeJ8M/Oz6isfwWv+Ga5v/6hVQ7GX6JtAYdzW208hwr8p
1OSYFnSfZYzJuMVTRYf4no7nK8myDmyiUsR6OAiR2OlL0FH5S0V4fLD4LJRLv3L1
rSOuRhbedlEowI0r0/6YM9gd45SYelIQy9cohOWJ5rgSHDSZRBuGYS1Pr9Wc1rnv
MEBFUiY+Y0jKt2Kl81onFa6zsaDF0X42bxFHEKmxVPHjx86ANxz9nRevgjlXUxfE
ygWaYQ4qpnIvRduJPTDRtH5oWZ1WvduMe7IPojR7wU4/xO/8t5ZDgq2lWUoW3Q95
NyVNb8ea8BKjuMdwAdkCKzbjUMr7oRAf7ey9HUaDsk+81Afo1EZG5hzgze4kgsIw
jIjgCE7xapZQZrBk4PGvSQ60QAmz5TyHZeHiq6IHsYmrLHcJM0nYA8gfS5lG8c6M
sz+moqL7bw+6nR80TuyE/H1IlkiR27oYqHx4bEVJAvIvyxlSU/LmuFCUSItTh5w5
hgtC9eM9umsR9B+fOGSkrTv16Zlao/ATsJf4/Y6u4MgqmUWMridPvdLnKwKo3plD
+5tedmWOhVuS12ckyChQTxJZ8VB64IDuMgEZn8AE8Ey9h1e+SqX4dP6pqrspXsOI
Dt9jRCb6lACblUvbeRbSs5PUsM/Hec1DiTxnoCFWRS7RAbArC8edULGWJW3ydtaF
yUlRCsWxw2EaoeAMlEhHcbZ0jGQxMn94GEjf3CyqFnQJqCucY8mA0ry0/+qSgJv3
jiMWSSwcvUg0ZKJqz9A1AKr9nnK94/HQ5oZK4t73KjAm5ufRvAwe5BCQn2pDLM/p
E87WK3xDUEXcwImfdSlAklQrPUPD8wsLdA1AV+7cuHGXXLEJRSQQT08s6ss/KRs0
LxUOoeaHmxL1sSt7tMdOwKN6su56MYYERhnjmIiLsNpMJu8+EgpgidHSKA3VoeUb
Wa4mNWHJ2uv80Xj+yL2ncqgdWb/qaVTLDaaXOH60Zzrmh6AEH+KqU+bl0EcfFZR2
EjyKByT33s84T9e8vZdlKcLEckAyUSfwoaCyxSQM15sh1SRSuwvzR75DFznjQOhS
xKo7bmqMs1TNHHb5Cnedl696HNF/ZgdL+31HM04hvCJgdVn2kByUV4LT58kd0YVw
VMibOIl7D/l5GBpwwXBaufYRtiulk8V3m9/y6ZZDM8h4lCSt0BtNjMAAPhB/YBxY
i5ry1GT128desFrUzyt/B5WafmBJ8hgeToGjpYzEQj/veV4xrZXamyW9rh5a9fvu
MWulc/xaSrocTPt2NnTu8W+taxoEh1jfbHhyN8iTeFNqhB1aBytDqXnDQE2FgXns
GE5/3Ilyp1aUwQBwo18poui+GZ0QDapDvPgJW2B7VFR7j7lzc9Dd+Q0u3ln99Ht/
q0fT7lLaHIW8nE2/Lo+DhfEV/uWYhA/QCePmT0LOC4wRoJdapHfLYVEePe+tbd54
ALlXcNrY2Rr19XAsQ/4xfzBKik5BGH+Md81Aw7tMG4X6wYswuQq0tPSJ+Jungth0
9j0TYJYlAJdKRgsVkNAwgdJz3pmE3h5NbpVCjxGXuNq5O6r9mh/dL7n4zyglehc6
2PnRJW560pF3WYI2X+McSstgbMMMqFMM9JyhsgQ06/qEetplJRR7OT1K+zzhzMrE
QVMg7wSSb7StSOeBED3Zx0ahvF+XQEmWivOASakC1FRoEErprv4L/sb9a2nC+Z5M
XXP3bIK3v8FenE6KJykiiNXs2WlOZ5YFgb7iJXTCd4mvjuql3RPi552quaDuc/1B
pAF/OlOC03vVUwsqvxQj5pZVOiaMg/Qr2BxMQQOf9U9JztWYgpRhvtm21ezoYtlF
OXR7jHa3E07Hn/oWjyb1YBQ/An5gmiDFIHv4qUGNHVbibSdKEP5H80ztYpkmBl7+
DtJY8tDLE6VEHXJK0z+vsocmr8Ydd/8MDTD5gj0kCl3iGVTqHLNr85Tl5Sif0LQc
9ZSFoR2YEA8wzd/Vyy+VNNnCKAul7SfJWfz+yS1sNhE760/QmRZBx/IdaTF/lzVl
clfc6/hHfpyBjkTm9HOYjl+rNCt/LfSVkaY4IrqPqZYH/dn6NIS37XVB5CNtJFB+
f/rYA5T2EXOtmtgS12QJvtJh6IELvOo5i0ZeudbXDIxFgwa5jRW0mci2ytsqX1oo
nnrg7tBrtifc4OzSUU6ycfvJbUtNqSpBUEkP6u2I0sFtUjQXMVNsoN58SbvWdgKR
lAN3KykO0sz7DilJCs/P/+xDFKzahlz0DFSTWJ+Ua9m+7y4eb/0IdrZV/2qfX7Mz
r0S1biGnIsi+O4PX9W8qcYZh3Y3Ro0/CyLJ/jloM3sAv41fiKSDqfdzBbgU7LwLl
MA5JZVuNcHj7HNeFdURE+/rZo8JQW2W4NbZcGJn6EQJ+OGQCu96RvCVB2FrmKdOC
oHCZhZ+P7eLp4R9DqySvCLe8+wXJRfPxzrs9L1zj0KP438X/8ZBP6Mzdqkkpk42B
oza1iFR1SlC1k77Xukif4D+5lL+aCdPQY+GDkp3HnyFkQv3C3COxoL1Ij4C0Q67K
EiHZq1p3KBssPcRTXVPK0wXEfm8ygGVRHF6wbl2s5nHnyHay2xW3BopHiSV8kj/2
tLz1iowZodWSX+q6SrTMl5gLkSsdYogpdXqTdY1iGiOEYrZK2Lx4rkOY4E5hS1Uz
8A535DbY0StmMe/XXuEhna+Z2CBO/OmNIdr9t5mhsMfQgqUPZ/7YVlNLoZkPRlne
4wphvNeQV5P3qBNhy/IxFD9dfvHCTaxzGBlguB/jrcXj85Z3IQmuGK6afcX4NlP9
AF23iXYU7e0xbR7mGYGNqFEebgW1HhY90ztbHdDM6v9PAeL/TwRCtBSTPd2Y9bkJ
mcB2OFIUd2z/o8AdDZVFDFr9U6DtghSPrEqKfyA8R3Uj+d7knUWcIfCwhe7K1KAA
XVNAO8/HfPt4orgPkKw8FCLJSeoEPpkJdkdbKljWCdHUo6eEd9+B40In5tBoUFJW
BDbw/8DVPoryMZbeSaZsQEJk34ExRcJ+K0xJFYsepwWO07YC12iF4S46c6i2JcHY
xcrnzbhbj5634eHCNNIMwUmIjLTgw2uywxhUiOEy1l1mv+GKqrmwlOsPDq6K/C7v
7DyB5C0wJpRqelD7p9VJVtglOM3T+igFMX8mbR+9RWYIOZOJlsWsW+H2zYxIc+Bm
XCpMJS+Nq0bZnqFWARmhiFWunbAgED4G8lDC+dn1oH4jEgnUe655FB2OEg7AnTfm
gbsc310bWrS244J3jnGWdNKSv444rXuCIxTsAVjL+ZlfyEpuduJD5AYDwOrmErab
3ifIVmii+MHv4MRJm+huBnK45qEs/lZlC7DEmGTBbTHOhVmEBq8SflqqNGJwQM89
```

```
nAmqB4m3MwXM5k54vbAt5Mq3EBxTgVaf04Onowai0yWEvtw5C0ijRC5kD2NPaA94
X5WE6SSnlm9NmoXjA2JSSqrRfWLZYRaOBgpPpy8RadZnOtouqYACHScZiZAbKRNm
52dKvcRWSvgM8pkdGZvRFwvRdRE3vIwcrN9FzFq/TGMq/UoWRujwypAYkGFEppsz
pkMB1GnK5hPGXuzkJ5hzJTUJq/RZ7ldYYeeP0UfZ9u/fbgBv5bb1JPWghvgbZVRj
wLTsNl/OVJMT8WKIOAzmIDF+rQwAUEeaCneqcHgku4BUfeKq92TnGQBh5Y/mVXmU
I5bUtwfN5XswGSaNEQoGlLTFTIgxVf2a01R6nvxvOICpwYhY7XqngBNNuHnelKYn
F8Jem2C5jGW7pUbYaC+K/n8Mf+21znutxY3A1ri1U7u2RBrWGY7zg1nlm8e05jOg
H2U4jZ6T5y3LFcbTKalYXeQ6xo+ZGEfaFZC5MFBsSEyGQ0R2BRopFR0zuJmoN3PS
yMITuXFa6zwkiE/iAAAFWohRE6zQrYY0Cvd1akpCgALUTIisvc8ixyPdjO17dKNS
mC1hInlNkT3qNoe/kxkTS+2D2mW4fNqXxpXksfGkLK5yo5r/oCKIzRa0a4gKseo5
rVJYJMpTHS7K248jqN2CbuPyeilwipnqXA71OuqsBmbNic/qq9nGg0q3fKqn9wkV
TCs6uHErRlDusJ35J3Mu8fNNxtYf9WwIhkH1X2O3TYOeWeMa3RUsOpnuqI0+KdFI
Wcxa99Z3Vx85St8b+Wf3hwETRCztjQeRPZLf5DtFJ0mmIeaW0yjYGMKJupGv844M
Uk93PuRKMznk1CIKXSQUp+kk/PVlMC0mWAYeVA7lZK/9oI5yOdi93smZF6b6D/8w
h/ku4A2/NDDy/AokZdWJ/WXkf88HpTc4xqhb5LUgHDpsFcZI9wDc5IDCWU5n2znX
IENz7Qn/TaLQCVgfJ8F8rrOPcrk3oIRkzm5PUI+UTTyKmN5b2y15ZMCx8PDjNtIG
SwGYhFliMX7DIjXcbSf44fnGJIRsdSrqFkyJfVXHMqJATPdowSJyzgkwnsE9h4IY
oCItjqjiYp0dlWkx5hoROpuz2I4PZdE2aXvVWAwf3DcMulZqm/0/JuebewB80M8w
n4E7dZ/X9sH/jrp3yokLBErXk77/l1OukbJTScv8VeIEp09hqQX4jQz2eIaODTXT
Nv0vEa1GiGccLqclFluX5/y/INLE0CsV/PhrMP8RQReRJTz4Wl0viruUGZbeK7Mq
0Fq9Em474lxN/YKnSVw+mfl3SuK89VmsG3+Og+Y/V1AcpyUELRT/6iNUneMe0d2F
51dPvPrei1MX58Vo5ATdmFd6OG8zCIomD97FXc9/FitFROqe78AumY+2XarJkhc/
HF18w4VfeJKCkH2BMvg3OvI6Zhoo+q08EP0hNCuNAispotnZoQXJ//a9BHtmECJB
FnNRxQZIbg1hKWHSV1XdaSIdbF5qVUIXMfy96LxsJnFB4oFWcu5UZMXQ7DSJgVbA
nuitWty84XeHfFmRyk4O1UmDGMxagtsb01DnAJ3G6EuxW19blT7XGqfn7AjQdEPg
loC3SZcvPDC2C2lGgGlcSPxiV/8l6ArmaXFP5vn/gbtRJPG/9LxW2CbfZysPpnjk
w51g7K4osMgGJpr+ks1GqfzRyhXefO+z44uNBUj7fEnUaB/7B6GC1+rbtzzNkHDZ
ZWAPRU23anfM9Gji8Of7OxoXe7yaFOuuksaIyp4aswTGUV+CnsvZbCHp61l05u9A
akBdUyfRYKLBnpPG7JbBa2eTVbSdn/o2btD2dakKyPHuiGwLsoTNAkP1XuQT2Yny
gwM4d7f4ekf0fsW/6lmw20u5J3/uScoY0grF/TgoXlsDTK4eaDWQ+cqsfczwUBXl
rWEI50FNX03ulypO6irXD8BRTRwSK/+HUX6dVmSzeZB/6BoiwEnLGmi8uKFvBZvJ
b1A6bo/drpySRyWlgmrgP3zLAYWRLMOSp8T+8C2z1EjC7ESdioO+8L4MwPzaCpKm
6V4pBGRB3mZf2ziNe6/koOZMbizxjddquFoNCVVXs114j/xyZ3DUy9C8HuPp6SNW
U80qVToV3BeWgtM4yJeDPYH1nHbKcBZoJ1E1YsRUNtdDQcwyDntLnoFlpG9UDeoN
fHqVCoQX8WN+hgYB7Y3YpbRM4vD8TgMABYgw0Fi/GI4nvvqAzYUYisrJg+9TwJkw
ptCxGl3xJfibittIn6ZSYnsqHo6SmSksHLttaOYGjO5rk+YmbidClGlP09hHeAj+
lwiNOeBTLAo8dxSs2wHd/eAEtcN6J8IKs1vKP09BbzXysUM6RfwXAmnVYJiGYpmd
ySPz5sC42X67o6FJKQ0SevPL3n3YexETMzTCdMJOQ6vYHUCK6pvUfCiPH1vMNo72
q82qQMw7u+EQSlKFZvmsVFz6RSvEBodKkMRSikqXQHDvo+QoddJuupT7zYlFjSSz
prDPqGs64B4DfSE34PgrROzasSyxMMWdTNegTpBYhFx4rmsRtltMc/ZKAzVAmJkV
DknQ4QmOxenlWUAxxCsNRCFNWUGPIaJUoLvCxQNqHX+10F6zb9XQ89P7XrR+muhW
9nFQmoE2EMHe2R+HIq/t7APlJiXisfnHDDT/FeAqznCpO9X7cR5y0mk1azlRgNTs
YLshzyf5+aAaOMIcCpyqkOCnd8K15eP9SHu8/sZiqSyX7EhjenspBBL2xyuox2y+
L55G0oKoudQqIZQQgQE/OVatjwvoZp4fFJ/v6rqmjP7JBQQYGTQz/eHmeYnzwLCx
5R+w9CoHtf3/8+9hR2TlP7WYAIVz99j88xalsKEVrqwH9zDpFXt2Lf84NPiUYfxv
bxnA+7u9Z+Ivjwkq/qQFNlLse04UqLUxA8eczSft2OelWkehTxzN8CPwAhLE8huZ
5T/nACOqA4nAXEgNdat7I5z/l04GIzil3FabIGzGRi8u4DI1rl6OJlopf72czRh5
B0+qtXydkngl8oyPeNZLdiRU/2xP+5szwBfa6xgAezNVCiLi0dOgD2zBBHuC99dw
0DStTpRE9loBGuA3B5KN/VPeMEZyc/rRq8Fwn5p4LK5bwOCi15AonwS5kyiGE22l
kg//8U9uiVyE15JYTIQzQayVfKcKJ/TqFTLw1hJ/AY5m3RQ49lC/xujRjZ97sqgv
EWPvb2Uf9FkDWHGReB3DKHKysQRpBGYpABXpGqvQDiCEHmlBm8W3W4yaUETndPBn
9Bt3TIdWrMs5+Scg/15BKg39YvDwaTYMbf2sicYeZNf+2ruI+8dD5eimGGRvOyUa
1WeATPdRB/mBpHSIqooS4fQTiXFTxdwFneFs/iXrAzakSrkQhDrbfWh4BDT3If4y
```

```
QlRx4ikVUnD5nVNaKsm5rgH+TAWf5xLBpjhOj924xZed7B5lF3emDP0X6qv2fsgM
lLFXnBjxR/hx8+rsrpwzK0IRlykOLc/vuVCbC5ywvfZQHG4ucfhMEqkXD3X4azTl
DqKwMxetB0+PoyHZ248EN5fF9upwRxM/l0P4GQgpy1s5c+rm699cijduaBRGvMVD
TI1Pj+4GmSizf4fk1hUYIcNdeHAwtc/xMUjWHF6njWmHzljxRwmIAtFMnWi430BQ
3tm22XXWVrqmtr3zfjF7jYOsWBfxH646xlBtsgRSkcZimiwjlXGkEem6NgwAeO8d
vX1EI6QXd/ptcJnGGGsxk6TYHGmJKyhyR/06IF7yuwEHyuT5a/fsVAuMFuqK3hFN
zUwIqM2k3A/90Iw5kUxTgkk3AAvGu1uboHxI701cMRvktUAS34WPo2gWPXKkrGUm
pVGFfQhs6t0d2hl4Ey+ZMJwN16OyBTMHPIfStUoOLJS3oxsttz52ThwzAdFYsmA7
13/b/J00TChCvjbLDEyQwHSGshnDsICz0ZqXfc2aLti3RBv81Z0bgPLi1Z+srfvV
vC6M6DiRdxqZCtEDx+PgCNj9BJ3XlYnQGXXn4CxcBobuDo+Uv4+OoUIYQYnfAqRY
VkaozbF7I37SRML7f1io+QrSnlrAEbZNOQ/4XNpV+dSxEjlSbalrTVv5Of3SoQMa
Zm2UgW5QC93NLnetVD8wa8fYrJr+xE8h/G5N+Fp2mXHz+BbOxeXfJ44t+hpWXU3U
RTFZ4GKcRzBRlCgrCqYrReKWgoU+DM3jbBFEAnlL9jq8Mw+lgwkLii/UR1uo7pTR
YQJtDXb0g/tOFAf8OvvbT84BmDa1OIaJRod+kY6RMYUjzZ5FSjxQ8eTouQPnARb4
EZnaNaVh2Q3J6PWgY9BAVkjFIv47oPOIJ26bvCLwLr0J634Td+9m12D3Y9lksBvy
KBwWHBL3yfLdExQd9U/tYw59a1OwPLKD0WK/fcNKREkLnaEOf4EmUUZHHiBLo2FS
Py3NFQUULqyngGW+5P50hC40/mVBEENYJZZ+svKUpcqyDsY8u74+MvTpzwC2kdHs
xL7RUOD9lj7/gyk7cIfoo75VtRSZB/m1/IJ28CgJMum11QChek7hEkgOB1/+d9Sm
MDuh71fXzy+5/EXBdZykkGSvY96e5gQuZ5mqBbG83PknJtceooD+BXzOzyP3UpA5
LEyxI6gqBzl6r2LFacBYOlIESB1ZGz4MLzV5rPMdNmvw4M6OoLU49ES6jczfHww/
RzuXH1iaxNMp7vSHF4aGCp7I0qGBYAcT9Nf8dKcBD++nlef/Aci8NQuQ3Or+Ch+W
l1soZjVzy7ENV5cvVnpEbE/jmLhxU4pXbkXxbMrLQUCCUv3afcoJmGYfhiFqwonM
1aucpamLRviL7iOM9HH4vh3dIYGbJcquF2wzB2EQFDN9XGLUkgXb7ZfSd2IXd8F3
yc1nMTDyLICluTV55iw17WvLQyOGUxPHMDqocbuqTdU42+00uJX99fsE+IwVHD5Y
T5ZRFjKGCjmlTbeTsqq3yaB6kJ8VLUhDJneh2xOM11/fvFvpUulf8GrpXSE/zsoS
v1aOAEfgm/e936Ff7o0baUxzO+qbygPxB3jUyJTEpT0vVQEtCqi+Pj7lFQU6Dory
HK2j3StlQ9htVUlU1ujHtbo1miJ1tSGKjpWX2a5zKBG5m/PgeQngTVxUYA9x410u
EUjvWf4JgzOaAzqMMONoqLUpi7sSSocMoB/76H9g2AQgN+f4FJQ6wAzO2mZbYZlF
a3IUgoGE18oVhBAOkTYC1fUI1Ejsqe/4tjRNQRSCn9V59h+aziDbwiqApMDSBEWK
7MRqGkuUNXm5StKlP8UMIAX9DOFlZmD2n4UEO6ibYXxQFmwZLjnf0EUwkRavBhxG
1apWwWisW5b7lODdafHp9TH2LJPV4mELnATLYD3mFxeUCpiksc3nbMlR69f3OxgK
XuOEjTk6dnraq1GVF4FyjpP+A13VJyYmOwTxpsiMab+4M1d5y8hPwd0G8Xx/yTEl
Kldtzq+Qqlh2DkpiUiHC6s84uXXyV6WPE89P25pE6viZBAWhOsRumGXPr9eKuZnl
EFtz5ihy/5jIDV7vJn+nUvH6T6Eym5YdEb/vEjgHCysWoQKcCmChxok4m1r+kE87
BMYSXnSt5hrP4cAom5KR3bO+Y5Tuq51vHbBDnrR5rtVJkEsGRyKA8QgiBcHdyRZ+
MtIsTbAwSngsfl9it5RQWLZKQFKExrn5P25k5E4Jabv7ShVTwR5ss9jEa8SMHyu6
P/vXGMNcLmqL1OeKLV/iyXLCd93w3nKERSw5yUJ6fZJuDybuWRITtZWcDkIHug/g
EBS9e/XW3iceSchPeUOPSaz1eNXiG5pxJElYDhjjZgFLad2o5JRsHk16dYy31nnS
535yEV+GjaVHJNMDpa4JzZw3ApgA25CSoVe2G8LzOwdRumGxxp+6PXym0rkri10B
eiVMGAJ1ZIcq3Uef1D6DqUTGlOKCDgJGkAJDmbTy7QWuFrip1wJqxk8jN61wpO5o
HpMfE5Vq/ANlH58f/6RUtT5PhzQ8q6IGC3Ye/hxQlpJ3hKUJF0cqBgYiC4btb1E4
7nzb+MbwmDbunwf+c6/NO/bUnkkBEMpa6YCb7YIoCyfYANv26DIJiKuhpDjUOxKE
SsHartCKHZLKJerafI+SgVBrSPAWGqHUdBbYPyqWYQ9ZQtKjwflG/rC40mQ6w1oZ
+JFuh5+Md9g+mh4p6z04GA7X/RY1eg7tK69qCuWtielppDCRngoBkThSCw3ZiCdl
OegKsLNhE7/Ee0rYEu4qrmQlOd0WrEc8DGjLV/9n5TuPH2lMXRdW7We0xt1NpBuI
NCSDQhL7I4c7RzCJb+y28Z+UszZ5mh2U63BPchnpmw5HwIVnnBinqMnN8s5Ft3+j
ZhGglhOK3+kWcfWbHBLpaW26d4Vn2N5HVjBIop3lo+eFyddzX/t1jcCbfw+lMPrb
5tyoc2YnEr+CjlGpV5VKubksAewNt8j+0/jarabHtLlCRccPNut21druO2DeUQPq
xsdLF1ArrHFW0JW7MnKNEsLv3JmDIOlDDpoX4mod/jhlxpRobgyvGho2rQs0PaJU
5BBTCIcxnXzfJNmn6H+ouCZk64yuk/etbwadvbx51Zx+8qXEPUK/A9Ht7N7x8Jjp
xBpieufJDUBY63TYdzPKJLIf1pduKS0GQqjC6nplmmQ8ofqkphbCDpTlXYA4PoVJ
a3+R0YZNBXIn0GqB2d3HyMpe+tmvvXKyfONm+Zyw0ILRjMhmKBXdVhoYmSp9HwUU
ftUgUPCKZO0OImw/HUF1XcMR0jF5uITukBdYqHH5od1tSa/EEq8PXQfZ/OsWEaAa
```

ZWeWw5xFqUYWKGXSbrEfU8JxMArmxZPnl/afz/n3za2AmxHmjFt0UTf2FfQmVPh4
3CNTiB4XLwdh2+AW6gfSP7dyAMPX/TR+nOugd3zGl+jbEJOrXCOkIR9xIo3sn3U1
IfmCm7DSM+kT+i6mDuEZ4RnblEOJAfcIp7TVZigWuKK56Qz+gEn/RX/yaNOlHK5s
pGdRKUcRJ3vdQXq49sf57NLyarjKT3RIFmLsbC7ExjgylIGfweJwKynl4Y2U/LAp
BW4vW01vhwAJlDoT6KmkortcOeqgODQBsa9PHyExgR5KN3mTI1JHDDYvFjyOftIN
6iw7BRkdorP3IWfxzqXJpWgcSHlIn1EmXdCCryVKr9Q3igdVhWhax9LyGTZvAxNo
AJGurkobDbgSqgxG2CmnrTJiKZ7Xw9bRiNMrwrtbykV4a1Rc76xuVhTY4G33H5o7
+Sw/kuWs+2B7cPZB29i01skyrSv5B8Ogiam4DAnM5DU7su9gydKigVMB8hQULI1N
iqhJzuOSNBbDnFGR5ymcr3uxMX67OdcyVPgKdq6VDHi+7u1iX/eT0Wn8MVaPcT5o
IX3SOh34Sf0z4++A3CLrWjmpD5yIMX+gWfO0Qp43rgkmL8jVM205tmylGVZCVky8
mDktCbw3GUcWkNdbgv+AwywUhzzhxNLqCa+NwpeZu+ho17mzhBiw2qxKMY/lcERB
ByNr4tBIadPze6Mgpon21qtdq8XSMJfAJKm9NLRQcE+Kpmgs/Tnv1FDIPzNy1dwO
ecBefsI2xSRO0Cvm9dOJJxM5UZskljU2UgxDXWWHqE5oQNRKEuMBBYGgeulH4/6w
8RMg3T5Zg1CKEyFLJkTtm05xi4MiSnmGodQLZy4Aq2/vcqKha9VA7+Kc7MFJJqAb
OaV/Je3Za1vcY7lhysyxs7uNxB5DXCfrA9ASovtUdblvaWHcn9M+hatYFp0cyOjw
bBGS25E6m8K+OQuDhA5gXfglhfuRdwL75W9+D0kSP0p5L6nHkWTIA0N8rEsOeTAn
AwWy5LRCZUIFGt/qzRjM5CdCy3V4SsbCr4fowR/JAXcU/vo3+37+W4n8SRkof7m9
m6X6EAVlNO51kT6rCtHHhtfMZ7u3GQYDyVEv3wK957iE3ZJasPgWUSAnib1BnayD
elBvlqqB/rr3dLIgT2Im6bixwyd6xWM/5ZpC4WTpyqOEcRlA+0jnKkHOZONs6F3d
24NP+ZmPxE0LIqgx+CU/GSnKEfcQ6oi/Ni68ZTSzgPoHceYbcO6nXK/ldgrcny2n
tOxUcaQSi20kOTNqDcamuDjim0ws5u6iBZEQvfh6+Wx9mp9/FBVGRPNC7bfIzNbN
IYUW5ljDJD7r5u3eT2ZAwjIwiLKcPV87NbShzKI8TO0LmCCSyuME+2Us5bGwRfpe
4C0Aog6YyLgzMOrpCvnLxzvJm2oPdVt7oP/vxHMzCB6KWMzxwMTDAaWdxZ6P5VSk
GqtQeclAWutjuN8YDbnpW89C9IiUaX/cMYUAeuxCKRlGtUNnYI9B6WpCorlRyd7W
oCr1eFr/nzjQhm+saVWo/G1swPZgFlfE9JLIZ2WJZ/8MP1Y37LPHuH+wE7R7ow9a
IDs6XGSUqwSelVeOVx9fEFMlcz6JhwM2fQt2ewureSdjxrzzGMXWVl5zCKr81MYV
tY3nT4OHCoM1yGtgZxFoR8ZfyyqzSmBpZZBpFzU6YInaq0/56ZcIA4B4dQhktvmw
QneykByDdJOufa+WNi4V2aN01g5UM1/zIhwN2/izN8lKqB8AAICSJD7sxLGCcmNT
anQQLcXxyjThMmHbp5yMa96rf35M+QcqcDPUujwslHXpJx6wqAJr+rjdVFrwBrRB
RE3y0wvPD9dmXGS5f6s7S0f5pF4HeZ01P8mox06cznZJ/r80YDAckTfaS4HUaqXA
X18WrqEMLB7dEo0UtM/fkhTjNjz3lODp2ssCCZIi8QMLmrD6Y1PjRHGy+QEuw05M
nS6cEoPzp+xF/nJ6Qjw9YZkhjxbzmgX8hi/o3C/yqxvSEGgfuul2bmN/NI4wOhxb
UW1sRkdpo4TpGLdnBc23cZ2dmpaT/Q09fVp3GKhdplu331r5+7or3Hrydgul5cPs
3TDenU4S5BlbW9PsUO+7laER0erFrM151olQSXclOnGkaHmbA8ETIoDJkmpPX90+
Z6GcSK+ZW3a1FNaXXjFijUG1DRo8qDi6ng7kQEj445sk4aY0wwXZaQ3ZY1RAiNK9
5ClWANJyfkMGv5JiKWpUDAyoESXP1sh0Dz/iFPzwnA9Dgx81srMsnPxnzCVBAGNv
tK3aWsYXZYl//2Tagqlr9TA5YnjVIcTS0PVkfp26p8a7vUxsLJ5XKdLpBujb0+qn
sh7A8d007ZAMg99xcNLRAUbeGOZYktVLR0i0uKG7NXJqZVLiByakig9/t4ZJ2VgA
Avk71aayVjga6ziMquZzcgNYePByLcmGnbRddc5OgqmQcdBt9znd9aop/FkFA4ez
+KF1I7TCyUhIoRkA0z9MUjYjNnIugxj67i5tDjHYUrir6bPgNyR5PsLlVhxspJ5u
pQ/aHmcRO1CjL68JkDIxfP9JWHDa16cjVxkILoPv3k+Q5if+GHtO1aujO46WXxU4
kcoDIKVD1f56aJJja5A+twKLYsX6CBiNx0JV3y/foSSDJGW5veLL8+IIXfvFSlWo
rtHOwM2/YQ68sYMBhr+IQcpgIh5e3ODNf3TWjUUFSFOXt6zIQmZn/Rp8G7cZlWFx
u7FK+7nPUgVe7ImWgFauumzNwCS3j3BhqRORWheBhoqZrrEezlIxBzzLy/YC6dP9
VwClcRn4nWVWLbEWY9UgpobKykTQSXuOcXsiH/DaDS7Px8f0OWqxnPrM9vNc19lO
D8nO6Yu/UmGPH0ep7raAWtjgVmRO2lH4JRhCyw+mcwWvjAAjMPih3+MaqY32aPz1
yXsxrM5yWizEJl+bFmK930VOvGESKxtJ2ZozX1fOJEoESHFMKQlturGlMg7hztIr
Js8Uz+X4oGNIrRfD+3Ty0u4IYyJHegcdDk9dcRNCe7WqlMr8QO0tBxr42mi+pYqg
qNAhCQaSd8q9Vqk/3liXZTPL/2Fsi1yBb832DYHWiYz3zwt98RFcKMYb1uwDeNv8
qoszDOEKEdT20o1I74HZbsp5o4e3vBRrklpUNzT2FjoBngaAfU7RYyeoqcqO1J69
xKlrCjvdC4x832EXwvt7hqYFo9fZveOWZNAPkAP2SHRYJmZ9NW/CcYH6MzS58MLY
3cJGDLQBtxtOO+V3nbXEVbW4XjXnaKz1juFsRVR6fyNs1qn8M9xZDrhxZr830VtX
SjNLAtDKjdR1qeo0gFjeTogAh6sngmnjnpN4GKMTFX7tUO4lWeL6N0ld0mmtP/gu

```
8rt/ASgJqWTx9j4qyutwCcI92HZwfznq6Oqv6AnmeCFBCbJpL9m21tu87/HGpFpI
JYOUcrJwFvkB2XPvGjnOTFdQb08GYUnjswqqye382SqcG5DDn7xvEfR+9J3hQCqB
sMYSdTK2s3jB7BCceGcW+YsptB91liBy4W5AEqQCa+MrOjRvknjxcSXf7Pt/i608
BImedrjGQkwOQ2FdBVp+nuY40cQWSUKoDuRdBUh0G2KVQkgboarwjHlK8GzjKW8R
go1cAiz2fz+sTLs1hqHfYqXAceAuoBYRr1K2dp+Sj5GzupDbS5J6t4ZWfHQjo3PA
1ezLDqwLqwPtNDyeR+2k6iLjLXxrRZmjA7IX439ffn9/heLrcujC47cr7BENzl98
eYm1LSLzu3+GSctYVmE4bAXWCE1aMebk8tJvvklk+o1oMFojVml4JdOadk7BkDgH
hPRdOJW6tK9geiayzUgZbn2MoXrLUdGL/bvMv8Tq2uD0o8WGD7NKQbQtDTGpP9My
auES3T3DfkG6kodpk/ueBR49e4UUvlMt74Qn6KkCAJzWubYJxos2bIUXjhYr3gBS
RigNz7346xPLaqQR4at9OPgmYnTg8QvHO6o0WG/BkLwXfcDxU42W3PwHBPey+vEs
+75vu3So4+vu8+zHLLq4p/+vvtrTrtSZud/KYkN2k5HM5i8QzneVst6Oh6W7FKze
LTfGYyLLOQi/TjlXWIuzxprp3f0p4C0AdKZDSOuK3pOaVy0oJx8tcDBochU9esCD
ul9rrXJivwF4xKRHThoAGHbkNZE0oMLZS66/HRnioKUPmcRUDDpZnPvZ1yzZV/UG
IfZ3iGjbufHmrVbET5MK9nzxf2qdBRifgdWvCRkoNoBz+w08sgSWa5sSGmlUmgtM
IUBwiHHYfLfRIb5E7ojwiJUgUQNK4lyyD4ooXVxyzI9pkS/+BBJluLZsYb4cdN4Q
QuuWz6qLzHPJet19jvmYYVA4tK0KGaEvObA189jPYqdYSlotcJgWEeIzfTCKXWdH
R1orERCnV/k3yDZ5BP0qVQUweEJ19zd/NZ3KXPaxrT568QJ4s3zzfSEqQLBHlHeG
+fmCjvfHv9WGKpwM1vZRJkfvg0zUx5aVE/Arg7167hZ0XpiUbAeFSaQ6V9+b8Adp
gJgu8TTDj3uwULCtOqjh3+pP97aYFFgtgZKnOBzXD7y73K2/pOqZlbyCghelVQEQ
HSVzHyeWcdj1p3+G2QGFMnFCeLihYt4jjTLP7luNeS7nzwz9kpX8DMBci5G7MT0e
xrHXVs9bEZVGCz3+FjX9gSPk8TZS9FE8Z2C8KgVYu0jgE2HTk4GaoW4mxcQHj5Ec
N7JWtXLUZ4G1uV3f2VDosh0wWvF787jpDP3dlIfgkrPlzSQUNwYKXXXB8o+teJvN
GbqM6QOq1yBHBCiRUzEDhzW4C8zWIQv1oQHzSqGtPwA4P9OOTjipUFYd+Y/7CF9W
uUoi32w+cOF9JwPO5CBdOcJxPniOGbcgtJqlN0/Rr99br9bSYDJHSQEOMMX5Exfx
DuLXku/EzvCTGQddqesEOd8uhmWKllX0QT/RzS88vMgEPiQ/UT76ux+zI3hl8AX+
+N4QaLRixUjkKM8lvEgdu9tYFU1BOBWk1nN3Ov8VIFkfGBN+xCDaGiZKtg1Foyax
crdrRwt2Bt068x6O/c61qoZeMW9bi5u+FnNhnAfNzBNHdRi6uT9pQq/XL4pI2FJS
BXokg+eLSFCJJd9ACN5Y20ZeC0WbmNNsP9XydDgjWx8+voOTFDKpSp0fXY6E59eh
fHYJUEI1RG9BiBvQt9CvB/uINLbBciZ9zYNc3abjSw9OY/2SmWa0Q1Z6NG6JUCHo
Xf3ksmu5cX2KxC+WnAqFbRAKzQM5bTifFSNUxEixCS/o4n895xBYt+XkmgbIiTyB
7SN5XpEXfwEwaIjMqEsssOnmDokgQ0r+x37Osw7JCkjTZ841i0gaDvw7chFlQ0vP
0YRWE30jk3Dp87weyTbVtm8+j+5pbBLK2nZpDgSi8ySLNzN4CdA9ppKNpIGH+grs
K/8nqMWwwDt481UII8ljORozXAaGt+KvcM2+v9CtaArPfW3ZmOtLMzEVl5GJe6+Q
wh9qhFHqCAmSNRI2LhmGDr1RYFh4qPvEH5s61j2OFvx067U8znVt5osNKYkurza3
bO4hKoRhX5aPSt/emN3r8ad0vTQExMZkTdj58MHGygEjWgX2IYTNrY8QDJ/zCP+k
8JsOq2KZpDZ120DOP4fFR1TUxJg3DV+kANkBdoHW1iKxKkn4ZfOZRLITeWssOVp5
YtjIShkczlSRH33+/ar/CxU6rIuTuwCBy8b+5M6yTkawZgA9iSicOylt/kPE5soi
1EzrD8k7MVOroggXwDEMP4ZGLMT56mBYmWouF9HE52Xs9wRcsS+QwZUPdJ6mt4C9
PhV8cBw1rrV0zJJUpHH2EnalfmwHwCmYw2wjH+74h2IQ+MVZyvmfPsJBhLpbYRhY
S5GLFrUP3WV0G1R3pKECTlPetTrhwTbMNt8Z2CrEXAxsGhIw4Tm39sieLW6eWVak
H5H9nrtpB88jRi5LLQBLXtDyd4dCI9THJuVH4VSMyD9Waq2x++DcQQ3NC4+fYnfL
5SVcsMqsmNu9lfJqWTV8D2eImAHRIAyv3GGG5AMeJdQL69cGLa25tQyiPyvPXu5s
RTi9NkktB49YXF24rEaeycHPJ8p0m3G3TOZoYfDCBh7Z7rCbgeR7XgafQZfK1Fhw
rslbh9W9tDsaku/i2/uPvjhyJETjPHxdHOCoqUT+EUOY7+1WVzalJDSMyz6WFq2m
RDWiCZ7HKrp3jT/9ecHscyO48XGf3VGDLdaciP59dlE3Ur51zyQShvSXqNne6Zms
1CjPTieD3vPVC23KUT5ZkwlP9X0h60tYnxg8SI9lWv31mcrbTOQQp/oTk0+qvnom
LqTPUlqpkX1vr7wOA6DF6f1C3UodlmYhIV6QWWX1Igd5awFHMKXAOE4eHPqx3pQB
IVlBmzaggfkK7x4Bk51EwWZxck8bZmDxIMUuynAI+kElzci8p9OxVl+B5sBodjwG
eLUPbEa+YEDN4/2CEYIWzks9zxQvNb2OEBqduyeEU9S6nmu+7npRAYnk+avr65wc
VjnEoNrfrqwn+6fxab2zPXbMfIeCfvCXR/QOj7gW0x9lIxUcvxdPvGbR78fTYdtq
BItrh7GqVyUuJ2JQ6B3slzQRCWbPC6qYIltJ6NM1AUOCveZaCE5bcHoQlnsos6+Q
cfBUExy1T9NJkcPl8L2ieT0wul39e3hHSYGijhw6VANN7qwn/N4xRs5BERQDLmg/
rd6o7SMMiXpRsqxJukFdQ60Lnss9FGJxGPprE9k8cQtq7MGF2nKnfilrhfx7i9p5
```

```
qX8QiQ5+RmW6898C1WaxsFlFPOZcmzHXJtV+ju4pGiRfNke5HyfEa4hvs9eBWLdt
OL08ZmgjtErIxh+lCaNHh+DWgUoYasBpxKFFmnP1XSq5HJN+rq0p2CVQmpB3CsUJ
hReKaUGQx3Wfdaxq4ua+zg4/TF2Y2bgXrf8i/1QZXG3fiwFSwuDASaJDMRQLpWbQ
klCp07d4Bz/GqveuckEBQzuxmTpHbHTNGGPOQ34ar2b/IG0XXEp387CeAirJboYM
bxltHbOU7MXeoEJQOOGCsebeuDCZuPB/j2wOg5sGnALC9RFSHpaNKPvstB4ptUBm
iC4hqk8EdejaaY6xYsUl/OkdLyS4+Nadl5ewMO87GqtG+w/Xph3QyONmhBdqt68l
/wB2g50uQoOi/BeEHLAbm6fe4cBa8M3RQSzllWJM2Qitajuwamv ZF/a177beC8a+
Yzg7cFl7pa9O9vcw+8EmLO5uLiYliWQa1RbuQNDf40yyCqQBMgd7tRrRv4WG1nJX
MYvebKgdRu3WPMGwbcLmryogqxB8I1ytDbRmhzwSxkwh8QjoTSa9lsAQr2h5OAqh
8mX97y6xxdvYjQbKgLQZ4A0ADNrch6DdZtDILgnAvLSjfKBz6b/kpag/MHI78irW
9m/86mZiUyPjG9i05PyR5rxEzV3/vqFornmg8rOdMXF+KjgdW0QBZRLZeMp9P8v0
pQcXi/ZcO7nEAzhfTzUjofPCTcNPQotw+sGVuvw1fjW0j+doXKkbLPPueV978gFb
rr2uuj/qyb8RtrFaisembhIH9lwqN/v3IS4P0s4CSQ64MFOXXVjvNfHXP7H3pdND
3Nq4oxj7tOUfpSGzgYwoGyQHJRNWjGQR3+jymIl3YHKYaDtcfDp9f37oiTk+gyyN
NXfabo7SnAmj4hhyyM+zW7foYAtGR8jK6lZ8tQA/Ap1N9+kQbIUMGM73bpWCyD+c
OlYfofHYAA/GWXHt4p3pACZ/efpKhlrTKLeY7iDEbIQX4mafWsluvO+xgic57m/s
y5aIsrNnLxQByQ9WQqpwSeCwNdW1DbopQoLBM1oa50idHpDW4RZCLe1WDmxxPA1e
AFGteJbO/fZ8ihcXFxedkVOUaAZypcPdPPqygkSrPjG4mnEIUsHji4es3MZ1gDWe
rTriutzzzvZrYF9YAxyZT7LRjd1Xz4S5FegghwMoqlYKLFor88LdA5HPFuxfWclP
A5zAIoZK5n4WGq2xI2L2LpILsFkS56G7KOzsdgOu2PoRT70+pAWaPFFcVbxmstlz
oULHGYeSu/fUqt/ksTxjOqbZScKCqxMLC64Yu/BKB10wQZ9P9blHQEvHbALrSp0Y
PoMJJWheFeh+C+4fTw39r59PjoMViSiDETYssRyKyjUt3IPJgqxoFm40w7JjVBi9
VDU/CkpEOeyaVUoTrGkK1dwuPdI8jPt+KmRgumsLrGU90FecJRu2nnRsSH+iMXig
U3i45Pv6yPVaYLW2IqkQLDAUKZbF4Ktxnt8ITTFF6zRslwFfPDTs0ir49/zAFCI9
DgRdt7BxBPJwnvauN0w6deQXSSyJz8CzZoQ3jY6qFt2/D6Lxcxr/Y7XFCBXWXeuZ
CtdOWTnYxzA7K8EGKGy7UcuEEqppNdsBVQSwzKtOCTaIlbA9SX+gIDDBgEZEJc4S
gXO7GNT7h5nbbSqFA5HpkQIEBA1w0Ebhg28R+XecEKUrDPuLebDDDNuJYEkVElHa
3X3LVYP4DtD0b61dDtankP3SRsbF4aqtAmW1iaR9i3Np/6X6xqyhBQi5iDLJuIVh
A031zC3YGiH1O/z8zIFdHav+8COQwp57ZnM5ZLpUPCNETLNso/dpf1tSgGBydWQ2
t3SLxt11vYg/pyJUMm5RuZb48PUHsg0NYws51NOXAoLVpc8pdKAFSsNLSAp2hziC
uTvXC4FEQCQ1nrA9z4IkR6ratIcypqAtZ0nDgbSIWs1FiWjPRdH/aYa9YsZdxUjM
RCgH6FCT4SPdZbv3J3fA4pdlC5tJks5T8h/esWdr/M88PwkUb5kiBTnOARbkxBRg
SBgynXpePkq2f+hoXzcc8cGq4u3MDzvuoAQ6TI9jS6Ybxhz3AcaAitQQFaYM3KWM
D52RvxT+scOFhx1vopZA/LV1EOYXo6VcaFUxWIEG4BPtIrAPglZcZDVuyZBL78fj
o8M3MdM9mrRQoehBziszpLzvoPG4PqucRwHzUkGQED6KxoCxxpsr5jfPAjHoCIxD
tp8RRgbB2NGrWwFyVL/hLqy2T6TQ+xhA2BJH/Vhey0keXZi44kXVVTrrH2OFFTBW
m6nxcJIONKT9hZO1Ir6sZdbjB3tCuedGfBMbmzPzGK1rnD2SeFpGbvRO8S+J/N2f
anfpai+eE118AnXZrqFOxgDMS3rJasTOEIOAHbS1mXI1XxC5oiVJ0ZuE5hESbpOr
70lMyXhBsCve8Odh93hAwVQ1OwE91STpbLvvo9H002juU5+hnGQ1dVEMXCIT53aK
bG3rm+QPTkWg/o22/it7TOPd2gByJVGjTGKJvk0WRh6vjWqJUpFXW4NstTYnSsc7
8JhVR4PkgZkCDdneIrP3NsBgOPKBoti25yNaxCYYFUbyJmcAw+izBQKHASksupk8
D8obeS1bCceOqc/zgG7kT1MNaMTQBJZ8djO2qx2UuDL/HxEyHoRsw4RO8zwrhPnR
E+8Nk5xNRcsU+iJll32LNYsfzjYrsisLR4Lur8TWSOuE34EHWB3TyE4kqQL4PUhL
axjX31qyRMnawgAQF7MRXMZDCPUPZwzBnYnmkuWl+kuck0DqkHjVTUA3z3Is6mgU
M1CA74PLwGLVkXtyeUGRoeBqV4P1z13K5F12e3ZVJrHbjs08FkXBxKgz2FFt6PrX
eHpxIJbLz3rjTsUagpTazmFacIbb6pXO1ghHjwLaoBsyP2PNo8RSUNtwjiYzrPN9
zTPvjehNLfQNM1dk5TptKjfol/QCc7ysrCMkj9Qm4wZtQZXp4pOQ2dFJDtRfHEUH
t5xjJ8VrYXUh9OYFKLJBC9IAnCXob/0SJzxPoNOEmsbXzw2bOsA/AzdgH/KAc12g
Fzolc2m/VQx7/43EmJajK4bC+nDHKPkW/1Mx/WI4mEiUbT/eQLtkDfuPhF019O87
is2NrOgruBk1HXFAHlszcXyBG/dye5GLRXs4f7yvpi2cGWLVy5lGS8LTcAmSMLSy
ezJ2zrE1kQF4tesjVX5Y4wLjsHUXA86hNr7Y/LRJmMlrXP6KRtyzOX0un0junhD/
PYLYc+qh4le3zlMJEHPmaPshOCKKd9s56EyggMt0jRQIWX9OJyNOIuG9nit9IgG3
wPuBVBo+IkQBwQzxKhIcLw5gOhGqN7csvjqjtIszpyqzPTsipGHm+HmciHDc3yHi
```

```
m6zuwA89XkFuacgQ3kYFHRTUmLfkXy/iHlWLinJ3uhyiz8KAQaRpXIdQPy8gugMR
uk3JMiXkzIRrgOPe73Zc4Q1zxz4ef1vTVu5E8KnvKHnifqSP1nIRlb7KqP8rRvLz
HxKsCGtTa0815TNlnZsLxtvU8EPKDHMF1tsZio1NcCWZHZVfrsBtxDIukdmZPoZM
IgHDIpnH1MPS2h9jOJnJNNsgs+jEThAG3im5R2iunW2k/xBL7aiEJaMs+u+m0Bu2
u71w56jBNLK5HiVknh1ZaIMc1YfGtT1ndDHM7Ft4P9eaGmUDalSHB/vN4oY/fUn5
z25FoKwZefDj3ea2Fu0mJHPlHhEwy4S+i/17EjmJTpuicbNsaveRrvmNUXYC8/9b
pyeiXVXTR1VscklbCreBBcZ/6jtXod8YslpXu7xdfkWJ47Xe2TiK0P5N4tWE8ZQ9
m04dTN1KG611KQG00q50qjPiSnA+RebwO54QtbJ5DMIlwT55qFdnDs+ISTxL2Vdc
UhW0PH5ClaSoG6cmpZerRVxrRsckfEhTAzCnJYQ4yKtPeso6sc5VGWK7R1ROMC5p
2r49Y/DaFt3QaE33GcxZn3eXw3g37yfBDq4U554wFM/Uy9wnv7sdCfnECJiIiG20
S7ZcH4B3u5UvaU0oEffdqYq2lHktk6Awi5+/VkElEUXr+koW7IvUDvzjAvh/1UQd
LokZ/lHx904fRBdyVv6bu761xOTevZkMUYjhw4Xfb2OQ5p3xoo8BORLUZ4HjrmhM
bN1DBN87KkMIywgelB32fOrULOzyi0cjJd6vRKCaI8zX2MeXQtc0NEDm+kDYSQDO
YPPsuYB9EObo0d4B0tGuMaLWjHBDJe+QfhPEiw+VV0gtUTOMVDuK17aYiJw+aG/A
mFspB4xDn87D8WYGEfOZ441RcX0/py9UxKD3Gc8taCEDXjK5nNsRvW2CowGLUvaA
QI3Yot15hgFudNQSOgsSWcqL9BwW28t/mAt8orp8gE5qwrom9AcJjTPnvM//TFyJ
DLJ2UicVNLAwDIwIR46OetvzkgCgFI2s/jE2B6Z5ImfQ2AC9rLLa946vmKNsegGw
/xfSfYzTdZeANS3qbg/05R6VUMIyBaQ1v8sX9uWJcAkoefwQNnyzMP/bp9LthTxv
jRxBFRenYtimcCHNQ78fja0ip0TrgzdkpsQSWAwihRknTZxJDTUV66S8bBv/gyOJ
cK2oJ6/7drm1DFyBgu5LrvjRn15fQ3oziM2m8ElJvytZaniYboOywbNw+cMh6V6h
EGtvezkBWJC+5AFAZEXYUifLbEJfFcMqk3BfuzuCA3atKhejF+aALKTI/v59d0yJ
fK8WP/NUBI3wfizmyjY5UGDwRtoCOaz7esm9PAEhvqWuHnFzUlc6/ZTxqjY262C2
vOp0qCPDXbaGC773ncVn9alpZy6L6FBPSQEemx4Nw7LHhuQqjbdHJ1APw4GS6U3S
bFompO2/30cOsyDH5duA2WP9xirWJkAOfTv2sZdVcOlYvRo2YuUzyIYK5OCnb1Gs
l4c0c1PuYw+6xLRgScDYmbxJCEMb7xMu399YBmmNd9/CfmX+7BuMV37m3GK6tKHg
GCYpGOtA7KZssGdCqov1NnkQpOsROpScta2EPc/M3QQEXx/q8Rke5mu/kxlvtWZO
UNkzYvLsG5Vxg8d9QFLTgmbSFw5OFttoMBuOjK5TVULSraZDMmqkk9O0UtznOiah
firENbyCfwkzmcXDfJ0QaH2EPfpAMXGgKx7oCEHmaoIDOXpp2HjJWhq3h1cA23rB
5EWoppw1+54B6JaRzAe7T9JvKYr9JoMvH/HEakp596dGAkC0Suls8hfGXfP1F0QU
WG79pXdoMekT3DlMjvMd59OvdNQD3odeiLGosTPFydtUtJBPtuOxZje3We2rV7RC
IYhWqyJu/OWVcxApOPxqlOzifoTJOyLwIfJBUJYGvhDaz7Q6fdv12ICxFblTcH9T
0WobGP9BCPYun8d6bOxUn+IBAMxm1LtEefx5Sc25ZBxUmIgy3tNY6qPwJqfXEHKJ
oR8j07o3iMjxqu0frf1HspSm0nZ8SeJqtxGdEvPfli2XBsI/5k9cZ8W5Xr4f/uOf
JfPZdKAGIFKGFCds/iOUOqB5JHBkH+S+LE0GKgR+UMQO07kCGy0Y2TCmgND36/9F
GXdxIYqepUfuru+g7cQkJVwUGSP1fHjdNSh4oXs0QKLvi5dYc6cC7UiiPjZV4ecN
l7Z81hNvDgLRSAUW/wCQgLM5DlPxQuuwM93E6UMGYrl+oonBSaAMhui1Lbr6kO9F
vl0ZQ+XJOciLotLztKTJ1wBTC51NQ3UTH0HSIRnuN7iUWEarGF88wLc+0GMXB+87
7ZegDaITLQ2C4/RzomenhNVWTMDmnBuZ2+BjJu8UKCxlglgcLZAx7sUjkQEBZHbC
u8TqZ9NWCUh0QSu8odZ3AuqB+4xRWxlKgvZ+ei8mGiWttL3yggd8gqUnwxfukD0v
CEWTXEUIuNlR7rcN+FWmFNUc56vhUgeXLBGS+6iNkOxlLQlmjyqqOyGSZbpUJTYy
fNF+9ks7Lj8XvIMypZT0Y4fsMzb2AWN/hYidTzsCpn6HQ257b9FH3e7QYvzsABpr
M2wrxd7Dqh+oNJTG66R2M7IjbxEnf3ih61OQKYZwQmiHwOi3HajpQFxCntFal4aq
lH708pAnY19648R/L4mi84JCG3ISsiuUlWBjNy/e9bTDxcOREo2gzwvWsfsPPKxZ
kHq6BanE1xGZpeFcl1w0CL5qG3X+T/PQCBNK7gjupzuwf+wU1KGrB514OfcLysE9
sFCMzJdIO0+TsO+YZT4rHN3/UYoiPpSrLb2LUWnYNk4DKMHh1MXbp0SUI3Dh6Ysp
dKYb52bgzdMJHqZHyK093YcwiwICeKmR4h9JqClmjFENBvQGXUzPAcoO+wTf4EED
8r9HdgnkfiwceTZgJ1mJR0o8GDdeSbUjiagno3G0Nqd+GxZvblmsagsna7xcyX/l
4OaqflhhBEkJ4W6lOp8SSImAmghd3A5gGKTCLb4ZFAynXqC3BQder0z1Tiwq4STw
OgTFkqriJ7nBuSMY5ChvdV9rFv6kHqfd2nX/2q0pO8XRdCTl+Lk94lPSrrqbDQDo
sV/YzpzntxsHrsjUY7xsl5nN8kz/wfV6cX3dvTAmboVxH5o6y4uRaHXv1naBT++k
z+r2KEJxZKfh46rhLeKUnRKE1ZIPBhkZuvwGjdrGEOJFJTVZ4MeHm7sAqNIkfnlQ
w4MCAa9+ObBqhIt8tWmrSQM+T8eIGvb5QXG2DhDgsfESZ5nuA2ABJ0wiaTSlHhs1
zKxjag50d5tU9djecebvAF9zD9RLwNqQY6X+pKjKTIqRmk2+rqVwJN3bAsD19xDY
```

```
634p8U8NL0QSvlx0qeHJCvuhmvaKywWQTxmEvORKWkwMA0jCBLT7waQPGQRtXani
w6U8eg6qoS0oF9krAp9ClgXevp06GchReI57wb66eENFvivcG1cgERyPYnX9XvJk
rg0cJievBwpCMIuSDECkZridoojpU9GrW5lLoG/xR/uaOlWd3LvsqzeMu1omGy+Q
KW/T/WJFy4XjesVkcT3v1fmzRs5UTDhVjHIVvfT+K7WSRGeXyePC1apx4lVNtPn2
lPC4O0OT2OFyHaikuXlJIGbFQLNEJI4/r37RQ0TSySmu/23mARmOUS3CtabK/RX3
AX6wAOzbPH3D++X6EoxgrQFug2aAV3FFv5WHCAtf+4aUwYg5arH8/dSBtTRs9u3Y
vqggFYAm9xfXEc3Kfqw8etM2Klc05H6PCxgPwMgwkQUW+3vOsvRTAKJPLlV7VTGH
2AUcjb15nD+WshrvCV8zHuZXH0i9O3Sq3YhcngE7XkH/LuygyDDDBaeB7Nk8DG2p
sk63Abnktw3wgUmp+E5btpTJeOSZI6y8tkuceAtTDlQqb6/p1tXcDAIGGWTejBqU
iCyNjQ461wvCOQlAommyVYqXhTziLXC1waUMrIeE7dFGZ2V7eJE68JyZ5fqklYli
4V1S67ck49oEOSBd2XDj/tO8OnfFjLgET6Q0EOOiyazvO7UcHNjMfFoiEnYjrwuz
b4AolIQ3eg2tpR2Scv7rvefKQbQvEmHyLB+/YXKe4Chcozk9puqpWyON1b75T/mz
4WTTuemUUd17k4bstJRHuIdRbNyJVz2JmIzk2d9vkWVkVXQEGjgSTa3BoUv+2FTt
CjcwP3lYWABP7L0kR1+BneG+DGfnmPtyjVtZno4nQ8uMxYj4+IVfpAID5Drxg+H1
dKn0XM/DzkCaCrQ0LBFTq+nJ9UjdD+bgTh+lA9kR3b+L39UDTiGQlBU94cJ/GbsA
gK3dIbcOeRuehA8JtEn2tpgE918bkCUYTUtFDWFcEAUBTG+w0mW4jT4O1yLysgJt
JUTEuWNg8H+GA2iCRsXhTOo9KRpJ5vQ02cZxDFW5OsuZ75AxkPvXmcTVpmuBjpGv
HbtBScW6pFYbDdX0ITYfPKEIakUeQP7gH/wKkhE6U2dBdWs70BWmjBtVB4i5alIa
/fXgaeJswsV8TA59m7ru4kmGBoLfo2DyjVWBNS1I7yLxuHeeMnPVQvHYe3bSGEVd
TOstxvTJTdViMvNoG5eR2+imC08XUKBGY3vZ99+aq52k0eP2IKnG8ko4lKO4lWhZ
sA2OpLPci+fBLnV3mLKl7YbLj86wuOaZGGB39RnirN+s22O6V3POlBmQ93cgVWUK
QDkm60nlKs612DAHzKCU5DEYep7L1swrr1lUbNqXy7mSZ7gNtr9b8Nh1QpIk9/E9
OK8Qwnvce5TXJ8mOETm7hktKztG0YPH0RMrKp2Vc0ELOJI/ovrAHfKqN0229gGQm
Rk/zjeUaWniac2u2zKrAfCSN6mWxdMIqj3wsnkqhN828UpIKarPwUixpnFHysiGY
QQ5xiC7Rai7KAbiifoFK6LjckMkkgxWBFMRE8sj/PjxfITcpLLRq8QM15B4yHSFU
WUwYPip72B9MaTue20alfwolgUmxbtniUdLepeMqGqnc0K8HTOvQfNHW9Nc76bpg
CiWh9B6nzkyLBY7JJfcT7DUXvcJ3KjgTFfsadp+fWjSVCn91bPq3ZkMf5Go+/AUK
K2dvBDKsK4oCtV8qelLDAgVrNE/qd6X8h9Hym8BMcjr690TtcilGf+HCAyIhZYZC
GEIT0FEq3lV05htWDlsCAa08Yn3JV9u7e/FAgxbAVNMBLg0y7ZUQk5ZGEzFjsvcW
cGzwbhWvSKe6n7O2F1wp4G5P0p+ydQyXHFwT18OaFKQ4rf8+3KTdW46qtlzKemfj
58H9u/4StUZ1lNOjcPpZVrBdbK2xr8qmsmxdaN/uk9Vp7l1LFCqeiuICBuTIjXn8
CQdI7C42jU96OX/btw2vWaWYVU+zbfZzIockr+XsJNiP0tvpCLx45MJ660KhE6Od
1YrF3GDv9Yfd1as3cRvlvW7+3DYcF0UTma8mV6HcyFoDa52/WDWrfxBgZ7nqdZZk
VMXpUzPWnTCrBzwsionwuILimjGaN7P0gncZsWXZy2aEcVWruadve6LKYgg+aYGj
QDWKuEYe/c2r4BO4EtVt6ZNaH46K5qJ9aSRmFcGb7pn4sEjKmPCh4z/u8Wkv8Rbg
XR1VPCVCSihiHtMjkLtXt2PIAyNQyoh40wasz4kHVIFlY3Y4k66hppgWH+4xvGBC
ekI09pAiBhESEHQUfqoGcvQOca+J5fqaUHVwJBzC8PmlApvCB1vyOW/vZFt8C36j
A7V4DBiWJeOcR4XGsiPKotfkP9O1asAi99+9u4mAcriGNn5l6c8gtLCQNN3isA9C
2/0tv0fwbiTJJuopqE6lImAvzMHmSszwafY+BZ+CfsYuaUSy2v8M10r6RAVBF7xJ
I7/dAI/ypJYPEEHvxhPrI4BqgqGS55g7kl6J4cBr9veDzE2A3iyZ9y3N7XLGqm6T
mJ1Imxm3CVb3YlrlAUrnt9x0Zy1EfW9YOGgrWnfQdEe6p/j1El5q3q8ziIDqSiTI
g25nfIcT1o9z8Gm8UXRr8N8G+FKXoXX4EQrYhWCaM8oMZj6S5TuwMWGDTfQ7Q6tq
/AgGZvNOepKzigxL9ORGcEAS9eDu0DtNikRR9Lmkzn68uihMfp6Hcw1qO8uY0RHU
sPdX0O65kaJQ/vcLOl1L6bkQompJN2bHHjLwwoZnZvxsTq2gTh9P4OiKSO4vpndN
qZq5kxdg2TP/TrN0kA8CWd5msKx5FM9x1EJNGuC0KzFcCYpcE4XFvCw8JnG4JSgm
MDwy0B+Ruu/Bjo7QJjStj1Lpu57GFCrmAX3HVYkLrv6QgifXhqaISlpmgXdss4gu
rwHjmsq1723rdASYRjRvne9n9TwkDTu1WpVKPF0PIJYauw55E03faXDuKhVAdQzs
ZQD/CUPo4RbPluo0/ZeDeHH0u/jYArFIg/awXXDga+TjiY6eu8FKrar+vaM28LHA
sF9DrDph2YHDcE5kD1DeAhcbcK0qsCyoQ51HASOPmb6W/u5yfjsHaDVtJMogwgEJ
0HlZhP+Nl+5D28j2akrS5nbEfDYFJvk1cO43uy80GmqkxB1/R+HfJM8sF6fkQFnw
QpyuImxP9KUbfcHyjNRd6gESQwQrvxxOj8mrOmThH6JnHtkIJb30bIJo6M5aaJk6
jUUb7lvJbkvDFxUYRqaM9qg0OSu7XD86tgcw/zR/NJ/F04cacIAxEc0w5VHVILwi
K+iVstEMTSIEMJhGcrTbZaaYkNWnF2IQuVyh/xmxLP/4wdzioix7I3wGpmKORLGI
```

```
y47MZZIa7C7WVl9Plf0d9ejMh/8vyEgXGX5KNgenpBmwH1Bzty3KQNPdIP2S0NAL
j0Q5nLa+ItTEi1pu0M2cvOvhwl96cdeWQgwD5PQj3iW/NZsM+4hrxrZ1vnEcvO0q
tlz2+thGWwttNrPp3+8V9gTScNynzxxntQ47fveMUogh0zfZ0IoyUBrl3AbcuzUf
yObU9Db+0+Ajt8n5lzJGYZIvsL5NJaPdPh4c/LGeQ5N15gZKG/BvLVfYg5HRzG0Q
CUqGS3FTnyqBqdmbfpE0w8x++yM1ht2Js65jDDMQ3TEfkMV5AquoRy5EXPRx35WS
jZke7m4b+fjspP0/TpJVKyLeIFql17oO2xyHpWo2xilcmZuohPeSns6NLtheRlCl
nQf9d2phr09UxHL5GzZb8RUkj+9hdk0REPFFJR+ibz9UfK48bKqakP94KH6b5wD/
3fFjq2NlEx8yloy27VGwy6X1sJP1iiNwl5kvMCVqsWws/NfvbsY8UQBL9dG1aaQ8
0Us0GXNAJiF6r9JOBCS+DkRSPQYAuXFy4j5j2xgSgX1Fv6LmVQqsmmClTy2rrD7K
XNcAfgv5nAzqDk6ESED8SBUIslGTC0CIFDSZ2m0X1oHsbHjdlAkzd0Zz/zcefGow
LpG4/30DYFegg788TD50BFA5ZgPtlK9RTZ6TvhKP0i7Qyd9tiBiAwQqLjK7OmRe9
QMA+3fh8iQPyCZNZx6UP//bhjBmkZs3nJ4swLhaBa/rZop8UHwvXT4+Y/YP49raK
NwUgyNO6m2VPFo60jm789XP3cnsSMU/0WnR3BruDsq0EF2G2LWnXucIT96gaeZLo
AWoSrIiHbtIrGvRa0juqV6Iqw7mqq/EYWVAN4NOBDm7m68QgUHtPGTNL3qqDc11u
QCwjR+Wx/RT12P5tlJMwuTD0Jt3iempdttZ3rXeP5I/Knj0Aiyztj0vxj3/PK42d
N7l/wZlY9M+nEBgd3/Tljhet8p7loaq9MXx7DPl9S5WqN3DNN62QVervhzmPIOsU
+09xplJcnYBMSjjB9LFmioT0dZJXMG1Ro/cYGjEg8/58snQzQvQLg8IVMMwa1Kcx
flt4EOoXncz8iuBsb2XvlV9xyfTbelGeT0A7Ih5JE+dv4VEiHhpym2/Zk8UBg4Nb
2wQD/nnyxiJhUmz3q94NOiTW0/p/F2yjO05FHkcCPoB2hLWh7BPGag89g7oNQ/2B
07cZPotRiFM/SVLL18I9dj9JhKsbXrwfxlLw9HT93LsfcA1/UBU0yvNMMkwu01RU
YZCX5OdVd5jxy2oC1INAMWqT1UF0a7vny1SPBKZnZTPwYZC2pZOT532bgzVj4iNa
2WobdMtqVOc8Oqj8kVJ6etc+xzLSewVLjF9F7qifhjbkZvQ4cKvpoHMX/PjSR5o4
hUr098oq7gekuQLSXDE+e2nBCk54mdrrn/GvLpgDevFgVpL1YicmYZbzXswzZNA2
goMeRJ2KRf+19rPUTBaYzuOD8F7hdUXs3tcO9Hd0bIiashJ5Pr4twtL4bzaxsNCI
pi2NMJ5CUpUDtX1vsgZMQvUEYlAvlE/OjD+/0Wt7F50Q7xQVInqNZmVgn+i/k/V7
gD95Nv3I+uJDR6nP/vtJZoCR6Zo0+VabojW0OMD5osUCMV+49rPTzyhqSHI/zfJ5
6FMZinXi2o3Z7SWP328fG7uHi2uBMV0z1uMonmdZbQwB9zRSPtWaTqXHlAdBu7jp
HKXhbFIT2GYMo9qtB3w07DBhGu5K8z1RePbz9f0RATSocm1lNXN/TmHjpPKdT3Ym
o37lbHSvfB4IMWfAkyNeGRGDQqTralQK7yNXJfl8/Zy7ZCw33bX2dC43d5j5OqMk
b3oBWOP0Hkp4ZpU6uEOspj+CAGb+UFvK8nL7mAZsD8JGHDsKLZec1Xf6aQM1o/4B
XDT+nThG0O0DVE+bGhrOhigCcnOGO214xYADbsZ0iwG+eVt1FRatOar3B/+/VsvP
eoz7tOUhkQjtnsMCulBVa/USbv8xYxEQuwhSS8oUCQQCBroNqoDITgfLwH1V4QGk
q32TWyNF6VV4bxUGtNd/1MrFKVK3z/FHlx+E6E+mMrSLbMy0mwIrky6w/xpoZW6o
mR4mAtphsTJ5ltpeC/yZlvEcQ/ujtFq0g3r4qFM9/W+UNIJEfpT60DvoCE5/E3bm
ypMW333yRN4U//fgEKCkalVzDos46EorXNuMInQYIZMo7KZf+dzAExRjME5lk+lY
kaQRLYULZivMCuatX3y9mNTTuP+KBbUZEUAm3/Y4lSdsAqPWFJwbXFBtMV8O84R1
LH72qlp3Ibw+MF4MbNFwc2AXKfIENNffSmQZhnu5mHR8dSEyJL1ULDay2nECXOHk
f4y2DOSE+LKNOfFd6ft6tk4i8OS3/AvpyaghYWQ+4sjhJ01gxZGyHSArFmbfrHZ/
o2RRtlQbYGHo556kssMpLSYIL1PtPJWWD/WCG8ZZGV73lXyKsr2rUm1XMfCPNgCY
tRhjHA6G49XyevoD9mCnhsC7mOEdf0mLN5U8WcimXKZpM5N9BdFOjahFzIwUUTF1
qP2fIIMa8EfgjfEWhxAB3pcR1EOCB+Onv1AsHhH/ggKGXeahP3k9EpZOWjhxH/BE
dZ0I4yr2gzpOE39QcbarQ2Zm+/sDB2+I6P+Jq8b+nOFyTb+wevPSiNl6t0Dvj0tm
2Yny+y3ybTRhzj0u1JkybdicMyPeh8WANXmvO+MxuFCMhp64fP6sNNHcovA1mWGS
E6sa2JTmlHY5kXdGkl4RTNBn2rSJvbFxxUHQd/kpYalFA1P+iyoMotWkWI6Uy3Sd
chVZW3vyEZvs+chnKT8CRoSnEWifW948O+LJt7UVhkAWDqAqA2WUGqqoTY/oW48v
zxmYhETWDaepSNhBI9MZXICyz/HGrxDViOnc2wIKrrAd+9Nsv4FNHqYt9j8X8ULI
biOLdX/zCL4egbl6bjNxCpES79NLAz6Bh9yXsSuCicebVD/oxBOSOoKqmDLWCWOY
jEEf6Ys6/EsZ5+GrT4eZ/9tKwhLqdG1uSwW5Ih373W7M/wYSrlO/0IDfXMQ4bM3q
KqJolMdQEDspP/V55RCalfo0OmUD2pSfBcvjS8Js/UXkHUvHHmBayIF6wvwX6Msn
XIQhCQsrYBwQzpkK/yz3SeeI1mFXbPB08+XnjeoHypfFziCkO0RkANLuXPPKCtbV
WJufrY3uZallwD82zpGYTRUXmK08IslaHJ+RdG/oxA3CFx7JlGzrCt1kOAA9q9iJ
bYL1h+j8GyS9zvCNKVB6Nu3zhxaeWs/JJQUre7K+0sRAe5Mu3zPVgpoV/ODvHzmu
uqtZ8zD9Uuof6wsi3oMKhwOiJ/na90WR/HZtiXFH2pkuRRzl413Utdff7SBaM4e4
```

```
oBp8jnbpme2Oe7VLB36ENVweprrXwhiRwJQfRYCGPPx+5j6fzCm4o8aLQwFB20Cl
omPPOmMtOPgececYN1b2ft5L9x34yFSRFeGTr3uWSC46COaqwocVj6H88ek9Bz2L
9Jf1EqYryQ34UtCfzcmPIEEVqDvIxR4WvqBTWmqYdlyQxEqQdk8dEtTl8dQNVxaH
wBKe9WG9FZ6ECM99P54MtacL4Bty76yKRB0uVAWhlTTibuanTF38S2DB95iQB0e7
AG/S9qg7Wo9lDD6A2sVdQzL7YDApGUMWaI1ePC7ccSCeATCO1ILj1DbxhaXQD3ke
hG3BAGvKlEhMZooWc8I2FaRrStp402upXtdysjizz76aBtXh9yBQJ//TLFv+HDLJ
gcPDPEnHKg7hieVpD2GwTs2VyQTbxDZW8VYAnEezscRQkehdUHY/lI3Sa55vYr05
XxmN/KFq9J0zfIt1dbPkbBAzstA0qFK+/pO+o1OeQRo4miNZBntSlU/DWn45q93D
fupFYWzbfOtdPYeuQ7h61lgyLeofsm0jLRE1DYzsFlMLNlSCoXcEPQY1IPGoJmug
9XHIDAcI2Q2G3U1knCSJVTa8TTF/P0QqEuJL+k9NCOs6KuS7+xbYAw0gJwerEMiq
LpZ+myg0HQvoqykdUGg6RzqznYrNSBzvktdizs3hodOF8VoETH9Xn0xl0qxqbnMY
UF2i7KKrtKHOf8FYyeV7zcWaJoTRR+/Dlj1jZoFSP52nG/Ye9FRchSBQiEbrPgSi
lhIGJKXmKNo+h2tAonEZFU7qBjxKbsbpNtQrA2zN/Y9fU4uq5en+xLZWKxkpB2Ys
VukPVXFK/sG4b3IgkiSy5vmaYX440ZSYkjtNrsiioG9EMmhtSnxZtLQw/vaIFreQ
s3iaNjMMfMHby6UljRrprsbP1NoQtjaVvGG/vCsGGCCx5N4hZ0ViFnV865DUeGwr
Qna7PGdnPwBMDEUIm7qRO39BJgYGCUfXEUyrgIFUcAH3acBy0k58C7fwtZhad/UD
A3hsx5NF7GWimU/D4u0P+tBQMO3B6Sg2w2ZJH4oV3p3QDxOvf+Yg06j/PmszH0J3
vlFioBoB9lDki/zXmcyFfcg2Wf6UMjmbXk+RZ17Tor7A8hJymznJfINCBlizlIDq
rooWeBRNRUgbzvTIO2s8v1Dwvn1CNaJHlP6nBYyrF3ii2R1YJmKcq8E3uwqtW4kN
D4r7XZ4d0VNAJqRJqpqXOPixReJT5Mda/+Gv+35iNy0aGOByvafh7T0wGCFBbVMp
+TC4AaLwvKNmm0rceKGKWEuo2JMYc8wBzife7R0jqmogxXjOoFwMzg5DL828BhFW
R8JLSMDx3vGXmaNUUJSaV64SsaKKPx+ikfQN0rpkQ8EaMxl8gTyM88F7eJFjUxk2
tC+gte2inSGiFgtecO1u/6fVBhGzOrof1Xv+JBAiaIBaVcj89GydxC7nEYS4LtT3
vd+w1ggrjnFro9WLjt3Rzv8c1M2kYBsceo8DGjTCTphlooBOqI8ROZA2MhVzIQGO
ZF1P4qOZWf18x5c1657cgv82YymSgtAWiUjO6OTBMuJT4BDNFhmHmO9k3GFr0PHC
9upyw2R1s/ez/B3A8nNADAXc9xl/YYEAgqfdiC+kyxoZAro2/9nEs6HUSekRBmPh
xQuRNmGxsJyDbG2zMzYLa7ty7GrObj0aT+QqR7aKQsbm+qo3idvjKmCS5OqCXMCB
U9GDKBb1YvwlGaGCVuqK6xQJ3AlQvfQ+CsuEe1mh2Y71mF/wTa4LDQmwZ7iIhFHm
E3L4HMqZllp3SeNis+LJlD3+YaiCSiyHrx8Py24iCCbzVLyMUeoG92f0Z5JJIfrM
VvZoKePdj0yl32tMtBNOs8+g/GJ61OWPD43SzlfU6w32RRjsjFJn/fbjPAk1zgsX
xL2ifxOl77iqgbS3LsGKM4etr93hjZRSs1bO2+owMzc0US+8LoJiZCjlXUl7VP2N
ESiTLmLRAiMzuA3ztnrOA/D6UREak5sKCM3ovZ7h6SJ71ZT6W/y3wxVfD8LVBKLF
1QspwvJroCSWroN8yIy9V52w0EFhN9WyHSiEGhGT05B3JA5F8wqPrHBxIpGM/L2a
LUCF71VAOZb3u3UkL04bgfec5FRELQGvm3FS0wBE/g84OLDb0710nUVwAM172iX1
VMshq1w1ZhJXGPEoT7IfIeCHfoZ3/iYkiUpNoshIhtvvDdxO47XbZBFAjvluUQdR
hxRm80bz0s+qa4KUWFkk4+8DhdSbuMGpI2b1Y8gSK+nRVy9kdjTg7mH5eDtdG+uJ
u3qkvxWlb53zaC/BE/XoQLnahPQc3MH0yKgSK/P8alPjR6yUoMSFSk6TjCcb8AuG
yF9oJ8ZhcXZHyC60kNwdP71FfIljocis4wkl88qV1FtmeeVvHpWc4SQNWWRxapAC
cYJ2j66AKR8pEBMQ7Jzia7U1BpgXqGw1tw9+uZRtymz9qnfUTDyHy18hTlAixmnt
H/HPQlDAkdM+vUVye2+tn9Prmo9IUmN7w3L/OGih53yneHPoG5G86sf6eQtyVYE/
FJOUxzXqFQzEdM6X3t67nqAblmSmlWLwtsQcfi+ZplveNHGy1SSQfxo1x+4jnf3m
Cs+2AVD47ip189gluFjOxA1ZQQ/o0qM7Xmk6aVScDemOIsHaPDuO/MQjnIaeMohG
1GdorWbstq+kIxZ9DCjqMqn1S3lpzqjwrGvKe9B6w2MMm5DnuFYTSKRix3ilUYxx
vYI+XXRrbV4fQpqFk2lLUGaTU42wCehgLHqlaHuoBWPnBO1EUiytZT5gOvHuVp26
gtrv3M2NaI0zKNtDAjN9HOD6eU+UF2kGxzkEPD4vAvVpA8YGmGoLS4o2IJHW+QU8
Sg1VnqqEEerdcpO274TZse3J7oMlswSCDiCZs5m57w33M/lhyZ9HPIcVJvwVa/Oo
bAJoNOEnOCMeHRMFiAK30xg7EhtBkIVUmrf983vi3crSoa7WgkB9uFBxFz6z/6IH
lom56ID0Z26qg2ja0OIdGwVtkfkHijssXBlCZCiq4W2QMOYI2zG+sNGJKMRunuTG
2qRCorEi0k10jTldn0ZZpFBGcPDLD9dyF/NUK3JYyRXrmjtCkc3OmYhFEKWXf6WS
+hX9HKAL0GwzqMph6NuNLPx2NETaTwNed7zCWCK95w0JxsxNc4A3nPX2EvnKh2wf
e5BH1BrPJmERmbcmC8Zbvsg+ULM3NUPD+w6B3GVmxC284ew6HLEyG0oBubMZfahS
6WE/wsEwEJPiym2O3+utrw9VRjNZ1jNV6v5PLC6l8XXYEpZwxpltuPR/513rLSq2
ZZu0TdcCNrlk3p2sPml23qHPC1SY9PHAEL3YKb804rKFmCH+lFJxfwMKUZn4Ad7H
```

```
Bj4gmLV9LgxA7gg7i58lJCmhMNfcB+vXKOvwK6Za+U/2kcyz3emkFf5q8S/wVQbc
GztVGywfhe4dCgTkssZhnPVKBezHmPX8RXQ5W58Qqw3cw5mQS+8qPYXGE5WeYEpm
CWsrkkhYJ4GDZ65TgokVW5iQQIepNU2HfHx5Sn+G1yj9foOwzXMK9W2/am0kSNxf
QLKieq0vXJNVKHv2IchbD/s+wn66kKFtS/sgdcSQLHZMbgIhl1PTYWd2clPFcWzS
4LGxawe5YOUDh5jOY4ZseYzC7F+vpRP0d0BpE7VQw8s7Am/yx5NUiO1d3oEjT+Pc
yFayClwWVuK9M41iwmBIRKqq+R+Z3Attpf0GaIegsyqC/NHX5tHsQBeacHPKcjZi
+lbFTnmE35t5oSJ5iU5mk9sMWY06VRbHTMpGoCri6NxjR4szI55YifkCSsXFWza9
7pP/ZWbG1q6pD3oeHaYsyoiUn3W+ma+CyRgLhMn4pV2dZNqUo4V16Vdytz7gNxgr
Wku6Vf0nmYiNuIfoGljZI6vbjplHNeiQAZzxayxi/jfj7mXHYgRjV24C5Z3eJslO
b6UUbJgwm7EA1AWfdJnqiUgOBn6hBOZDutxEIDICi4C88kOgwVEsKsq0jUB2hDDg
1srnuJpdW2k3XduWvs9zS37djBaicv7SU+j3EJVOSEURWnPloKLAoG3KQC9bUACP
13N5EWi/woBtzZnTGLKNZLvF73Chd7Q5U8/pBOsutIEW/nBpx5weLCbty+3kIaWI
CiSUNi8SYf8QdUAvGNgxzHKr2wcCwCwKb2VMStC7dGY0+ZNfNTltt8WL08IntbKo
dJ4uDH/NF+rPkdWWttA3mMRj7AAKkG0AdhWKMZjFd5s2GEh1uSaDOumXJBVcMwPg
MQUQm6EUK9tgUtwer2Ye/N5Fg0tcEdZ7Tfuc8QJUouTQ9K6+7vF3DuXIfOsMuBF4
1Zti83QcJbx96ZTdbYLMM/us5I5G4vzMj4lnDoV7/9T4lepPCVkI2KFui/FWDok8
jToP6p0m0eQNKb9VNOd6FbMzorom2SnN5Rn1Tu2/nO0MfVjzSZ1Rxxj5ySiJmVRi
nCdOWXEKL7FbiCPTD+3T9gFdZmLAgXJlpfuYjSlzmGhdocZfiQfjAcRisHBalxjW
ZjibyUfLwW/WgQ41cDlAZQSW5MQG5blJ/3Cp9ukr9W+cwaQjB4Ia9fwiyEz4HVMU
RfSpy3+2cti0Xsp5G86xegvVX2GU7ahyblBquS1nLUBoebPGLEhcnL+YdWpQmUrR
qTE2SDCQ5iAKeBx9TGcbbfSLvbS6diU9zATiv3UtQtypj6ziDAz3QQdLmBCYQslr
LTkC5q8VYew2ypiBo0gf8aPaG4qvxJYbLbVS1DyGN+o1GbJVSVlOu8qtp62NXSpV
fHc1/OxPNchQeSsIDPfnBskMcsDQkrMXr4Pjz7mDbBW/VAk1Sqm+MA4LlmaDtRHG
0Hioz5isRebxti0UBWiJuM0BcjDT8r0Im0algPj3gAF3sBmCcNGtgwZJhq+inkti
Jlz4euhUXIGbrj/rIvlK/L424n1eNoI42cFDdmQ6WqTkod6NYWhEC9NWnQ5NAJpF
XcpIiQO3LcfwnznHamp0oY+3SAJ4dSonaWUn6Ik57rmCyvUz9qYxDrg7rAncvNcS
68Y88pD8Cd80hJmi87SlF4dF2aq0QsPX3uqf1IBPukMh/59lpkeTzlMkr/FnKBNg
2p186yuxGRZHpk/YOImu6SLRX5QOmwBGqExKbw8HGsXY7mNQwHfgXc9XaOnM1mV6
oW3s7t1XkEq/k0DfKx97QeyQu0vX3LxnXdddp8t8uTdjYwB2mYiFQ7UpsWS79rvE
TWjndD76fDJvDNZeROwSuIn846im4QiAc3GbnhCSpWDeJxmOoGUdGrMCImiFH96n
2SopLz8k+jRDfFx/kY3b0pmSXkBt7CZVwGXCx5OivJR5xQXD/LPz4OukF2uxHBCh
Fj8ZNVAnf6V2j+WFH8RZlSoFnMd/jOWLktfGsI7Jq7jm1e4z6ut4x1wlnZnn2Fvk
+out/K/B2Ty2gSuMlUYQQRDtlrKBJFQicgallYE8IOkDbSgV3E4ZWKk387L/k65S
byysHwFdQvORndRkYWyN4E+LUyf2cteDHcQ+jSMoYsc/OqJVmNh+/bxcpeiM2Flm
+cPzKTu9qO0fRenRgNsK14smV3Q4ZmwEEIZ6cMnoKYwUabfFQUeWrQlrejm6tKBC
21Xgqrkay/mCiPEotDMSBitxCJzp2EkPN2jXwioVcGRNsNdwTJNT6mMcp9HeijeF
vQBwJxcrNv1eGe51bhj7QiwcEuSBq9yVD7CkrxKtImAUn/Pq5Zf5JYGrCqj6Z2Of
70+YxL45Ju5KMOqyd5i/8TJQ5vNRhOXLkdv4fJ99j7ERaUR5OMr6XBGiz97HMblC
4fKA+D1b1q28n3C+n/ncZp8xRiYWUDCdtybF630pLg6gHdlgW3ogPhF+jQQufKmw
afGe+0iSC7haeub6z4E4az7VxKD00YWYx/s02zPwPuIZRaEVy+C8mFBUeTCJGgyi
yOCOiE2HeUgGplarkcoMAF6hNmilM8z4Q/ppXXdzSrrBei9NyaVGDStdToHasR9Q
JXkU43m58zdDPcqM5gfvxIWe8iDSgA8JUiCKQ4EaPHkRg7gHJ5pphz8LHd5Z823v
KDuvQKgvIaWosbEUVuINWmEvA0NMQw5wkV0NAX8mZC579U+bOmvAkHU88ZzY9HBM
Mo7iSt7ETTQWMOEp1Hsf7WF4hi06FLciMiMCWxRG+q/dMntqX8XNSm1jt/8kV790
XfWjYR5cetXJsmdNlTItKJ8WpBLQ6XU+tTG7xIMiLE8+CNhk1DiApXsUDTegPowW
b2ZZc5ijTtLBAmS1hn3Z7RWHukSxxBI7VR4KCP/4n4JJclPGReB/4YzoWsEYDC9G
gX1Hvw9w5izk3zjw1Eh+nLq5nYf7ql/SMi3WJTyEWGyoqphMHz9TCp8LnEpr609l
3pjsTN0WOcUYuIeVySN7DSLz1vvG8llASYmyrYjUqbdrA5M8KePb5A1M85OuhcIL
xuWQy8i/appFSSRAEkTo3ZZrPgg7DEJh3UP5zDTJNkzPMYDE/c9wkypX7SneoIer
uprbrjckjvfGtFQOdkudg48cDAEpAdVqbRt5ES16gcbUgUpYHZ6rad0jIkGyfIAr
waVIq/OCt2LZjXHCSepJ1WQIpzuLd4TrmWTP5Lfa0ZLs7hXuoSYR1pSwhS+Hn8yq
TZXJTcIh5B7vezoHGWam3uyrsZDtK3I7ROoOBrTvi3kgR1LxiaQWRmhV3mctJtJH
McO2GlXtLCq3AHxgKvyWxM+SSWMEheb+p1I2zZHsE5MzCPIU6j4JpZVaQ9/26hPO
```

```
zSCQX2xdpydHqY6P1WSTgF4T0nL5N4mwGHjkaArM0mxusRqxH97pna0Zdd6MEWT9
BJQgrnMUVpaX/Bcze3NJVMRaDrrJNPAAeXQhFebYJ4pvgABQbPTmBguvg/eFRiA7
yJE1xJDDNG5NVBaerJgMTz4XXPtZlY30stsNaee1e6E8Sk55gcyYacuWL4oWC510
7aztFDWLpsjTV8/NWzwkq9UhNX0q5+OP4bH1pqijP6qlUahXJQk2usP0WDqbG/ji
vMo6cBGU+IM5D6P/AopBimyrbjqPaRXc+oeBetfPsE9n+97zGdIScIXd8GfLiyzk
m0JP8NgAweSNKmO5i8tm9aR4ViqV2k+pQnFnW+lKsapcwpR/MmKzkKhSm+hbH+cB
1rWvMWPd28JepPvGt7Sj90UqlJFvvNZvKWOE2HxZ256LeXKnsxqptLevnmDnnVFY
gEXBOlkJ+HDV/FNeOyKLBcmWLCX8LhEjaYWwCqIryoqcv1QTJDTFspBzyjvf8Atp
hh9X9edQaTRO0Il7xZYX7VcG4WW6pIF1VwcgbLGzq0VUhjfHigo+6doxEDBUduTw
40JBwBp5/s6JyR4G5jZRxRaKP1WuzMgjq8bQ+XkOvN7vNBgU9XkYxOYmTAP3hgWb
WPCZtKWkfVbraHK7x7efQ0hEtF7tea+4Kd9UgNx0labbkPu8cpLoOrPQNKxnkwR/
wRt65y8r4YJudNuRaUVWyd40/EewCYmqBa03UgFEDeCydTKiaFupRiZrZT5Van2E
Yc65UpabLacSyc8Fh8c0w94X3mMFesiYRpYsK8RGJ6WO4YRU/9OLidhffmCqIlN4
RpG/0NrX4r4zXCt/6i61nvB/VAmZf629xlTlP4kiV/BZfinWhqvqKR/eL/VE/o5z
LY6yPnKbeOZ2CHmjEZrRmhrFVuPSfRIlPynlOQ80hgg2tucdSOH5M56hcXblEDxH
SDAAS9FQK8WuKxhiLbERZD1b/vc38mPKiOCqMpHnl2tY7kmK16TODiF7EAKsATNZ
Gr4dMJ5Hsiu8jFntgDSWYBOZhX/ig0ByjlcyqSeKZLXCb1XbXm7xuiyq193Grabc
Ad7Hz4OHER6G6Man83n1lrPojNzI6G5bWQgktTou1zKS8il7O+58VZuZ1QPxJVAY
bpD/pj6RLapOD8LgN9J89IUJLUFCgV27i1gzVxEqDzc5ktPUQZBIy2BemT0UL2+v
elZsnAa4cs613Y8BTu/67EhgOSa5NZ7oQAQKQpyZQt8dOcjDbPLI5sO31RWeEABS
R4smWRo/5s/gxRJR4WLOQGP8pgv27IvfIdetH9Jtr6ozhepsznmx67BMbUh48/S9
hyrPlfulq/cwAdDZIuW3wCBh7Wz5zzk35FHjpfrNYGSPqRakALnqakYFsAhwVjW/
4X6femmMoRZI5L9mQVf23LWpVGF4nDllOdGSm8MTPBIGsqtQPmnDgEgTJ+oMl1Sg
d0i3+jcIcNljq3QiTL+ZhY5coHSzpcVdCujR/lXVo40f6ymxY7t51mMoXMU5JlJr
d7MTzhs5yf8wWfZ/ij/OQVarS27SzeIPQEGhvSC/jrHXN4o0RgLuoJkOES0nMaDp
ug5DlrRgTQt7IVqxe8IItY390k9njVWoRj/PyarBVCFKAN408OK1ssTC77UjmZX3
M5exdsnxw3mLIqG6xDxRAnsMG5N9rjY39ELs4D3GHtVHjI8VYKKHWy8zFRh5rBht
th6M/lQfrZ/PL42mJaVbUfZmaaS8XAiWXX2o5nj2HD4RiiDGC+vwRGz0nNj6xwVh
nbpeUm8OdRn0lxPBx06zLiSUkfxfBpFCKnz/KV/hdApIDlbKBp5YhaIzoeKQahbh
aFc7IZR8HIYwz+qfqgr9O+r8DqiBwBDNRttYDxXY/dgcsL2qKQNa5qHiCQzH1zJR
oxXPmQPZqGEvdLPvYFnN6SmA139ca2+1N9wmScFqayVDufHH8U0iEdzYZxgoD5mL
ND8bZs238oOalmAN0z7PgmBPAywiwvMiPjzHXCB1Lhd37oh1LN1HPpj3FLl7FfMe
gvHOEA9e+r8V7USk2/cbTo/1q+1d7M95FXStKsjnnNUYGINCKYuSxgpRaQcNFR+s
zaUzPGFP2IfZxKoDbYf0p8L426NpURMwbOUVG9yKF31jPZR4+DwfNwxS7YNmNlv9
Y1irdKcwA/e1JoKso/ZsmXWA2LikT+q83GVFU9Gg0ylWR08zGv5eKv72uv1+xe0D
fbsfKw08Dad0RymdDhHAcUHt8TPvWxOelQn2vB3BhMw4vgYuQIgIvdXUeAIaIdn8
KHHukHnqZt5zrvbNTrX56yYym1+AUGI1lmSBxp/mRxZ2xe+FwtDR/jSK6jFdKdyv
OXPpbemv5aJb8Ie0S9QBAFnFskfM9O7rpP+Cpc/AeH7sgSVOJANczu6OnlCeJ4B+
bHSU8nYuCBW7ahBd0zv9EGp3qhIDaGbgTRovWAUOuiJVu6pqLV4+gg/BPjK2xu1b
2NCnKcSg9jX43p+jMcwJj4f+7TGAKcKyBjMVbBIWYU3XIMvjwdo5Ji71lce4L/An
KXEISeLZ6rZ2S2Ejf5fAbz/0GvxxaUQRh7SYJG5O8vFF6xez7903l9pPZxmxG746
Q9+ZrFqvtTRf0RzblHV8i7wpOfS78YDY2qkZt7n9FZAQ6g3xDq3kYfhOS8JrA3K3
RtMNW0uVwhYlJdWEEauNXSCXIOyof2CmNSrg70vqiRZeMwGOUSFi0qWuZIUVv20d
/u+QCPRXQaaySXQoPuVtZWt4raMVcd3utNKJYsiD3SeTgELK+5S4w6LExxZJG98v
DuZWV1dWa7guTB7ORQ1ZClTV+t/ua+LyP9YzxhC/Nt3PBEqLOXrxd8Mz+xOwhurb
QinzrW1TDl901UFx3PBHs2z414YSOfgwCopdUeTu7vM/q1y8JEdBCFn2+HS8K7PE
6uYM0mYKT7TZNYh/Qa/UKctSyYahVXUt9dA4niJGDee0uvoyP8zwaRpHCWTdvor7
6/N+Go+ea13J0GktpE90QixixYpL2RmOh3RuZ67xURvmoF+8dv16iPy5ZsmjDIY/
0d+47cxv3s196WJUFHBsOzAykReDzc4lwB+joJGKcKba3M/IDjSZiXAonCImhc/F
FO6cEmj2rHNi2kwx1DhC41V5ehaMEkifnsfSug3m5tyciSE51Q1mphYHOzGINQYV
mwDqNuicQc8u7GTVn14ugiNPgKiUEfWxYHvXdj6sniWfBJ13FwF/PFgPJOmFOxer
SrGZpfffsSZu2GMXFVOckvHuIUfWkbLCtOn0s8QS5ttPBsemX41G7k3f1/1CP+R+
ErKYca4DD7YXejXMuuvmJ/fAnhSFcLDkHuBdo4RW0I3ZhVC26H9P246/wCwzWTtx
```

```
8Z32UHOP3saWF6z5PBkMTEis2KYFHZnh7WrNtPval/Y/Cf0N+KcEZRhoSU85Vkkd
2LGEFNQts9OzbOYddeR9jzAzvn6jOdeyYeI3IudA97t8uhgZldwi4HwvUY3qvfAF
he4SbqsSMv011+WnSuNwNKUKoHsh94f1CW4A+dvbknzaSR9Mpm0jguSSc8OgWCoP
mUvU1IWvIlW25axaK6vsWo0SmbNMoQuG8ITSoTtb9Sm4tm/QfZD2bJ+tu93aS24j
4/vreU/oZR26z0tJh0SiaslRxwC9dF1uNKaO6GaXbX9wc1LFKZDJgfqo2O0wP6Hk
88Krgm8rO5Td9+nDSm9TIscHVIveo96gL+pPkweAhBDJg1v6YHGBvb8r0HMpYsTv
ej7h++9Qjfr20v6e/f/Gd2Saz/TlWYl+Qlcyy5QeDzcMaTXVBHdpWi8uDEytG2PU
UaApyxZlzR38Q/pDhfUFBrgnO3+c/FoZzrFHG2Dm1HEqrUelycLTZyyWiTaBkQ+e
7QbKFV5ZBhVxDwDQxjrsEqzdl2w7I7ftJFo6Zt/CuqGRybrtZLQ52fHOvho69x7F
w6/LdigPmmsyQYF5x/THMoxj5DjU9KtLSZ47B1ReBnHQKZMoILtIP9EeuZPgs694
9IhdQZuzh/PbDg5OcsOFxPY91WT4zJuSY/xE2JyGpk7KY5wMDAXQxzrwFFbCoNEM
bfOXQ9aI6GQW6o6CbjipYpXmYaI46hJZc4PUC+FH3rzdIcLat8XMuXCictMKGpY+
smFAzkA5cVlzXRfChMJ5QpGU/qgl1SP5BNFfHbhJIfiVPPLFoGoNlZ2rE65tCTha
Z2VPNZImn8aOcTpkXB0ZqDUxgUuq1Kb258gki70V5K/vKakK9DFkmP+Du2XN1QR1
O1YD4rT8Kop+Ovulut8eUQjYb1N1X2/QrtmKxtpuZDn3zfZzW1pOkUS/oEpmKZh5
sFX1QP3geDxHZUCa6k0RqxXxUwZTty1n+u3A/JvnoQecGjvK87BHHGSApw6hbhJR
688WTlJqd7imPsWoz2nd4sWTT8fK27QtbQ2+TjBPS6aQyVqiVRSyF9RCaUcIvEFH
/XasDEeANuhOltE29/Z2o7jk4XHAFdKq6ltUKWd1qskuIex14YzAsJ5yw1rtyt4q
m0JgVA0BxlUvYv8OcsVIiw7orvjYn3wPrRe3NotsJWKOtfxoKXHBLvI24OjmOhN9
AVQgCAnKYvFtmh5hHT2klePBFL+OH56O3DH1AvbR56gZO/dp37RgSevFN43WT/ko
hQTgCgeidlOCl+DCCa6lP5YF35sDi8kXU4pZMge2gL5JC7IlMsTOhIMwwSi6kizr
YPBK8NWof2aZ33PPqD/YYKWUlj79Z8tp/x7L67c0o41uEnxfVhdzFlUoeUG9qgAo
V1k3FB8urz7ObyOAh+QO9oZFoJxi+L4HYKv32qhxLqNUuJYFY5r/aV0Upv353pPL
rO1RrF+Kqm5uMwqMX6K7x0WGmMbn1wLAm4dDzEv8n4DYg4EBDE8idXJXewxSTzYy
I2rOMdOpMRKYiaqBZUvXJ1uxOidVamqDlucehcZSt/ehhNpXfmTKKcvYJeRJFvDZ
lAr+srpjCjSjHtzFK5XoaO80WbrhdQDJvNTlzRXkmk8DonaJExohVqFtprMcrQ5f
7wtsBOeQss9/XSTqZX9zzTBjC7QcfWuOTYm+UspyrSgE+gqpjCsI/WUGrby3JXQZ
z1OFqsPKYjkguJUmQQTA61dwYGhAlA9VrQaRlwXNCptlgV9xAShMqGc5Qgcnm3TA
VOhmiAB/bMnqU28PUOT4MaZ1dxHHaX7uKxFmx8U3QbNtxiJZ1Wqve6epQDKRMI19
CguxtbQHy+Yy4XEm+vFfHbUgsLR5JLummc7zqE1p8lnIaLlXlzCILjPLjtnZX1PA
3I5EckC50kZD/5A7M5Qz6bk3mSZQBaHj8tlsO0WaJue9/+asI04cg559ESOTJeC5
4pvgI9wWwa/cYUrBiVn61s7Lyanxx+tkohn4UOW41yP7V6xjQc1CJIAqSJcx5Zy2
XkQtVXaDm2NzF/+y3rbisLS0mAmavoCTwo/CuNHlx1gNw5nDYmf045MuqhUXybac
VO8+019Bdjymh498vZpAfJY/PZKt8CMvYAPnjrrhrf4qsmixO2i4fWK71Bcj5bqg
k8h6tr7P56ZI/d5j4xgOYe5IJV+CgEXcrS295oFAlNcgHjtIAw9LPdcnU+JJo7G0
2r7xPNAJdVgNaFs84XvN6GNEsgQtJROoGpPOMAzT4mAtZBtpHh9at6zUbVXsIG6v
XB4+q/nyFsFvJeYwP4iEVccK1IS+Mc5W6Tz43BPF0AvzG+43C/d8YoYXuBoAMeqB
REQ7lk27SCeo1CD/p900THmAEkLgg5IC5VZ7RiGHpjB26nJU5Qhl6sC4I8VNH8Ex
nbfMu9whdC2UAOL2JF01jhcEydhxlgI4CS3FXUBCzZKBiTuIL9Fsevwhl7Z5ax5H
QRRLbyFRKiBgL5dpwZrEdE8/TSo8tFcP8BAfqvWXf0hs0HHtdUNtq/1O/8qrSQAk
Tp2zqabbOeNSf9lsc1hGZNyZJN33HQFCqj1scHLQwVwhwGPkDUYKkNMTNWl37ML3
/FPr/6wo3O/qn3URs/pPDjEeOzpPaMUIx/c+d/BesA+GIXLU923xChpgUbb2duTB
g1qXXzLUsVQLqaWhGFG3M2VAak2jaoE7ovKaNzjpRQu2dBFppWj5a7Qz/PjAvHMh
vpsfBRWwStwSxu1AmYvcKQ1Gv4bHvkQU841XgzsB5PCZAQOseY3oWtb/Npqyv8nT
5198TYf70X7FoGAJKgjtBhzwOyc1GrB9WuKrXkCk49013BCN9LBB3Lk47qUTfqF7
oEy2f8jloKyt0Q7EpssU5Cc8F+pmV84/kILQuZkkX7usA71YIwoXvd1fzGUBFzGY
mN2QQxgkAMNwAXa5vbCaylCVL2yXE/0Na+5afizJrJT5pCHeFT2af/c6OGPxnSIL
NlhH9xftayffo9Xtnu0K+iTVZ6EyIIzwyTqk2knKBRvnEAOVdnP9CBVmuo8KR4/a
LR5mW44DAfnQWefcLQUPlemQDA365SVhgt0BFlslxS2a1bTUs96/niFYfD+yjWel
w6u6PGYo9i7pKUsLDxUPC+R1jnmhCRKH7OzOMOi+eAHgsJHFJ/Imlr6PB+ZdZKQL
WvcYz1GOkip0gfe+xId51MBBiOEGWpAreYpFv5Zx9wBhT4ttuIDb0+wh3CC1ohAA
V8exn4oVmZCAIvSxttgk3/kOZEbM5TxLTaYMg/I2jsbpuyaQFaA5/XdD1E3k3WC6
wUF5mh3ljazSgQEtgDp7eVtqheSsEqhyasFT4q7e+bi8J0sApub0AkUfaxit710V
```

```
YhXVMfj0yofotYM35Ajq+kEM298tWn6/KErQ9eEYcwJVPsxtk1S7zg62GrvpMaaF
DKuddQ3gQGKn4u6FR95FhDVpQIT2gQ3Yp+3wKMoRPhzpIHIXAwUGcYPQM6c6gZtg
EZ+QYP7sl6JM1RkMMJBT//MWKMunq8jEJ91AXBoIB754DWXqH7qWCG932/yRVNm1
RaFolxU/jXFcNpzohntmV0PRsZK8BteD/Ft5vhhI1xCvANyvGdmNVjeZe/Grqsyp
C2FnrPdgxrtVTZBIbOXbY8B6iQbHiyKfe5WxXrGN2UoV5lsS2eHgImOUDifXOzke
RqZz+1p3SUzQoA/Pmmngt7TkvYN3L7mDWHf4rdgp1N8waYQPxJJ0DWFGOEhgnVXh
F+gvJQLc04wk16ScoUBGieFHBjFhjDAItv2LwtMeKd0PntVOinB842xUAh4g8Mhs
VkDpA6iKipmh+KqC9MHr9r58jkQcbH3tMfP4YoFlFf09XrtIVWYkgiEBZCIOVGlO
yQKxa4RBKMGAqppmtoE6aZtkea00y/Z82kp+JpS/7yNL4JtSMUpCyINYkgsv+fjY
HXv6bHzHjF0+gNoFeMEu0g+3SnaszPZmFWmtDXs3MQfOGgd7tJCQOzUO7jyI3qJi
JjjUycAl5YaZHTOrz5IVye7MYbpapUoCDscMHDfa2kEVOM580ilHlIYEpjg+zbKv
yR9hUdvv5K/H43UHrUjJIw2TkCL8OBaSxiSM7dqJmjA9XxapVX2XE6QHjfgv8k8C
xdV3tWFL34sR9FYT9CExQbDDL4Kc8m+eMMLw3iv3Z38V7RGef7IZ7hEZeTWesCy3
Ul5X+zWHy++uBQy3qyFVq+e/EroIq6csG3e96usyEo062s/5zKTkHBVtUrwfEsPq
OMfYFyWJjYK6xntDlGQqH2IScRGRy2htCwtc+etYQaywFXxOTBjxYKVw6D17hcOp
cdoFMpeQJ+TWViLxtzGypxtJ2YNNf+uQe7AlVe3qDacslLa/r01DGo/h9ZCcMqZm
V0h2seO2T606rZQYREUfX6UX7AqKSe6UQkaug4h71rOZ9e/XCKw9Qoia/t5S3qXZ
h3RlI+OkU2HAv1OG70pcy9DH7xoVY4tEaDLZcqysiePt5QQuk7/MuI88fyfwk3c1
bl7OxhwKA3D7BW4P1wwPZeH09y52iO/9x7Gx44gPDoiUdzPzA9L3Jg5Jp2RTTyPc
7rOGmgkL52L3qiesl0vxf/+bpEqcDxRPGEARsE4z9cJVJy3JyvYFUYQskASxPzPc
YRdpxj/eiexXT4dt/yPgWmKGtwN4roJ0KS1kPfZm/mi20yo3/wUq69eZlEpLV6aV
w+kRFpbvO5T9teyxEjVpYEyffMX9rexBVeyeCVbwBzlLJ8xJh5TacCX/wuToLQSO
k8AXft2+ttpg5UgsYA2ehthTITH68ZG0aceNWOXHQPtgKEBEaTPwlmJ0xMMwSf6t
yPLCOXR7T5qr7yqTjY7EwM4GlExY5uoJ3SNew9du+6m7lf8StgWj6zOMfKEYbhQE
tLfY6/y1AxDggIOI0lpALmo4DL9z7yf4T6esfHZOdSKuXl2HJ7MxH68a0MWmXcE0
qsHgtES6udP28uHAYfcTh8fjrg9UXu9YWFMBH9dI7dCY95dB1eedSV0He+gUhlx8
kZqxeP9ySWMJDk6I6NJ7ORE5RiTQAckII2ljRlfq+qKfr6MKTf1JQvPQ4H51oj+T
KMohQ3OE+wBhzrj0c7AQt+ainVlt+jWfiznfyh07L+IOogDl1+4Vz8gA38WxzgXt
cMe965XOAhIVXnO1TPgirGKcg3YecK7O429Afs2Ov6XRvBkQ76RKY3F6MmIcHzUP
eK0aN7BoccXHVdJCXp0kMBXCo2S05BzjYs+JvT5xuhwQJ+LN8USUvVh4a5lof6M9
xQp3Pd8v6eEPV5SCQrRpZHbVTgawWmetUptEMQbuWI4ckA6C3kU+0aH9SBSTaPOj
OKfQtnjqNnPrbErKf7o4ITGjkwsX9IaWLzdt1PwGXijS1jx90+sHySXHwlpDJCrU
tMki7Czx9UAFy6SUcLa9sMNmEXN7WoNBVSM92s1nBHs0wv6nePw+jT/39qjeFPX7
VEn4eGKVCDnUZjqrUisNNveXsto+Zq4KbEYfZJ4ja5wwIcrnrw/7sScoVzT8nWXe
pUPvyPALXqmKK9FWo0FQruCiOahn2c53Io+xVsxYbbGrPhySoCMt7UFuShggs230
UqdWABt+z0cAnCokPEprpi+U5P9EaQWbbz7ZrzbZQrSN5PPwSRvRv0fgzpR+Q5tC
eaY3OHt2sNZJnefQVfRGKPQMostN2XL3+dz9ALmK+2E6I7DH09dsenbmAGYR+iul
dM8qHSUbdvWvURzMBAQZCJGsTlMuOSkU8QPzRAhqXeOb8DNInM86ewox8RUgPJIi
AfXNOYTuNnKsfCiNeQbRWd+vQu6ZVXTdx0mXhmbB0vCfWSyTG9Km+1xvRLe+V7yu
XO+CfylJhv5oiBuDsaOEj09tY383h1JNVKg6ibv7y7Xh9bl7sV6DwFCho3uf9zWb
Ikg2SxBMUCPyPpmJPp4RWT7DjbMgTntgiQD1pXloj1RZcPWvtFM8KOxq5eocLl87
TWvyQyr9iShCykB2VhEmyRz9k3JNS58TTzWvWRs9cG3ZjJwp0YjBpeDWz2qR3Ig3
I8eixf7Auc1RCCa1EOAiBV3+4+YJorRa+okHlMXnFPxcJl7fTfg13mfiTJ454TXM
VTmV0hMMoCSsXWvbcavbsZGgg9xDEOIPcBXFQp7PHMjqVSps8zctJYQOTn2gAwq1
lT5YpPqjCIPNwr1GjbiT3G9WF3lkoOtKVHa9B8nVf3duEmtAVjdZHfzRBUnl+1iE
6Wvx8P1TPjncp/MZUAxZT2oPousTzB0pObl/0SRz4fFVRpJOtdueT8Luk+wzpW8K
VSswhk9t3wJcpM2My/xBgbx8URSL/zKzCalbMc0mSnWre3NfcEfPDRy4x2T3ciJC
wGVE8sQFlZgO5eiHovorrX3VtYBzfpESjerP+XSx4Dwji2qN740b65bUxK3WDFGR
SuGDi8gOUNPaStAkA3W50jWqGisFAbKmN94+XruovAJW0YD2AJNzGTn86+3RnGln
4YGjcLdf8GFfzqBXnzkKsR+kjR/ZZLkQI/Nl1ZrctsnMXKREjRGQ0ad8ZqnFpTXL
+qN+Hc4snFm0MqEEFyluBOecwfNuGP9tgY865RTv6Vh9hoJucLw3a0czzUVh5hzu
uvxxxVd+KofsQITcRLr9mpbbeFqQIymttC74mCujCZntfJGdYypTx2UVV52KApve
YBXi+r7CoSDK7VLiPUz63UNgXt4uozeikkdxcD4MiwOH3BFi3wVMl348C/CLAYqp
```

```
pp9NyaElphbVrwpBWKJU9EshsMJy0Rk20gMr75s6gXSNhdqwxM0ANvGXwx/9iJCw
+R3ld+RfrbQbV2tkon1wonZ5cz9Xboyt5wPegvu9zTBJpgg8B932pGXHOu6vVj2b
QP0fqY/gUclsOzvt78xfNLFj8iuKYMF0Sm1fGnk0W//hRtfZtkK/olbdKCsOKGnT
W041Bkj/zfmtv6EkL73HgjfE6d4QH2st83rucAS9ilK0JpmI8awe1grAKnPIR/hZ
rCmZ5SfZoJVLSwiO3Yf/12Ueift/27CpwYQY7FKfNux+47L6M94GETTwHQ9tuRJk
clYP1yqq9Ku9i4wCxvdIwTco6Zg4GjO8Zm8F2GjCzRbRBJBvcAFV7l1zjVptCha0
jrAJrtdLvfwzyDpjNMO5iyftA/dO77k9pQmuNK2PzKJq+O7s4FZs0MtzDYmK112k
MitNDfPyi7eccs1TIkzPmYjeeC9PTg6B+gSTi+gePs42fKdB5c9COYuhj8uuzvtp
0o/jEEdYxFrIvxr/gkxspip6dVKelnHLZIAH8NUap/aL5sCnUuEy9KcUaitERjFA
stzQYwXJAVSgvL4wEhVuPG1gL3JnHPLSYjN9ugthpAyaWNt14gm+gFJfjb5lRQAS
HN42kC3CDeI1u3QcNR2qyc38wnvg7SiBT3Px8I7TGOzsdjn0LUD1DzpR1X26aJVQ
SeaubLn4QPG7NB8oHuCXfVjEl2iQ2s648Nw3lMHBo6qjw02d0SxcasBVyYzaN28/
MI3Spayn4UWvJuZrsNIbNlniGkZ1PMcdkfoEeAHA+Wmdh5rn6LXlNZon4QstkVVg
DfsaGuPUJ7m3va+XKpasR6w/nLIZ2hGcCc+4za5fQ6nuOJDLISpkYewWkYhiwkXG
cz+vRSWM3F/alIWhTUPwNKez2yJQ+uBS55F8l3pFZXWOlleEuB9c3DbYCfagh8Nz
x7t5sc+15PKch7ZGBNx7nUGSuOJvwKvt2oyw4SA=
-----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+z9XbFCVc7pYvl85Dk1f53xYmhB4371Og==
-----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-----
MIHTAgEAMAgGBivODwYGCgSBwwSBwGG8/voxg4JTpUDkfYZepMvbzddevaXjA9LC
yl2/uhp/6a2DYvBAC2ITM54TBS0KTwrPWanRxKSo3j+L12Yg0o5HHqqXn9IJLUGQ
T9HqevarVrhOuwQl8RB0RHbvshG9mXdY8/HLuNIn7P1dsUJVzuli+XzkOTV/nfFi
aEHjfvU6Rx6ql5/SCS1BkE/R6nr2q1a4TrsEJfEQdER277IRvZl3WPPxy7jSJ+z9
XbFCVc7pYvl85Dk1f53xYmhB4371Og==
-----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-----
MIJ1GTCBpwIBADBRMRAwDgYDVQQKEwdFbnRydXN0MQ8wDQYDVQQLEwZQS0lIdWIx
LDAqBgNVBAMTI1NQSElOQ1NQbHVzLVNIQTItMjU2cy1zaW1wbGUgU2FtcGxlME0w
CAYGK84PBgYMA0EAvUCC2EqHM3A1hYoRDdmLUH0rBpbDoKnlfLnFbpInHjct7cMX
0vRd6hFzOfIC69yciXgkOLaYuyUGww3i4gxu+6AAMAgGBivODwYGDAOCdGEAV7mo
vLSyX5Y/qXGvr4F+5nRd9Pf8dNEPkedqqlhKkuXDfXb3Os60Fc97R1pqRDkMlXgE
T+TBhmIHbVToe17lkQsTBTETQJQ4w+fpFcBnG41D6oagVU0RQoCJkDW2Yy14RGRb
LQLqwu42U6aOZ3cQJe3h0u06fsZwxB3hsFwyIaSri2WFX/DqJ+J+XCGzWGLdBneK
578M63deFCpFtdRQkMxgvW6IR46IgAlxc2xV1byQ0mKMqsaGe0j4m+7I4KXGWQlw
WrIGpeL5TOFzJaii3m8e1knKxpZGLkgL/QnRhVC/e7Dd7H403oE6dLxE/UEOo1mo
YVITQjOBetCDwJh7/lQ9sqJ/4uS6izmCYM8a/3CharPGDJPlbTncWx21qF5Wt/2W
HDdbeJMCRC2jXSMytLRrc8xsuyBbc0WjJLw0vJMQmn/XU8dx0hFSbUO8ZMJDYyxz
UqK5Q3tqGr+7BEIzgNVbelXZkbf1kpYMrXf8jyJntSGAe2nWw4SwXi5jke9KzLiY
kdR7o6ElI+c1mexwf41nY//WtKsY6005jDwETYBtnaVQb4R9dx1+0ateHcI/SkS8
5uk9OJ2ISBEtktU6Ve6vm0dLIpPZ56aixbFJD692LFJOB2ZNTmv1JcfjNSNuN8nT
epTxtT+k7puc7YiT+sMIccHLRC+ScUdfhcYby25mi7xJopw71UWPu6WjkqFxrma6
AhniVA7fBwD+rS7lwt45+QKkDBAFyeiNigc3sty1+epwaBUls5fECAf04urdYxI1
jt/yiZgRhfF1aLUtTUY81HOJ4H3AiEVgFyIr0Wjd3ddDTb00M00jqlF5iH8+9mzF
HdqNbWUUJKZU09urfwFP9ewGNYyDE16+ix5YfCqFttLWBn8jkjwqBBCaqi/Lz1IX
LqtCUjaGz+/aJDssm3SiQdQQfVNVqidThdPHJ08p2e8XYjGqV8zjju8rH6fHEY+q
SMC0qmbb3YapYGaPwewvVZGGk6bhAdBYGem1DRpNkR9wFN+i/Iuli4L+kyJRdCS0
60+Q3XqQEIoxT6wBdn/0GJpDi2SfOLA1hpwnuIVr8l/eM+ftCHCEqOaMFayfGjpO
7XAHk9TkhI5dJnwbkOHvl0Iy5E2fAHVL+IXjrdWuS9tQLK9FNf7SpspPXQFfJYsv
lgQbJF0zUy9jvFi7TtuZ3TKJoJhJQ/M1zfIQ6vjSMjJqQKAb++c2pZH3DEY8mc2l
sMxu4QmPnmPGs1pORaDcYNw+gHvYyeiqzKw7RJDQkmzanJ53/vxZW60TsZbbk7Uk
XTsv+IZoNaUhw7KX+OTIzpOCCtrU2K+osacYtOEcgXsm8Zvx1/hxE1uhTL0IGxE/
269tQZULA5tO68ieNKuP7nk2vQ/T1YN9bX4aCLgJam35aWCVd5NsT9Ko7lFZNovz
fGCGoACZUW7QpMJsB/Mi9zXwGcb0qTY70fAJ2PR8y9gfTJZq1GGSEyPTimm3SIf/
dYTrs/sJSj46Ge8zEvLqMbc7796dcvbHNuehCLEWKpBRd4K4a3JH/GE1lXOJuJKD
f4csgSvLzniSvv+poBkUg8o0QI+s16+OViZmflAVLHKnaraY53UnKtOuqIsp1Yf5
L/35kkIwCPKZLd8TsJy4qjv1oSKazNSjiA9Y4XKd58qTlmdllOp3bGpt2MshMOXr
Nvg3yqkX4dw+LIfFrwv4vl6kKiGakkely/5HoYZTPcHY9iTApYkD6wWol85ebmkF
+DZm0KzM9E8Fzb08k8FczQUS6FE0+/+auPW9h+hKKw4HNy00nYCnTwyzUs+BDt+T
64MQfAc9OMTHgZHuukU5a/KwQ5ArI28FUM+1jiwo4p0jWml1XpOzjkALVCzsExZc
CK8uiIslNdoBqKQAQ42hSssqaQVNCQkCSDJgPd9sFSkO2MesAHSHKU7RhIuU5u+x
piiy9OF5vZWDvr/NX3v20edJWJwudJNQ06Y7E78pZ6ipxukyafUTynYhASghFoMt
fh8gyhnkLO46faeJanPrIegkZsUAuI3YBpFz2nVyoPBYhNo7NE/yvpirtxu7R7A3
P11e3wk/x291ICQKbsvGUUB535xCjN/zBaEE5RVGLx/SRKjwRx6rNqVofr4QFwdX
ThH2GSYLYTUXkbLM+nN+APjll0Swr4CyGqkPMRVlyZ/7JHPtpNEdpCrVhBzpp0ib
tvgZsh7nseJVw2595k0Mif95Ne0AS/DcjhCDwRb5l9cM3/2rBTI0RkPgApQfibEs
9WPHJs5q2j196IgHU9HwKlA4AZkRDsFvp3aii6BWTi9mXXgG3sJ6tkRAxOFI44CJ
DrXf8dwr4WyMy1qVtf9+O/CzG8/Y5jG/RCBmCic1DA93sut7j/bjnxxzZ3NXaRwG
9pF61g/boEjSIPRSG9Cl6hwK4GR8KaBTUDB6mb0RC8jT2do+wKXBnp1XQNEIeN6S
HG2oZOKWw1UP/SNqS5NzWZA6IKHuHhe7Ke2vwziB2HZA33/qkbgl5jfYRh37DG+V
lwAXaj0gFWXQmWwgYOWLmUx25jc/WN+4I4ZVEMy0bOF7Sxqmz8UQtu5hpMjMhe3a
eA517+WVhkWEobX2y0C6A17HoZSihX199qPjgwI0AGmumExeVGDvMYCzqAVxGUua
Y8OXm/QoRM1XzKM6z2cN0Ts7CVpY9k5Lz7R1LUsr35XaCCsAuS31xGZ9EYSruiWQ
6kGpqkTn46XAQhoQplsThIQiBX/HxuS1/p4wOV1NxQSNaJsDRUjPR7USORm3V71L
```

```
6tNfVjQJRy46UBbFqXaOdbSaCuFrhipq9EgffiP5PAAs3JDu4NolRkzCcIjTTEnh
zRcxfc+Yd/Fbenxgqo5Y3tfgXGybRdh+CNTUvroTAjltRGRy+lOKDvh/REHQHZyA
c9XYTfOorX1C9d5Me17yb3RxoLO/dTUWEdkhPbNvsZ7HeFbOLqnX0qpTvzaEHO78
khLcJe36MiCTkUJWS3EVCZXFEQo671fFrJ/02M84aRjT/7lQlofyM/BDJqxm3wH3
eHgSBy0TSyXtcbcFccSCyQovM/hy3FqKesEBcdlR353nyt5+I6leSyE8ppFtMa3k
3jFbKijEZPLzCXH8WPocKjh12vXphueg9S8swkotvIlp44/tTXq+Tfy3nDysR4G8
HHnH2GamjpSGHcFg4PXElrVqtiGPxPNYVergxyQLK15OnAx8yMkd+any2iT/WT86
E52PlErunckE4X1lS/4DhAeWBqs+zxc32xa0GjEHqijEngDMLdtAif7/iwwqLz4Y
oL8S6PHxnTO4kSD9kj/BLfbyZoWQdhlPmUTvYKjWqChX+GLnMqRdwm14XsBa8yg1
qErFF0Q6xRVORqShsn6iKk2H4pAA6K/zoGUAf0d80Kah4qHrBndJHkcBE4qHc+TQ
9oTKFucrkx6u2vnT5ICKyb0aSBQl6/sqUq3Tsmuou+Xz81Ozlptatbpeq2rmcgBB
xoJGJTgwcs6IhU1pX4jtyUvI3vqF/KIq+zF3CWMfH/izf/VOkeiw7UmUGTYvZUql
XghiAp1AtmHJVUBMeWLDAy7bNp6wvhUgBB1vxBzaiu45xplHJ6LGzeqC1OAWfrkx
fhdGcSD9iKB6CnYVnabiOi0G3nGfz1FfbvVWoN8D0QZw0OAjERdUI3A/sz7q30U7
Z6xRkLqTfZGLh/veZY94EdY769khUSeOIRq3UxfR2hyY6GXj0r5/m72YPyfl7jhW
MKsbmTPiu2AuAYZ1UhWjXKbBmqu0BcSK9sSmdqczr8r7yblpL3gzN3m7qQFoN+NG
hR24qpZySPcNMTt4QvEhQb5RYF/JUpYv2qFCbyh+oxbwLZ5lcv8fpvz3SIyiP8Me
HFyZ9jIf4pkkEGqzROGMaG+fg+9mQRvvgeXXD2qprne2wJQGwzBnTdkYbaDsfgUK
ESVsslzuPb1MZOS/HvOLRSgGLHuyvcbjfCLNe6Qz6lcX9HbrwuKL1SyD68Va7qZ5
G32phyoZCEV5dEEgNjtx4IILM13Ey8Kzc34BTZbMxyaOfouhKfWD1C0eY6liwwtc
zZOKiRWw9bGYMFBArO+L3BK/cfcob8GtQG3Xe+jl/W+KdZ+O9zBTtep66TCsNGgM
v1d5tCySfaSY13eVYBN2CCugjNgLA5tdmkNyC7sS3v3TiOBYyBRTMsgm7eG2rEmF
kUWgVqZFZxCo33+xeL+YvLQefVt+fZKpJ1V3LCJgM7UcaIPpX6sG1WPlJPZP8O6U
f68rfLaY1i6ls+jzJ6uJAHhb3y3bh9EbIqHUOrWDo5rrhOsTLL5c/FMyVIL8pP45
++iseahk7QNr1QGKrIGjo88JIkRyIJTM7LkoMgvn7G3+edKseGNM2JSGQIWlMzff
vtvTsUzg1IxjEq3LVten9BGMb6s6BAeM48sc972LJwNuPIQb3xArvqGTegaeT6BO
YpuWtksGP7yhKleSJ1CsGNG8cdikkpmK2rFqtpefOKQAIzIginAnE8VWi3M/4jjk
h3BKuSWORTag+K3h0xakApBO6ZY+/8Ynce/7nWH0hgJfLAH7ogHHAtfukHJcYcnq
lZH5fDe3jdtfo4+srE2xIMXT4W7cVMV0MERZXbLCHfhTTKwTBMczyowP1bjCM+ZB
ZFg1tawQisrkV6aqUCuQmnV8ehfkYYhQ8+aJlAgCPeYuT9SMKUirj/9OF94XjIyO
Tj8SPERUsDnfvI2C1gO9jS/ltk20FWoxOrxEdSEZSQTvniNKfIs3o5DxzW3gsO8G
LM8PIDcZd7L/NeeF8W9fK8bgK+qq47gkMfX7CI0e6plr1+u8PcRkxDGjL0JvF233
aCWM0BFU5RHuPhybVfMscS+sdfFOu0aGmHHqcMgc3ZpHqdFCegVCa00zSVX8DwsD
OOOcLma7eIyLeMggtsLsY71A5hqSB1BAzJMOtyo9XG/ZvRs2ncd92FkZ4nej0yPB
xXKfndPfO/gRlaInvbpyTLcIVhou0/deaRdijz6rI4LnN945BnViZGbSGNhX/OK6
GqIPs+UjIxUukBgD54XQ3JCiJYfrbInxrONYcxK33nnyZ/K0U3KPbqmD4IGg9Q6l
jeVlytNoxPwXAzxpe+49vTy7UA2YMGmU8ZnSK3pIGyx4VaLXnHZnbOk4rjt2AeZf
ii4pIgKQbgI4hqpt55IyJJ2Z453ru0IOiwY9zprY1saHp3+JY28uiAufbu3UfelQ
MQPdDES3BXanB47rz+PhOhoLhz4Hnl6FPqNijAUjPXwCir3zHZUdb3YOW220E8E6
P6Zr5SCfn33jDlcxWzm0N+RlOdpDMfWCPxu0oS/uGuS6HK0nU4FIhic0pEcrNsld
EJS6Lwg5fH8mk2LJU+ltovNXtMPpqrEpJ+PHov/jXUiOv0FK5i0YNpZztTmONQea
ZJCipcsAghPrm1rHPFYWp/S05qJRaIpzaY8y6dGHVtaddN5RwGxl1IuZUsvkv/h8
iehQm1LVJ8puGPGrcdujUn2t03yRRkyl8F2fQXzoLo89J1CCuToqzmyJr7lS8RsU
1Rm3xZvZLiuJwwJVzxfDKMxDl/qOguj504vRA6OvHYEsuwXBa4m6+XsvuxUn7JBm
60VdtjrH7JEQUpHIR2A4olRpTYZLI6EVcl7IEQRUIC77CYYjWlFH8mtFAlNjRDm8
8JYHglydIIgGR9MrXYezAM+zCvp+Gj3H4g5VZwmpZh0LxH6dx3c2fmw/esuhr9mZ
4LSE3bU0hyHtkKnGZvqVLQsHr+nbVUe2uUN+rnm60YJbv20YnbevFqqTghEpyeSW
HuYGHyQnZ9X3OXiyd248lijelQz5djqKzZhvyOwb5LZsODild5E9sHz0AIXxqIjb
c3TuG4NyDy38TiHaciOxKEW3PDTE3JnZCNaWhXh7muG8+RCUb3uik/4AcfyijW9f
d0Ig1st8K96Pu4MuWHELDpyUiafp2Qga5f+uLkvPeLiwhFJtKqsJcYUbnNtTBJ1z
e6prolF9+sruDkRKSXm/qr8ObViGRZ1EPjXArFyCGN4tCePL3CkISfa8uZtO33pW
hqDZ+/0MnBZtr0r+h3HeiUHzMZeCNc/6UTn1oDBPvB/2TZlxPBdt+swb0fFfjXS8
IXuXAccwHXc0GyEds+gaHNspkjYx+Zvo3zU1fZJBt9ojnK4LQE+KRifeN1vUl3Nl
```

```
mfa3FJJrKUz7+aBY7fCs+f9UTP3kB5U/4SARbKAaOsh/6JpKi9iR6zPFSWy/vY6O
24MaHgHom9CiRH46vRhz6dfDqpIvPsbRxOqPvXzq0D9rDVH4kitPa8sP2Jt7rFFL
81BIPNE+cFXgm2MAyyaa/ar+aKqU/fOLrTxVuruYMCkwvQlzdWAXaXS6rg5sE6r6
QEyScNTVkoqGoq9/BEhnflpdYiDH/OrR1gyNhMHahOLJ9ujw2huTy+BGJ2DAM89A
SlO7opbdwgE6u0RvSQ4CsVvKdAiKhPotO44IQ/sLagIIY2+vBjsSPj7kvDm3/wtO
e+GbiYEzEGCK65w44pM1UG+LUV7e2cGAMi3IdObVk4gzK4yolkkqZ4/lnxBTp5AC
tdoBcTnaTbJqmb2OJFXwFdkPc+fTLNeCu1DrY/eQUoeBz80CRDSF5ptRgBM7Dw5N
EgCEfMANYe77nhsa7bN/3hKq5ktwqa0EecqfLSic+SKDLfaXFo76910i86s6NdN1
FyNOfS+GhrGXI0A+W06Cq+uEuxghu6iR58ydwm0jGAq3xYnt26k9Zcvo+X455cHU
amTaYqmjJ2rywG7a1HM1J6K/j8xBdtI7MA7RbLWWWBdyHXpSprGMFV4EBp2DF0FT
l4n6EheW5MrO+0oP3jB7E7/TWvWv46CD87uFMt+yvObTYXULwHnby5mQrg7osaib
HUeZjYsLkZH21WankY72KmLxBKPPr1Mvpzdi7JHmosMHdtiBQxP0GrSTXBGJR6EL
lQDL3k+daP0S9SBhurJ7y98y2w5Z0uGAVI2YU+9z/6YkWwllyHCzalMrb8BE+8gq
2QX9Ws/MzLDSVxKwq3Ur4O3n5pW7bk/35yMBujmx8wvVbyKGxMGUnCEoa8s818nI
zkiO1IHYT/vWqukhjItk4iu3+il7ohCcr8Gbl199v96qFheCnaHyRVODyQkSqFzf
MtgDjyJ3gtvfyO/ZDb6MtpVCKB7NhLu8Pg9AC6CMcQI+RpYHNoh3khZDWcUJFjRa
ZSdFGwQNRXHr27HB2vt+coE/nTsSk/neuKl3WyXcbejbx7QGkpNpMcjU8dA2rZhk
TDUddNeZGqodM2Wy5UOBqeGcDDjZX4Q5ueKjwZY0f7xV8jLaziIiJuX0BCegQVmC
XckzRnhmNbyaG5374iGTpugAJtY8bABD60fsTsl2Kn3DKhfLG3eC8WHKrGY7JqbZ
kAkhx431cDLgwVTlE5FXAFVDS1EQoYlZEbgrsfYAHzDQZI0v2K6LSa5Tb/wHn8/G
81lvPm7HqF8/dxNxoNmkP9tjIp212YTonC2oLh/4RVFl6Nig2IqIOfzYD/p0GGBg
M8eJaztwl7NCyBirGxKnozh8gi5JvqGmjQ5GSGDlxtgu7ZsbhtIk+AlrDAco8LvV
wGfFT7TnB0uGTfW3aQzTEaMAumj9mpWGcd66wsAvA2Cc7eCncP6UPymfyVAnCGDC
wkVXH+DjiO/alK6tTgaJEAnaanaDk26YersmzwuZC9AwKhBTLn5Mat0F5a8EXf5A
bKceHo0NBefl1eqgaZExcqfLawh6m/tjycQkGlPT45CWyxwBRWohvLCDeXqS4Zhv
72N0wlKv/EI0LLKO0n22IWb6yI2lfZR5MeVPrk4t4fhdB7wLPmG0zfJXTYgfYBMa
fTbWqxRZqdmFI3VmR/CgVQOkuIwxWtv1Q/ssba+UaBtH0t38hcEKuR8Jdk3zEqo0
tP4lmaRNAkBIt5hda5Fpfso+Fvf67yHKqM9VCkbW4uVPHcUbaQPo9aok0TVfxMII
sC0TXkGovnb+YfHp7tT8XczuKOIBt1mzNMGxCkTNrLI4/ZBm6mtFquMOqm82Hdaa
9f3qvPo/fRMgYGCie219Q9ZX3I3UgH3e1zFHjrFJn/icPpUufzO1MY0+R7yqiPrX
VwCsosjlR2OPP8rCKRBVxz2LCUzED2I+GDhAuZXICzw3ZoqH7l7d0vUdPXTTC+vJ
EpTHCLZsfA56YoZ9/FAaEIkmav5acxe40zMm/Ikaymbs9YgowThUAk0MYN6ZocH4
6bIcetgeKXxC4kqp1BxUjcPpBGrQLtqmGcyiGRlQP/tWoH6ThZuSuyC6i6fRYKny
NowSOQu833jHhgd+LfyWgHLf6oLkcJqnJTl3b4Bz+dvH8rmwCtR4aE8W55Kqdhc4
N0Adw3rgFEWSY8ynRoQgMuHxWU1f/cEWgeOtJAxeZ/XQaF/9J+ozVU7Aes8f2WWh
yAWk/E2XnKvr2spBk4rz+sBwsBD0wp9o7Nvf5gM06PCODCfAMRM5IahGgeHGlRDK
YGWk1kuLbL1yNacdRgxLmtekUclrf6WRLjEXfJI7bJmfTyTtikOFdesSgWZTlMcW
/Haq4LllQpzTo8kTzmLGVCuGPgJdG2iJyPMg+YhGWnPWYkCOZCuhx7uUadXRYEL2
m0brmswhvSVf7eVtPOQZyL2LnIiKYmj0cLSo8IZvmlHwAM8dRbso5pJIFBrApLsL
UT7t0nKBCEwyVy7kA0+k0Y8Tj9D5wdUiRaAR11iIr4hEobckq3JxBejDoLTQHRog
pR+kdwpn2vLK2ha6hV9+zNTYlVrLFLohwf15swKN0DOW5aM1efa3/Xi/mi5+JG8V
nYVtmvQMVhnibQLhmX3liNbn55ZP0/qsZjByqmnvOIwcIr6fXF2zgD+Vg+b3gub6
JjI7aIw7Y6NnoJ5XFWYKNlJFtNr/zojvYwHJ8mhsUc+aEJoTDvTN+D2NeHM5P9ux
4FWvedD9W4yTiIl5uYzZuRhEY4zoblla7oewWdJO0ZeW9nn78ZzGBzvwFB86+RdQ
2RrnXxmFKVytiOaT+pOc5+yHD/G/lPfdes4Zogn8qv0mitDyd3X3zwQvU6zA/q3m
l7krmVOPCGrYOP0CHMFEPzTsfBWcfJXNYxLiM5YXLWFzdCdlegWZctJ8IUR8yyZ8
noSobJMozWyKelCvKqnml8CFMkigJeTFAR5atJ0Ld6H23UagpWzfIgxLuVDvO245
tuFkiYG2c+S6hGixq5JHHWcdLpSLt2rIUSrOh0m23CZWxmBbefj3n7f3GuZ2y8NL
R1yWsA5fAfyRHajm9qbOFUpLDi4oFS3bP8MgZf8kkYON4PBDKt7gnqG2VZ3GnfFo
yvl3gnG9H8XV8f42c3MNfv0uZErow0TAt6F1TMN2ElzrZehS3kDluiPBjx2v9BzV
F0CuwGhpV2CdiQaumF2uARpR/SVfW3DqahtuVPq5UaXkpkvLGebI1SNrMvBlFKRN
gPahwno0ybGInx78QZ8+/dYxsnrbeNcgWAm3bbR+ngRorB/62IzPrTVUfwoukUBj
TsOf86QYonJUSZNtDxBYD73Vbqz/YJ9Dg6sFc7UrOAsFJGr4pFzw5KmXgM49aElw
```

```
5O8t6FpJcNcr63/G+ZHjhEPlK+Yk9sRIVbwQgz6eMqjJ+BPewGLe1O9e0hHZ6JB0
WqAbn8s6tC1pGKBqI6CCRKSQUQjaCY3wM0IFLQ27LoTg+KFXg+H5i0Q+JPlvbN+x
MXMIZcf94wGcqKZjvZl1b8LqCoPc+un4cYZLq4O22nM9LNifbu4xfggR2BqxpL/k
lyp/aFD6fvnIQWsGzYqRnYdN3PTXvkdQZSJhci0dtOL00ibF4xPdC3ZdBzCmNzWI
TM26tL/i0gMYZKKqlaqooN4/SR82wUtEeHmhTZ6MLXL61+B9AdVP0OhHDBLtL4Xk
bJ2M3ljHAcnfQFJ4lZhJGUcrkG6Co2jo6VJf91nv4xzjV63op0tgOjwz5r7H5R4z
PVOI16B2TFu0R46VE3Iw9EhrJiW8keSrwmSDFJQOxlTcq39mnia4MJJGhK8GMANR
0QdcsHG88Nks5D7aVcjPwE4beL/qbbp4B6MNkdk+AjYZwx1IBuK7uHDZ70+wd4Fk
Ix78zZs+safiGoWovziFxhqcNPQdhJ6B/vrafsTQOm6ZnS+pyZBEiNwTqP6CU6SB
6jV74yPnSLFzqfpnA8sOHMYzyYyBsTwi+MC0GAU9qTfGDeudFrCm8oaH4fz4oxUM
1Z4fZqgugOoBlsRdfbMasu2tJ40MkPn8grJQLLCuS85jCVQxLGx79MShtHZc31Ht
ctoS2iIPEmNp/nit3ra86yF8MtaIqalhuOw7vEG6Eh0Zrw0yJfdVHb+P+G+1UJm9
MfkG7LCGU0SvkpuxXIzBfuggA68LJuRqbZmaCSKzUzVe5NH/n1t3cYXJXfOWhZcx
4DzLcygXt/wDf25mbXwkbcdFl/D2iFuUkDSuwI+HD1YG/QOplHBchql8XrXOy4V0
/ztnaaImva1JaDoLB12e3w6ulDV1rXIOhBOYOBrAKM7AYMl13RuUC6EoLIbkyaX2
iDQRIXIyAfHzgi7roLzxZSnZOrGgUKCR1tH9YM0RY1GqhW29+FhBC4o+Aq5xcW3v
YY6Zua1E0LzayfN0mUjnlxvUy/Teo2nK9gvU3FyxtnBgWCrVN7T5JcCDKynNIT3r
L4tI+ZTPq7tN3WcICBcMTHz1Fiz4Xz2bOS0uaGcjE5Pp6PnStdFqQisS8KMjcQYo
VF74cR+o0A1un5ko0OOT5SAUqxkcqNTfYKiul72n4aVnAd7syPxL45AofIMqo3xR
p2zYjNy4leMvQMWulaqU/gCfAJHGBIgS+jVWy64i6Ne+VqK9hOGi4npwXsAshyvX
y/RfOhafXMk2mrUUINw4sCc6/DsL0lYnlTvXTnaNrcXBjKY+nNWgeNxY6XMXgYqk
kLyUxuE+ONGQRATtESW5gM6lOUU4aUn1uV7Xu0DXvDikiR/jFUeoZVrtiRBN2koD
M8vVfElunx8FXKMMEz5b5e3pV/YQyrctpuUAMNO7ZnreMO957McRKcdw9n2NmCcs
qXw2eHnmE1m/rUtKHwaYEEHWaCpkZLAeL7gf31r2PkrdL9MxYrKqEJM16mOZ4Pvr
NtdlbKzy/WKIHUot+g5cv26jC8Fd6lnrCgNlF8RgNNQVJTfjYHullBdI4e1OBbEc
s89fTjPfWbngNOmSmKA9E2pEmH0GCBw54RJjDOHge0Rb3UaB9Fdw95at7DQDRlFu
9Ew3U9fn07cdo0eR9C8I2yM9aBdZDpybFQo86MJjb2ZaA3yyB3rv1OrL5dp9Actf
WFMIjSSy5zdjcEw3tfBslbv/rO6yzq7XJfikBd2Ysin01omp0gSJgGRBIF/vHEtC
c1ls/8k3hvmrNhfH4pAwJs+4YwAJBhl5/NLtXvK3YYxvoDHEC/2ouVFMteRI3UBL
D/kLQpx/aimIPHAbejtegQL6ijgrhfIvXj+6FlYpJAKalNf/t7j//a4uRW9aG60Y
Y4GntW0wQg5joFoQpPklag+7QuqbIazY5jc/8HKh2gwZltrxJxuzit+14/NrL7sn
XO5dhz2f2e0KUEV0SHimkacmjPZMsZIr2xeMpdHstsGGQLWNWskTP04qgBTIgH1G
u6/G+5sSnKhdJ6Xg7cVE6wYE2FF0lahvYtLJRnOAabqpk5YAx/SwzCP8+EQCZucd
7ZUbKS7Y1ES1wfC4bXeUfvuqLJXwjvn4lIGbcNNpIFnmCCPpFdLfysLm76Y6lTWz
9zjJmo+kQetyaIa8QJrq0D7hfZlEEUtkTO+LNd0XLXwjTdfzb37v+qWYyGPxgrJA
30Ml23m1B2sLG93bbM5eXUuzWCY/iKqd/9yOXRu6mRkNT0/DJn9JJFYlD9NzuBID
TLZCkHjppTTAMAHFGNAWYuHoidJSk/9SyNnSam+PpNUBezzJNVgpvn7RByTY6cNx
lgtdPlNYr/t3PN44js6IQHMCmjIqad8JO0OhmJM6f1eMNndAbitJJ8Vi3zvedf+W
5gywUfwoEDGRnfP2sBsVXxHZMgvZYdU+0Ijfwc17x42QUb0YJCKnVWa0s7r3hInZ
ywmP99wEEr3eKvEAfwrIt6rYOVsauj3YUc+7nN3R3UOHDnVtJ4GMl29F+rW0ZFJW
ZlJ/XM5y9/yKaKREsigF35xxw5IV634/s/TXrgydJO2ncw3AvBPhBeSRf29lAIc+
MlzF3Ww3TjQB+KlF31qAc18fswC6KnXOjfuW8L0NYT4B7q5MrdtPd3kc4zeJY5cX
Bz7KjvEF/CFqc1wQUyXCSg5cwiKqUqSIauudW3RsVeB9ci40GQFQqz/bJtAPHzG8
cO0caaapRs+LwXJIg1ZO1CXbM3/7NMr/1OHMSBWBxkoZ424EU7JO9KI2GIKs+oPN
bj/P7Vh4kBSIAoSZxfaaIQhxJBSdVatdDcYg1brbL0XruyYE6KVviI/a43vgU3Lv
5LO5vYnKeAb3kar6gpUon1GNeE65pNmgQFiN135wZHUUviEvrlOBYcHTzmYOyyJa
8FGbeg5eP8ELX6J3ZCMgTl1b8a7CMC7d4alD0D7NeO1RImEuOWHlsAiRX2G4SV/P
JU0Ft0nkrsVvaTgkYPmgY885Ed9breQW0N148T/uld0CtMZ0fVqTmedj1jH8CB5b
IPOCAfPHuAOWL41ir3o8JJYLX1yaAkolDx9VRJD5WIZIRSPYJ8zAAixqE/G4p+iS
MskpFjz3KZ/PEHDnslvZpc4Y16mUJSJ8REul4fnlO2vduYioVrQvgjnnHsjvmLmP
WbLwN3044sukYNmRcqSnujMUk47IESgA5fZrf2+2XNugACR8uguskc659niTpqUi
mK1HJcfayaOtix3AfhMw7GTHB/axG6uuhvVk4bFM9fyE73Rh2H3ZmRm8OZJw/vcK
x7QP6A1RWldLlbGAN8dWBt0kqs0R56j02xi+XGzTnW8YBdFQAKy7HmRITWZA3PU9
```

```
Fmm0h0pDXxK+3/XinNF0nz8XTiBho83hfS0HR/J+BrRoKuhGFTpnMJqfrnGU4EKn
XhywG5Vboaosjjf89lddRFaxi5tAHAt8fdQWXVxWyfhKDVY7Wwly7BgjPx6/VW72
R2ibaBeGrm/A5+o4/wlQOlOrbhpEK1LQm+3N+ylSnUReqx/2eRHR8hdxKB2HZOUP
CxFslghmaWxmzZeMuV1YqC2aLuk/eSrTqsWQUNCByNtsArHcqtPFYG+bDg1F9h1u
VX2idY21rgEm0Sk176ENVyxblfdvoiHQjG3pfTCe12GA/JsmmIpn360sr2Fv1r6v
KvhkjwV8T2oes7/SjpBwRAet31sHKEDjt3RGbPKriRVhQLGGIwKBFFw+aJvwJP01
B94wqKuQlpnq6+Qe/GEawfl8XKOlDU1o0Zd0IKgty5vahZggEAzBIw5r1fxPGXYK
YHGGxK8LT9IWWWhvPRPPkDR1bVTOHUmhIgiJf4ggh6q2eUN+bILmHCIQkBV5TIpA
guOjbSzoIvqA0CcgvDAF2reBm76PcQr3mpK78m+s0h3oFXX/xGVednKpDilt/qgP
QANxjxjAzSvzo0batP2Oaal/DWtKpXuMcRMIvVZxa2qLYJv4o1r0OH+97oEdkrG8
AF7r+y9yh14p24IKwOtoTwlWhhgCLnQBf2VQMGM38296RaFIjoDzspWOpyXETloi
8Uy2s9AHLRBVIxv9hadUr440FPFWNG03zEQ2RcmL9D9M5j7C0t7qnqBQ01O7g52m
+rRcewukbNnlXYPgKZXiDx/0uL6CuabZvi9LIL0zx8uSRqBloUSR5OxziuoY2rnK
1J21jp2h2JzTnKP/HvW0u3CUhG/r1/vB7xr7t0vkfUEgreId7Xk25J0hmppV+5Wg
HFz0nVaqWbN/e1AK3lCSWPonBvtEpVt4ty11hsQCM/Uen1UZxpAfh8FpEsNsIhPS
Atqwkjb0OBCQMJIleRPkyk4KCtvssqPmVKlEvPYR9iEI7IYdT5N+0WjQdX+Vv8Nb
vBh5bzimMOP3RiJWd283BH7frewMzWQBEQ4er2cidNcMwq6jgo1AT+PCNpzXu7Gt
yMAWoSzfWpQCngegz74V2fBAzXK+KfAIzCghBwqLaUQCYKB9xFeAwf+r7iuB9+kv
qExMV8ywzduwC9ty4mfL+ZUpZA2oPNrIRvz3Cid5JYAfLRZxlZjkZZCG4HEKyzz1
rNZS+a3YVvjosLZMFJ1GlD9TwoNxHnVZ1BSJfb7NNUbY48xNzf0E6jUsxRZwFAGP
Fv+0U/1E9a2o1HA7WgRsx6vOlcIuHnw5kc0pcCuEDDOBrGYHa/4nyhjt+7isoyoZ
RujkygVEoH9vRk9SrvcDPk1GPznb6Q60ZO4Ls1GyXNqnWt0BpQ3zm6FItLfINGH9
9kPZebdrwKTNs6HbtbVKOOQ6kQlTvwDTCOSUhi3Ael+52tkkCd3fYbAVNBL6v5Nm
g5srI8hbC+xF220JXxp5DOjc9RLcT4LTEm7hZqxG8HOopUWBsuqLcjeASY7IEZQy
qfrjVICNdECwHObffXChijydrgJpytDTCvoIH7a5f9uvLaO6I4qyCV1kvKryanoU
rU3Oyhsrbds+EkDlYejeRcmj7w8GWghlsC+uQzlNy9WKMWDecheTBaJFgKLy7mOc
b8N7pcvnRmxUBqYpILZnQDfN7qZ5x0D4gRd3D69UQCphzWu7KVIkY6nK8yxYAqIc
DIy8T7Wspy+fEcVeZdWpMgV4YDGEhZftzoDdjMjwRwddu3rq8AewQsEyblOTbo0u
6N31mXAQxrXbjGJjL4k8eJMyBJQgUBfRMQLsbHxKhCc09DlV4SUlNrtmGOeUs4Wp
eecZGJysSm2QZwa11SEgpAMrZ8rLi9dz/08NbdVQpmYkWthud4NQEEG17D3OntTu
2/fhMdnz68nWGlxg2ZIeM57AaMZC6nDxECGgJCBi9OoWRu0Sya2bORD65G1oKsBx
onGjCsSkby1CsfRRliZ0wGJJnTyz+qccdmoE7sEYBkdqPpiGc29yAtpbgjKCEQLL
6tRX3fWLPgAioRTxngGNZIcPklq9Aa/bagPCuV7oT6PG2rbkVUQAtKzd+XqKXQAJ
Ovtj5ebIRI48BX9n3NuCTCaE3MmtRGmXb+7wLACt7/gsdYA+Bt5wFJ+2B+jozEpY
WN5TFAG5Pp6P7vWc5O6IS3lAOHlQsm5Kk0FV+9xgeeaxSBWN77Q3PHsghP5VzcNN
Fij0N/JGVaGNO4MgizVdaQt1C+T74Dt8p3TJWUtqb8ThDVeA0K/Jzx4JEHDC4kjP
W94WqWyA2JCwPomdigay9+4Br8YnqcwljOMu5F5AG1nPCWKu8xp3R/Citm1LSJLr
kw3aCW9eLEn7Jxtt5FEl/oIoBHswp7V3+vbrAbP4uA8wWuDdOYyGSb+zn/dxisBC
WQP/BFhU3ZuknXDoH9LoH5sjiFyQz38QCYBy2T29nW6adPz3e1zGuqPoAOTXcQAN
EY+GV0lCvZxafH1IaGbiQki36ki/ZbUb09Y3yz6Sw+U7A9YMrA220vb9CSBa2qgD
hDGqq4Pbz7EnQZZokh25dbloH0WyVNCpnLy7QFBNa36CtBF37NAzgE6oqVtxrRXy
b0VgvoikCGHHnrav7RMfgvlgoRqTeUkfyi/fEo8iLKJhZaPKv4voGIUCYC9kdZl/
p9OKaLpFRwX728nuQ3OOH3KaY5ZJ8lXa3BW9c3s+PAcRr4Gl/hwxORTmKjxL8GJV
vGWEqqh0IJ4qp6cdRBQGOQ91qWCiU2iKk126KK5rm3p6lDTbDMUCoZA+rM3yA25D
0Jg9xTw4F+gCgD9PCdZBQsxRjcID77clGz7+GxsudLMKbZnFt2bC80yTlpGMv9sa
8nxAOvrvU6VJysLh6obTCS8TKRM37JA3+0OqL5XJuMuS1awruzW3ThPq0KUbEZ/b
WyNlCBoWdbiN9TObO82dZ56jceZN48V3j8j2tG2eTWFkn/eTiXMygmgpljb9K6xD
L9uzrjs04HrG4WhpHAx7AZna6JRTUPDeFEh0JDR7efut6/8YZTLdgG45PezhZk+B
aCdBJjrR/yWftH4x7SP3Sw+R5+BShleyp73aEz8EpP0LERGVOvKUnKIhS/PWVlmn
XYiLUPrdgufmkHGfYNiYmIF8DKAvrYgCsTCrlHKC3dt959a9Pn0fUMg5Nr40myRB
3TTdt3oLwKycGYMCMZil0I/myRE9bVK8BaRI/wVhesjS4tdGxvvR9LkT+1TVk98J
zsA3sZzc5uHCpBMlJD3TLBC+EFcukeJjWwjAOxrZnUgSasKiiJlR/rZ/YngKazEE
CmF6m9wSApkehcbJuNpLS/1vrv15NT0AMClRV42FTdiWywQm05c0GD0VXpsjwjjP
```

```
oHwj+9XVsu7dNUOU4a3MdFar9j319vUf3mieJFNCB0qPG9BU/lATqV7f7r5uxC3e
XVZyRvZIpdaouY9nBRIT9yXwKHB8ugdCayepHMa1p5i0dvxE2x7AF9qQ+wc/+x1u
SLD4qT6P/DvTZUTj2Y5wY3LPJIIkeywO2OqXeSHFWKVL4nnWDmJia/38pTmomBw6
1NK9EyRbbrLIkAucCX/WmOFmKgRwnAA0KtN3BX+csbHTQhaoJ2j1nVdwPgOUWle7
PnTWsdIAX3ZIn4Prqb2fhm9mUhRerEjIclROshOR6iszFCynLbetqSLdejILI74m
k1jLoiNLXNvhK9z7DEzPSYTsHeQK7QRTQ9ktvU/iNi/xUvoJ16ygYsoUaP1wcgoC
tqjPob2qmbe5QgmAhaO1PZn5F+OclO/RoWX7grUk+1RigUkbYmB215W6KYGeWx2l
91z/eJHa241jMfOoVtiSRBCbsjMfnVT73WO33XOVpO2EIUkLSHOvRKTceeyLf4uD
QsydtI/GJPnuZycRavnfxv07x5X5pGRwr3webMRZ2rY+eLaSdETOFF4nJFr3+LKm
LJIF/mik/bplbGFFv+3PDd164JfdnHqOJ581exM3c46gYuVg5XJIQpPfr8LWeWGe
RKoCEBy6/l2P65qIWRqRccBpiR12IKFWcMw+a0p/JR87QxCbid8fivTPDj5lehmO
q6P1Hyhbtyd21B2GDf9hdVc9h18C74eYKnfpzYgusBfdm1t4T+FoT1CmEU0XD+QZ
ze6QGqgXs6lzyrmVcsae6JXMuHjBhBx7qQgQ5/Zi5F1RtqUhojsS1VcY/TRXWTRJ
JI7xUWUXPzMRDxl2wIeHhzgx3jgU1pI901dwNsqLvDPgWQ8dYULSJy0s6RnBjT71
jwbODKKlvMPTdJH0PxqQWQtRITYP+mSt/F09LgdXS50M2u/lE0KytpGBuSa0BuvV
R73ndwYzp7MF26KygL+vGDsv9uexum74iE0bRf5RijlIQ93POdN90pREUtSglyT3
ccMfycDxycz8XVJFWC3CrhDV1CPijmuMtScGlTOFTFYUQznKI9fLWCI/ctrDzhgI
REtuUB65eb6QMctEOU/UcGPaSrhu6M6Yaj6GBjf6hkMREB7m6rSgASzPsNBKfD6p
Ih5BeXPQ7DBIEnwtzLgiMIdBOn4VCGS8IErMKBp/AR1O/iG4PprfcLkTaZMTHFIP
01zez+w7A/7z/j6Gb1xbH2/1G1iS7+sgiSraRuqdsh7eXMHiiwiGlyJSPbGUxpO1
90pZRK2SFDI6yq45CLpSnYccJnvEGQn0+2ApzYkMmdjoFmYYSrbRR6f/wXnZTVyE
VePGCCz88q5/MrqugaPRPRO+3frvWTXG5JTqKEICaAIH14U4rNjQ6Pmjdl2BG0QO
e8OP0wVyh9t5LNdiKxq9A+wdLMm5Q7m5gl63pWxA1Ger7vkZN33JktP00xj+h/wK
vQ7MDXIKBhBx5EpxAWyfyLCyvEBBYsbLU20BMsMeJxQtYDmlXLz0KRjXLB3q2yk/
NJuNTnwVSjkCVy4i95h2byr5HcalnxHZ9vdFMFpDG9e3a5y68l8JJxwa4XNEk2Rl
ICjKnOkAFERMy7w8cfJI0WU91tnO4tTKjmVIZZXUb9Iap1RcaPj2Nl5G39lBvEeZ
+7o4IQ0vEeDozIzfntN2AYnBt5Crs+izlMG1fCQVzdAGP69CF1wQFpAiC5HDuFIJ
rdgvXYg5V1LX3pP6ms7QIk+1Wj7/rM9Tn+W2Z9z4FGuTChTWYac17Rb+jFOlgmYB
S04AFdjM9oxH0//yxlBb9cMyDsRDVl3307BMBt0NuS84hgd5W+ymyu6Osexp/5EX
YRpaflHb87wZ4nkiljKqGINNSnAaPUS/dHmVEaaNVXKVG2KL52xxqG1RtZMOJk8E
a0RCvxdpeTJDxzTPI3M0cmHphAnRwv7p42NiMpYEmALHiq1Vx0fbIBzKuEunkXaw
UGcIEK23eaKcU4Yy73nYI9W+54/bUrcJKGS2RQ0mk4STsEfuj4R0Tl40H4Iy0zXh
z90ARxFTfiXUOfuPJ5OSZrfS4A4oH8qnD+LDoD1pOnhADjMjy8VT1n/fiWv+wnlv
DrwyQ9oTOHfbeB7+0PN8UWMTjT1CLi12qMKstDU7g80X0K8j8XoddNfmOhgcYkOg
5pd63SBSHxYsjeb4lC4s5hE79RvaxN4k/+/1KEfmeebhoGOu4n/NOqsc93ShWrtK
5ENBh6vcrCDrsntQCaKWOJ5q3bCNDuhpfNVhNxPiaBaZOLcuVjHrLzzSoFaNGtCy
RPrjBxmZCyvDDCjFhzVavp0WgAT/lIQPLBr+ILzCq2nvPIdI3jzSpLRuPGbDK6Hp
9RNn8vvo8lHUu4bCTtenYLXn56LXgVh8TRygAw8pxoNOYjvLIbLlfI/ILhox+Z1i
7vqUeNn3vfXBNOvxaUZpsmUOfDNwekt2cTuvi9fY1gDs1PFc0x2A9fx12wtCKWqB
dRsuElXHtpAK6VC76Yti8tzxWouinDxGQdlyS4Wi1+Bi94xDsGiLqCpFxnbSblc1
ItNejXg2QP953kTC9Y8LSfz+0LPaaMQYx8cKULrXLCZluswEnjUOuLIHM7gyH/Qy
LDM5L44Qi/ay26Idbkn4NrqOW5xBEFNlPV+oBscfg+87A/XogXCqNUC7X2UBKXov
GGTh+S8RqgNTW6xMQh0IgMew4Jr6ahptz11HJ9IYhxyJyR1U9pPiWys8KGRoo85o
gxWNK6LirQ71JsfKM3XSrKWi7aDnLsSSc0MuXAzFnoe2trcnRrp5ayM25ILdUgEv
bRDniqLayTsJb6+OHU0eLMPtaXwcjO7iTYCI4MpReslcOxnpltTdI5tqoYD7n8Qt
E0tyYDUlMJKG09hcJAygOv+YZgL5agtD7J6q9dB8PU1lOau++FxNchSwrI0Y7o06
z+lsHKrHgn2JBr/pGbf64WehO55xr6FeMU/TIPkZfYNS+JjNjR8QY3xTDIU+wMHw
Fv3g80nzXxgxupjEPnqvwb2yt4gRcSi9HVqnWsEVuMyfOBBK20NaHG+1vmeMPHJ2
Ay51/spTqCGB2MMtz7sMFqnv+F3n3sTxIbDZlJJpEXUx9j42RMJ6KKCQzKqO1qGR
S+CZKjZKQh2gIepcHcVNu7Y42uwLFHyCb1JoYz1NoLVlBIZFSxDgKCRfOxxu9qd7
uU25QKUJcT1kSKBEj7atgCJLhYVTs50m8o3StJh2qL/zVM/guNb7ak3awz//V5GK
L8jShi4Wn3VgEOVQHZeg8VcA9wjBf75SuStz/bVFa25n+2n+GzFupmux6UFX1l1H
steLoLIho7XGK6a1LjLFyr+yWimRGTJTSTzFp5HEMoh533k+7pIuQ5ZHQgqHtBtF
```

```
BlaMzI75xQD5o1qs2ONGMeZ6R0RF9mdjIUVGW3+jsuodpEbJOjW1LUcFlrNzz58J
OcjVevM/ZH6fqK/7t39ZQTDgNr8bVfnSL+fvZm9Yk+gumn2vi4JLEj/9UD6re9lj
U7ykZEGDgs66wrT824QZi8N8+AXaO3Su82D1AcnjN0jAYMODf8DYBHfZhJ02/qrE
6ggSjcDT3AueLUhTd6MgAyNN3S026t/cR8MN7UQmxHGZvFB4JGu+G8j1yh5tQmBl
wXoWTPyR/IpFWhknW3rK5fli2aI08F1aChqkUL9rFPEheQpDqVSce9YVUMlZzhQE
7aOV1KZ/1K+7n35U3tjut47VEXVpM8Zdm2M8dUzNlAXNBuni3uLJqtP+8/mOyhTk
TVPXqIRAFuV/MXzrkQf+dRos92g0o4JVNBCc8u+YQ5y8g1yzJ1o1y4YzeGtgX/YV
2DjnJx5nk6t6BgddE8fKsdKt5GeIudI5+HFdzTs7/VeBzpZCdU0CFFZgFv1UQw/d
8UZEcsypz7s22v/nVdwRNyY/qMJI2RwEJB/nPic++TOX9pCCGFu+gVbIXhoGVUkl
VQKYre/XdbpgVgyTx00Wu42cyITGaJIEe/Vz0v5W4LBFOZueiKai3UBKkOb/3hOD
z3lGV+iJm2DfrGA/srR6zu/zpqGHAI21r7T8U7sMRn5optLKyijY8rLi68p9BHSs
stl70md7zgwqnAlIKwB20OLVG02Pehi10dplrJCcgBe4xJJHgwbGM8/kQp6GhTVJ
kFV29t9U3g/+fj9scQzb76ZKuF+9AvaOD3MN1iR7SkD+GabRbcwLCaBEAhtiive2
iRfNrSae8qGtwZfSVXvpvrkK29yCJEyIIHeVPyB9LCr0cl3wcezLkQr9x1BKVtxZ
7x1kGlmXE7+OlJEiEe/GXFK0DGgKkvdQneABIpETvU6eALqA0ufV9e4I2k/uXkwG
a9hB+Bn/Xl41nQt96mfNmXxp+OQ07+siTP+ETRc7LOSXKFKwV3/OWajd1G8qouN9
AY48IXqoPgQfXk2gI4mwhhNpJgo3yfj1FfQxU/AXI2sYZZVK7QYqQvf1UcNRspcs
FuTYgH2HxUubpr4lZeqtixm/it9tCXCAUtu8C4a0IN6pk6CReY9hT4ERetHKOn/W
LtaH961dckaJF4qsmuYtvLcXasWU5sJ45cS97tBp65zc3nQdsdIgl7XnWDjddYF1
gFvRpidblg/ScEKDtVrnrwoYHNk3bFyEAUZfSQOMFFoSF4Rkxgi6tGNhvjOaO5/V
kVcEnljMST5ekKezOmXUTL6Gg71eVDZqbFLq3uIcB7QbWJjppl7BKzp5Lt+EmBS5
ZGsf6OhVHFkdWmwRGoxgygwQ8XO12wNHcGYdVrQx2nwUuoN3hEx66JfuBq2lsFks
abLxD8eXVVgiiKHw2Gpd3cgH3H+ncVX45SOIHi6AFRvCd0zdKXig3K7l1ivvoF0E
+JYVuBVO90xomjrIW+octL+545FZa9bF5XBCpR02B4NzuPurW6imHUh9E7LwVb62
xO8grO1daGTOMt+cMwqqOWeG3NuL7d8t149yW8D9gmh/6B5tI/845mEMvH3a758H
yXS/6WjltB3Blo3H1qO1E8DLIzNFBgLKPrbhg0YPbHshSwxTwnTX1txyexJL1L30
9ivoS0xKJFuef0bctDR1O3Kq4eigP7x52WTPbUtqzmNrcFOS+m2Pc80urhHn+cWe
VCdKbMKG0qRt8fhVis4rtX5MmYf5zBC2hMSVts5PO7X7FVwH2IFplH3KKkqxdi4S
MTxM95CTN6Vk4aHmr7aJvY3qGP7SRWOUc0q0C8w/g7lf7G4BE6tEVnY792guHzrO
/DpInPAhYlSxBo2HP5Lib8+HXRgDZ45HWSjSr38mkbghIr7jhOQHUB5/ln55E/wT
lOmsA43d/oIhm5lpTGBN9GNzR2rsqpsdlXsr7z1MFOko7lvbBc/B22dHLPiklGc4
JdYER9vJKsNr42SwkU7BGh6VOcOzPH6cPy7XKncLi7OhsGeqs+KurSO1bDOKmu1G
rFllRUiHdcSFlxU/izwGUEyvrQVaM5W5+tpSFm7g6UKMiajPQiJ+APlnQh70csqb
Djsnvj5Rg7S8IgPdmglmZTky8mZE3DLZWFC90aZH2FKAaa4yPFlWo/+0cqwHqA+1
lHe1DoYcz/6TEy1+sY9BWpL6yvNoJqHaL4xPzKk+TN5iH72D+wyJ04pfXEH7tObR
T0totQ4Poxux2NXZSe3SpQkpUvNBU61zWp/RRJLO8NLAgWvZ1fu2rZY4vhh8TTDO
PIvoSWnuWXJsHwl2ekXuLLulP69Fy5n+QB91IiBlFYoZVwtWl31W3+8U+tPSkgAq
zofrdG0BRAN4qJ28Xo4WvmY5q6AbrQ/hxNi91NP4dJ8t5AvrQmduqazlvwFhO9MN
n4zdXF/shgpqCouM7w96nqtgMPnlznGP675vw+PFXShVV05aN7vPuXQCGve4fxA2
DXf+LFgE28gosgIwdRSYjx95/FKE0rs7QgFxmYiSpH+psPl0NFDHv5bqifA/RCoC
vJhrvSZaWOzBr9dgJMOezrjy/MsgLwLbn/gTVU8sBcw9N8cTCCPokouEgdL7E6Gy
36jGoQ1RSFBbOzxooq3rX6OeOibuWAh+5kL52SnCld8jQvOVWVZ1NRRhx1eJDlfT
D+BQjwYgcHB0EOvfd07qlkPE2SxfwhREa9VANTnNlc2ners9Bpdzv31E2GJYZ12/
9hcMhLxPCvPZ2bbMgO200gbf1qYQyS2Dwfgu2JRn4K+If21TXPYvQNLZTKXirNgL
yu9JiuwJxUc9kPz26/1kRAprXIZhEiyqcG3uNNhPYotYDfhlMuYI0SCZq1lVeZ4D
PTHq8RmcVNtUkmqShfis/uL1bxkwpOpjpJPFtmcNr3JSbZP0ibQDl+LvEAxNHKSu
zeeZFoa9tE7wjyfPr29h/25iogwaaK1GIa6dl1wzFZiGsN/X6qhEJ3MQOsiPNKc4
we2sfg4jVOk2Vf9HhQGjchW96zqKcZbbnzdpSjtl5n23+LDBFRW0z1OaYb2QOn5e
82LI7Xf0MHYhMYnzQpIs/H6QmKDL1Rg5W/+fYCavoVZVDWYtUwNpzuSqt70cj5Ey
WhuCdCrbL1Ccr2Ylyid3rdulyVqkBFc8ZxweMW7ZucJTt2PVEALutMncd545tgYe
O0nRoHieZFxrRn9BbJIRRoeZDkEg5DKfFwkG3J4t3/I0z4CSrZFm2kUZUvHaI5zS
qz9S4S6ku7wle41SQ9f27QVayhL5dSeCtgS1ViuJJbqUSXI+c7Jp13TpvJbCIttN
I3Qk6RpU7VyRZYqYUNUOxw3CPzEt3Wiqhh8TBo9DixW57CRxtt55HgZ6IVWCH8O/
```

```
ffES99JsnsH1BtE2EUPbf+SFjbdjagyHj9qQbSq2F4KZGoLhY0Bc0fKJ1FbHTyA2
cxualILCE5Vr2a39mSaubGcpNf008T3SA+f5/cCRceOxKN3dVN07BwfaM9fmx+Rm
dBkyhAjf56WxY59dBxLuNu7iRpLslk/yrZFz0tMVWHj5F4gAqG3a1hCdrfk2uacf
vmZ3ce0TosNK+1At9EyBvJfGbAR3A+qf+UErbCOFiCQMHb9BTPrIa5giB+2qD0T2
9WCwW59KSfPRqTN8RlAZotS1AeTO5SYVac0bxrRilrhze3nL8TjjMNF+VkB0HP1O
eIkbQGT6ViJSySDEMhI9zoSGgMiqcEd/tLuTkjNK3UXM95dME3ZokSTTwnG3JL/f
hUtPhT2X1Hxd09Ib22tOlq3chxP39uWg1MsAUDTjevEQQRNTJAn+r87XbOEjXGdi
lf2VvLQkIcHKf8/VAK26fw6+P0Fa9pPMWQZGhDs3XDt5aJdbbxmb6Z55Sjo9ICgW
wOkTEbT9/pycW1R6DLDULZSneYWvfAxUJX+XlbIzrbVOW2vGxfEgcEEDzt6cQFE/
wvF6EbSaGYRFOdXt5UEdZQE1sfZ5qTJbvZR4gXRBhBgVtgW+DDz/lnP9NKHfayCl
P1Odf9wujQTClawGeAWDLLbE5dANDBVUSEtbWvpuNEuEZ5yFIwAZzEkfk/EjOy+d
cWU/OZdj0irnUO8xiAIMnTZ+toshJqykpmsgcljN3bhV3t9LJm1JwouGyKrogY89
ssfOwFCNfBBfZvkpqwgMvauOh6gzxPH7uHqrh4b5TQa5toQHrcH4rhTyQ5/cEQFM
WbvKFYO9VqyIw+VJGlI5S2Zml5S0xDKVxX9prEK/ltM2Z1ULOXeNfis3JzRW2EQ9
+MGJqBa0L3kJ2WGl1FXymK2q4atn5PLosKQcthIZoX8+M9eoG9UE+VMnAgczNPH4
mu8m2j+GLy6v5Q5zYZVliSk8vT34G2o2BQybVjB/4F7ciMsoAEIoiCzrp7DFDZOl
sMb6UxZNwma3VEE8nwLp3AdpeNWx3hOEDznWMpb3kPvoYm9bjCXMIwIF/I+kMvX9
RSCzL+tRNDhhH/rfU/vLQXILit0YsB1fQIDG5z7ENcDFvYS6WhEQ2x94gmhoB+Di
GIpsb6WmcRZA7Git78tPcR4stos+Q+yqCPuo0XZzU/VQ0yKG3JhmmgEHKxysRUsI
SBO7QIQaydPphTCGzveRwIAArBQS9/ZvseI16YdQBvANGt1EG5xKczN5E+zC2atI
cSSx4REIwWSm2jZxGQ/YSZH16TdBUO3Kj0boOcGyQFTTVY26muMZAKTtcKrm+whU
BEnCEIyz1spayws9Se4ZAkye8ON56eni/GyUxirP6aFYBxS9fOe4gHliJ1n1VQv8
jXfi0W7Mq+9EzKfoE/Pmjj4d54t3O8FACJ52/lvtukatPvo+tCvzYqKBP21xxHJ/
9i8ZrYEPG7NQFF5LNm0keJKGv3Ke9baCIf02/M9CrxNuLNMji4JxpxSNoP9lj+Ox
SCULLWQjaY6DAqGMOeBzb1OO9AWqMr8qr4/zJTA19SthBdahGT9y9a1zvDEC/2Tb
LC2Zg0ZmfcdU+8Rb1eX98927WA7a6gHClRnP/v0JEokKl4sNFu4nl1/f+yJPVy88
a26eIJyI8iYtoO1WNuhsiQKbXfzblNM2+bPkKIfOZm32DkWH6qI13KCLj8Us0GJL
f6e3ZCyUTkI6rpcpT42BOL2hio0kW4Pepx0WpoGJaSWcVWkU40MKpVWUdw3qNf7N
y5w0Rs/oxw/ydrIBjB3EuehdYquRdZ0IPbeOY/qjFyHJzuRLSDJzjZR/iuQTm2hf
sa0HO6SUWxnJGwwDPFFuRRtzyFuHDeIoG+VAXD4HovYpeo4cKIpPU1Y20eoYk6YE
Ue0VzaQKtFqNr83RYJtF/EjFYYbtT35kWO4mMx7do64FYkFdweHdsAJ7rHpVPSpo
zhJVl2UGemNoKsGWKWSi5dyAMtq2HjdiiTvrcbYfYWF/tpzNI408xhQO/eXpfwmR
SBqDRVmNM+Hng7kSTovPAre9ri6xY1RHy2qk67bvv8lhamDQtYhW/5iGTjurZh2/
8ZHxUgW0Adjgbkbz7W1y0dbpEx1xRgFWSEEFt3nH/XgmxOdGjA2EcDB6zzNRR00O
bMx3i8Pf+gkB5uI7/YGX+cc+cu+qPQ7+ofFIrLjepKuRncmMwx7GGb5R7btBmgf6
eQM0HWP6L40068fEDEuhEcMoOdD3dTI0jo4Kiyb/Zlytthd872NEQi53Rlx5BMYb
DpBYHKo+Hf5c/SwPXE1jb47x9v+a/Eo5YHL3oquxHLI+Y01VziScwta3MhR6JR3l
Wjlw+7sLvLB/0dcll/xbkJXbDMOxeE3bgBksMDEZkpfzyojAGZR11krXY5f8btxz
0Lem4tZ1XWrI8zImyTFEcL1UXprSSoERvAm2i/Yf+BdRaGT8DCvwbzAt067VqlV7
4/1q+vh22rmSX3DutOeHaIFBP5e0nd8WJmCGAi78fI1iJcr6yojJIAB8zGfYqPqU
UjjBBZwi1MbqXLdy6DIUlHLmG/a+wilWh1oE3ALxNXXN/tYhwjGnjENQrUCZxKqJ
L0zLzpbKbXfVIHsbsvMapWS6rjkRUcU9d4Qin+jsjYnZxHzkKfbYODWLqk1OURuf
u/gasm910akum9du48LcrV/RqrjmHS78PihpYJdar3SN9JCJdhK+L0CLsVKGPrw3
k5wk0ivO5wkAK/7h2EARxQzafJI5yL72Apwa5s09uhTUu6fSiZ3yTeldtVQBncDr
e4S/FWUs8TqWhbQExs/J50uQqKGPvnvW0ihs3IhvFsqsk/GiUN7ldA1TNu/Y4gh0
WTi79cuSqHvWGZW/UWvDuVOWl0xXlj1m6rnkQ2VjpcktCJRm50N+6YkRzzVlLYM1
h7kqKhxdkqozhOXhH0JmF0AN8Dp2tDlmYekW4G5geHyQxCifQTZdMxnk6ft6uw1+
y8466Croj2LTaJLK3s2dUR8CXRGkJ8egXX0Q8hlHgBGQn3JG5FJ4KKOgcJLh0UgO
iMkaUSnVSk50wilQeIv/bNUO2i0ES+R64CIritLftQg0VJD7lOTMOdx8+Jcw29Ub
zATkPpwXcbp28j0piVEtE2iH4tTKamBef7OMKHPSztKKzCse30cnigz2vslaAy7y
iyOeziyEaHUgW/uqW4ONaMave9MDIuEwgwc9lE46QhlblKGmDgrTbpldkpLNK+2c
XThojULRM7aDNB4qKP7jE3mfFdTmxuos8Z0GOeIDY11jS6FmR2/wzC0y4PJ1jXLX
cN03V26FnKVHffnCN3stvOwOvRUQENMQgSXdE1qIO8ze4f6IGtj/os0QJyUlf0R3
```

```
wQJGNUX/CDmW3vkKqsMzF3SoTfgxc1PPx8MXH/GVnKdZuJE1oLpjQj8XPDexme3/
ebWL1Rs7a8GfCQvLqzA0NdItBm3GsMHhqhL6+GycgQGojRpHbNggkMfjVvw6TvFE
Us/+Re0BYuEkXCsQG5OaffFmnTEXv2UHZf9s3DJjZiaWBQCbnf4ywl9q4ZSx0sf+
hSAjB+X0YxNDp0HhuYDYBSUHe/NPTTo/2l3eo6TFLNX02tylXUvDAMGzBW3Oz5o8
4bYuVewhb18IRb0h2+joW8F2Ztw0co8ryQgmdRuLyzZLA6dBd0DcgeZPv1oz3BTU
eP1S+oFnJLmdxMht8oBy96JNWWhiofeOHoAWc3mG3BFeLuoKP4v8WjDVX+5Sa59H
tD/ysMEdZIWIPqc3uxMxSfT9xnr9dXdoL+o6Hkgtf43LWJ+AZ5zXPvI6gSEvuwXs
1L8p2wQqSuVkKAiMdTgcFegm6kaxXu5e9RAcKkrO/X7VMMCzj9CWx7GiWKNfPlbK
/xFu0NEwFCux/FyijIB0NfJDDtPf9/l3vqX72BWVsumgIf3q8x7+X1GwpTPRxU87
nWJj3a3dLOt+rf51luiAFHAv23Vo7MdnBv5yFks8Ax979xi21mmA1igfw5KNhAZS
uVtmMOnqQQ0+USYmSZNp7/KzRIIsFhyV47G8Bwxnq1UVOMPmI200B83Kwr30vLzd
YmRdpLKZTGEOhCC0BeUAbf/vFbpCBAmSwMVUV0cp446llQew7d1pezsQwKCv9zgP
IWhTQqkMvEyD+G8PEH+MrM0enghAyRx0/e/vB3xO53rGN2mSkcFUVA1/yqYxwWrl
T7J3ZdPhP4Aveiept4dHoRyPHqvvSwFaeqZysyZWg27lPE9vyJzlcEB89mZu90U8
3NYe2wRAoGKybe9mKzz4pxlkkAJS71CIwMCYwX+iUjC8Ivvm7Dtqre+Gq6MQ11pj
/J+luq+P6vlqAGx26zA0feO+atk2NRjpL5wQF9ExKVZKOJsMDnOIcuWsrmz8+Ewn
vtgPYOWze54wS3A9owc8bP9A3oNJhJjOD1WESUfmwZp1vE6TRiIGNIKGGGUg/EML
brzcys/b+gO2v88wJLlmTr8XpwBwa6E49lp4r7KKx72k2Bt1viQNYO5E/KsFQd8c
XgFedC2jZ9P+yv7Y3UfWryxbMzv3uENVDi3irD8auOmD2Xw4B70zYHuTkiX1U8jY
AAXrBgoh5nUDNsdvIXAaW4pKd8YhCso/0kmUqCSVKglu32f1ipjEQpVLSpFz894m
hODNvHgicsbmqBYAxqrEe9+HzCjqTUvMIIOqj1qlAgQTnC2H/SzELS+JrsGj6JuW
EnfR9xlp/BcekWTiuXhZeP3pEC4AMyXSoaLcJd9qPex36/ulOZbyE/j41O5rkpx7
bJZtHzP1bTPFIVd8GOgdqVarhYIOfBKOU8N3Z5bfehIuqT3I9VRQMHE87o/B9sYS
9CdFX/9ol7C5YYk3bTAoQYlsKcacopo4t7+5Bak1+1kl1Nshc1dmQJrkeUMCAfJy
AXSwlsYoZcZzWi7iqKJOQ8zHrjvEjs/9zxT7Qk7dz+3wiQl7peiWNvZHCqzWhr16
fj1Z8NmrYr1WXQdnZTINJYBcAc+oeELztYWPO/7ZQp5LcOaCowD8c6C72p/GK1j3
pxQMNqSttiVBpayNnF3DLj2nQ+U2kKLMZp/m9uf6UUgVIppk9AOhz7poFikXCcU
Qkk2mpKTWGHthzoWFongyo14egz5hVZ2QZ7+cWHZBrR6r6T++v4pthhVgIun1eq8
sBhSrfm/IqA1/2kJRRXRQ3qDu07Y3DtoduT7mFkNsunWpV8HmzGXEwYSx4qVLV5s
olb0f6QWbnj6UQWUDjfwAo+umj/y9rF3MGI4s1NnCtCrdtE6E3Ca6FW7MBUQotoF
BmOvI/UmNTu6hmeFsNbGe2KukZM2Nd9I8aAal2RSDKzX0yxD2qx6ndsAVspfk5hy
AwcLSLsTc81LFT1lsgeXt8UxQBwPzzKg4VGIoT4CAYI4PQrrC4hM3EXZKxIZi0Q4
4XS4I1ZSkVGUVRN1OmcsM2VJlizFhRkfV7uTUjjEEjyuA3M/54315cEB1cGDaPan
koASqojtAaJPRs31sMMmAm4d6pn8K0oKj5T5D67EJR144bmP+ZGEM9pGSqIpep6E
aZ2HbKkqvoz+bLVwEfBDjjEDmNQD3CQzWjuYyXWxn/K+z9M04uyXQgZbX+Zh0+36
Np62TygoEIa6KB1mOokvxS3rIsI3jMCjdc6tg/NJsKg8xskl7JrhQnbHCcjZ0IAl
6VVr9D8vchXx6QbGgI0RRxDRXGA+hEIKcymvCUpaPr5bxfQ5dXpDtQ5pBoe14SOH
F6q9sIL6OwBc5cM2GH1yRqaro1lxOj3GHWAGddaTTiFDuxML1GzRrBU1O376YAwN
+5h+wDwntuFwdQO1V7MKxwh3chVX7jUDHhyf45rJ3yGEd/KasWPAmi/rF9VwUSjA
vtWkgue4kjG3O5inNSrkvrxlBbI38X3WPbd031DrIfYwlcgJemEFpUtGTq+dCMmt
1GVxUo6gOLX2mvIgganVQr+AqMH2cavsTUoToulhlITBAW4KRzts1p7rzBxc8CfN
awaoVqguPbH3GzgvrCUaZywgg6e6SUlAHnx38v453A0/aL3NPLAuw3FBfZ1TC6cm
w8Kmxf2aT55+buIys6iRch+hip1IfnIk1mpO78URn4b9uCeWZRH2k2gzPNoilR/6
kxnMVL7EgmnCNX5b3FU5hBYkoqfhPa8oeziwxtk6/GJED7JFfsUaLhL7ja6zcZHI
ebCfbWf5SROAwO7Nf0id51Qz9NU+1lqmRLZriGeK70FznFt48UaUJ611sRP0axgL
556PCPM5UiBJYqyHPOz2o+vXkDChfr9xuWwZ7jMZIA24IzirFp4pR7FjPpPni9d/
uOg2AbYfIwgrU7Zvk2OyKboe2riEtLBfgYIiygvBmYNfqHGKsGrYqyQiFpUrTHHY
XMuOjzLbSyL2RLxgAhgfRiJMjtCZd+zvqUqcFjsNQJ+O107X+snoKpPwfBfGrrh3
YhpccTTeJMy1A357DqRIVkWJh6whpEDN3UU6EBpmt1ZuTWXDP8qGqXKEt1QZxr14
Y4I/qP4YzvAW53MX93dybg4PTPClMSv4pqao9g6nfb6+z2Ulk1hWXJY2eGuBW9Fg
Go2XsWxSQIB0DM/NwS9fB0eytppI7ia4/6v6VP71xpPPl+TaX/gHzIJF8dyausaJ
PJ5dj9BfTUdZ4eVtgjphWaDeP3Q8VqkHGIyc06Q19nJTKcn72DOuZ0ltBEzLBbTX
Tm5RALH3NPtop9lXIFsG5lrfCQoY9yGRki+7nVcT4KKDdTqzGawbqqM2JieXQ3XM
```

```
5AbbJdxZzE8ZTl1B6hKEHc+ftPf34TDB4Jzmawa9ZrHXNRvUIfdFd8RDrluAkF3A
uMJSVNQQn67ak/Hy/QmKnbRTcYsePGY4V6B6UfyL+dOZpkISa1L1jY4KrgJNlg8h
0TTmap6SeDPIwzzDgOo/42wD+ZlOzJ4xJj4hhJivg8Dd+igUch5zeHLZIDlpSZIC
fN1fqmbt5dGIk98Ubk4zFa4by0rHW48pS8jhHNA91ln7uq/ICRgpFonp/AIFL7g4
718j+Klib0DCfDL88t1nOD/NhnwuDpothqEjvTVOct/3g0QyHdy839f16aOqaAAB
A6FvjPDc1ubhpA1Gfw+LegIU8lPsuT3TGgzdtmRnlCaW0iVQnaUdwd7Onc6GGoO6
ovjOBPmX/xab0SdBZ5ZeGX80aCpXemfk0jJ/mslNxtYLDsjOyYqMUXJWIpZt9SJX
wK6d80zrDFD7GlqZx/d6BvJf6ZPCbafPoLps9+ruyS+B/MXG/VDYdQhTohw1YkwB
p5lUWafxE0kZqQstYtHjAuEMj9Fg+DoYiLHCXLe1yRt4ujpioWpPRx6d+8nhtGtd
Jxo2rfcxjhjOVd8z3M+LBtBjhdUC74sYG5ZTLq8LKYp182/JwqP+hrTFto9N8Blj
/WWjOnTua//2eR9sO16qIL8uVgiXRSaEhlKBSnUsie/cxPNHxUnbYVDRfQYxsNTD
8aIJEYeKfFQGYtn6XFHFxFDrYcSLO4e9eBc7js2RvYH57Sj6IcwB0mSx69b2pCpM
+1MB8tlkUaQrOtEKmVil9w3uZ7R/2M5VNYCA7fpS0nUoXTUsIJLPosLKHF96ti1i
MyAwOZptIby5Ryi/v8wnsuvlAyESSvdfufB7F/NgVyUmauIfSFllCRDDPy1izj4C
XweebQz8HmRpWzUIlAiR13FqgQ1vv40Q284BkV9ojqDR1ZCtCImR4Yyo9MJPRxOe
bsNwrMtHrEPnKcVbzmxFFcogzJMU6FfglcXt/U49CoyC1TWZcZVpRpLXdLGT2OEQ
oT5xtJQn73ujUSgPsxiUrvl4mUso6AaU3hgznSM267BPyJIR1wQz4HyZ3Q3k65SR
hHg7LyniCWizVJZCjR9EPBI0hCX+rzX0Loc2XUXmxK4qZUgaOj4z7KRnevMah8DR
f54y3LV/LQgq3jOMZpKQSBkg2BEt7Gy6KPITKpncZjma0jipAZpA1gqlx+QZb4Gy
nBl+PCWaJNh/8CdBuIpDZeamp/QKLHJOkhP/Z5YzwVkw8wPCyBK3q7ih/fU9icLp
o/yELL1xYBj0n1SZT2uQf9Xilea81BYStW+nJ+IQA00vP5LyhffLau/KFf+rWG+n
nWmDuxC3kuOykPHcJVGcGTcLJaMdWQ87n29XUAkcjaPw9mf1mWWhMYIZhuADU518
WTbJ15bbhMP0pL7ixYwKEHkJ+ZIJjqqTMOo0hy0C8X8dWG9mN5PAmRr+3KVy+kkQ
2Tvf97qNuMSE/jhIKvLPgbb57veMK0EaGGWeh0tqiUNmTTYhvOj1axdxnjmE6tM0
FGTulBGN6rWI8VBf/T8G4nMhjvpapPSzJPEIF3b7iQaEfR10+7rnHnFDUug1Mud+
hlbI8r7qIDxQd1ceZh4LVj+ugx2xylcmtTDzMXicPGChPbRwm9fCfHsudP5ljfBG
KQBs0veSlZxq+hM5Q3FRVezFLMonbFAMeOCpfU5wbVsBqCQqJRbj9amGw9du4ePP
pzLoPa7bjbqlopO7qQCoQYrmRnBKid8TinDxMMYLXUuWZQA3tEX4g6A3uygt4Bdd
369Wjee8/fmedKfooSW6Pk2hcxZjxPt6vYi78HdDfti+VNhSsKLfeWA3aN28neqp
UuISFdAkqb4p7FtAy6l1bF4vyJWm9fFJNVr2h4XTHwS5/dDnoadpr/cVwr7JiRgR
qVI9FBE9VWxLeNXCT/JKdTskdUx2ym9YXTGKs+I1ON4/P7V1J8RjvxYnSuwjHwjk
LmDvuc9R7TroHZ1XEDJp1AqKLu7TOnvVbcg8hqgaxZIiN7fiqZeF7K/TJ5SXTW7v
yaa7YlSFGG+viQgBrx4Uwv8ciybyMOR3sLClT7c9eqwwiZ79vre12JUzg96Da2la
c9BUTJpymCpWBU5CG3UnMhXbui0OUQYnMwzUjEH1viH5EmaRosdo7HndD2goa+kL
DPxRJUsW4yXI+JgxEBLwlEiukCeVHXQ6h+P11KItUO3Aj+coXgfnbcZAaogeebn4
cpfDFey3iYyhVCWFdFgQEKASyfOsOR6ViaeZH2/oMZKIZ224AlmSd3XHHGWk21FK
VxXFAaqTHH0A1G8q/EBtWOa/cam3JRmW/JMQ+2NVwDo+3e6wWdf3fCmef+BqNp/t
ei7rVZ5Ksp54mgbxlapnk9Ch4IILVpy8SLf+MemtscEtEzEUd2GfY1Mp/2pVjnu1
wA0u9nHVmF5iuXpjTnemYjneKPCD/jgLZ4v0l5Os4XwTOqCNjnXVltME9E5RtOAn
3Ui8yOLP7uy/m4KgureuJZW+1pFmDZP3FxKPXPpHhitouvenGZacB1OZKqDuYdY4
upKsvotD561yL3OcjtzLb/LpHu9aZ1MBsMBC+6T/XEmmsQLkha4755gj4SZBoTa3
+7RNJOIzm+pFnt6KyfZFdRu5phrinVLoS8r2TCmEZIRaT8xSQ3j09KTjDFpoIAlE
QZNmbuUxw+UTPZe/HfbXoeP8phRWVrNvsNDYh6gxm3zaA7uK0LCznaxxoXpokMIF
b4TIcsguyk0wmkyPh/Tbg1Fb0rmtgxhD/ttgaWmtlVaMLNWdlhkA4uOY1P7xj23j
wrGlKzpAbIXrRK+mF821fZBQd87Z8BtFqRTvWwiTWDAoOMuS7b4RPLn65fGdzU/k
2seet69g5xebWu+CzIquu3CEEL44wSUgp1nmjorK2Rdr2moXBtxbKnGpuKNrGSUP
et6k8+zUqn7/vchMTKqOyhsDCPMQ2XsrW3l26TcQgHvYQhcbTmSzKPzS+qV3cze2
MrFEbx/qfez6iyGU1tkFHG1sD2JifNH0Ag6Dyc8bn2fKvO1s2Jwaq9iNlFv5XD6X
SDCDXwl7GnIM3NtOXkyAGPYE2Dlm1sRfL4VfgMe6Zs9WchpwhuFGdRsK4EI82ZKd
e6REeqVYN8dO/3jCiIbGajIZjKn6/icrn67BluzZHEd16p0JM2mMqM3ikKOTKS+h
7P4JX9aGADfx6PG/l0XtksgVTciDV41fduv3LbPIoFZQ3Wi7ElcO/Ui9Vf5NIJGm
9y2jAvYQOpLk5JhcjZNRZhb7G7IQZCCLU0Vyxe083H3MWwRMS+lWxF+E6ld2uF8r
XvWVGmNdEkc8huPtoeWs/bSFEhLwwuz2IcmNZylNRRcV4kmjYplq8bJpHaQ0xNdy
```

```
IX8eX91zHekjqBgC2THrFWFJTtOQ2428IU+duFHKBZzqXAgTLC+df0DOVS6exPQf
TmcPqZ1I8DwAqwhd6Aul1v1eWho0puuk0bozpL8fukAgs33YZox+Dbu9BKIdVdJ1
jcH1+RUo3W77NEtkJGB9w2r7E22i7VuFrFyQ344PewjgJ88Y92eSfIBtHtDkuup8
FYB5FJGroy5ugCjuyhrU0/D6yez+IMaD9N9Q8f4PBpJ/RLFlCFHaL/XiosGlWZn8
IbgTvBPKMjFQJTud7bfwdaOzzoDV3HMdbJeiBEbap4p5n0YQiaMoPlmxXEdFBRIs
nCBfIpWefP4c3sUYCikoLqLgEL1HZwWn0uRrAnvNV2hGeCZGNX/CbCYF4fcq1t7I
97p5jOi+urYikrTKaZBBhKTYNX9MNzoaCFfMpRpxe8WM3a5t2nf5bvx5peCS1IOh
97svLh4fC17IXo2ci6LLFwzgydNSkK5/DsmQhsNxkc8pAVPkwe67A+ovVQiFd9cl
fApoQ2v/Tk+ePbriVpEpPA5bwX+OMhSME50/vcD2rzavRe5DWvf0kBb7m45DVXY5
H8yXj2fssgwLad2EVh9W0C0qfmUnII09xeMWpFeSLfXmyGckZgo1A9wdMj1LcmQm
bfkKVeqa4xBDkzusDiID7X1bCabJPKzOGaGyrxjnEkHAUIJUpoDtvQKbaot7FbZs
8I3eWwkm4JF5c20lzUVU7BptQ25asdhIP26XVfVoHPDx2ibP4KsrZqEEM0T7QHDT
hujKIaLZrY5m1NglsmQDmWhHfGIqhWA6TziJ2RhkmvC9EaSddf5x2QpwzXqYg7Sb
Ju+jKJ7fNk1ioi1HVTCTzNjnHWyLjy1zFsXOS7pdITPVD8NXQTdV7fQmdx/KRWIy
ocKJqiOwjW18osKXM2s6rxw8u8tp6eUThsWB1qw1ncfdwNaO3p1xL08n0IdG9mnJ
iGODS0qEDceN1AWLxPLOVCrWXRKuD8yPiSRbQUD9OPg9hpIWnOU8F7LT4b8TqBDf
bbui+8R2jzBSBWaRG92HySYKFbyKnXIzgDKDEy8Md5357UajvzLi+Ua5OHYfUHp7
v+E3OlkxK4iqSkhlFTcZjO5xNqvEcobPHrNfzcurhNnCL7Ak5+rp7P/LEFzFJlDd
fBnMBtkANQ105ETuX59G2Jw1TWa8c/ove+HDdHKfujca0eSc28AdkdlFyBYrVKpq
cjO5o7Twg8XDkwSsz2eXmwdNFKMhJijbSvh/Bq5c+whgXur68N6B0+bA57a/s60x
bpA4VVwXaE2/9tnky3IVPmyhUIJa6DB442BCVUymYy8ATguOg2S8WCrNVenUmrLP
UKb0a6NfatO3eFcaH+aoeAOEZkD/St9Cop0eurGhiQGUsZ0zb4YYn/ppgfeY+wud
WJXkRAmTQI6OSVg83WLJqXI8unBHzObRt27O1UcL3+oH6wiR36zZwUzI9gnqxQTQ
avzEyFYfVRPpmZ++kfNwWzBq8tqoZfWM+CILvQYKTu2QgFO72hhAVBSe7f6Bcoq/
vkNsnZNKkpMXa3RWe0TFJ9hxd6FEyK53ZkooXYY2+cC4lugkcN8YY5eUrIyGNlFB
DCOHWodED/eN+hZPm19G6nrEhHIPcWOsERigpW1r0K8WnbD8eqpsf0JT46FfhWXQ
mckWIm3nu9IZyR6ITpC3VoI3lTTJ06wnVaxOemYfi8FCQzb/CnqdxT0pH88/hQoQ
d1hMKhv9RoerQk6MMU8dn34tDWzG9CT5ONZrPH1VoIiz77U0n09Twi2kzUJaaM7O
TbsHNnIS6XJtaGjlRqwIh0/VNlI+gcip5ovLbHupWvWtN0w0zkBX7M5vLLyhK7tG
KFLLEO+CSNZeEAk5TxUIovYdwfeny+IwPvfuBdhabvFwHxpmeqU+3zZseY7/f/PB
PhymXd8QLsHMBm2qt6/HuVnrSsYhkUatDO69hCc4R/YSpqypmOQZS+Hh9xJJ6WeO
ih5+y2hi+hi0NHNLo2qtPnitXlMTeCYBeXbJypprNnkOmtembXe7m0BjvfCsnw3/
4mV+xqXmaizZaPDqkx5DfmB8STQ6Ej0Fgq8t/5cS2OChrEJO8hK+NMOwlj8/y+dh
+DioI6/936uYVG448NZT+lNOhZgQquAinobLDV/qjZAaiUtN4OF5NmmsLezZsOnY
P3CK9IZ8fOVIYf44BB0z6dgt7iqjDH1aCB0+Zgxp1a/zZ+gl0rwPZQk0B6aleAme
WmS0EJ4Mq7LnqlYZ0zfwVHAx4GliQ2G+KvYJwLHHTcNWwGVIIIM5be63XFIUula3
PdiEs2cUSNk9x7rl2aaCpRmJVWCmUBpTTWtVRSvC50aKcFP6+1bp750O3XeFj+Yk
msDfbdD8nApAGU0pHD66bBqha+MY5G162yGcBNpVwJ2AbFUaBaXmxZzWvH96W6FX
mr92oa2n+qyOeUaxDxivzXyN6NPKPu5LA/HMg9rZPli929Fb9DlV5+QBXKw5jf82
58RXGz3TD+Ze9NvJOlARSQ1k5nU4tAXY9Gglf040DOTENpnzdz3u2uuruOh1SXYt
PkrK4wgCmZG0lxqczJkTsa8iruurqq5YJmzSz90TwYpO+vkF8nWjCGZj1X1A8pmg
uDW8Q++/miIXFU+okTAYmr2h1s26fpevYYL27MGVUjAheChXU+Rcg7z/bwwtjcfd
lmfvOX2frGB5VrA6gnP+WXX56Dvxwwtq28FUoMceCewbAHUrVN5ErIGHAulWHQsA
E4gmESgcdjyBa09EYH+DcVepLd/bf9to9sSFOgG1Fk18AdSRftR6R0FS8JYVnpVE
CN6o3RF4T9GJyo/AEofKHSWBl4F+OygLAG5s9n9yfvSB4ip1K/q4EQ6ebw62AE7J
wQowF+6/cdFYiQL+7vzUCTcI0ixcVWNToPiD6bgeTJPTQDordtGarlvXi3UmoLuU
d0BumrY0vMFapOu5xKk7vuNMkzr5TdHpwQsx7z86bkemoeW1nJ8FFE2OPR4I97yA
HaJmXMzMfVNGOcEltGb60oG9bHfaciAmgTKgLvKmL4mCNv6ptezVufEuAxLTJUyT
lJdbh4rZq7ieu4PgncHnGz0kTrtfDNJ5Rg+Gt8TUWn5SUrhZol9xsBHd2/3nAuMJ
HI51BhQ2l7Ag06dqDQwh/7gd6v+q4EiJ7ApXW3ytEAniG6Tqvwz5Sba5kJT/Y2a7
FWO9zcWBNr1a+7npDii9znnCsVierWieVGhkPsJH3fe01Vd0s0FHoFY5vB9dKuFM
lF3fyDihOOa27gpOmEBQbIOu2yIL+azbTJ++Zc//+hBzUe27V4WVyRyLtxD1HZ/F
oxJgBLnKi4VGF6YKLQ8ba/V0T80+4LTllZqE/EYYyqUaDXVtkPlEWce3UccyJiwK
```

```
POFPt32aKNGX4WBScz2Zv0xmeMZPfM6FYLH+wSmMZDNuGYgB8988H4yECy55CT0x
LYnzoi6ZSGh/dXWdmZq5yBvNsgy5a03SJfhLtsC+dGkD6Gw4ad5dokZPrzHte6a4
ThT+UN4cyJikBeJkJLannjCuZC7evyCVHgfP9ukE0cHiLKJvbu5KPXbWLP1m5Yfe
sMwIg2r5/YUo/syM7xIQ5E98AdEhKSXbrjKqHCwflzws9gfUKo3RE2Yn9Fa4lU9T
MQ8YE0Frh0dG1xeLwbphtpAIYTTcQ02Tkm1WWbWkwc1RPWec4Gtd//VzMnN1JODm
qV0gyu+EKXsgzEbbAzRaxTe63cLEXS9o+FommRqHVN4bZHRzEzF/gE8r9ujMOM8z
2uRAClBWRUb5iGR28cQpkMt+McH1PCKVmiNV4O/subgwSt0n+aHwxRMCzcIWDMTP
zHMvMPb17qHzcdiqrB+dbfsC0fa4jcqwJGBOikVb1nzqRXYJiVsu11FtnVsMp8dV
MQvQTBcPDybNtlVIxWF5NhEApS0TLrypP8yR+7kYqvXvZ4xD2DRKZmHBZW6ePNCs
kl+xUlrLUidFQaYcxq43gGJWzzCyYVFx5GXoR0ZaUbJnzsw1YBTgJDCHHyo5kpDx
q+FK/7FVce8ZmDhc1i3vdBQ1DPN60qSlTkABfdJkF1pPSgBpobNU29uIUeqdO2zN
rjDbgu/V7NpISuzYFOombEz3mOrnCZlYDmPic8YnQweq9YncKRaC01qDt1gjgOK9
Flc9sPRi184Eik9EMSkstvPZ4RcgwC0k1AVS3eqiCd0VNoe8fg9+fHhNHiIGSPjb
5F2rth9S6aItpkAJIrgirnHEmBDPahAVzbZFK31LxlwqiQZPVnE3Pjuskv4CQhiK
54MYyslshOzF5hmnHA/BxbK4FdvH7w9fUQS1tktaycoiQvizes50Gi2901aQkzmo
YgkIK/8wF2b9PFvbLQbfPFA/nFO3LBEmFCpNK4uF0tIDqVIPErp0mYgcHX0QFSXH
rNmuDjOgsxP8JsOpQbiZRsCHcOFOfhK9MIInzMTS63Z/j0wkEWuYBvbtwwAAsZeA
mlkcyk/iQrMp/rflQZk68qMRJgEe+SMpoaI5Ssxqe/W1C5UDp8FgQoRHEXXwab4w
GKsYXax8rxxUHI1YJO85bLvWevz6P/J+mBSYEmsA58ipI0RBrKIIoB0jnXOXMOpd
DIuyM3Sqd4zxMGALNngINAYX3ZA4zqiPy+NgVbgY3tdYT3cBvk7pyC2zvFvqAbjU
nR8lkL6H5A5i2IbWOxg2elUxjm5uKSY1thrpaiBqA93Tzgh4AQ0A6zsm6inh3Fwd
iZ5sArZtMg10tl13w11x420028qGtF3DfjwTFrvSySovpOcjtlE0MEdJIS/rV+cy
/5QvRDcV2eEKHA2CzcLr7sYLLaM7JDTuPtiEZFFDK+4rxjiJTCsSNHyuzFBLJPMC
PyNrH1Fic+MeMJqtZdOlTtx205LklFizXpaqL/KQfCIiIb041mXy6/e4w+etXxxs
v09LY8u2yxaCUFKaoYilkKUFl5qCnJFWZIGdxZxlyjHtruMUZ9P9dGIQYcj6n/G0
BLYqgLQjFQtwqcx3/tQSJUDgfAFc+EVL47qTEIwTtMIF9wO3JNrW/+GhIlDF7hUj
4STEMb7mgheq8C5qVkeaXmxt493oZ/qGPNebHX+oXxuHiXrcL/BF7Kq1miZWz4q4
TsyaKRReXo29AtSx9jc7k7DzZaq7hJKCp2mueRFV0lLODV+jhpnNC5fYnDj/KFV5
1CGYiGzPQ72l0kRNBG/uAkbvxwFPmTuUgcSQZzW6rKtsoPVt7qxOG1EHniLfyVZn
Q4Z5ujOrkl0zMjsY3XDfEkb8wRYHJblJFoqUsliMH4TxcX6qF16Qs/XOqHTC3Jvo
zyaWvs9IAPfcjz9loH1Ty2P1oT1VGmYpl9zj+So2Dm05Rjo+nuh0FWyiK3ZDZmig
/3Txg2LSb+WDfyZzvkgaRo/FRQNmjGYHGI0OVdPRBR/4KWxGXhxgtNN+DnQ/SIuT
hYCy4n5ncfmflF7VkK3npMrcFqi5/GljzcPH2zkWMyyF8rZ/hoWQk89h4ONW+LxL
FJKuDRoSZJ3a4P3tkUrhmVZwFja+4GulCkNKVDu/3wpaXw7luhyerW9pg6IIqLYk
W/LcPrfT+eMYsSvdXedI+K1CSMsDfqijAdGwaQ9JUgBylnbyeLuImQ+XTaRBKpXK
BStA9s6fWPG57fUcJbIC+lOk86hqI1MYa4o34WydKWHyGorzOPzWr/0HoXEOpRoJ
tFR1Qs30FhFV/LKLCQoVTLJyVFi0f2utPinMz5MmdWBSrphum3hQtf/fqilQLxiG
SDiBdkagfjlbDVu+ghS21geQnH0M+JnFpW+xCYaUyTxQP/m/ZZYYfZ77H4pNInc7
nT96atjaMr6yLWeWhTPTTHYTNGNOGR5a5jqQifjn40yuhoCZcerQ/bOzQjhCXPj1
RYUCkVeOFxfELoqmDFMPKDuGE6z6um+dxtlIXvZrQo9gL59hvPxDR+zM8C35zmg5
UJUH0uLziJAJzyeWGl9D/p/e/sTFZOcqXtk/lxKcMvFwizyfJu/euu2UYg0UToF3
sC3Wh9yszYvJEIWy6UtIcqDwIFkMJFp/kSU72URoZYYyw5TPb/e/YBLNSXgtJqXz
Z2hdXwIb1kkAqKl1C0oSCwjA0+6w93Fqco0yc/ejwiZcsJy3xc592gwqMpQQ0R6f
KxYxKZfjcxJVF9U3MLZ6Gc+0ZYfsbfCqBA/Zhe0munBrNlZ5U0gRfT5Ub2ZfO4x1
g4aW5k08MpjIS/Auarmzsuiehkkyfazhmeh/6i8CGId19FpY2SUUHp9/le+c3TAC
pFoXFhE1xBlR/LXz1mcUhldxMH7D2BLGuiast1dWu2JRuiXeIGCRSig27fa7mLyn
aAc5tYUVjB1J5LUUW/n4SzDOM7n3rcMirEAlzl3nSxpReyd+aoixRYMBru5k2FHt
KE1+b+lOzg8c/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-----
ME0wCAYGK84PBgYMA0EAvUCC2EqHM3A1hYoRDdmLUH0rBpbDoKnlfLnFbpInHjct
7cMX0vRd6hFzOfIC69yciXgkOLaYuyUGww3i4gxu+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
jibx0U3q0a82jFnjEGKQwZLcwbnysFC7N+Y0ENN2+AgPJT+wB8S9QILYSoczcDWF
ihEN2YtQfSsGlsOgqeV8ucVukiceNy3twxfS9F3qEXM58gLr3JyJeCQ4tpi7JQbD
DeLiDG77vUCC2EqHM3A1hYoRDdmLUH0rBpbDoKnlfLnFbpInHjct7cMX0vRd6hFz
OfIC69yciXgkOLaYuyUGww3i4gxu+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
MRowGAYDVQQDExFGYWxjb24tNTEyIFNhbXBsZTCCA48wBwYFK84PAwYDggOCAAmn
FJOlb5xjjzVQObUEy0bozaLCCMuFAj5SPBn4QfCsu+XU5Ul5DphvG/qNHdMpHwIM
vsrfmWPVAgZ4suOBUGiQpLI1HSk6gw2cUMCa2KzZjVWzidhlHqs3IYAwZt5uC9Gf
bYxNDKXV1Ls7QbS7+NMdEbablkfpsZIG+LFFohoeKCPZdCIVvw0SV62UiaaKfSdA
KahNmcSGnpOKfdBN0bsGkk2J+RljLM4gOsY0OFFqK+hRSzKW6T3eh1YZ7QKbYZUn
tJxOTTxja3kgZlzJOoE8WLQm5Bz5FuNOXOy4mxfjUAniXvn9AUS1kgTyT9vyrmYj
I6yiq1o0wpiX4TsMGYKhNFRFFBwCopMNiArJE/OXjJNVoeu5j2kpKmg3p2AP3Hfx
XUBcERpmeLzCDxO/UWUgFXHKFUjdIKSNW1IC0EwbWEmXRjbxGyvqnHwMaKgqDCmi
GiLbNu72dYANiJUSyI/0pCWpXUsvIZABxIZOjkl6aYXK9XISyIMaHZVbMvTAyo8Z
az1exehdJZ52g5WDyMc0HvDxDy85jvS1N8+PCVFk6Sai2E5FDT8ZDlCtXzQTpwZD
+k0mqMTNg8Qdfuv6/y6rnoq4S3YAuE3pgfQRL0siMmT5MqyBg5ook4bfXXs9SbdB
hkhCsJVyNC7NliARVi0popFZtTPZnJUYRLv7GNJwMmxzIWqOLyqt2hrRk+RGfpk1
GkC1BtEfGbVtZawdEEMDDGC4dsCFBSDgbvC4qqoDZHWiDFNQzU1SMBt6M03dJ2U+
```

```
RS/dmmlupJpxrKU9hR6LrNBhTGGVcPCbdpKSVhFqKsipQTY7tiIjd6ZLi1qXehB2
NbjTkcRGAgJGWx3fvS2oqS3RME01iRW0G0GZkvUg5c1XvwY2FoFYaiIMhLW9hjpJ
XnZ3hFjThmC2x5QX6x1abMGUa6krzke0jl4ksFFmpu7vmZqeKpe7bBdUUNU2n66g
P+pl2uPlEFXRPnkMDWWFptqyiwb/WOEb0fnZXJg9+5qDbna6LcLQsayHJw4vNRPO
s0q9W6GTD6VVref7QBQgI/6gMtYbVl3Yy2ktTNIKEZiTtK+srQi0Z1bVqQEtDqiC
T/RKDRTx8uYLXtY9dbDBsltIplIY0mMJvEdy0Ivvum4pZwQQGTv5BcvjAFE4mS8K
O1AsPsJPs2yjSxCaLgT1bJuN1ufmtac6jtrug6Hpf6AAMAcGBSvODwMGA4ICkwA5
BpW+Llwzampqt27/3rtgBO/HXLPe1YBuzZX7B0pqsmfT4duKoZnicppj23zLETU2
LBI1EkFZv8JCsMVPDPptIRteQUnY6riojJyGrEZlErbCtXm5j8yLU923DsCWdW0w
XpvCwlX637rPybRh8zlFvFLSvGwFO9hxJQ4rSkMRFJ1hbmP7kkJB3VNqzBiGro9B
wy270iexiOjUVn0TVVQ0l2OvvkeQliaTslST9EnC2NLs+LWfFspT1/lySoGxanpU
iqze5KtlR7PL6Kg9nk5dGTM23KL7uboES5vUv1enyUCjeTaVE3cW7OapCj465qI+
wyfoHAs0S1LZNdHRIBNL4MbB8QSh7ZckKHmagroJatpKEjwZAJRRGi5PMVbDxcW9
SJElppJFrirx6MxcuWlpeqh8GMN+PvqkUHUc38EzqNG6CZ02s7gwiNZBhX9sK450
mNG/eI1xr0cxyFOImFAyHR2CLQuUG6OzX4EtBKpp3cRxWTPs6bCN8ViKXGSpOXau
Vb9y12M5jXVQL3skQDdZBu1R+JIHhFFkZWDLzTFigoakMZizNy2zq9immkGSi64Q
dcoPbtthedkJn+fWoSRs9I9VmZGvG8p3jfWU8nJNUq1nZJcU66AyOTckg7jxqQnr
93k5f1WmQ2JnONy09xaQenckiL5v3DFaU+L0nHnP0R9qYxc6hMWrwlMxQ7SZ2cFQ
L3fuggXRIvOCUqhp6dJDbvNGYzzicJ/5sgx9rsSJIpBNugA6C1INrEBj+LSj5sVv
Cr4/OTLb4WqowVJEUsI5EnG3CEyHK6ibXlV75NiEdT8ypkFfhDr17KRiN0L/qjT8
fejJP8hGgcSR/r1ubg8hzWjgYpjdKKbZcZ0kK7ND1OpA
-----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-----
MIIDjzAHBgUrzg8DBgOCA4IACacUk6VvnGOPNVA5tQTLRujNosIIy4UCPlI8GfhB
8Ky75dTlSXkOmG8b+o0d0ykfAgy+yt+ZY9UCBniy44FQaJCksjUdKTqDDZxQwJrY
rNmNVbOJ2GUeqzchgDBm3m4L0Z9tjE0MpdXUuztBtLv40x0RtpuWR+mxkgb4sUWi
Gh4oI9l0IhW/DRJXrZSJpop9J0ApqE2ZxIaek4p90E3RuwaSTYn5GWMsziA6xjQ4
UWor6FFLMpbpPd6HVhntApthlSe0nE5NPGNreSBmXMk6gTxYtCbkHPkW405c7Lib
F+NQCeJe+f0BRLWSBPJP2/KuZiMjrKKrWjTCmJfhOwwZgqE0VEUUHAKikw2ICskT
85eMk1Wh67mPaSkqaDenYA/cd/FdQFwRGmZ4vMIPE79RZSAVccoVSN0gpI1bUgLQ
TBtYSZdGNvEbK+qcfAxoqCoMKaIaIts27vZ1gA2IlRLIj/SkJaldSy8hkAHEhk6O
SXpphcr1chLIgxodlVsy9MDKjxlrPV7F6F0lnnaDlYPIxzQe8PEPLzmO9LU3z48J
UWTpJqLYTkUNPxkOUK1fNBOnBkP6TSaoxM2DxB1+6/r/LqueirhLdgC4TemB9BEv
SyIyZPkyrIGDmiiTht9dez1Jt0GGSEKwlXI0Ls2WIBFWLSmikVm1M9mclRhEu/sY
0nAybHMhao4vKq3aGtGT5EZ+mTUaQLUG0R8ZtW1lrB0QQwMMYLh2wIUFIOBu8Liq
qgNkdaIMU1DNTVIwG3ozTd0nZT5FL92aaW6kmnGspT2FHous0GFMYZVw8Jt2kpJW
EWoqyKlBNju2IiN3pkuLWpd6EHY1uNORxEYCAkZbHd+9LaipLdEwTTWJFbQbQZmS
9SDlzVe/BjYWgVhqIgyEtb2GOkledneEWNOGYLbHlBfrHVpswZRrqSvOR7SOXiSw
UWam7u+Zmp4ql7tsF1RQ1TafrqA/6mXa4+UQVdE+eQwNZYWm2rKLBv9Y4RvR+dlc
mD37moNudrotwtCxrIcnDi81E86zSr1boZMPpVWt5/tAFCAj/qAy1htWXdjLaS1M
0goRmJO0r6ytCLRnVtWpAS0OqIJP9EoNFPHy5gte1j11sMGyW0imUhjSYwm8R3LQ
i++6bilnBBAZO/kFy+MAUTiZLwo7UCw+wk+zbKNLEJouBPVsm43W5+a1pzqO2u6D
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/gABBhxfO/
QOQPvhAxf+w/PxfQx+wfA/v/exSCAAPBevwffgPAgfwxAghwP+QCguQgABQfQhAQ
uABfRvQwvPhOQAvgwwRe/gg//QA/QhxwQ/AAuBPfvAwu/fBAf+gPQgQRhQhRBQAg
wgxPgQ/AffQfxQ+OPSAASfOu+vAegu/wwPhgO/hywPx+/A/x//wAQSQRAPgvvh/w
wheyNxPQAxQABgefwwfwvwQuhOwAgBOw+RuOAAOfgAhQQ/QeQ/utvxQew/QQgggx
gAt//vQfQgyAf/Q+uSP/PewgQvPPAgwvRQwAB//wu/ffwgAPQxAChewvP/wAfexP
ggvOuhPNPfgw//wfg///fhA/SfPggPSfgOuyOwgvABe+Ru/+gQPvAyAe9gARQBfR
ewAw/vgevfvvwuPffQvwe/AxPwBfxOgQAfgAgAPxAPu/AAvOuOvARAxA+PAAPARg
PA/xhQQBe+/hPRg/xfQufw/fgBOAxQPgQ+wPPvQwvww/QgP+vCxgPwQgA/ffgPwg
QPwAvAff/PwffQQAQhwRgxffgBxvvvgOwBQQ/wOiQPgRPfAgARBPAvhgfe/OAQgR
/ghiBQOxRvwQPvQ+fwguzPghghfxv/uvhggxRiPufggvy/ggwuRRCAewRg+QO/we
/gAfAxBOyPAPgfQe/tgvAAAiPxAAwwvABA+u///BPwffRvhAAAReQftvtu+hPQgP
vxvvvQuugBPffwAO/Av/vPQ+/vBwfvPwvvgPwfiOv+gPxxAgfRPfP/RfRvAfOv/Q
hPeRBAQDPQfPwOwRff+fwxwAwRfvP/weQA+egAgAAAO/ggfgAPffguxPwPQvOgP9
/eh+QwCfAQQvhvfewQgwggOwPQePgfN+uwvweywgAfhfvOAPyvgQd/BuwQvwQf//
/Av///BgQQu/uuQewPOw/RABvwwwSQxfwwfwxePgfhwgvvewv/wgfSSQOPAQAOQ+
fxA/wBA/tBRfvABRwQhwQwAgBQvQPgQAASDs580DGBv66xDt9/YBFw4exinx9OPz
CyP8DucnDgHeAdLvCP3y9dsH6AEpCQAT+/oF+NkjzwDjDQIS1wr/8g4ECxHhByAH
EhDs5u7/F+z9HBUR2h7XCNAx+wbz8iLs8+8H7gkCDAAUBA7s5srU7w4dCSbj7yX0
1AgRC97gAeDs+fgdAAkHI+To9TMJ0gXXHOwU+O8KGgL88erqHdzl2CCz8uTrCg7v
NyMS/yPYDeL06xYGKhbQ6AAdAiTq6QHcEtwSBNbd/hTRwv8ZFwke1e7pATAHGvz4
HfYIUxXsK84K7OTP58XuIQEayBD79AroG/8N5RUMAQrnAP3a6hg9HA7d/gDzAv27
9vsTCPjw69QTCEYIGRcI7hYJ8f4IIxvxGPkeHhQN4ujwBtLl1urw5ioAA+7s6u/4
A/XRBMzcGgcL3fwB8xLq+fb/8yIR8v3VJ+MQAQk+MyYUAycY+h/2xBADBuwgF+ry
GBHLE8kiDuHn9/sJLA8A9Qg/KfL/MvUhERL+Abz43AD8FvcV6zEg2grh1dTn1f4D
GDEpFuU6Cv/w0hMOBhjzDOk5BSX5P9z42tIa/dgHFvr63OEd/PoOBzsK6BAw6eEB
8AfpW/b/3xYqDSPY+MoK6fr98h20LhUGFQgA8vsV2gMJBhHU+Ck3EOz3ChAVDvIb
Fuvo+fj//ugHCacUk6VvnGOPNVA5tQTLRujNosIIy4UCPlI8GfhB8Ky75dTlSXkO
mG8b+o0d0ykfAgy+yt+ZY9UCBniy44FQaJCksjUdKTqDDZxQwJrYrNmNVbOJ2GUe
qzchgDBm3m4L0Z9tjE0MpdXUuztBtLv40x0RtpuWR+mxkgb4sUWiGh4oI9l0IhW/
DRJXrZSJpop9J0ApqE2ZxIaek4p90E3RuwaSTYn5GWMsziA6xjQ4UWor6FFLMpbp
Pd6HVhntApthlSe0nE5NPGNreSBmXMk6gTxYtCbkHPkW405c7LibF+NQCeJe+f0B
RLWSBPJP2/KuZiMjrKKrWjTCmJfhOwwZgqE0VEUUHAKikw2ICskT85eMk1Wh67mP
aSkqaDenYA/cd/FdQFwRGmZ4vMIPE79RZSAVccoVSN0gpI1bUgLQTBtYSZdGNvEb
K+qcfAxoqCoMKaIaIts27vZ1gA2IlRLIj/SkJaldSy8hkAHEhk6OSXpphcr1chLI
gxodlVsy9MDKjxlrPV7F6F0lnnaDlYPIxzQe8PEPLzmO9LU3z48JUWTpJqLYTkUN
PxkOUK1fNBOnBkP6TSaoxM2DxB1+6/r/LqueirhLdgC4TemB9BEvSyIyZPkyrIGD
miiTht9dez1Jt0GGSEKwlXI0Ls2WIBFWLSmikVm1M9mclRhEu/sY0nAybHMhao4v
Kq3aGtGT5EZ+mTUaQLUG0R8ZtW1lrB0QQwMMYLh2wIUFIOBu8LiqqgNkdaIMU1DN
TVIwG3ozTd0nZT5FL92aaW6kmnGspT2FHous0GFMYZVw8Jt2kpJWEWoqyKlBNju2
IiN3pkuLWpd6EHY1uNORxEYCAkZbHd+9LaipLdEwTTWJFbQbQZmS9SDlzVe/BjYW
gVhqIgyEtb2GOkledneEWNOGYLbHlBfrHVpswZRrqSvOR7SOXiSwUWam7u+Zmp4q
l7tsF1RQ1TafrqA/6mXa4+UQVdE+eQwNZYWm2rKLBv9Y4RvR+dlcmD37moNudrot
wtCxrIcnDi81E86zSr1boZMPpVWt5/tAFCAj/qAy1htWXdjLaS1M0goRmJO0r6yt
CLRnVtWpAS0OqIJP9EoNFPHy5gte1j11sMGyW0imUhjSYwm8R3LQi++6bilnBBAZ
O/kFy+MAUTiZLwo7UCw+wk+zbKNLEJouBPVsm43W5+a1pzqO2u6Doel/
```

```
-----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-----
MIIMZDCCB1oCAQAwQDEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECxMGUEtJSHVi
MRswGQYDVQQDExJGYWxjb24tMTAyNCBTYW1wbGUwggcPMAcGBSvODwMJA4IHAgAK
fok/+3VjiJnOONk0bjw5WVYh0Gn+pnEi5YnTab3cMXtPTIxnHTV1ru/aJNBs+jhC
eHWi30YxFFKxEc1qQBXwLKnZsECFyLISE/Pm1Ikwae7G4erUs3YvAzdhAmEEYbTj
mVmW/m8x6alFvWTXpA1DApUmwKrBrQiEZvRyyp6kdqQXI0StOad9YQmDYgwN7HFI
omTTn/7LcKTqa2NVLZRCJ2MWGpAJDJkXvhnICVnPSbmq4Gi03TNDvFgZ1Iybgfhm
Ik5q3H+0/WWTJkA7bC+bQM9Aaqg0yxFjwhFCnPhKLo1/rYdQqm5xpejB244sT62c
R2To7r9EJBsBLidkA/oKlK1Ya7MxotdfnaVhebJRfVI4M5pP8poCyBegeUALmCkD
DnBQduXdViQnlL3dR6LarQajR4SI+n3z9k4KIlARR3cTNRPZNDUJAz6DQdMYdJ8t
iDlC0rkXVjrt50TW4SNtoKF6d9REspY3FMRAXRo1z6FZUKyKClwkzkZvXWrnkhQZ
Q7BZlKAXLh5XhqMUOd8WCcj7IQdVg2KG5wo0XAFeTTASwVsMRiCcB/4nYJlYLXfl
3hqbdNtKBBwvPMXR2EHm5WeN30rAiJpxei4nbEzHH+nIZalJUSdC4NgGog62FkTa
E1paVSA19s1PTUGxYCsTrDVpZq0KiUeHo+Y6IiyQS1XZe0mjWD01eIALVahZN25M
CaOQQ1w1gIR80SyjFLliwpvLjdklVweRvzFZpaZcyRo/2kv66CUQPb3jUNDhol2C
t5CxTvyFgUJD2Q3TM1G4ggallgOkO3Jvn8qGIUvQPMD9bOgEIUMRHD9aH7sJRS1z
Ed0kPKuvMbiqA/2giWBWKuRGzVmIkZwIF2Boh+VTcnghdEYk/JNUo3adkKwBGWey
Yp1C61verS5SjerP0+dBceGTD+J5nELyYfaoXJCxjEJva1RkQvzqgcpKIG6j0q+b
eWctfWjpA0wxrYNqy0QzmwLv+LiQ64LkxAi/GDq3ER6lJ2RiUqIf5gqOcq8YmvQ/
jlcKieKRw6CRRi6AdGEMc5sF0zvnle9n/QQjXFwOknIeppGadq49QnqLKepS0Cf3
IQ4PerZmWFYi8mHix+TpJN+afKhEpih+DxxeQBmgupREbbC1j81mrs2bAlrHlRBV
ObfgsZsu8hnJ4H66lm9K6dcUvHbEU26WeTnawxeWGSaiRREFq6xFILxH8wOGsHiZ
WFdIKcsLedX5beS3Y3oelrHsE5QQ9tH0LpVWHOf4jBTMMH3wE0QG8yKdaYfqqziX
sJPaLm+CqFYBAF9DbT4pnuqZUTmZqFS6y6PbP1nzCfoPSb9OcbnQXtyKJpxbWRNS
IZVYGZvJe1D9IHUp7RWnjin4+6kIpqEHBo0l0y6crZBSzd8farmArgmvuKQAWbPt
I0Qa/HGWznYhcsCD6U2oEyle1MZa5ABtMXofFr9nFQDTVQfKbcn6ZTzWTGaoHyX7
b5yaVKMXOkubijV5RxFZ/jmcfiIsWPtWHIHpbiATRL0hShkPuUhAIvbHQNGUze2X
F0CxNySJV3NhPU1F1MU3G9UB1OT7c1xrNYzT5ozBxT6GFejxpu6r0TijhZZnATzq
+x/R6z1p4xM0jTNh+r3KEV3UWXoAKyWs9JZiWte5UwBTDJuI2cNHhEmoE5KK4Tts
SbKHTtyLdjzk4a4pctYQpdMsyoNSIhouQIUkFKoKydiBGBWhkzNKdHOt5PLZWziv
2mTjxhiYF/F0h5tiLF/1vPed5T2hyPB0DQ9CPW2Sim9kpb8JFjFUlF5wPRsQwlXD
VXHlqz4lExfhaADOVTQI5q3YM48Dd7rREIfXQGdxR6pRxNmUxadIcd81T8IYgKBB
xrTQHoahDFamaa+a2kGgQ40SCy3pG0yE18MWnxaanqsKkKxximRNYO0PkmAKbxj/
rz6DuX6WiaB2Jt0hSCfFq2HyT4VoR0mU6hLX5CvkvtbYC4WIrrCMXkYmJmAXuGTx
e97WFrU1U2GU2rF8UuJJTte4UFWLgSiCbH7mF7Zl43LIVkkZS3NW1UT3Eq4hBLzh
gDSpCzwqBHj8gEpKDB7EIMhrN6HGJlvdpT9VomH1VP0p8e86CY+eCyFhs86VtHnV
```

```
HsJvk0eYDVCUuABpr/bNti1rmmnBeYKII24JUnLRWFLmcUzjAwLHlIsClmSN0P6t
IAb2VBbEBh6kAsalNnA2qKewJ6JQtLB3qh0TQPI7drXlP53yK2rRB2NIeBik5ikr
dBTuYpxbmy1mDcSTK/AVbURXSCwNjxJPKhvTc2puEZCGLMVL3jEr4hKuXQBTg58t
E4HlfKAATqkYaqUJkE6ltIIBBDMKOb3peParosuGac1ZEmwinknzJCQGrom25vGA
4vR5cnyi941iLqTb8BOq6aAAMAcGBSvODwMJA4IE+QA6kWIJRndOzcZwBN0ZPR/Z
Cx3O4j1uYxwVLdCcbnXxJmXyAdnbXI8s7vtBDhQQzsfon7K1t039EnQQYYia+TZF
Hxgk2GuSOqbWMbDjoNetxaOPhdxhmKoLxNg/Wlpusk6sTJgl40q4/Gk3OvPztov7
p9mPgnXkfV3PO4f+yBVNMxaVTWs9cZdH1q/u+SI1qQU3VNriHq+hf0TP/UNyYuCN
YzFwvEcjvSMJKYulFxr6XVxkW0E5yTXOGKyq57T0T6V228Ks20mbDg8Kw5jHtuaF
y8G6nw0s8O7N55IOP1r9s4nTkanEboiXrvvINwib63mCOOORBH6C5KuOIcj2cL9p
Wd+lE0S/OzmHLfk6FVYySqh1enYnSGInrQIgjyT7wK0RWArYjyCI5WL8q+gs/KaM
1npkEiKO+PIG3TqcMO/eHNOnyZPuwTn1vnIu3PypfhKGUmUqQeFb9dvFVSFKdghO
9yc22PI6ePXfaRDEorb9jSLreyFFA3akTqPW9bqLvdWjtFZn2lHsbQYE0GV6Gnbq
ARnZtntbbUZDzEIRR3Ur900Sie4iByyRvRwuJwKX6cIyUe8Wfkzz76TSF0JqxkZc
REVHDViNkIbZa86glIaKReuxyJcf/fIpmWvz+u+eRazNvL60FQ7tJC8TYZee06Po
i6w8CWjsKWWyNGPRX/sOUF+xrX57/wiZx/s32KaVyqMlXl4jkGwy+YRxgpHqaTGI
JEb/RkVY5RfypVo0Pohn4qZEf+tkaFRcdBvDkc1E1iHqYBQmjp7Nu8VG9K1w9DvZ
NBDGmE48WytXjWxP9OEDPNAyAErvVeqEkudey2eK7QmJmGhxEiYJyoLr43Erpy7m
wM5xSJt2wc8ZcyBRU2g2jV2XOF7Y09s6sDjtCgRMU7NDwh0mygWOsCKMWEjIttWb
GfTBSOiiPOjKcybk3W+xVeLQSZF1zk7R43sbbdSbUs5s6bJViYEQgxbSHdj+R2xx
GecpC2lO6Tclk/dXCxhvkQ7ZIKWhrsKlxMXiyyHWIfi1Ss208MBZSAox5KkqG4WH
QYhDNYXeMTzfeOnL2xtQxZbIOr0r3nAnKlNduUHIlyCLdegQVdZ1h0UICItf31km
HkahJ8XvX48MIfJ15TIsMb+rq7nPxWl3724sC5NPuqVgUMd23oawW0dre69mkyb2
yS5Zdr+LswTgGQjTzIt45Ckrx4NyN0y1ajpEnb5bMV5sfcm8CTnBRrBKJhJZO7tg
m7fSYHh0it2ygo+7yjYHQESVnaspOZEcJJDbn42jhb1i5XscHDsJySG3c6XXY5P6
QTOr/VOow7TLeH2SAxbM2CJOGkMHijF5kfNLauwJKeNmvJ3M/rsVwEhw7cIZt9t2
6Se83M/mjpyC44nP9pbNviPsbh5PLnE+m67KVomlkrfqS42TsjDb+RPonTBO/IDf
st2cOpxnkFXp1E6XGysHTU+dCPkInUGpXWyFZi1zMI4SiUa38FbkYEGojCMLlec6
2VLw1+IMrZ4Y+JxYyrVIJC8mecPMJrnOrSynxi9aUeHgjt5/XLp6W16X5xmgzXvs
T3YKlaLU/blcI9TTwp6cANllN5q7p2XBw2mJFgix0IfauxhOMd0ySyRpVqjZr71m
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-----
MIIHDzAHBgUrzg8DCQOCBwIACn6JP/t1Y4iZzjjZNG48OVlWIdBp/qZxIuWJ02m9
3DF7T0yMZx01da7v2iTQbPo4Qnh1ot9GMRRSsRHNakAV8Cyp2bBAhciyEhPz5tSJ
MGnuxuHq1LN2LwM3YQJhBGG045lZlv5vMempRb1k16QNQwKVJsCqwa0IhGb0csqe
pHakFyNErTmnfWEJg2IMDexxSKJk05/+y3Ck6mtjVS2UQidjFhqQCQyZF74ZyAlZ
z0m5quBotN0zQ7xYGdSMm4H4ZiJOatx/tP1lkyZAO2wvm0DPQGqoNMsRY8IRQpz4
Si6Nf62HUKpucaXowduOLE+tnEdk6O6/RCQbAS4nZAP6CpStWGuzMaLXX52lYXmy
UX1SODOaT/KaAsgXoHlAC5gpAw5wUHbl3VYkJ5S93Uei2q0Go0eEiPp98/ZOCiJQ
EUd3EzUT2TQ1CQM+g0HTGHSfLYg5QtK5F1Y67edE1uEjbaChenfURLKWNxTEQF0a
Nc+hWVCsigpcJM5Gb11q55IUGUOwWZSgFy4eV4ajFDnfFgnI+yEHVYNihucKNFwB
Xk0wEsFbDEYgnAf+J2CZWC135d4am3TbSgQcLzzF0dhB5uVnjd9KwIiacXouJ2xM
xx/pyGWpSVEnQuDYBqIOthZE2hNaWlUgNfbNT01BsWArE6w1aWatColHh6PmOiIs
kEtV2XtJo1g9NXiAC1WoWTduTAmjkENcNYCEfNEsoxS5YsKby43ZJVcHkb8xWaWm
```

```
XMkaP9pL+uglED2941DQ4aJdgreQsU78hYFCQ9kN0zNRuIIGpZYDpDtyb5/KhiFL
0DzA/WzoBCFDERw/Wh+7CUUtcxHdJDyrrzG4qgP9oIlgVirkRs1ZiJGcCBdgaIfl
U3J4IXRGJPyTVKN2nZCsARlnsmKdQutb3q0uUo3qz9PnQXHhkw/ieZxC8mH2qFyQ
sYxCb2tUZEL86oHKSiBuo9Kvm3lnLX1o6QNMMa2DastEM5sC7/i4kOuC5MQIvxg6
txEepSdkYlKiH+YKjnKvGJr0P45XConikcOgkUYugHRhDHObBdM755XvZ/0EI1xc
DpJyHqaRmnauPUJ6iynqUtAn9yEOD3q2ZlhWIvJh4sfk6STfmnyoRKYofg8cXkAZ
oLqURG2wtY/NZq7NmwJax5UQVTm34LGbLvIZyeB+upZvSunXFLx2xFNulnk52sMX
lhkmokURBausRSC8R/MDhrB4mVhXSCnLC3nV+W3kt2N6Hpax7BOUEPbR9C6VVhzn
+IwUzDB98BNEBvMinWmH6qs4l7CT2i5vgqhWAQBfQ20+KZ7qmVE5mahUusuj2z9Z
8wn6D0m/TnG50F7ciiacW1kTUiGVWBmbyXtQ/SB1Ke0Vp44p+PupCKahBwaNJdMu
nK2QUs3fH2q5gK4Jr7ikAFmz7SNEGvxxls52IXLAg+lNqBMpXtTGWuQAbTF6Hxa/
ZxUA01UHym3J+mU81kxmqB8l+2+cmlSjFzpLm4o1eUcRWf45nH4iLFj7VhyB6W4g
E0S9IUoZD7lIQCL2x0DRlM3tlxdAsTckiVdzYT1NRdTFNxvVAdTk+3NcazWM0+aM
wcU+hhXo8abuq9E4o4WWZwE86vsf0es9aeMTNI0zYfq9yhFd1Fl6ACslrPSWYlrX
uVMAUwybiNnDR4RJqBOSiuE7bEmyh07ci3Y85OGuKXLWEKXTLMqDUiIaLkCFJBSq
CsnYgRgVoZMzSnRzreTy2Vs4r9pk48YYmBfxdIebYixf9bz3neU9ocjwdA0PQj1t
kopvZKW/CRYxVJRecD0bEMJVw1Vx5as+JRMX4WgAzlU0COat2DOPA3e60RCH10Bn
cUeqUcTZlMWnSHHfNU/CGICgQca00B6GoQxWpmmvmtpBoEONEgst6RtMhNfDFp8W
mp6rCpCscYpkTWDtD5JgCm8Y/68+g7l+lomgdibdIUgnxath8k+FaEdJlOoS1+Qr
5L7W2AuFiK6wjF5GJiZgF7hk8Xve1ha1NVNhlNqxfFLiSU7XuFBVi4Eogmx+5he2
ZeNyyFZJGUtzVtVE9xKuIQS84YA0qQs8KgR4/IBKSgwexCDIazehxiZb3aU/VaJh
9VT9KfHvOgmPngshYbPOlbR51R7Cb5NHmA1QlLgAaa/2zbYta5ppwXmCiCNuCVJy
0VhS5nFM4wMCx5SLApZkjdD+rSAG9lQWxAYepALGpTZwNqinsCeiULSwd6odE0Dy
O3a15T+d8itq0QdjSHgYpOYpK3QU7mKcW5stZg3EkyvwFW1EV0gsDY8STyob03Nq
bhGQhizFS94xK+ISrl0AU4OfLROB5XygAE6pGGqlCZBOpbSCAQQzCjm96Xj2q6LL
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-----
MIIQFgIBADAHBgUrzg8DCQSCEAYEghACWjECEPQBKQfxE935/eB3HwB98xQgARBA
C54WviB8P/9+EBAbHsAQj54QBcCLpQfGMIuhQfpQh6L/AdGQHi6L7mxgBkPwB0EI
gdJ0A9H37/Q++TwC97wHRE+MBvj943h9F8A/hJzXe/94I/AEH4BFADW/D6H4Q+AA
JQ/KD4Of+HnOg30fRiMAIwDID3fi8QIPjDwZAj7wfgAH/4wi/8HAkFwQACDvoABD
8ACeCAoQBDwnvd6TgCf8TnehF/4xk8H3wBALwwbCH5QGED4OgEH/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/vi18HvjJ4QO+8QgfC8L/yB8X5heEYPwgIMAwBB8fACAQIQ+8PvBC6DRu
A/4v/B38Qdi5/wOjAIfvhB4mgeGHg//AYHuAAMIQk9/XQcDwIukD7mgAAAYhCCTg
h+8IYABFv/u977wA++ABRAF/wQ977pAe+FAfF/gowe/8GggD7vfAHsOQ9F8AvfOI
```

```
PjAEX/g/AQ3ygIIAQBIAQAD8IhhB/4fwiCE4v76Pof9EQIf978XPg4HwAg34gfCH
0vfdAEXyfCPwyfAUfQeEEY//AH4B/GDpBEH0Av+7wACeGPxDAOEnge/sXdjIHpO9
J8pf6+Lg+EB4AP+EEX/lB/vQd/z4OfFwPwh6IoPiF4BBd8HhSAF4PgdL7wP8H/4h
+3wHQj98OwcGIIRhCYIQcEMPzcKD/ve98AN8IMQia18nP+5/AQdB7wDC6AYh+KEX
wcGQQgEH4P9fH4AAgGH3PD6D5CD6IAO84IPxiP8nyBGAggcB3oAi77hPe6EHxgEE
QB/8UngiDwGwED/ZPe8AQ/+Jr3+BHnhd8Dz4eZCEHxdDwfxA8AA/BN4HvhGHgCf2
T4gj+MAdg/vQSC7wOfdAL/9j8YJue6IIBh8ICBcEEAvjB4gR7+UGvCIIgTbIP4u/
+IodFMDYSFADoS/94IBeF/ovfKP4Ag6MoyeJ8Hg5F7/gg+AXSG+L4hjEbfgiGYIA
+F7wegEMnxd6EYei8IHwj6DwBCBvvv96HwddAAXx9GMAA76ERgf5/X/+CIYyBNwP
PcAMHe72DwR+7QDkJwj4Fj/QIvs6+fX1GCjvHw774O/nBe//AA8XFP3OAuln9/8U
Dfw3Cff05hflIwr56vUOBu0C9ObyBS4ZKu3tDyXtBigoIPAlJPLb+P8gC/EK5/3q
2tr2NQT7/+bv4+IQHtUTACH9M/wqB/fjCRHYFecC4gQW5fkP/gv0BxvtHE4PG8kh
AgYUC8AGAe7t8+se6xoB9Pc5+/Mo+/cK78UN8OIZ3QNAEe/ZEwoH/wsUCefzFDgR
9/8HIuYU6QYC/SP7EvM5LAXlMCAAEdb7DOPX09j+GgUN/9rqLej9+z0JDuv91iMC
NBgS7Okc/OLVTRQc8x8g7gDMBxUA2h/0AwEn7/Ik7+kHA+UE4vYHG/zgDvz9Mebw
KvbyDNXs6xPCFvkH7RX+6O0XKAAFE/EgEuYJ3/r7BQjR1RASCAP2DggJEtgE+vkq
FxAfAPruH+EXCu0cFAf7CRAP7hAS6PUb7PMZIvX6+eEiGx27+h492ecC+wo6sx4t
5Oj7KRb1E/7lwu301SrbEBfi7hQK/xQ0C/b5MvoSAx7k+fsNIf0B2SMM/Nvk9kcX
7irg8uQr+wT4/AfvB+P+CPPoIQn39v4L9jMYFOMT6RDi3Rc1/QDo2eIS5eoSDhkP
Fw0S6P4h+PgEGBEL/iInF53r4fba6AHbC/ETEPvgGfHnISPwAQYZA+0e/Q4QM+Db
Cv4bOgzmFwoe6/vwAtPh7gMM7+XzGvXd9AMUEM4SHCLj9gLoBP4i7OcuEPS4yAUD
IwAU5PURERbeAwARI+PnLSXTFgnQ7O0TOxQD8P0XAO/+DgoALRYB9sQL4wT1Bh38
2xYYLQoS6ff7CAkIIwj3FP4NG/jY/hYiG/H5+wEWAhDpEtMhBx3q8C8M3P8L6Rga
7Czq0g0UBecAvisW9PM4JiAGHgoQ2Qr4GDb15gAH/OoR6ej44PDtMw0H8vQX8/D2
Fw4a9hXU7OgUAiITEyXt/twrGs7HFvUw2/DqAB/+It7mAtUODwnOPAsexfLjDyI5
6xzQCB4cFfr89yQeAd7m+xPv9sD4IfQV6wsLOd8zBufzJQQC7/0I8wfcCeoDEBTJ
HeIrNQgH9Ocg3/nN/hQRKu3vF+IhHv39HeUI8SES+fj9OhC05xrOARwQ8Af9Itzn
3to9EhMK+A4B4CrR/Qf6GtwF1e4myeYB0DXfBv/+ByHR2kcH0BPy8Av37PMpAf76
DSrv1fzrEeD+Cvgc++cOJvYU8RPSA9wKJw4UNBAH/u7jHCjb2f3wDx8H3PT+D+zj
BPIAABXm5vMuERbtBDEu9Qz0+u8ZAdX91fEOM+veDwUS3eYHBxQJGv0UOiojJsb3
B9z21/ULEC0V8gQBG+H6B/sQ6wUhHOfpJgp+iT/7dWOImc442TRuPDlZViHQaf6m
cSLlidNpvdwxe09MjGcdNXWu79ok0Gz6OEJ4daLfRjEUUrERzWpAFfAsqdmwQIXI
shIT8+bUiTBp7sbh6tSzdi8DN2ECYQRhtOOZWZb+bzHpqUW9ZNekDUMClSbAqsGt
CIRm9HLKnqR2pBcjRK05p31hCYNiDA3scUiiZNOf/stwpOprY1UtlEInYxYakAkM
mRe+GcgJWc9JuargaLTdM0O8WBnUjJuB+GYiTmrcf7T9ZZMmQDtsL5tAz0BqqDTL
EWPCEUKc+EoujX+th1CqbnGl6MHbjixPrZxHZOjuv0QkGwEuJ2QD+gqUrVhrszGi
11+dpWF5slF9Ujgzmk/ymgLIF6B5QAuYKQMOcFB25d1WJCeUvd1HotqtBqNHhIj6
ffP2TgoiUBFHdxM1E9k0NQkDPoNB0xh0ny2IOULSuRdWOu3nRNbhI22goXp31ESy
ljcUxEBdGjXPoVlQrIoKXCTORm9daueSFBlDsFmUoBcuHleGoxQ53xYJyPshB1WD
YobnCjRcAV5NMBLBWwxGIJwH/idgmVgtd+XeGpt020oEHC88xdHYQeblZ43fSsCI
mnF6LidsTMcf6chlqUlRJ0Lg2AaiDrYWRNoTWlpVIDX2zU9NQbFgKxOsNWlmrQqJ
R4ej5joiLJBLVdl7SaNYPTV4gAtVqFk3bkwJo5BDXDWAhHzRLKMUuWLCm8uN2SVX
B5G/MVmlplzJGj/aS/roJRA9veNQ0OGiXYK3kLFO/IWBQkPZDdMzUbiCBqWWA6Q7
cm+fyoYhS9A8wP1s6AQhQxEcP1ofuwlFLXMR3SQ8q68xuKoD/aCJYFYq5EbNWYiR
nAgXYGiH5VNyeCF0RiT8k1Sjdp2QrAEZZ7JinULrW96tLlKN6s/T50Fx4ZMP4nmc
QvJh9qhckLGMQm9rVGRC/OqBykogbqPSr5t5Zy19aOkDTDGtg2rLRDObAu/4uJDr
guTECL8YOrcRHqUnZGJSoh/mCo5yrxia9D+OVwqJ4pHDoJFGLoB0YQxzmwXTO+eV
72f9BCNcXA6Sch6mkZp2rj1Ceosp6lLQJ/chDg96tmZYViLyYeLH5Okk35p8qESm
KH4PHF5AGaC6lERtsLWPzWauzZsCWseVEFU5t+Cxmy7yGcngfrqWb0rp1xS8dsRT
bpZ5OdrDF5YZJqJFEQWrrEUgvEfzA4aweJlYV0gpywt51flt5Ldjeh6WsewTlBD2
0fQulVYc5/iMFMwwffATRAbzIp1ph+qrOJewk9oub4KoVgEAX0NtPime6plROZmo
VLrLo9s/WfMJ+g9Jv05xudBe3IomnFtZE1IhlVgZm8l7UP0gdSntFaeOKfj7qQim
oQcGjSXTLpytkFLN3x9quYCuCa+4pABZs+0jRBr8cZbOdiFywIPpTagTKV7Uxlrk
```

```
AG0xeh8Wv2cVANNVB8ptyfplPNZMZqgfJftvnJpUoxc6S5uKNXlHEVn+OZx+IixY
+1YcgeluIBNEvSFKGQ+5SEAi9sdA0ZTN7ZcXQLE3JIlXc2E9TUXUxTcb1QHU5Ptz
XGs1jNPmjMHFPoYV6PGm7qvROKOFlmcBPOr7H9HrPWnjEzSNM2H6vcoRXdRZegAr
Jaz0lmJa17lTAFMMm4jZw0eESagTkorhO2xJsodO3It2POThrily1hCl0yzKg1Ii
Gi5AhSQUqgrJ2IEYFaGTM0p0c63k8tlbOK/aZOPGGJgX8XSHm2IsX/W8953lPaHI
8HQND0I9bZKKb2SlvwkWMVSUXnA9GxDCVcNVceWrPiUTF+FoAM5VNAjmrdgzjwN3
utEQh9dAZ3FHqlHE2ZTFp0hx3zVPwhiAoEHGtNAehqEMVqZpr5raQaBDjRILLekb
TITXwxafFpqeqwqQrHGKZE1g7Q+SYApvGP+vPoO5fpaJoHYm3SFIJ8WrYfJPhWhH
SZTqEtfkK+S+1tgLhYiusIxeRiYmYBe4ZPF73tYWtTVTYZTasXxS4klO17hQVYuB
KIJsfuYXtmXjcshWSRlLc1bVRPcSriEEvOGANKkLPCoEePyASkoMHsQgyGs3ocYm
W92lP1WiYfVU/Snx7zoJj54LIWGzzpW0edUewm+TR5gNUJS4AGmv9s22LWuaacF5
gogjbglSctFYUuZxTOMDAseUiwKWZI3Q/q0gBvZUFsQGHqQCxqU2cDaop7AnolC0
sHeqHRNA8jt2teU/nfIratEHY0h4GKTmKSt0FO5inFubLWYNxJMr8BVtRFdILA2P
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
MRkwFwYDVQQDExBNTC1EU0EtNDQgU2FtcGxlMIIFMjALBglghkgBZQMEAxEDggUh
AGJP3qXtI3xxFkcc6RczjTgaa1oZg4rhDSzUA3c++EzhTdJ+Om9TFTFnRg7+HElf
GKcsE7S7Rc15HbC6D0Ny5GoEiNBm1glcKlR0Aywzch4BLBmyLL9y/qIwwFPYFInM
rdyy+B7/LIZdaJYpxNkJ7wO2fVpEFJ6ygwaiFpeRh5FcA8RVRccKCESwX6Eg1Yyk
/CoVgUbhh2l1jjmfSe5L5vJ1brRHibTCEdOjUX7ekAiM7hHHApBgKlg1ERI79Ccj
CsUHPswV32aueHQtlzISBV0mtdnLwRMP0wK1klhWVuquR/TBJQaBGlq+iWTIlCpC
gGoGrRrjqjgupbnouot9mYfmtYLBcnhxqcfe2JqA4mewIDt4t3lWmggkYN1AJ5BV
qDFNbeU/w9b2K5CX0WVY9+vqrnwMt3OVVgXxkw5Z2arnakCSYdNVq6W1+hDca+kX
a/XUImALigTycKDCsv1cN48O2NunnKYGOcS9wZjfJz/f0t1ALtsjoUPCS7CagRGQ
E6i6KTXR6i6wafIwCRoPHW0pwZ0dyLKITgXA7ys8HBlmPN/rIWJHIAxv815d+fui
dtS9/B6NiwME9+FmjSKYV/yi7Qeoi6n9yUk++LplnYJD+Yy/MawIP9w5YydtdTrl
ufTQMVVCUhHEdBgvZDYDCN666JIVp4gVaooGeJbgDocbxltGalmxlYXYh7rJ7B6m
xINIv9eb6GGZFlarnrxYML3MIU553K5+nju2cBtv7scj8ABZTWz7oYviLVUVVNns
RVFpW83c78U9eIWnO9Vj7luJj8ilpyehamlhf+W0rq8RaB4639FGKuJqNbXMXxoe
dwYByVYPqj4tptiz/rAVb1KHdfYpKjKJ2UgD6UaDujXxH3FXBCl3M3ewTiLT1GBJ
Gqp25yUNYejNMHNic9P0y3yduEW/BVJH0QnRhBTCdsbnqZvVL9hoeWd2L2uGeXxu
4kOC5FELXNtWVpCty44iXP20pz+CfYvg6WzohxB4QQzioLJmGuU1MHJiug0ZbFJ9
crpTV/8zxbpEa2MHs4Rim00LsvqfB9wD2jSYSNGZYgzo0wbi8NhRyZuRtheQ9FuG
FyJFqrbknFBX6FWly/j1GJGNZ+3ShOLfqSP6PIhGTLva+cTf2/lEhSK5LjxMEDx0
```

```
ARhP+LymZaUiGDyrQs1Mb41mUFSsibnhLE3rwyt8hMmtrO1Wm+wW+OhDdYmS+RJA
c/k8+Sph37PoUgbs3jUyvIfz53xO9bkX2JWd8Mkl39Uv+xqHghBcOWY4nkAOWbX8
29QxIWnROjaTednIFH2FW8I6Mw++zt30V7/tsHTM8g/FVkchQowvZ130vnY/yUL1
5UqbkuruBR3qiv/DwJAKGICzqVVRs5u3jG9KxFm7dAa+d18jbl7NVh32h8Lw7WlG
6nwR2CQUG1/J4EuM8LrbXzsWRgkbyryYP0us9cjDX/Du5UUPltQQg9jkHUUnkwfx
3kMFlJkF7gT7wIOW5/hRi/tC22BMiopvlZC42ruSy9CgG8ieC4BCDEV3k0LcVZ6X
7zG8zqewnJdLQW04t696nWyZeB2/G/zK70lGsAbkvobVg6zP4InXxzIwFNIIFbS2
ieElzhLiUs/5sbOrzUOxSSol7mwUBX8fLa0zSCvF/gTWPNGLO2qOr5TffLJlvUNi
T+RaoFvClAFd2qumpXs8dc0/HuyjaL//cSc4iK5ABqlH2ZT4974kQtQcRhwhI5w+
vKICbWCCE4qehgd/5ohE3iKgADALBglghkgBZQMEAxEDggl1AJ1cBgSZme6AiRvS
dI3FryRHHEuF90qhbXmJkYoF/1ZqLmzwb7tVC0PxWgdSMS3GvzX2BN4SOBhRPPqj
8aWHuvBoy8XN3iyrIqL9xKOiHl4sBJH/zeut8EgkGNvaRhLoqG6o3ixZFT0CdzRE
JRw4iTe08z0gbN9NZA7fAMnGFioB/ebknGWK8jRE5VVPncLoWJY+RbDj7qig/uKv
7G7UgwMWa5v0v22kjql5lSDqMCIm7p19eMtX4zUMNldKp32xfok6k/k0giPDbcnB
Krzdlz6bE1KKWR9MBrmZ8YIXFrOehIyseU0jcfq96+V3KYiI4kQq3855NAa6UxGQ
sGz/wV5AtjmhYeut4TRiGk+JPR+8BH2dUTZ0XtUgawGfrhdeJJtiI/pkprqukqEN
Td83BTaHxONdPuexYyZWEb5eh4AtAbWqJI6dhdbF6PQH8KqfGurfuV6ttBkoxaTg
BGkqTjQ5E0om8Wjo+hGvl3Yq4sHL40WHjv3+pE95TQhoXgBZd+qca8NAjpuw6L7H
ZilFtDSsEW9OXnKkSVcWCzB0rhBuvliLFv5aouVC5t/WA/GPgFP4V1mnz4kphiH/
t1Zo2oXNwVovy7LIZLmaozLzngynv5dgMyDG39zhGXEY5L+5uaIVLhBe9Mg6tfXH
G6DlO7QvyONBli7EHurmXiDYaxwtcsgGbrATtMpr64FcijNNX2FBYdtutBdqZKrj
Nl95fUd/uHslKJIY71Mq2TM78nUpIP66aeT4d80L8MvDkmkW34g0PWvAO8zik5qc
UZpaAb5OLEu8VTEE8zrwzoriSUHWiYNDgA54db/1mDG8BkUVc4+oZdOJbeJx1qrv
K3TCqxaF8rEj8Yf/YDmqP15HT2macuLThAPqIzWPymlFC6Beu+aL51O3UKwj604q
VeXBtsvhml3DEqUcHf41tlqVLg1DhjtDk7hu0Ntq6YDq5aZu+EaR89W3szeRO//N
x4/H17RXgb2EbL7nU0NzIWRL7UZ//rjGr2vf2VE2g0kP8UrzzEw+oUAR9nen1RlS
wXAU8z6c//1DkjeAYlrQkeo2t3kXn9i5EsDl9Qm5Y/zqbLxcBLBn4wyenjZlnWWg
TPHdJJIXu+X1bbHb6xxlDtWuR64YYQA8A38Gy865ch9+9CQNEnf5Z1d/eZrgIxxJ
iHDHGyb6ibDiskaj4WzE56kvEZgwp9j1trhpXTOg1ychMKJmsFuKbwUGmKYJIF8Z
p+j8vsnYFMREcaz8t4sua3nF+F4KS5fcSjr7yaHWnGzRaD1ptL+H/WIawVhr4Q5y
zroN+PazUuRgeuIz6xl0vNQQlZ+9ZhFTMLBNlIiaQ21Lg6xuKX1/b7VUoDRVz75j
0mOFnnqAMLg9GU/pmyPjTJnL3f+NRd8KRPmQJ4ohy9uNXdh5iCe+yTqS9oEGnF0M
v5G/3L+6MzrrCUJBQKWopT+wCt70V5Og/i24NsTaxe6z3RGIQJyYrcas7o6kEz2V
bz7YdIhjJkIh0Io2TSid5AALBo5LGn8j9kA61Dpzop9JKmaAqHSGeFueZBAfJpcB
btsskrD+PUp3ah5z56hiOSaV26JH6kpMwWOy7+yI61SMbPbdUMbgahfNR2QcHvc1
WgagNMhBi3/FzUMymAlyLaEEWPzmkk8T5u26Fu+dSxc9E6QYRMhfyzFaglhOqXKX
ta/+4KFJzSIF8nAu8w7Vc2m76lAYPxrtOhLjp/fQEtmWKTtXaiKktgDs0WZWhNvg
j2zO4+n+0kksgWyUoFUvEy87qyv0yyPmUvHcwxqoSpeM24qqhkjVpQvl4aynBeUC
jYJ6bEMUoF4uCsCM2BqHRcbB28IYXMms93qzXKO22VuOcx92UpJ98+bdTBoczYPi
Sarq5xObjh3S0zXOrp2WEHS1QkBnbvpVwMjkBEBDMlT8u9z1Y+EVS7JDHU/26EsA
r2MX1Sr/80jbpKnrPb1wyAzGPOz8+aY2JCJN+4DEc9KAi9r9LfeQdc+DqOk28bNI
x6Rjd+UlKn3JZTrfNKqe6v42TTvf6nlBzpSHpF+f41qjBW5wEgJF4ADzJAT9Voj0
hO/snmUU02JSsHrIkb4s51LUvI9CkNoyp2PhzO5lAdxRAHf7KG8B2S1yGj9uWN1d
lFs9wsEZq8MlWF0Pl9bSy50lK07Gcxg18XwxG4pdyE3ubwL09fZAGM+5OTQSAg4G
A5yDzHNt3xD1+UlutQ4V/fsw3KiCuuN+W9q4u+Jn7JjZWdB7azd7GpwemuVAUqvL
6aSMxfZ4paJoqXc9zc3AMfMGf6NsKB9lozSRgm3debL0LNlq12R9FKLwvF2vWI9N
u3gmE6M14GVVDE6Ebia4/9PTklL8kHrK6i2dP+dlEihmm37iKyG1LFMaLMVi3GNP
U3gIShxgNl4IqKULckMoWQySI85TKmQkoImKqa1R8xcAbDD3MwAFsynO9siOLnJN
OFdIKsHCauTJYkBKVMY9Y3IZXlOSE9WTSPPW+vkETC+OaTYnb8l4ruBwuwA3S+k2
AZ2NuU9cGHK18kSko7UGadyfiEx8iKMobd8ssmP00Twz1MgzPiS3eUxqTlpFFAjv
bu/DYyq5E76Bg+2qno5XjsB8h9jVNWdtlGzzqOfivXcZti5uFMPfHB4GW2dS69la
rWDdFSUytAmEQyfWNmBfz3WWqvZJ/ik41Qf93n/7EiLcapHwoiP8YPedQR46YMWb
HOLyIZeQdmVKxxoYG1kHemAbOrAdxEXnZYAjRb2ajWf/0AIaFfEtjEofGu4RpdpI
```

```
nn0iJ2jZFIO6cW9nfZnr1mNlVzsFS30HfidfiC4UTJsJEpqVjrgqVXuMZPEaftBx
gmR8SzMw1ZXwz/Mn7L+3R2Ak4/i90lHJDGyvBxyTYkartkD5AOE91BWEVlPhKOO5
OAATuThY11EZzSqyUHTBnrVOp7xeLcMPhj4PxCEJF+gROYHZnqO7h7/vBRnk68DE
r/XlQS0A8MKnUWe4gnBmnOnvB6wO+wIwCNhhFh2e2nbSCI+xc01/wqJeNduNnt5Q
nwq9LcXUixzP+z5ltzuj3/8Yz05DFztfXEt6oLaSf1utykTMuuJYaeuGaDipIe7u
MgNiKia3igfTCq1Gh1YOfFEsSrr5Bxoid3ugzPD6/AYMGigpLC4wSElxjpOrsLK/
xMjJ1+Dr7/ENIyg1TVLS0+4HDhITKy4wN1OTrf4AAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAKIyw4
-----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/qIwwFPYFInMrdyy+B7/LIZdaJYpxNkJ7wO2fVpEFJ6ygwai
FpeRh5FcA8RVRccKCESwX6Eg1Yyk/CoVgUbhh2l1jjmfSe5L5vJ1brRHibTCEdOj
UX7ekAiM7hHHApBgKlg1ERI79CcjCsUHPswV32aueHQtlzISBV0mtdnLwRMP0wK1
klhWVuquR/TBJQaBGlq+iWTIlCpCgGoGrRrjqjgupbnouot9mYfmtYLBcnhxqcfe
2JqA4mewIDt4t3lWmggkYN1AJ5BVqDFNbeU/w9b2K5CX0WVY9+vqrnwMt3OVVgXx
kw5Z2arnakCSYdNVq6W1+hDca+kXa/XUImALigTycKDCsv1cN48O2NunnKYGOcS9
wZjfJz/f0t1ALtsjoUPCS7CagRGQE6i6KTXR6i6wafIwCRoPHW0pwZ0dyLKITgXA
7ys8HBlmPN/rIWJHIAxv815d+fuidtS9/B6NiwME9+FmjSKYV/yi7Qeoi6n9yUk+
+LplnYJD+Yy/MawIP9w5YydtdTrlufTQMVVCUhHEdBgvZDYDCN666JIVp4gVaooG
eJbgDocbxltGalmxlYXYh7rJ7B6mxINIv9eb6GGZFlarnrxYML3MIU553K5+nju2
cBtv7scj8ABZTWz7oYviLVUVVNnsRVFpW83c78U9eIWnO9Vj7luJj8ilpyehamlh
f+W0rq8RaB4639FGKuJqNbXMXxoedwYByVYPqj4tptiz/rAVb1KHdfYpKjKJ2UgD
6UaDujXxH3FXBCl3M3ewTiLT1GBJGqp25yUNYejNMHNic9P0y3yduEW/BVJH0QnR
hBTCdsbnqZvVL9hoeWd2L2uGeXxu4kOC5FELXNtWVpCty44iXP20pz+CfYvg6Wzo
hxB4QQzioLJmGuU1MHJiug0ZbFJ9crpTV/8zxbpEa2MHs4Rim00LsvqfB9wD2jSY
SNGZYgzo0wbi8NhRyZuRtheQ9FuGFyJFqrbknFBX6FWly/j1GJGNZ+3ShOLfqSP6
PIhGTLva+cTf2/lEhSK5LjxMEDx0ARhP+LymZaUiGDyrQs1Mb41mUFSsibnhLE3r
wyt8hMmtrO1Wm+wW+OhDdYmS+RJAc/k8+Sph37PoUgbs3jUyvIfz53xO9bkX2JWd
8Mkl39Uv+xqHghBcOWY4nkAOWbX829QxIWnROjaTednIFH2FW8I6Mw++zt30V7/t
sHTM8g/FVkchQowvZ130vnY/yUL15UqbkuruBR3qiv/DwJAKGICzqVVRs5u3jG9K
xFm7dAa+d18jbl7NVh32h8Lw7WlG6nwR2CQUG1/J4EuM8LrbXzsWRgkbyryYP0us
9cjDX/Du5UUPltQQg9jkHUUnkwfx3kMFlJkF7gT7wIOW5/hRi/tC22BMiopvlZC4
2ruSy9CgG8ieC4BCDEV3k0LcVZ6X7zG8zqewnJdLQW04t696nWyZeB2/G/zK70lG
sAbkvobVg6zP4InXxzIwFNIIFbS2ieElzhLiUs/5sbOrzUOxSSol7mwUBX8fLa0z
SCvF/gTWPNGLO2qOr5TffLJlvUNiT+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++EzhFi4fAFgoySp4hWKtCHcF2DCWS4AfPdpDORp2ZpI8zGHaAQxW
gmsGLY80X8gZRI+C47M+lNzWd1EyUUL/JeMQTUA2sE0wLhFj4APgUzyDjNUriRMP
FHMdUS9JUHHckrxXIjiQo8RskoJpmiCSZAiMHEIqIyEiESNt2MgNA8WRA5htojQI
CDIMZDgoo4JAGYkAGEkulBgi4iBkwcKRkJiEzJYhhLCIE4IAIgJRIKko5CgKQDQN
IjIxgEJlQaghAjWJmEBsYEhw07CRGqYkGoGRiUIIIqSBIZAswRiJJAmFG0lyYRKS
WJKFYABqiEYBQLQhExdugQAhyAARGJhRoiQACbZBXCgmApZBAQMlYkJS5DJhJBYk
2xQCm7AQ4YCIC6IxDAJlgkQg4wZR05aRjJgJmzRB5CJx0YJs0IINQbIt04ARUigg
CwVuGCJgzABxi7aIESSN3AaAGsgMUjJuwbQAyLiIWAIqSiRmlBaATBhRFISR0EaN
XKRRIsgpHDdw0AIp0KAgCjBqjKYoG8MBkTQE2aIQgEQwXARh2iZF2qAlGAKKJIFJ
FIAFQzSCVCBKUzhxiSCRhLYwI8QoEzIw3CgqGjKNGoZQEkaS2RhkABgJCscJ0DJq
AgAm0bIBk4Ih44RISIiBWbhxCwdgUzZqGoNhgaZI4SBA2DiIA8lhWQYlkcgtGiYI
wihoFIMMzIAkgUSNGMcREQYslIYBEZhxA6aQCYGICxYQoghMgxJwGTORZKCJorBI
08YNACRIm4ZJE8Nw48BpyRIt0QRhkiBQXCAqQKhkIMNRSSJGEiIJGsQt2hYoBLFs
IrBIwJhECANIQcgsGREGkhIMEoRI0KQp0UZFgchsCBJqIgcM0JgRg8Rxw5QkEcEx
GCRMYMSN2whyYoRpobRsiEhlYCSKQrhJ1CQwBJckCqNwIrcxHCaMlDYyAMeBGbNl
mjQBxCJx4hAFgBYq0jJlQARNCxSJmCIIIrEgmsYlSYYFQBJJwARiQAZsYhYBmqZJ
HEQppLYt4YgAHLSBlCCIFMUAEcONw0KMGrJQEoIJIykRgaKA0TRwoTJKSZZljCaN
3BJkkCQRoAItGBRFiZaRmcgsAYFxIJJNwUQJFLYwWySKmRaQ3CSMGiYMkyJxoBQh
CgElogYI2ohpGrIkNtR8ug6qLJc3a8m37dIFsEpHs8tm9QBlDzZBuFih6kphMK3r
yN8Z2w1tPlVOyd1ZjWYOtdCabRrHP7iDlIaqTqQDUn4Kime5w38s5R8Q4dDeGY+0
wIhisQUp5eRGqWJiePqclaBiM0Ga3QNvWORIda3UI616Hq8f7Qh1mNC7H0Y7Y4/a
IYskzSB1f8L5pir0TUFOdeBCpUGHyq7EolN0mFs9s52DjZ7hqk9WPWEZK1JIf3bb
e7D4WC0jARbWdroRijPTqMAVeEtiRPZ9lSZdv1Fhrf+aXjG4l6UNP+biBtoAAg89
InPRICVsgYwTRq1yFLKeYZQ/1cIicGFTARSHxClYgNRa95d/f8LbSVJvPlsU2Yen
33fuAjKA84L5LHgA4vFI3+Fd226YO0hIIhWh1gXluvY2Cwp7R0f3iM3/UsaRilgw
zCqvFR8qPpe5ez3ydV08eYcf+Obt7zBF/yxtZb9cwaQD7kczZ8d7my/W07Ui2FSg
9lgDPvVcynr0lvqxdg9frMFrIEsbxVJEWMbxfW+BrAHxLwl4TmlqvxzH5TogmBFi
hkVTTBQJFa+Qg7wAgGkRnU+nLzpxqACliZCPvSLRZiPun1bA1ECHQc3Wa6cofoCO
4xm1EkjgmNNTA6yqHWApecXbgD7rxRyp0FMqrmD7YGRVeY11Ntky9cQaS4DcueSi
t1h0ekklKKHXsd+DP48Lc2hUyhT3JSU8SMj1oUsjSQ5jPYRcsIeHt7UpCZxrCqm0
GJTFd1qSRFEYteLNwgCPqjzPmCgJ2IDW/NmEqGaXM8orVDMxQfctwpIkJS6Pg5il
J6A9T/YUHEJwXF+sC2mPkNntuBFWkOcKiTN7EXw6pijgqw/BlRCTsTuR0A/vO877
GzHJFX7wGoASe1KuGfDTiQWHNmI5NZqv9wvxa0IdxyBv7+EPjIfmCVxGH7/HM4BD
a3LF82vCCbVdsmlkWNLs7K6biytrK0r4Sc50ClJguQoXYPHgkDqM5MuNtZfDg/LP
J4QFtrPk1jQFuAS9Ap+s2XGO1cu6u77oVtaJSn4ZxRP7KUPfvHFsidy0VRHpTi5A
hW39STrE5omwztThE0XsJePN9eMKu+CI1Q9EVADwKldTdieanTShTqrAdLdhuI6G
gUfENV/Oo66aoTqCm96j3v+c2yJqonOjMK2G9IS2BY8zxWzoO/0tHNvMoPlolvWI
2Edi8JBQKJR0Jv+dHih1bP5MJDYT7mVQpoVHZmx06PIvHW7sYdC/jawinT0F8aly
xfweRBH119UQqOyIa2dSZPQz6MQ9w6aQlJkl98SfjQY1X7i9+/K3dN9opjv0GMDC
vn5OkWs5XDT9BULpvnYNxUjP9VuNAlP5Vkpn2zjLXMqWg4yoMopTS03W+lGoT0mw
lSNqTvmVIEODuzLf6irXwFd0MW+4ynH3YxyuxjipeMlputpDiFFltqMEnOVc+hn9
cMv7dnEui7BPE9x96cBZ7YVWyNH6BezGryjXTbkztWL90n36TSCSSCG8zvjExPY/
gO7etz5H1iqoHN6fbiGO6hdM53WyJLv4Z6ahq/c1aJdjWesC/NripPm5MvaIge2Z
DvDGMGvE3K1PmuC2AMmskt8S1821M1s5YvSrUmFqdH6GfR1U75DGqYvzzIJPqkQX
Unl67xx57R23dOXx93PejVbqcAId+vqc/HxnNpiCGelsUIELN/h4nI2oWvs4SFdH
OhL6BV5WMmdoFqTTdcnci0Du31PVhxtImIFecMOzK88EVJgCfZNe/JVCIiLMggvC
M1PLf4FEdoKKEfBtQvXkYWhR2rRPVlGWAUQT31wmmxDIbBSZESysHkOXMT+obllL
JomWgJmx6s1tc/JCnUOsvC4ii0eV+6FuZ4UW0fAOpW6xYyHm6b/VJDKq/V4KPCYG
rrBTm5YjyFKke6n+gKqZgygU/AtRoGJgRv/W3EUFkTZXqM7Li4qlsqkLFGQKRmX8
/blCZWAyZCL99MUnslXjRUoxcxdHloavm5OdVYQtgs6HkgL9cAgdgXnOI06pugSi
```

```
AfoiyD+sq4GSq0LJCxEz+u7GIHaXICsqRlnYzhOPkN+c7wZ7n9vpBMAJAQVpca/o
HLtQsahLl1DtsST6Ba/aNyN7PcKrRxbOQqOVUlSeH2chIhdt5u8NfWTwGYKNtyWw
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/sCAQAwPjEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECxMGUEtJSHVi
MRkwFwYDVQQDExBNTC1EU0EtNjUgU2FtcGxlMIIHsjALBglghkgBZQMEAxIDggeh
AK5Oy64HopzilOFmlN1hROrZnUg71OP/wRLpPbfiCznkN2vhXtpCXzROhv0AWVEw
ic5Pa2AzKQAj/rJ1bMJ3iUo27P2Yx22grTuQajTQIvKGkAiyVUBOjKRVvCndh1Ul
JVSo28UUWf2Z0lqQfJ38/OIbeC4sYguJbEyX5YPZNjzuDHCvp0kPdLj4QzvQyy3d
EeryN/oxvO4YwWqsWIYVovvGxCaZuWtY7gM/6PtznX3YFHMmsChLpP3qqlcOFL0F
xwxEJMXBjF0RwaehCwDMO1zEuSFw19bmKVN/yXpFtKvepY5Y0Sfc9gHzD2NvHn6v
F5x1AF7wd6MZLn4dq8a23dqLNVMQgrCjhMPg0ZfkhHqq+LteKbKrMKxpf/gGgRv9
iSzsTUnj5Pk80ylYM6rKALxT6rr4mh3LJjv1CpPCHlz6aDiSPTp+gEYX9DkXyko0
twWnyDAJuApBm51xF4gssAfHxKswIJc2hm+cYemzx78ZTqQ3nddVR5EDEYYijhwv
/t3gykEQCg2e622Sv7usZ+u8TwEwmwD6qQjAr6X+6YXpr3hckNLFWbfMD9lPY/lX
tSTNVoUaI4haPvMu6aHXyem6fCFZ5cB9EDUPMq4eygud2ZWgGgzaj7I5VVJfjIYE
Gf4pgVgH6o9OeHhroHYPZphm391437wPImFKVNaQDePoXgxas93mbk3Jq4Ycm+bl
CuHWUdWrGpMuOzZIC0AO8RzhxRYTb6qtCoARbL0Gnn/Xyf7WxKVUM4o8hryA5LcV
eXJFPbYZvy7OPbqSwtkf4w5NLf8fWQAxegftBMxCCHOOnZC8BNFxU5N136h3DIOl
VBqsO7yOg9NNVRS4St5FdZzKxSdszWlyGiKImLhrS+Znnw30eQBA4nc6/ZhdhcTa
xe3lYHZ3Ql6O9nPf8TmXdb98sCQKkxIszfKAQ3o2Ag+D9wAj3mxMwLBOG5ZEs40n
gwcg6Y8p8uHYr8RaC3karUl06AD/2uee+sw0JUV/xQBKHNFTgBUMfFmHg/NrCNfY
w/cGHKvaaAsa242FmolnW2VUpE62VW0js+zE4uLm/fB1pWguNGJZg0fnNh23PirO
qd2q6c5b46Ze1cDAPMNWzLn+CQmBCgWbjma22ty81K/s0eYNaIhvsStdgbRU7XkQ
ufAbs23fqDhy1pVZf24PejQStuKuqvd0gSaY+GSs7bxMp1Xf2Uk8aIKGfwLIWUcc
gXhzhsHsVsvwgA87cyJoj2gV4QhvMdMYFnMSDNp/9EM4zJkNrpUZGZNJbtSDvdKS
zAxudHpaCLt4UnvOYtyAJ2id1TSKb3VLaPTlxnG60LijpgzHxQMyfX3btpW3okqy
M7JteW5091rJj15u43i8cxdO4rzYfPIhy7xK8vHA6aVDZdWW1UEU/GKNqKu6p5Dv
0eoTsKkPsll008RQ7BGbZmJbQ4vC51huGXFD41zoqmvsF2oYBoXDFDfsPhTyfTqw
goazzvKciYxbd4aj6usP+5iYEDx4ktnLDe9BsfT0M5PGCelX1BA523bcPhPJ/qfu
6l2WreTNGQX8Fb+gUVSX5vb2722qhycTDFivMM1FABqesr7ZzLaTCdeC39NV/oHo
F6F1PjOJveS5DybWo0pEdvPPlIqVJcolOmGmoITVXnNAh2+sE2Joa86tPs8ShCDQ
Im4F9sM36kBonY5VB/galTErdnkf1xJQiFp9Pxb+bjlxYJ/zo56viZBpzYpzgdjG
L/zi9wCRrcSCLHIgw1FWRopFwlTos5m1sA6R1eUyCtTWisnUwxo1ipXjgFXelFvD
M1hnSSxzYov3Ntf0YxDcKHqIrgG5/NwV6XEUSgLr4jQYpUvdLp8lU71UYTwDDmCy
C6BdUE4yoVIvYdpY9aveSkMToUavTj+fn2ENDEhVPp9MjVLU85AKeJhXap45HlQH
```

```
BTgdE1Jl0Z88rlss4zxSmRgBRR+4Hx7r+XrVwMpuKgyT/52RPuHBAWAVBtZUWSQP
BbHiQUX6SBq0nQJAUKNWrPHwiVu+N2BTu5mzZq7Ky41FKMlhegw764vkPvlrj8iR
voOkb/UkpEhGq4n7gNT4KFxfA/OWKVqS1ho/tbxiiCjrM3US8zmkmMZUWOmPAgtc
KVQtSoBmENTRF1oPKZzes1KHckBY1YzjyAna0Gyps5CedP3lLWUAgsvm7wWgWFmc
5artdPBFX8r1zCJVsLQBDjsxc3Av+jbLFw0Zjq8Ft7dpBGbqq02rPxuFdrulntdc
Rs/dnZNvqPvY0lMyGndTUYWQED8z4TlhoeghAt2X68JHKDlAmyEZg/9PdF23iC8S
l6CTi4kkOKudDxh9tiXoOL9ysRkOXki6ZR+4a+v1J2gMWSC08wWEjiQ08+9qI6QD
O+ICAKGPpsiHnw1iHOp6+z1eqSzqwgG6xbEHL5gyMIX3I9uB0+9+udXzqven7viL
bI+L6a08HzvMkZmWl3ONhdlYyykVUtLGSsOOP23Tm0gtgNdrGJEqMFPyaXpw4i5+
OROcRBVVxnKL7bAKhgsZ6S1ut3gxGyYxhufBZCdnPhLYOq62UAsxdYKf75+BqAc1
ktgkSPhmuK6dvS1YzBRFA18DzzVBE5VvVUf7VBicLbHYoAAwCwYJYIZIAWUDBAMS
A4IM7gDnTIxv9jv4J/IJqW3NnBmMI4NIoRpzqjwNpxVYmGMPLkdNFURDfHdc5TKz
s1n0V/wX1xsJn56BWkL/RTrx8otrqX5Jfzpsk/bpgBfjkxb1ctnatkNXAP4pAv7P
MttaFySNM+ACWVlneA9CBHhYmOvB8p/8TozIHS37yunC9gXd+wNDiYCLUh4ydiUq
j7tQznRr/fivKej4s9bBHRYAD5lrjcZWwQjHq1BoQ6p++CimBKSAl5znNCvQTKit
ymV541ty1wCbVVfPVnvSS2zHkP63KXaOOS2gwpMH0u8GMFjyrWjALb343538pOYX
p82xiHO8feheFNt3uDibHXYGBE9WD/CRyW3GDzkuwHWoLEMCaOg2FWlRfLWK3BVt
yX1Mrag/6F8G0vyrCA2/pnAnf//j05LX73kFTrvuiIcvXNaNpQOHMTXlz4uUM+61
urns3/euLE6DBgqkVngg/TVWWj3czRMzWKVZdC2OYA3+hxxdTpST7VYJgjMqjTpj
eek4+nZ9fXZ3UQ9B/Td/5iMwS78vvvxxSOTaF1OLQ9fDxx1RgcfSQ4ubcSKkH7DP
JuE6oRPERRnen7MFArzFPb2zesE6bbY70YTyBRV96TAk8goebDe+oEaq/VxMppG8
hOLlwj8kh147U5HQlXbeCFBDIsfnt9X/9zPfq97UNlMKJnrNLB5Jayezl5JOFYgE
AifDt028wGkdNEsJR2iVA6A3yh7X2k5/S8PgsmaHITVuU7uj/u8hN2LPRMXR4RB1
uzXWr9eacvJm95swsY2tDnJDfzGbdO2qLa88L520MNDysigmfv7Z6myYob/Hc01q
4YXOodEHHI3daEn5Y+v8FtK9JcNhWmAA+D9/8FjB6iEwdQoruN4XFHU/1XtOb91n
Au8K2xQUQyVWyOqkiB++4Vbmg9K9Te+sQCuj+C8S6nrhROTq+98H9dQTpRHaO0RB
iqk1Z3L1bJhmdGJ/F2O+AG0Q37sVigxdzoGneqwunhbH6jsFNEiXFD1kfwSYknIB
wnZGIfyJ4JGNEd/q8Xj26508P130OE4MJVhxPO7DA5LrXlgowxxWR8ODtFXxNDDP
dvQA/MwO2sSegI0WzoiSqk2/rYhD2AJDWrlZj2t3zMLzqMkKj1VgVgsOl/vMrRcw
niHatAMfZfLJtS1LnPCwenat5MgTM1lQlcFP1p6eRoqA6PNLB8mlQ3RX3MK62ER6
faM2KOLNLjmG0mN9xU7BD6TrYnjAonEnIIMnaZtKdrfq9fBIGUTf+okGnwtpKVVg
SoICnxAJiecLh+ZihC17cxhTl2Fw03Y7LE/YV0vMUu+OaWfScDbVh7dTuPMd5Rb3
cO9JZnpE4hhV3qbHE2JUVQ5OQGrnKlov1hrsEWFqFuSnS2QupkcGTmg6Zi9BJEuM
XNjv2KDqkBe36LKb/d2EzYudhKhgMy6lNovEGC0vWd/qahs4mI7HLSHfRLryUQB+
SiU2LW1g976CkrF3EhgI067+2RjY3BS1Kk/Xk1q1zmZ7fu28ywrngJQVMTaz6BmX
NpiXdv1SaKpoMBWynmnLQB4wcqc8xWt9tF7VyENBaf1axdrf2mLEzTbYosz2RQID
fdA/s3DzgkKNADTXtQRpPSLes9Ud5RC8SW42a7pMh5HfAXFk3WL91QcBky18tfbp
MO5Gjjk+krjIG6hs/mTVv69r1ZNgPBpbhgl8ALLeXg/5vyNw/9336zpz7COPOTIC
MSRnQlKbA4LzjqvJThqZw9LRPzXkggvdHeyabPuz7l65ckSfe7IIY7iKN63eayC+
ow0S6N+RWCjby1qxwP3F35gQWJ+rIfmJ2YMPjDn/WdApPMJ6X6fXukrPchsHW31I
vEQl2P/mP+z1M1VKVRiBQFpGniavIl0n4UJbxTeEaomRfKbLAJzC1AALFg5HZ4QZ
KbF+acOd9byOdiiRu18LwFrurzC77f6fX57STpWwBrLJQJon4yv3wQ5TKTSAHf2G
EvoVTuLSiMbTmAMig9nrV8m1k8Zgc/VEhaKPygBNU27C6Wd5N8WnBAGp5yV4vsjC
Hr7yEkGieSgkDYqmMs2OakyUiEb7q38qL8Q08a0SOSbnpL7AGzncr4n9No8rehbt
7Gx2mNoTGdStvIBIsIlgak2Z82UYAqa1M5PxJMFUObWAljpJFp7YrPEn6j8klmtE
Ta0axX3koAzSQVL1qL9zdFIivmZ9SQ7nDooEVoPoX16MuAvj90SNaPvZD9dYQAgS
S+aWPHA7j3ZAW/4TNVLdH5WS20VIteXZfCkG9M5iNJBCUVuqBDOKIkSSblPWaPG1
5CmrklAce/Ud+gjdMEOpscwEHbmhhBn9OlmOG7AVmhgVSogZTyPuNuhRYJS+P/mi
5H58JzHmfUbuyMt46gejRXA735OqTrStqTyu4UD20fq6glaHe8gSJRiUPdPpjKCZ
niiyHr1C+i6aYqworQx5RSQTt8NUFB34zfTewK6gH1IuFS0RHOP6PUTF0EEYoqed
vcVcNYpLZwxVH2McS/Wp7cY8H7SbRVwPx7k7OPPTN5OHIZSLEMxqAsG6YIyOzBl/
Fi1iWmWo5aHWPS/lAs+pNzCTdH12PuFAsac3EtmDG7E4YFuNc68xmaWTWt1dzhd/
ndhPUowKVfIiNiWWraM63fVzI6YxC5fNXno6JRBYikK6fmtoKqo7MdDCpnBr/v33
```

```
d2ie984OEOPYO/SNKenn1dSWvlKXcQuMoZhBibKnrDbAxM1v86Vot2+AW32CXBFH
GEQLCIWHvuC5J+Eh+O/bZNE329m+7xlBx8dKzqNQoMWRiOnC27iQg0PRrjxJE0ZN
DJKGCxhRFkwv5hMX/yHU3dIhNkCbj0dCHTCVBHZC8hy9AivG8DUdGLz+obdxkiRO
D3F1juTrTK9pgXECU11HDzd3hzL8dNuR/EMjAT00Y62l7yfD/sP2nt++NMxXBHlJ
/qkNNYy2P6KhObUuo/VVVjNN113gmxzACUIzzy1MiKBeKeE715F1Wrr7eZD8rlhy
5uEBTOL8QKt0jR/Sk2FKQ+ZJ+Cl9TRTHLAQ29OYI7+LxWGLNroe/4X3xxcjT6PYn
cH8og5DhidLYqogTvFh52FgyaCgNzVCA9yqhJe3yW3orTRkYa8FecqETq+ln13tS
IG6SQ5RV2KECH4gJP+I7EXO8SUM7riqkEfYwdbqWMvvzh91e31wf8gDsYjkm55Mg
LfWjg13VwReyzHiP4MtSUKUf4bUf6E47QajZJVtIoHQLE04r3jVStbIQAeWgIFNT
JJL9OK/6zQB/PspTw5sM17dvi9v1xkabz77qk2ygECI4TSaWnZH48insSU5Svx0V
AvaB29DhOx/GiKJwIvEm653zKxjjOc5bYjBWpH2MWN6Za4OxJTpEYWV/ptzy60oL
VHYnSDSiOyt28WZIONA56ZqtY4mRd7IXMPttVP2I2GeB0NzQvvzuOewRdjbwzgJ5
IqtO8mgm1vp2/qPt8BMKkqZO2ANxzBW65DMtmHM1w9HRunuJwAlEFLHz3e5GPJ5k
K/1MACoDHR0O7pL9AtFtOijvdqNeEr3OxFsXtHuFVGy3viKIKPLepL+IXeSfWAe7
3HF84BSabYRDhF3HwU1/nAJhlpsFKrEUlpRaVidLAVn9OeUhQrBtQie02rcjXp/v
B1EgFwe/9wgavbKK5eaEk3Zzqi4LUNiV8DerOvhx7zfVv2o/Wlz1C3u5DPYSZQN7
QAp8YpoeizSD+4LBuHi4W25W2udUVZfNa7zjbLCjnUknVTyuIRiIaUMa/4xSwsBT
vj7DJxddU79+lcodMlsqTfqyDzygucrYvIcX3gyy1a1Rr0xb14F3ly9B2ZnwG+5o
wholsOoQ/bp+pZRlAUZNTLu2FVLvd0/I2Ktc+p5wkbwcqV6wEkRgjfybtzo7ZOli
/yT8P5uykTYnibg5k4FfFq6gORVMddAcyFG3507GnVg4yCRkT+brraTENmZK+JDc
LpulYnbkaRujg6dRvfoczr4yTWHF7PBj1VB38+F2ziWrFcTO+33IHsMkM9Cf/UzZ
CLx5PfQ6Lv5x/2jNvRWh5Yj8XAXHFkxE3bpfuxigfP1hXT1YNvl/nRvnB6ZJaeQJ
qST8KZKrsON+exus1+9C9Mla8EciWRufTXnB6Z3FTdj3Utdx4Wvj4AEQg1AhgQ2Q
L0QJx3Tk1HFBQPOeeG1cfBSdnFkxpspqHBCm4lol8f7Y8jQMJt5hVoKRC1o8+aet
6gzOQXDi7qSj+zmQnmytx99Yz8aYCK3hGdLJExWQhWVr72FDcCTDLFY653fr9A63
oziuZPl2MpQNWbEM5nqdv2ZQvgg4MtB3a6Ec9zJQdhK9jF2vsEFbtMfRB3WpvdcJ
Ez5jZwIEboCIprG44OHrITQ6YnZ7gbjBMWG+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-----
MIIHsjALBglghkgBZQMEAxIDggehAK5Oy64HopzilOFmlN1hROrZnUg71OP/wRLp
PbfiCznkN2vhXtpCXzROhv0AWVEwic5Pa2AzKQAj/rJ1bMJ3iUo27P2Yx22grTuQ
ajTQIvKGkAiyVUBOjKRVvCndh1UlJVSo28UUWf2Z0lqQfJ38/OIbeC4sYguJbEyX
5YPZNjzuDHCvp0kPdLj4QzvQyy3dEeryN/oxvO4YwWqsWIYVovvGxCaZuWtY7gM/
6PtznX3YFHMmsChLpP3qqlcOFL0FxwxEJMXBjF0RwaehCwDMO1zEuSFw19bmKVN/
yXpFtKvepY5Y0Sfc9gHzD2NvHn6vF5x1AF7wd6MZLn4dq8a23dqLNVMQgrCjhMPg
0ZfkhHqq+LteKbKrMKxpf/gGgRv9iSzsTUnj5Pk80ylYM6rKALxT6rr4mh3LJjv1
CpPCHlz6aDiSPTp+gEYX9DkXyko0twWnyDAJuApBm51xF4gssAfHxKswIJc2hm+c
Yemzx78ZTqQ3nddVR5EDEYYijhwv/t3gykEQCg2e622Sv7usZ+u8TwEwmwD6qQjA
r6X+6YXpr3hckNLFWbfMD9lPY/lXtSTNVoUaI4haPvMu6aHXyem6fCFZ5cB9EDUP
Mq4eygud2ZWgGgzaj7I5VVJfjIYEGf4pgVgH6o9OeHhroHYPZphm391437wPImFK
VNaQDePoXgxas93mbk3Jq4Ycm+blCuHWUdWrGpMuOzZIC0AO8RzhxRYTb6qtCoAR
bL0Gnn/Xyf7WxKVUM4o8hryA5LcVeXJFPbYZvy7OPbqSwtkf4w5NLf8fWQAxegft
BMxCCHOOnZC8BNFxU5N136h3DIOlVBqsO7yOg9NNVRS4St5FdZzKxSdszWlyGiKI
mLhrS+Znnw30eQBA4nc6/ZhdhcTaxe3lYHZ3Ql6O9nPf8TmXdb98sCQKkxIszfKA
Q3o2Ag+D9wAj3mxMwLBOG5ZEs40ngwcg6Y8p8uHYr8RaC3karUl06AD/2uee+sw0
```

```
JUV/xQBKHNFTgBUMfFmHg/NrCNfYw/cGHKvaaAsa242FmolnW2VUpE62VW0js+zE
4uLm/fB1pWguNGJZg0fnNh23PirOqd2q6c5b46Ze1cDAPMNWzLn+CQmBCgWbjma2
2ty81K/s0eYNaIhvsStdgbRU7XkQufAbs23fqDhy1pVZf24PejQStuKuqvd0gSaY
+GSs7bxMp1Xf2Uk8aIKGfwLIWUccgXhzhsHsVsvwgA87cyJoj2gV4QhvMdMYFnMS
DNp/9EM4zJkNrpUZGZNJbtSDvdKSzAxudHpaCLt4UnvOYtyAJ2id1TSKb3VLaPTl
xnG60LijpgzHxQMyfX3btpW3okqyM7JteW5091rJj15u43i8cxdO4rzYfPIhy7xK
8vHA6aVDZdWW1UEU/GKNqKu6p5Dv0eoTsKkPsll008RQ7BGbZmJbQ4vC51huGXFD
41zoqmvsF2oYBoXDFDfsPhTyfTqwgoazzvKciYxbd4aj6usP+5iYEDx4ktnLDe9B
sfT0M5PGCelX1BA523bcPhPJ/qfu6l2WreTNGQX8Fb+gUVSX5vb2722qhycTDFiv
MM1FABqesr7ZzLaTCdeC39NV/oHoF6F1PjOJveS5DybWo0pEdvPPlIqVJcolOmGm
oITVXnNAh2+sE2Joa86tPs8ShCDQIm4F9sM36kBonY5VB/galTErdnkf1xJQiFp9
Pxb+bjlxYJ/zo56viZBpzYpzgdjGL/zi9wCRrcSCLHIgw1FWRopFwlTos5m1sA6R
1eUyCtTWisnUwxo1ipXjgFXelFvDM1hnSSxzYov3Ntf0YxDcKHqIrgG5/NwV6XEU
SgLr4jQYpUvdLp8lU71UYTwDDmCyC6BdUE4yoVIvYdpY9aveSkMToUavTj+fn2EN
DEhVPp9MjVLU85AKeJhXap45HlQHBTgdE1Jl0Z88rlss4zxSmRgBRR+4Hx7r+XrV
wMpuKgyT/52RPuHBAWAVBtZUWSQPBbHiQUX6SBq0nQJAUKNWrPHwiVu+N2BTu5mz
Zq7Ky41FKMlhegw764vkPvlrj8iRvoOkb/UkpEhGq4n7gNT4KFxfA/OWKVqS1ho/
tbxiiCjrM3US8zmkmMZUWOmPAgtcKVQtSoBmENTRF1oPKZzes1KHckBY1YzjyAna
0Gyps5CedP3lLWUAgsvm7wWgWFmc5artdPBFX8r1zCJVsLQBDjsxc3Av+jbLFw0Z
jq8Ft7dpBGbqq02rPxuFdrulntdcRs/dnZNvqPvY0lMyGndTUYWQED8z4Tlhoegh
At2X68JHKDlAmyEZg/9PdF23iC8Sl6CTi4kkOKudDxh9tiXoOL9ysRkOXki6ZR+4
a+v1J2gMWSC08wWEjiQ08+9qI6QDO+ICAKGPpsiHnw1iHOp6+z1eqSzqwgG6xbEH
L5gyMIX3I9uB0+9+udXzqven7viLbI+L6a08HzvMkZmWl3ONhdlYyykVUtLGSsOO
P23Tm0gtgNdrGJEqMFPyaXpw4i5+OROcRBVVxnKL7bAKhgsZ6S1ut3gxGyYxhufB
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-----
MIIP2AIBADALBglghkgBZQMEAxIEgg/EBIIPwK5Oy64HopzilOFmlN1hROrZnUg7
1OP/wRLpPbfiCznkxasA0/wAg9Jzg9rBsafPJ+rM65xE35hGkYBmnJaA+k5iZv1C
6rSgqu0iIN1+x/9XyKm5Ohvmu3QmS0Kf84WZ9Mgfqiggky+sQW5OM0cmdGQ2yyWr
nJi6vKb13F8E7HP0J2ZwYgADZ4UygRBTJRA4NjByhHJmZ0eHdHcxFmMXCCF3BAQy
ZTAwEIJXWBQng1YWGIaBF0IEEmh3aDBQcIVkRBcTVYEShzJFMFNFOIIkhDhAWBN4
BmhRQyI4MThRgWJGZYUiYReIQ4dyhGE0AzFVUCdXBxYFE1MSdmEQYoJhM0BmWBQG
AAACeHJWEwhzYxEXRSGBU4MwhjMhOAcnMCcnFXUYgigyMlBGJCQ1A1Y0ZTZRMAFl
cEWDhgElNHQEaEJ2cwRzhnIxghgggDUHZTQTBzhCFxaFCEhGI4VGQGUoOEISOIhW
dgVTRSgkJTV0VFIBUUVkI3RjhHhEMmhlJxNjMjdhcXETZDczAYYHMjiEQmWGRURS
AIKHJXU4EmGHJiQ3NwF3BiBANWAjBiVECDdUN4QYgzg4hzNRKCNhQFhBZnQCUTJV
QwdkQRNAYFNEUxaChxhYdiWAAoGAODAVEREiV1NXgQYxdngzB3RxISWGNCCEhgFE
FEFohRIUUTOFc3Y0YoYWhIdAACESQEIBiHB1BUYHUAc3FDA4NUUkCFIUg1NIOBUU
hRYwVCMIcQVCYmNDJ2glgDc1MWNkgxAxcThTcXByQwd1ZSQEYnQTKDUmGFJoBIQk
UxQzcygxgWBwUDIAIgYSMVUiEzR3EFADJzcUeIJwQkcTcmhwdyBBCBBgBwFFgREH
eDOCOCBUd0UGY3VjYXCDMHBoE1InQxcgNCRIJyRIaBJIGAYnFHdnNVYYRBM0I3Q2
BHJndxIEUzM1cSiFghZGEwVhIDeBQmgIgFVoaFdYhQN4dyQIFycVEwBmE0c0QHcj
F4GHQxQTNDSEIiJgYIAjhVNggQNnQoMyNwAYBQIhByNBQAQzcQRRYRhxhmMCgWhI
MldmIlNYNEBDRWElcoRDB3NHIWBgBmeBQ4glBxYycBcjMHOCVBgBYTJHA3YhFThA
```

```
BEhyhQRlEhczBERxOGdIMxECAkiDRxFYNxBoJ3JgEggFI2FkRmFAgHMVIQJzNCJU
NBAHNUIjhDEVAkaIckhwM0FldHcDQmaEZlKHd0QwBxgHGAgQYFNWZRJFEFJjEjRQ
GIhiRIWFARMYVQAIJ2EAGBNkIzdWZ3KBBzcFaDYYhFRYVAFwI2MCOEUlGDhxMBVH
NAJ3NGhgCCJxcDgXeAFxGHQjARJCRTcDiGiAI1JhhkB0RRQyaGJhNVI3gXITAkeF
JYGEQWdGERBFiDh0KIJ4RgQhGIg0YVNEMQcUVAQmcUMoUGcEhVJFYkg1QnMjZViE
Z0cXRIEzSEISEjQjZnIjAzUEcUQ0JUFThnJFUoIiJmCGBTUWRggghnEQYYREJVA1
ZYI3ZhQlZBZnZjVwcWgyE2iIIXMiRHRxUzh1dEgnI0dUCEVGYWNUYoQ3MYhFc3IA
FlNSEUcGAmBwMkMCglElRVEwghc4RARkJgeAhIADYoQRNTiAAHcFdFZRKEFwN4Mj
AQBnBRZCCGNygQiCKCBlIhh1ModURQVEGDMyA2JxMwJgQIF3AIJVJGgSRVQxATM3
F1aFGCAnFAWFQRc1eCGEg0BEN2FjBVhTIYhwUoYjIlUDcUVCJlE3gRIEZ2cWeBhT
JIdQYhBDhkJAJ2MoUFB4FwdlhQKFIxEQQ4iDA2SDYod3JFRheBcDZWQYIAIBZFZ2
MYVDNCQhUzQkY4h1dnYYYXgySGGAaIgigURGaGhXAxRnEiQ0RzFoNFIhBzhXZBCG
c2Mmc2UGR0N2YzUGRwJCCBNwOFWBRRhkZIiAghgiAWGIhoYyd4VRRIRXZYAEU3QX
hlQoA1KFE2QghYAkFYZWSFaFWDQ3hnhidHBAFUNiZHSAdoFzBmEFRVA3FDUQAGFE
FYVQJUFzeAUXRwEGSGI1RTKGWCOFM2FWYnhzWNdbGKmjgF2DDtTdyEgFN6ES3nDz
pYC5eyit4aH68I/JsGceAdAMu5NlOlOJkcU5GyWx0dSkpQW3I7bA7jpKHmCiYDYV
Y+1NSz2nIHCXVk7+tF2XyiccP9U0fS0sg4pR2qArefbV+6C1fnvPhGvwOBn3Gs/n
2UUUxQMWw8UnfmjbWqL5rNv4cBTN4gN1Gl7Rdlekhh5fR3ePnrbBHVgeisewmxFk
w9aTyknTFpAhe9nvmPbXqO/ELZqcoV1b0d/UNb6Z+lr67UU4EJPImOcVJfuOsxop
3vuQF/azIAvnwOkrVRJ6CG8t9VKOqB3wITU8qXFoH++7q4HZ1SOxT7uX8FBi1smi
wGQDzyUw5ZeUzFZqf8vwJJMZYsypUlfNxyzYyKeDa+AeTZBiPnl65eXr70FAIyaF
ai9xpQXydQwKUg8dQC0bWlecFM6lFAYbQkf36P2e+G7hCBVTuaTE3QXkrMPFvhcC
C+eDmZyVjlZCmnUvzt3Ydk74eLDzYnXAdh1GNOhESR3fCKj0oWkw0ErdeBUNO0EH
lT66USWcw8F1+yrKEI8mZs8vZNCJiWC84UebHGRsghMPuHjXspHM6ax5bxairkGQ
Db7xwXxxiKxA41w5XGwuXojHWNilZ0qa6ViuSjOA9visMVT81odo2GgDNKJqs8wK
ZEaEI3G9ACUID5iBHBMmKAwi1P1baQtfMgTzOyM5rO9NWTyzDvnp4lwMcrs+ZEKM
nEilPvjw4gdQLk99dG/1jf7Mwsw7uIGkuhiDfcxPHWQVYYs5/uhJLHccHcA2SZgp
iX+CUduNci9HFf/lYg/KpMRjNBxJBhJNmFBWx20hkAxZrvxzLTMACPvHFTjaMTQB
hGdeUjgZ6ocB8aJc6c/Sx4mi2wXSRrX9zPaFburp08RJAdQjypCdJQeej4DoQXTV
0lgJvSG325WPY6o6urJyIkrAv3Z5n3fcytLYsLTDvhLtWuJDhweZRQ36oFTJqa8m
QZQRutUzWVWzJMZNdmSkZw6ZpxQJOMff1vAPxMKrvgjVG6wYz0I/nCNKeq7NP2jI
emlrZNs8Jho6+esnuxA2x5sKxJ/SeGtyiD+dIP63VlNbzq8VQTtKqV+b1kFQ/EIK
tqt+QhFJxlye6m8KUL5e9PiGDp5qO8TPjL2pNOSqo4SRpkiZ3/cwsEAJgoCsRjxx
z6YIrPjMV07yCLaxOZZZ1scI87aftu1RupJQxBs25F27IHq4hQ3WI6yl/JkSLjUm
dnDIigKE1VJwzeX+rvxon3SKLldQ1/V5/0K5l6ogGcUOqQsXq+PRurn788qGrdK/
5dCxw6Kp9HKfIERo/ExlTZ/6cyp51I6hCyn3u1ir/iNyn8gBXl9PID1ZpG8J7QEz
a1wMTtk4ReuAnhSxgb6Vxpuw+s/TzoKEntBZW1m25yYR7GqtIEb3dWxMfNeRavlQ
4y5NFGqaSBGyhlRJWM1yPySkXADYbJ0Ga2DtPAMVaWzLX5GNdOSy9E4XfiONIMTA
wSIy5yvGVuzDKj3uTTO/XLcSEPcY50tJnlV+oAv4eKznkfLIxyvaJh+vEyAVgqnH
kbV3l26ju/UuFRkS3+SF8/5PSpgI+5bLwSGfyIFEwb7AnAlIfOeRa2vS+XuBaqn+
T1tHr1P8PtMF/yHyK5zmA0oLCo1nSZILlcoUjFnsxBQdzuKTza5E1qpJ0OhoN6Lm
g2EXcOwcW1QCxMe2arUFkETRq5y2EZskZMop+I+vFvH6q1cPs6+P1//k+UAIqaRl
NP7hbNSV1sPR/92csBLSF3VfyeiZOpd0TpolBwNzRxhnPTaQStvUbtGrYdWzTiSA
6GSFIGJ7EH+ag6fYjWP7YVpTAgLoXVf4+NOyGXOuuFvr0yZ2aa77sGX/Q8RmcuvC
TqpTorOkkf0yBxnpNTMG5djRxWff5H5eN0B5JlzoWyq1JBdOaCkkxWXdXAyDoiRe
d2sN5rL31F6yI/hDHje7tMPo9C4D+bHTr9b8Tn+O7jpJKwzgBGUEc748ujBShCE5
BjyS71ItALfUdUcuVLD0gnMmSlVrBlpsdeeyIntI06PX8h/BoU1kMvdue6Y/04ZQ
NLuvOtForWBzrFDAO0hkf8348E1goOBNFjOcmYarsAwAkG1CR0l5H2CmZ2cL6ifv
V88oDNvor+bnaDGqLTgOxMeQGgzCP6qS61Duc6MUAa/zJhHPyJ2dDXd3u519gLCx
VOyGYerBlXvSwNt1DU2I183lDxJo7ojyDg8h1Ep61JQ1lS3pXawpyJuh4qAdcZb/
BkOuWiMzFH9k/vZall+jOzgfFa27cWrPU7re15j/zG0kU67v0T8x3S1ZAxRLJ9yl
9WuUewg9Ok2MvVGKC1n1dz7HQBMEFhpJBnXLHNxpcUW2eRB+4Kf+XAHBwD7nsMxz
sG2cagGLclKcsDojQb7dTeN6hPMjvoIwgRUodKUbfEW4P+cvmvI2ZPZRMuuzSjGY
```

```
kOV5PuvBoh2ChpNTwtMJCb9kCsTOtB2L06z+m3tTcJ712NAdYpEzMSseHSEe9G9P
mbS5PP/b231ykP3cKO2Jk2Lct7pa6wkLRJI/x2w4sq0H1V5tTWO10/8156OOEeHb
fRJLOqOrQlHQXhxpNdAhjZQ84vqKBzffn9xLKd4QCWBCkcK+9FjNsEXPojhgCzxy
hIersoTIA0NXchojeIHBGFcz7uSEDitxQ5kRqwdUwPIuMkhNnhkF0f42+gQ/6L2R
MJuFCbnd5i8slOb+dFcpP6EDr6utSmVmtgHm1mnTEmeL5TxyMsHliofaZmQblyTK
/IGAH/Ez18dHNmiATUkwM2cXpos/lB04xTlc67d5W67j/AquDju4Qd13SFdbDUkA
NSC+ksBMTRALMcmX9GoY8uQD7ao5ipagUmCjQj1RypFtHjWGlURcYMnbCuIZPhYi
TFDtzO2OrUR1M6fyffuehfqrueuAl84ZJ8h8D97mVfeyDQnMFHHtoTA1Ey5IdGf5
TxnLheS6BXZQu0vaHp2vjCKJNyr7+YqBpC7hKuSOF4T0qmb72KJRsxW7gDcNWWgC
DdGHe7wY4BoabflCOxifax8Wqwfo3ti2iy8OtQM3tPp/YaF8eAsLp3jpqGYl3KUO
2h/rWDHkN4m7GorYq/ZoCYn1ugLu1seImj+HDrZTVRhpUAZXyV6cBdIeSXwAoCAo
CnEh/kOvuzVeqYH4K6Y1O6FuLAuzOpl1AjRAN3rnpJULtDxxI9TMvGKq30m1cA6y
Dj7EnwSsF7BoYFn7jZHwtFXczjjTyFvFnByftemJDvFywvB/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-----
MIIcpDCCCnsCAQAwPjEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECxMGUEtJSHVi
MRkwFwYDVQQDExBNTC1EU0EtODcgU2FtcGxlMIIKMjALBglghkgBZQMEAxMDggoh
AM5xelVwAnBZd6BpAyyzJjPQjb/UBhQ8CzT9GYNDRT3zJ4icdMwqpGupWIIBZD2S
+msROQbmw4jRcE09ZrO8IV6UHXrAP+Csf3H/w3M1m9SB7DOgbqLBHTdWZuP0Jl5K
VkGi5yO8z8ndT50Y9ieUqLRHFwsntDJgd+3cV4yS3sKvYOV7bzMegMmvPDgqEaVc
Bj9DBKnH1j8F9iNAXA8TJJeS/D1I0kGMrVZTyuDP4EtfehgJweTz+hVJF77t3vlN
ea7ynNN884BUPbRw+QhKkcHr2Kjz2WsKwKuo2GIp99M4KkAM02qECzbPNCEAOIfv
Q3FpvUWX9X6Z4UxykCH+sM+d12cfvGYSmNBl+jqCM280c29BAzr7a2/yC2G/fdSW
3+0pmL+CcmaxhIUq3NSZLFi56wiGQaE0MyDTrlBf4s+Qxk+58LIty6njS/KG38oM
xgIR/QZBkvPEGLXACCM15snADsNi+Lebw4seIJU0G6+bVqwouu9bDzViKX0r8qXe
GDoka3VTSBqEOdwDymbdcfB+9sjWWJ7Kzwa3Ek8tePPv0Grz34QBfxyN/mGmKdQl
DdGD/YoU78kps29VRzAjWGdtikgXulTtMv7FrhVzbQH+HayAaH7BIQtj/yzqDZY1
dzUgdMXgAZqvOjKWCpETAXHfH7N0s+WxtDu5BKmxyn8w0dncoALiAUMb0Hsz6oMy
P0fXnaos/sWroU2wcyqa5MGeCcw+4DEjvPeRRMyeSkPAjQwrQpOWs+0MOOItoDLt
6hzQ2L6hrkv3/dB7Ggz4hYXHGOw0bjVcy9x5tZTiJ8X3Hc8cApUtIc9jv2yXPGdQ
BCN/mnx7co7FwUfMiXSqoMkprpwO/VdS7Ug/cQI6YyLJgQVVjaLNk6zO9NbrjQL/
ujg6onhzO6i1OBSBxa3K+R2QAH3sHCJnhl9r9Rle+boKO9DZSjKV9sr3tGTr7UsF
sRhmaXdbr4tPZQs7wGZWOHfZpJ2ayqG+l9EBqcjWU+RVc7m7u1QutUlAd6lT86gb
3CzFLTtimjqeJVS/D4sPiHRgjA2dEd002rADBwIOXbqERuK54jCmED1OuyNPitAy
0TTy/yATBLWVCKGJWwuafXS4n3oWYFfY6HV+mRm4qSwbDhOFlrBP674TkclINgFk
0X/+Uq08c72EC+SVAOxC9sk7ULwW77gngjTFkEdDSrMo+XoR1Nbiv8DRhQh9vLBM
```

```
svmIJwPK2htIrQLH1YbNxRcD+/Mos2occ72WdkTO+wWwyvHARzflpsvi8syZLYG4
rEz47ayWJ5pXhjCHr6u4NDHeb2dPLbQSr+T2kwO6CyDZ2UOpp5+6qztl8LjMhsFv
16T7ebbdD3nwSZgaX45ouJO149TxlKTuH/XdU2ymY6N8UqdHcwnB9weQLXyDsjMT
cwebRi4CNO7Mxm1/H71dPTG5jPI215HlIEtdNNRTaPWORI+fcFHCt0pb1QRgDFIB
BWodW3ubjXIjVlU5wbFIJ8qjqo99+Ln5FdIiWSFzUFYoZvIVfy2uEDR63VK89WrV
7TfLmASIPWeswA+91GkrSpOVyF8cnstyz+n1sYTNJChjjHB/rRoeStVrgIQVNjhT
M6UxrT/glGVNgclEJZPTc42dzbTZXFSNfQwWjn83hTBGt1aezGJy0sLaf0EZFTUl
iVZh9sh1HsMeKYY3b2coyTKu5gPe7zsmVTAkUhDa8gvZwruRczA+q1peqjLmp7zo
hdDI4FObydFnE3S8jedEfeHIoks1whU3FDrS2Gi0xHvJGwZmBc8w6coXJLZnPZRi
2MeTWh2ez7nfakhPdxG88ReiE0SWF2Yac+gYtA+Ej+uVrhP15+QRdNn6D/mmNjZk
+rJcl2JSjlYidwyagY+uo/sVhe/spEomd/1w0r+T/UiOLgmL1Aef/V23viFpTV8S
LKFVCWKwa598n8pUpfjdolp8rTzSC619iomTbrgX2ixslaESkOkHTJXid103e2BC
SgwzzJwlveWcwVeAad8nVqFP+mG5Sd430H93CvDuGmeTRlu4Z1By0AzDGeZoT2mB
c4qdqDwSDjSWfptOmZF3LtyANFif22Ds8wPynE/LNjR6q0GUrGuJFRc+evcYybwi
Eg9qiKE0SlMCiISrPEMZ8aDdrHtiIn0IOu4BfoJsJKNeoDPRne346hJnS2YC5OO3
1JOdmVeVOEV+HGAlZdnz7YnqdHQo7iF3q3zNGq1mFrlTKKDRVvd7C631nuvGLBye
IjKoJZVEuonUXPYL7/tWKvxolsbZKJerxjBJch/igjKCCe4zW5DNRPwW0vlzkerl
SblvQps4nYQENSsd44yH2U4VN33ycaQms85KhxnQc2+AViqEx2gIa/BMKM7Alise
U/NH5xg5bsTIamYeL2FXFW/MfOty3wAsUZtUzRtfrY/DihfGX3Kl1bf8i0ehqO7D
AuWlmDGVTDrBPlfT1hArK/0Xa7TveqhwYZDbXW5qLcloOtzW/SKCw+CAErh69Up4
ipu1QE3WzW6kpF4B3YJVgIWeiyVhOTfnN/EIIGU6F7D5gUhTOkVzjOns9h1o8NRO
gPgJdsqSDJ3n1+MT/03s4qMTBbnHACLQmu6VIrVliQplafBbIiHPI5tOr5Loc7qZ
bkk3m4y1dIytoIxWFJJvUsUx3u0kygI/FGJwX3IME300ZxRPCey2OZlCWwA5tkxf
rorhVp/pnihMnDJA8m3ZNiRvLNAcWwYk957a7LohSaKo5uPc/txccAI+44M1vkOQ
uUWiDNTLFzZyLxi9vgcxJD4vjnD7lF4uD2eKynAtfOITmzVpVVsolay8C93HW9gD
5n8ovAP9nH5/vmoT0VqsshjM5oBA/vnixh63pWoKnS5gu/5ecy/SdHVOksK0S8X/
OflnUlr4TgC0r2b1dZ0RJ3G010NPr2uJJWOitBapJT5qQ41FaY7yRdAXigHut2hk
D6ntUG6ETw7vZf9Ecaw+Mmmz7Od0Sfv7WcqDfGhw64+5+OGHRm64fPtYNKbncmLo
+oMuMjWPfbnrC1uPTRUdw8F+R3isxvJn7iydHp7cQgWaoRqswopLRUjnv75R5R0d
SM4Mwi+gpxJ35JzPU9Pk5q0lv3O9SaCU7XiXwiJcgLJpMlEwS4T9eQI6T2HMeCl1
CdQxw//uAMkDtgBbmua+RJFG6XoEfIUMm7xPlwsSsuUJXaZ2O5a73OT5oJLSd9PX
5W1fCTdrCrQVJ0unT57zjKxQgm5ll/O6m/yTMkqDjXri97jtejZt8Uy1MTDNWd86
lQtbEJueYJZ8D/N+cyyr1NvOCEpRmFTtmXY1E1PJvzFk9ETjAoIys8eOYc8YUTp5
IE0dZpDE7YteeJ4zXB8gv1pPIPaaHNL4JOaXlUSQtyjINd9oZnHMSjjsTc5jeIdp
7vywjsrUNy5TafkKHdvY9UxgDrxG1bsiC5EVB+syfujdRcJFxI6hYZT2136//ZNM
H6AAMAsGCWCGSAFlAwQDEwOCEhQAmIhbyanPa5XS5Sq5PQYtB1MmV+ZvbRxo7gQ7
SW+tO2Ynvcf3EEsg/mLGz/nf9ELqoZSbbqFnhXoQC1oBGXhxd8S30quIxbebjg6T
OaI99RLlBd9fJGyNB22gROvoXJCeaWJvhG4z0Ue3M9c0ted9cePW0PgpFaufGHQm
TN7eAQ+ufzbBLBjfYgAmhuX2I2OzkmemFmD0L9z8wt7fAr/apBvr75Bee5cCIr3i
zNta8B6Eqq3uJKy7cc6N+FJhqpdJgGr0Gtzn/HA7m1WuoxYDq7qeerZqufIRYKJb
hUhokcJeE4ZcWaU9aTEBbTv1TDo06ikkt20xzIPNQoBy4O5DDusHkSHbHdsko9Op
QYyXC7H3pzVgqNAtC4zK1GWpJEQQJ8u4QDKx/WeoWipSABzgzPgDpfIQ6t+MMEat
wux1T83RNTVGYb4gc/DS9HNuEsDM6inBrRSS70QdXDuccef+mul6uwsgDO3OAXYf
WbrdMZdp8PSigm2azI8FQxiHy+jWRJPx5Cw7FzbKjOVrUjUW1ASx52asJLs9JUIs
EO2H+2/4gvkxRdUiuEnSiDrSXjFo7W3EVnhmX3VOr3Q3a3Ewb3mZM1Ubcrt3t2nc
NRzgZx4vt6NyN9N70j2TMvgAKLgUQmDJr7buZDk9ztl8+vyifUKTQk/LjyXDI74C
+TKF9AC0iq8iWFl3b4xWV6fO4yCX4W85AE1yVwxYGIZCyT8/kanwdMx3QX/u5fCT
gTrDa099fpFe+AXei5h6mo/1PXYr3vwn6EF8HJzfcIASraJ1DtkHbN1pWgJFkhmJ
f5uF8yByojOMXxF29YzgHDcZ3iPUQmMmXZLQqDQ20O9cFB12GAgxpPrC6rkwY9cm
ZNC7eLAist4pgvuu/GYZO86ddBGWolwf7EJ7vHuW6yLEl95/xiDvVo9CXHoWcYKF
SBxXoQ1j8Stlp0qu8KluTVH+mAStErdRDi0UOU2aPzzDCaH2PTZiPuGMcWtV3SIO
fTVnEvhY2xgqPLO26rnBgwwPnen8c13bUbRHomI6Tvbed7cpOuHf1YfhD99aE83x
YIxriU78f//Vw1nNI0+9oykJ19qXq5UZONJ0pWvNQIWey4Q+ahg+Bvn601CDMBYx
```

```
rgApN12AwzIS3D3MrmF97RKrVZg3kz0udG2sOWO8Y4t1b75V/JgX79RvybE0jo0A
XQUQjsi+EvWEUz1RRGmqxVLSSeFWMKck7PwIggPu6kJ+qsFvBrQYLMEDpXFxdCo2
uArAkI+p2Sf8oTf9WxFXJwmqoYCrTJaAOwloH3zQWa71g4g2gdcewKxMCxyzIOF8
FWo6lZ9poysKV3TNDa01HTo8P7lu6ECvuifAv++DZSiCFDuP7C9+W/nX+QzkzrUB
N0HUrPEn81el2umbWFFxEdOMmnF2Jiv6Dwp8u+h5n1/mE4a5gxFwkeY24ef018b2
mnqTngOM++6GAO8W+ScpeRE1qpn2jSSicw3tZbOPT8MQAbomxNQI3HcF1V007/BU
/TXQJbZXOgnpcZ4R1sw3lFZOX9h3sOnw4oPDUT5EmE3nU1yeykJmX0kL751s+Fsx
n9wXMxICLGeOledWe8u4X5T89Vib7A3LcSONzsirGiUgWnvNFDG9fnhWb/eevw7N
pZ6ofsFPD+v7Id49DbTjdn06SBa9WJLpXsNl/BvVoWfZpP5XZvmTrDbb32y3idUi
ytSXvkrdlI2sUsHQtDtp+JDtYXOsMPVkzVoLkvhtDZe6XpqL5kC/eZxLVFXpmTp6
J0eyKvkt7efG/SMlr3Bl6dX6DWn3YaTLwfoB4lbU0uw9xjZ9DoPSYnmgv1aoLkyc
BWXJArFRSLEcRbeFRnuFtw3NCRcT9hu6+p9RPtp8u+Y7gfsFC8cu1tSxr2lxsN5u
FkJIXOdcLGF9ChqcCE9RNThpqNiK3+MrYlErhuqvaAzzsvRUpVTiz36WCSOixuC5
0TPure9YjzxsGQyi00UiNXLanOYwDrN3iNtDAuvdO9tJ66HajXJ7Z/xhFcF/LYeq
Fqk3GRA1fbxxNrwDqo4TX884OVBr0s4WbThpCU6FMFfB/5wlDveEvsZV25mDIReU
4o/pFNdD2vyMxyQSI1XXn/S61jaQ7iXrbbznb+nOyyDxoFNSZ+S97fh2pwZHTEC1
fjxHOZOCji9VK22/M55V/hQmyrkM2QvoypMoiISrk94uMMuyk9O6Qs/P72UNajO1
op7/4xN0LNNKrOWmRIZ2J+D+ceDwnayiXJxe888VCJKFESnhjjZMh+AgsJTj4X+g
HAsfxwRdg7nwAaJTA1wy/StO3YD7TyUyhEaLDDqsrQCX/ku59XVxfILGMC9SZPQA
S60lzBXpKT7z62yqYy4OnrvPCUIeQX5vQ+puMJfEnK8NJ4S5qDG5DNxu9cW4YUs3
JzUYGsPfAJhReuAzzdBRRAa+K1govnEw+ruRtbFtL0KzEI/mT26nEbesseZ/TwVS
l0XIOkQu6e98m8f20sUFRdM/tazRsrC3RMNZf3NafwAphpvpbSWCiE/XNcrNK1fM
R667OaDzd/qjFiRGDOoDDFZpyZxOaBuiALrxvZWnVdnw9zBVfh/rM7ocmrVEPGra
b0RFrxNRf+LX1u/DTaXq21ZVz/WBE3mGU4zir+AjokRh2DKq0qCUjI8J4jpDcXOD
01MPV/ZdNxd8/yaVATwoQVmrdff7SXaQixI4vxr+tUsmQwiOeXCbElSk/Sj2BosA
kszW0ZlLsBoBVg8bQDs5Q8hdZ+yhBQtfVaISVYTMD7Y8GimVTK85ZJfxkEftsn7P
GSyd3DDAGhUqwNizi0kRlXZc2O98omcQ+BFqbB7Khh1gdZd3Ch/op5JbwvZFrwbZ
4QdHxRGR3s0jecQL9cGwOB16ZBmkcimFgUwxO0Q+ofiwQW53TEkmp7bY0FE8eavP
v81LvJOJzrS+S6gJEBrZwPUhMMJbuCQ7Tl3UvsxHvZke8GZuQ+VUJ3TsDj0motuQ
YfD8tmCPryv6/2642E3Ef2e9AwfbyxYf4l5DVcUzEH13BI8Ifwhlqmxu83ZDihYc
SJF343+Mtvgt41IyN7Est3f04lcJ1CY4ZETAP6kbBq17iHzcK8IlkbAjAU+h8m5c
DMiUjOSpsG4d9e7bwX6nxE5Un3Sw8tUDN1jidCBaitLhxRnaWg2I/36WCG7eSFeR
dK1FU6yAsCnSKaiS/25GLS3sKj7w4/q2s16JS/QHscF2bYUAUjuGLKWXj3xOaEDk
yLIH9SmkW8H7yOKqAxINKLXYjg0Kfe6c0w4+RoCd4NAk3peufSZUoKwB8DkQJrE0
aFcFR4JcyAXr1nLyr10Yohlsx9FzplnFW4xfw7aeBLTkpRzxUZc/uPmoMw75BCDH
npi1cLAUFxDOGtYWUSwqsexLmqpwaxdG83QTUuIyc3aZU4pJZH8iDbNLfRZPJFpl
+pLlaZcvpwa2C1nNrGF726hFsOkuXnC2HnYSVhf3yOgKVjDhgTgDEJKzvkccIa2o
+oODQpCHBt1vFjhDu/4rQVqJGqgcLGcFbq/hcnRcHdp4p5rva6W84TjogkwQxiI9
227aevf7mfP7MoGjHgCIPuTF8WmznA1ZVR08cF2RkoxXD+iqnB75RqT8ncx1+rx7
wwM/DEPxQUXWOmJ4MD0Axmxs3ZQr/DrTPF1iIpYIDIpqE9YBgpjGoPUiTGMUPeNz
2uCfAaM19AG3csIEKByYI+WBJDSu7aKEtQhOSqwroLEPQTJQVg9sevMWM50Nhrfs
vg/p4qjuQreMoFGf5tfAgKlIH8MllVSjF5IdFI3gsZtQNNqPjBGrZzo+lTquPG7X
+jRthmMA2T3PPYWnhrwBJ2aloud9kULQSCTIleTK0sfyMivddNdCzrOPXFDYG8qP
Jr3QpRYx5iF/IF8UJEq9Km3qD4Gx0LKi2Ng43LKSHfr4LMQuyh4qTSUmDTfnt4br
4D7HQ4pJq3LkoQ9U288rhp+FAyTpVJEf37i8FVVhU8hm1gtabxcqhrf8Zl5xvoOP
WWAkVtK4MN9YMU/EI1MsQ4c7HuvDm9+/6Z1KuyY8LuaT3X6A9Q8tOyIt6eip4Hlc
pmGu5sc3EzdXajMn8tFZat3yZv/ZVD9R1xQb928pcsBjSz7AuanZ70i7BXsy10Cs
sHeLa40qlwMfqtQGgBg+XMoyN+ULPjQSksFsfxK3dIYjP6mBl/DUCVSIZ6FibhNW
fLKy+/jyeir5kncO3mwlsi3Cqv3eG/rFuQN51cMoHcM/NJwbD9AGDVgqUjo8z3kN
vS4K3VoaDLvPaUFU4qZhpr2n6ReGOz31XAJDCLkJ7Zx5spHVpBTI9OSdAgegR5tz
cHuxWoYAxL6tz9+/Iol7qXTAIQ20aQ37BgJ54D/hyX7Q+1ijOctF87WnySBbyU6n
qU8Z6/02HKqn75rTsFhzETd2B7gZewtd01hfA6QG1tK/Fu521ndaLCbqx9+iFOZV
5Ad7L6hY2gnjwfBDqawvEYozt4dNJ2gkR5dbJPc0BMAbOyHSITkSj8fYzkXVNd/C
```

```
zmwA40Ovtib2lnoyi1kvmy5h0kANjIWE7G0Elv5Aet94r6lN0txBBlpDbDTrIlN7
HZSWJ9Gnvm72L0KoPQjKrXvf45kYSlcOm/ThL0ebWgGxWI3JER5KN80/IfSFT3CO
JSyB7c7tcaPPEmENDoN3J7i/92TL86qRLxNJZczMw0txrkpnVokl+9OcpsTkfncb
Z7llMt7h0wE6DFyQwnMGVxNaYcO8qdBZNWmV9iGvJxnJlQizPwJqdLTYvbQfy4YR
4Cr591oPULwyikf8anHpI91sZokBExPhUC4JsqGnt+lzSZTESvepaxx7K8KDaXHm
36q5E5ozc9wSfmZdDlncvuAu74c3Dqww7x99T7Qq3Zbe1MWfU915gQKo3gW6FA1i
Bt7P3DUNyA7b7tEWEZSsD/I6KkvkBpKwEMs4WLncdP5CxkZWBQZdDVQF5KBIazjF
iS7KW5r0sln0mZUBLg/vCgltZOmvYZpjzI5V2MAVyaBa2G7COPARrrgm5SM1wLV1
Igre1n5idaMi/XHB+rr7Ra4nRtUtYNNnqVHQN91PuBrLVhLtAvOcD8ERF7xjILM1
ChubrOQOalS4A9n/TQZhC4n+P0t1lD1ASlmHJ5goinq/DPK4aOIc1YG28XhcIra4
RshRmhYYYqxaxzl6PijyEFnd0/c08Bv+fumM2SXlvdn4BEyiMCDynMct0nB0Pf1X
RnjUEByxv3/h+enp75BLEZ/jFRLFAW0f33eHbeI/xY2qbV3WNI7khoM4T5kmp119
lFtRfs0ZTgvkJXAD2CxkuIi7YO+03uidmf6DjZECjBf7a4cmwPwGzzVa4wrjMmZ7
9awIclaOxV7TrVnc8LYY5bamaWjaQ1bNSrYff78fDQAz4U8YbTlSCg2lJhH7bWiC
FrSy196rGTwwfJB9AF+5X64gPycq3MdcE84TXYQSqLZny+GynkTFedXQYEIxZJm7
4+6R90xf3XIiEwyjMtTZJkimWUgux6BRakjZkqWGEP2TQ+Jp8gnAFmfu6X4+L3k+
b4murPlZWpDi23rHvgC6kmoUu6Uqq3BPKSJrOR6Jkl12VluVOOzXCOE4NYPew01J
LfkrLDaMyKWuUkt6gVkhP8YyHutoeNVFKmt4EiVplMD+3WMYGO2HZZKo4fD8l+bN
nvBciJ163+V3AZcZZk3Ej+pS0EZRSuGo9EClH0zHtJlC9U7VOEIb0zHdQbqJkxvG
JQXndY36xbwGHhUpHzmIprHY5qi+IPt7Gq0v4ukjoEghqoE8seqKcEmczRc10QLC
/9RTNnziBZCCHSwe/vgOyNc+sK9GjcImNdPEXE1wzK3atFW3jRblEnnxlJdAOmp8
kvSj/nfVU7tlqR1mVMy2adXUw9xsn1gqzeZOEAI7y4cQ0k90MHJJ/4CXjP4AAxUI
nkHLG/PB6sFaKw58+8zr8ICkiYVXRtzh+iYqKQdGjmt+b87IC41CLUrFym95XBj4
q5GX1rzUArBFEsWdSggnFTjaRBbW5l/wF/FmzYJ9BkVQnOaNLjiJQdpkg380uT4p
w1ZDwggLD1lucY6fpa2usvENb99Pb4GgqK2ustPpHzxLYovc7/gpTlJldXyN8g8t
U3ez3uX4UFutws7xAAIOMDdajZaexAAAAAAAAAAAAAAMDxkhKTE3QQ==
-----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+msROQbmw4jRcE09ZrO8IV6UHXrAP+Csf3H/
w3M1m9SB7DOgbqLBHTdWZuP0Jl5KVkGi5yO8z8ndT50Y9ieUqLRHFwsntDJgd+3c
V4yS3sKvYOV7bzMegMmvPDgqEaVcBj9DBKnH1j8F9iNAXA8TJJeS/D1I0kGMrVZT
yuDP4EtfehgJweTz+hVJF77t3vlNea7ynNN884BUPbRw+QhKkcHr2Kjz2WsKwKuo
2GIp99M4KkAM02qECzbPNCEAOIfvQ3FpvUWX9X6Z4UxykCH+sM+d12cfvGYSmNBl
+jqCM280c29BAzr7a2/yC2G/fdSW3+0pmL+CcmaxhIUq3NSZLFi56wiGQaE0MyDT
rlBf4s+Qxk+58LIty6njS/KG38oMxgIR/QZBkvPEGLXACCM15snADsNi+Lebw4se
IJU0G6+bVqwouu9bDzViKX0r8qXeGDoka3VTSBqEOdwDymbdcfB+9sjWWJ7Kzwa3
Ek8tePPv0Grz34QBfxyN/mGmKdQlDdGD/YoU78kps29VRzAjWGdtikgXulTtMv7F
rhVzbQH+HayAaH7BIQtj/yzqDZY1dzUgdMXgAZqvOjKWCpETAXHfH7N0s+WxtDu5
BKmxyn8w0dncoALiAUMb0Hsz6oMyP0fXnaos/sWroU2wcyqa5MGeCcw+4DEjvPeR
RMyeSkPAjQwrQpOWs+0MOOItoDLt6hzQ2L6hrkv3/dB7Ggz4hYXHGOw0bjVcy9x5
tZTiJ8X3Hc8cApUtIc9jv2yXPGdQBCN/mnx7co7FwUfMiXSqoMkprpwO/VdS7Ug/
cQI6YyLJgQVVjaLNk6zO9NbrjQL/ujg6onhzO6i1OBSBxa3K+R2QAH3sHCJnhl9r
9Rle+boKO9DZSjKV9sr3tGTr7UsFsRhmaXdbr4tPZQs7wGZWOHfZpJ2ayqG+l9EB
qcjWU+RVc7m7u1QutUlAd6lT86gb3CzFLTtimjqeJVS/D4sPiHRgjA2dEd002rAD
BwIOXbqERuK54jCmED1OuyNPitAy0TTy/yATBLWVCKGJWwuafXS4n3oWYFfY6HV+
```

```
mRm4qSwbDhOFlrBP674TkclINgFk0X/+Uq08c72EC+SVAOxC9sk7ULwW77gngjTF
kEdDSrMo+XoR1Nbiv8DRhQh9vLBMsvmIJwPK2htIrQLH1YbNxRcD+/Mos2occ72W
dkTO+wWwyvHARzflpsvi8syZLYG4rEz47ayWJ5pXhjCHr6u4NDHeb2dPLbQSr+T2
kwO6CyDZ2UOpp5+6qztl8LjMhsFv16T7ebbdD3nwSZgaX45ouJO149TxlKTuH/Xd
U2ymY6N8UqdHcwnB9weQLXyDsjMTcwebRi4CNO7Mxm1/H71dPTG5jPI215HlIEtd
NNRTaPWORI+fcFHCt0pb1QRgDFIBBWodW3ubjXIjVlU5wbFIJ8qjqo99+Ln5FdIi
WSFzUFYoZvIVfy2uEDR63VK89WrV7TfLmASIPWeswA+91GkrSpOVyF8cnstyz+n1
sYTNJChjjHB/rRoeStVrgIQVNjhTM6UxrT/glGVNgclEJZPTc42dzbTZXFSNfQwW
jn83hTBGt1aezGJy0sLaf0EZFTUliVZh9sh1HsMeKYY3b2coyTKu5gPe7zsmVTAk
UhDa8gvZwruRczA+q1peqjLmp7zohdDI4FObydFnE3S8jedEfeHIoks1whU3FDrS
2Gi0xHvJGwZmBc8w6coXJLZnPZRi2MeTWh2ez7nfakhPdxG88ReiE0SWF2Yac+gY
tA+Ej+uVrhP15+QRdNn6D/mmNjZk+rJcl2JSjlYidwyagY+uo/sVhe/spEomd/1w
0r+T/UiOLgmL1Aef/V23viFpTV8SLKFVCWKwa598n8pUpfjdolp8rTzSC619iomT
brgX2ixslaESkOkHTJXid103e2BCSgwzzJwlveWcwVeAad8nVqFP+mG5Sd430H93
CvDuGmeTRlu4Z1By0AzDGeZoT2mBc4qdqDwSDjSWfptOmZF3LtyANFif22Ds8wPy
nE/LNjR6q0GUrGuJFRc+evcYybwiEg9qiKE0SlMCiISrPEMZ8aDdrHtiIn0IOu4B
foJsJKNeoDPRne346hJnS2YC5OO31JOdmVeVOEV+HGAlZdnz7YnqdHQo7iF3q3zN
Gq1mFrlTKKDRVvd7C631nuvGLByeIjKoJZVEuonUXPYL7/tWKvxolsbZKJerxjBJ
ch/igjKCCe4zW5DNRPwW0vlzkerlSblvQps4nYQENSsd44yH2U4VN33ycaQms85K
hxnQc2+AViqEx2gIa/BMKM7AliseU/NH5xg5bsTIamYeL2FXFW/MfOty3wAsUZtU
zRtfrY/DihfGX3Kl1bf8i0ehqO7DAuWlmDGVTDrBPlfT1hArK/0Xa7TveqhwYZDb
XW5qLcloOtzW/SKCw+CAErh69Up4ipu1QE3WzW6kpF4B3YJVgIWeiyVhOTfnN/EI
IGU6F7D5gUhTOkVzjOns9h1o8NROgPgJdsqSDJ3n1+MT/03s4qMTBbnHACLQmu6V
IrVliQplafBbIiHPI5tOr5Loc7qZbkk3m4y1dIytoIxWFJJvUsUx3u0kygI/FGJw
X3IME300ZxRPCey2OZlCWwA5tkxfrorhVp/pnihMnDJA8m3ZNiRvLNAcWwYk957a
7LohSaKo5uPc/txccAI+44M1vkOQuUWiDNTLFzZyLxi9vgcxJD4vjnD7lF4uD2eK
ynAtfOITmzVpVVsolay8C93HW9gD5n8ovAP9nH5/vmoT0VqsshjM5oBA/vnixh63
pWoKnS5gu/5ecy/SdHVOksK0S8X/OflnUlr4TgC0r2b1dZ0RJ3G010NPr2uJJWOi
tBapJT5qQ41FaY7yRdAXigHut2hkD6ntUG6ETw7vZf9Ecaw+Mmmz7Od0Sfv7WcqD
fGhw64+5+OGHRm64fPtYNKbncmLo+oMuMjWPfbnrC1uPTRUdw8F+R3isxvJn7iyd
Hp7cQgWaoRqswopLRUjnv75R5R0dSM4Mwi+gpxJ35JzPU9Pk5q0lv3O9SaCU7XiX
wiJcgLJpMlEwS4T9eQI6T2HMeCl1CdQxw//uAMkDtgBbmua+RJFG6XoEfIUMm7xP
lwsSsuUJXaZ2O5a73OT5oJLSd9PX5W1fCTdrCrQVJ0unT57zjKxQgm5ll/O6m/yT
MkqDjXri97jtejZt8Uy1MTDNWd86lQtbEJueYJZ8D/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-----
MIITOAIBADALBglghkgBZQMEAxMEghMkBIITIM5xelVwAnBZd6BpAyyzJjPQjb/U
BhQ8CzT9GYNDRT3zkKZQXL2gtwFz2Bz+sc/vtd+9G6KAFV07h2V6+7SpgK29Ostj
U00Tvm7FP3XSdWLDykUQrTVoFLB+na9AItp8Tf7P/N0W30sWOBTzU+UFb64zgqFJ
Rv2bEIOOBoNujZ3RwzJGyCKEAURmXJKQQRCCwDaSUpggWsKNWBRw2gYgWoIMgxIs
IZhJICOAEyhuIBkkAwJEGRaCSxYxGjQuAUgxQLQti0iFpEBxQ5KFUKYFChMBSpRB
opiNzJSNEgcKCwKKC0UJIwJw20QACjBgEkVM4TJRwKAsVCKKhAJqDLklU0AIEQUu
2YCIGcGEg6Bo4LCFYxKMkkRE4qJlIgctGABMCCiG0oBNJIkFoCAqAceAwiiJGgRC
```

```
RCYQpDRxTLIFIAJmCBOQCbSNCaghSQKKDBlhVEYlCQkyEyCNiUIhCiMGIjNyGcUs
JLMtxEBSDEkNghgyIBhSjKSNIaUtwBiSWygx0AIykaIF4ECKGidyE5EAAkhJRDBl
WjgwgJIlSSYmykJxUwJxQ0aOmcABUoYwYCho4ThywTZsnEKOIMIpUkYMm6JEw0KQ
WIQEYCRIGcVhC6VIpEQxFIZoJCQFGQJI00aQICSFC8dpmLCJWhBlQcIFXCZBGskl
AsElYEQEISkmDBcEEYcsE5SMHDGKGhZIyBgGisJtQYAI2YYhIyQQWBaICEmEWkJR
JCCIJEhA2cZNA8kFQSKNVMRkQbQxQIYk3KQoEbAhEZcJI5SQCqQgAyEF06AsiUKE
pMJkCBQFigIpQkBg2bYk0qYB5BYAGqREGjZRJEcMBCRoCagsC6mFiLhgGRZuEjhi
GbYhDBEykiiKTAIGE0YB0ZAI0DZmyiBKE7Rs2hBlCZgskoBoITIBw5AwAJhFJAIy
2jYCGjlOgRQm2oREgMghEAYQCJlJRBYBECKJGqiN2IRN0TAwIAYsGkNGABkhiggs
wCJhi8JR0BJOmgSAmCCQDJlRxMBJ4BYtFDgNlAaOAhSOgjiKJJZMHKNEyDBu2wKB
26hRk7ZFhCBuCQmSoAYhyzgygCBJjBhRUQiAAZCIUDhAIRMS2gBtE0AlAgKGCBgm
obglSQgu4CZQBCciSxBBW6SMzKaIQUYCIzNgGEksiRYmmCgJkxAxiphAYkSQmUBy
GzQphBRqyqYo2sZNCBGQm7YoEROCnDhCkEgpACeEgTgAEzRRSDBNEpVEI4RhUwJM
AwSNxMJxkgJRiBRSlKRFQqAoQyYACQgxAjkCC7SIAqWJoMhki8KNW8QskyYyyggm
FDOQUzBKwkABgcRFkYRhQUJtAjMgmoAJUBIsWpZJGyZG0xgSCxhFIqcoCEglJBNu
iIIwELdpTDIGJLKISyBEIEMGGSSF20aB2UKE2YCE4SCRW0YSACgFWSRNFJEppDZy
AJQEpAJIiDIlmTYQSjBFzIAA4MAFIsiA4ACRA0ZGYEgGGpFxBKYBg7BgEqkNSkSJ
yBAoWUKI2jYtgTJS1DAs0kRxobhtHIhgwYZxksAgkpQpIpMkSsCR04IgGIUNWyhu
oLItoiiMQQYKnDhoFCBBSUhMWJaRIbMMEDgJQygFEoBJGoQxlJYNIQCJHIUtyEiC
mLhI0qZw2jhhWgAMGgKB25gFIUUiiQRSWMZxwcIwirIoUriFIcmQSZaIygQpEsQp
BMBhWyYgIyAGGhcg4xSE0Uho2pYAoAhiUaIMBLQhWZQwmoAo0UJJ3BhMisJsAago
i0glkESFCQBIGDExkRg5KKJmcJQFDBQErIJAhhMIINkVBJyIQCM4SIOQgZKmgZK
Q4gIGZloABgiwbaE4IQAoBBQJMOJUEBFlBIpIghsGxdi1CRK1MIAkahoC6QMybJN
gTiKwySN3BQNyKRsETVEIpdFCQJiQaKNEEhAAkUp1MJgEols2ABSQKZtYwhpmgYl
YrZoSSII0Shym0REGZGMU4gJXKYxCocwopSAmhACi5RIIicyERWSI7MM1CaFA6gN
wkAhSLQECScE2QQEW6hRy6RBkwgygQJwFDcMw4JoDAkuJEJIHMZFWBCGoBZECDQR
iqhN5DCJCjcRFBOR6oepimvp8nHPr8KTY06t29s5kKELOeoOdOKmUkuwscobjbu9
nVpaTAP0C0Q437jwkhrMBvaceUUGmJ/tdGl3VdcS//l3ht4z06nVWqnfXjop40BW
U51Srr52DHhaByGkndfr2QxksEPdgtXtmyluI4ehOh+uh2lvyocGdUCUOQvOLVTS
CXeKxCS3SsSbg02zhGIY066mbfLEvDIbUPvzu5/AMJhXs0yxFBwkUPjACjn/zoZN
zDULk8DrLVDotP/62+WyyLrZKK6NOEj2A3iYXMwQkpHcPac+qvRGvEujtpSyF9Sl
K01mHEU1KOtmko238KLwZ4QIv2OFMkbOWneUPJGfWCS6k776Uw1ZSR8WYc48Uktd
DA4AxJXGUa0zBYK9aagi8dmqF/ELk27dc3WVvSrts43REinQ7oKAuA8tVNowI/jU
FRpHJRbuIXachbx8Qc1jKFjfMpHYmGaikJm0Lsv97NISoYSjCWepkARtriem7lj0
785ZsmsSx5+8k94HHDfHP4kNlnlRJNGYX7leiRMnEprwZEUn9+6gg7KMoe8Es8CD
D47TGe8xby0rZhZS1297CjDk2VN756/wxLDzPN+zctZkx0g2NHYd5hhVzAdvBer7
WN7b/mu/ZjPYvADHg/1vgT668Y2FX5wI3eKbMv06yqnt+dWRu3SCYVkO90INjoj7
S6AmX8SDliCMtpUu4Tl6ItMe3ii680ekHdEoivc4rqjBFAzY0lSXqFEbj/Ie/b7L
XJFm+PT9+M7hzGHvEN5GbTJICPyKjRdW8agP3FdHF+lMnxwJMrkS2lDRMGKzzm+C
ij0Gw/q71NcNZAUkzTExX54hqyTtcBnfmYSnc1djFPTI8AaL5L+iruvIJve4PkZU
NVLgGFWBvxRXi+R8v++zSPEjVLbIYNoRZ/6oO/UVAj/jgs6P0ZtuR0tyXGrAnF+X
rzJnTkd384iVVvSvBnQosioMLnYd/QccBSb5Y935Nh4c6WM4UhroEfR0qtL8T5i5
xS96dKhcwknqAQ0JdSJc8iu9sOF3TAPfoXnwheBdlRZdrSVRsv2QPcNzbxzR+Kut
jOMJMmgI88Noxr/uABqdBre3nh0yqxSc/ln7NNQUk5EKFIAx6nW7h5Sp43c6dyXp
OmM3Hn/E2Avt1rXpZQRivCSC2LZD/cbo7EmLtUSjVWsgIN2NaZVBpiGEZ1xpnEk9
+aPAtT+WR42cFuJPML2RNwHXQKdaqf70IHkE6Sr3qLjnfN5SkLojLXXbtssXB2WL
8qTL9nHN2Hphk4NRZ5u2+39MjeVgxPr3qVo4ydpXOy5QY7MuRVZbbWOlcmgUWi7a
GxjbpOmKJCeg3YOva0dfi/tr2eoylJ/k7bxDaImpVcdXZsvxcfUkkA/5SO3pGyDj
5oeLgVVKXNV0n7P0q5HCbfJxBDQxenYIWKQzTGrYtm0ru8q22nkiGBtiWc5ZxG7V
salHCGwuDEJFllAUzc94sodl6qYVpTwyZqg8Q9plPa2s6HgTeZ9QknJKzfktZ2lz
3j6dxXhlZrzKk7tH9Xs4Q/1NpjMdwp+4NYhpMavo1NOsQ6B6t3TEd6FcaK0y+GeD
pQBYZz0ZvIgnU1mSNsUJixm19wjIwo3yZd4yzXlBCoMwrRauMco0EKxASaSBmGcI
j8yvt2VLlWB8keZzsHDjquOJhT0KxkOVAc07zij+WhuAj56fE1hBDvvRT9lA+40w
```

```
fEoQLdnFCHyCizLvH4hbfrA6xGzMoZat75LQ+7bE0TRNbPV57mXdGxac4zVWKch3
vP2sShMTtidmKUrvFEQ3gIiNmP66xBa0UzRMwCrcQxTTdMMgl5SPr9K+ItOcsQez
wTc7ubzAtPGfC6jeLUjP0lu45FZYt0w2j9nIUKcbc84mO5CLVecQ65jQ1W38bLXC
ZGfjdszn5DMszxL4H3htx5YStLz6YioSrlR8Sfdh+3Jdq6104bIU5ljTo4/9dn5a
culMQZljFZp5KHRp67ZgMi0xu2o5Y6NEpOKf9BFHb2KJzpEKVOAzOEACdfN+ixeI
Ux3BaBIqSDxvW7m2YYIVZnzwujWzgizAJMOSgoD7ax0OTCVjyKATA/uRwrnU2fmK
APGGQTwJDFv97Ieptav/HNhlWeUifaX5uDkPz9TgzIuikF7szmlXlCMQhwZQb0LG
RH832bt5RBKv5gBSiqYunRNvzrC3CjDXqXb3aAQFovayj1l2ZP9klzCccU0XJCM3
S4S09Vzpud7mpFhZYXBdbZV0XwANtpih+GUYjRW6m4NClMyrgE3onh/myIb2lB//
LgxkIR94TZrJnR4YOpVZUcdtqV5dOdJNFvblWNy0DDHs2tN7aYYxKKaBq7Rs8HBj
XwoGuwwVrl1abJWiPi605vwjbYL5xR8S2IxLqgzOD63Nruhj31uCsBHXYNVWU715
44ebgPYC54Wt2tFRbmbKZtLM6HV64s6vFtrqpLM7wyAtHQ2oeyfWHJPNKMEBb4XL
ibeXn3ePZiRD1yH3/uIDnBvMOGmSBKEYRfpYTIvfYZMavyUs2e8N5dWBCdmjLkRr
wPPFzaufA0ZBTM9H5R/MspXBsOvCrAJD6+p4knPCrYqcALKgP/YKG61EvnR8bpWw
eQwBc/log9IwOYrjVLcarbNm7Ka4X0R/4eHex81CNGu6+UKkcDMWmd5c+XgO+QOg
d079i7id2wKZfjcMGkqbcV37udJrLT7P/JoKM7bkLsd/jNs8TcPyZvek2TPxLjze
Z/KxxTS6INkfhSpcykEuad4hYHz1+0igz6VheEMHdbKUj2kskJfI72N9yK4mRYKR
f14HRg/Vf3qrBegREVG0jckz3+hNkhpahx1767qhM4U0UbFE9OnAgKm4ChBFbaBP
9q/nSbjrK9THHXjGkiqR1mMF0hfvWdXTLlCr/8xw5ajRVEfoco6OKh2sHbPb7kBE
faHJfzKVkw2WCnHkq1gblT7I3RL50zpKeKiHNoZbnTs9R7m8rHAzSleHfgQ7WXrZ
yZ5u7jAO08ct/RCUrUXB7uRN+RN8xswzaCTKs2QlpL3Xm5BXPQtxbNHWoVUpIhz8
Xsog3/bruVEXFjaUy8KwbLm4gaqsluQscZZwrd3SshXI1yWhmtOpE8E5OeanHLeg
oiJNR/CrAQUfLVs1JOQ6CPLuH/j6iBxgVmyvd9BVNZviFFttweWR6wicHsEfOj75
V/WBcb2ri3yFgR4VnM8371DG06gcPgAmzQILTyKh+wY64+AutnFQbny0BVyP9gkR
GyL6svEt1RNFrX8iVZ/7HunFMC8hAQFnZjI4HI9hlcAd038U1fItocMwYQfeNw2s
b2cs3RcmiHYFB0RT3Lo4AL5ZZG2IyjNgkvnR/IfY75727KfEZin8512cWFmXwGQR
2r83ALMq7aFLjq7XVvbmGH340qvFv5Y3QSnCs4YepHz2Z56fnM7CNfjg7AISwOsi
jFPrgULPU8Yvrn7W31lSX9c2Ex3gky9qNtq1HlV+9fWu4xYWXFL1ODQeYIgrnKFE
bLkov2Oqe7cm5P5Ohv/rxhXGXySJ2F3NA9vZ0Lh3YhPr4Rp6LN+Bvt9+ejw+OgCk
3BS9SVyltZMQxT7GyXhMxqYNBF9ac5SP7NMiD2XcuyaLBsWuXJ+d3kZfgJ7+R2/u
YvN4Un+w6uMsn5rlBwf6C1xY8M8SSY6IRmdN7s198XDu1BckMDJbdHj8C4PY9taM
1xsqXpiwlgFU2imL+59SGgAIUGe9epFFDauVrMIRRwsg4B70rTCto3jzROnX27Bv
k2PzIzkduVYK3yh+drdabuOPwR5wKWuRUcDyUH8kS9UbzD6QaTUblBEBSLtG+wui
Y5QXtY1v3NHFmA0jjLhEL6/F7H1r096EFhP/+2boOlhrpHSmF7w3WtmBqEFRS8XH
aPAu7plqmX2HETQ07JXLiY0Ay/yrIGrjRe9GGR6GDcOxM4/Fj3Ab0xY1nq8lSyfS
/pvY452JwMfeOwPt5ADiIdmc8EIeClIhcS/i1nUa2BaxhjRBUDG2Biv+lgHXm0vA
agzD+QyJmy6T5/VtRiYnqM11dKZDJ/zCskbQG6w3+UKelmzMYCtQqh3aOsUedaQU
pwAWk4akkE3j/SFXLYDiXsWRpWdLu2eI7MWxr5O1geagYj88gY93tCtPUzxg3ilg
dRieQIjd6lcih1hy5ULmm/ABXdW9RCho3RRJx4aDkzrfKljkJg+7a8Q6c50ZmAaE
JM6qJ2VTNEh1Veza3KeS9Ch7XujitNfnJqengOR3DU/xSZxi8mrS5lcGRvi5HExL
0ad7CcyBQx4h/qJAYZkOSDrti8ABSGnerR1srZ5nEX4XICLdInnl6H7oRV4sjIbn
VFeuN+wMD73knIe3dHgbZy3QQvhA5pDlLAr7AQD8lnXGO6JXdAwcKMNSSKONVFhf
SMfrxk72CcoihP3vhgBeT5abiFsdZG/+mEG3nw==
-----END PRIVATE KEY-----
```

Explicit composite algorithms

See below sample requests for the supported explicit composite algorithms.

- MLDSA44-ECDSA-P256 (2.16.840.1.114027.80.8.1.34)
- MLDSA44-RSA2048-PKCS15 (2.16.840.1.114027.80.8.1.32)
- MLDSA65-ECDSA-P384 (2.16.840.1.114027.80.8.1.38)

- MLDSA65-RSA3072-PKCS15 (2.16.840.1.114027.80.8.1.37)
- 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 (2.16.840.1.114027.80.8.1.34)

Use the following CSR and keys to test the MLDSA44-ECDSA-P256 explicit composite algorithm with the 2.16.840.1.114027.80.8.1.34 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
MSIwIAYDVQQDExlNTERTQTQ0LUVDRFNBLVAyNTYgU2FtcGxlMIIFgTANBgtghkgB
hvprUAgBGAOCBW4AMIIFaQOCBSEAJrtZIg9uxx9FNUIHqscfZKM2PFIfmp8mnFb0
oCQUDoUS+891HsrMFALd93pynT3sOyRtFa6eCcg/+Ff5xJJNNlvRLAEUDo9NGtn1
r5DaAjOuLIHqIAnJMvTS6liyrDldWcp9CA2hiuxBehU6fjUma9t4muP55GGWCzRr
zKUW8BJ7+8sfnp5JrdnQdfyt/hwfTG0O4uszdgNJoPM+4NkiTkcz9ukJecV7rwOq
88RJU7kNwCBjCO9nc365sX83nqiVCEb/uQtcfrKT+wdp8GTLtwF6omx3wQsdGVOk
o1THOvY2wPhyMrtdWvwzQn4KZLtMVe870Z0HaqimUdm9LcP2sqV9pT1ZvDTHWHDA
aakLXIWuAMdoiAFnPvaDx7Hh6ptFvw5GAAl0GJzPU/5TgvQN21HzxKOSgCz6+BX5
6/wjs3Zn2o7i6wwG5TAUg0PbG4otv74Rs/ZhiMpWSzRW+QQSTQgICgAtNCcfezhZ
oEP+Khn7fO7N3sxC8+iQWIkr9E0+3CkTJkyLkKMx9lh0cssUSR/bSdKpotyy8st5
BlUu4G96gMreaecmRMAoDe491ED3yHmKWnOk3wQHSxMVU1dTfxor2vIhTUqT4auT
82WN9qzPb0uJil1foTokvC9RGGXqChJ1OOGh40h6IeDMEB7Cq8XR1oJ7LoR4BFMa
c/qXd4Op+AS8FKKf7bZh7AK7vSdmOdfapQOUVEWMHEEYdV8ksP7UWYBnPy9CXr2u
pMUh6kuu6nt7mni23KRBZYqEiKe3f0D+tRC7BQBDG2gJgtR9y3HO4A3roaOpYn4c
vlwHsaexYF+i0SyO/9IOlKRukAjy3vfafwkT9Qw7O/CuPqjWJH/oAwHo9jc4I/oU
rTc3DPVxSxGsU6ZwI26vx+UQeISVRjLjld4qVvem0KMc23TgOjc+H1zd+riJixn8
HP8NJI/a/4vz7KwQc/qeiw7yZOCgfKQHNfyoTcwuu0XF/K5sdiS0kmNCGMS+fXVw
ZjelSryVrYO8OSV+Hr0T8bN9CQxPMwAJnMDIIbvqZMUUwUYSdsQAGMB1u7+c+Pry
gwWazUdULNq+ZaaozgcfP9xe90JG2FbwfW9fhG7b7QdByFT1QxyewWKUTF615NhV
kBGuIIo3zQ7LIRxPvfSnMDugmlt4cka1tEunquWlFpq4cDIHDG0EblsmWG3W8U5O
VTzb0STcKjsakI52yEwLNvVBakTFZoZeGxHh941WNK5A3OlwfFVZmOcYWrCB61JN
ITN0MKH6ZhG6XmEomwfYAsIVsRujVItIyZzPH+1MbMkoo1+syru/P6PeD9axpi3i
OKiUb/FTLytPKy2SbVPYZOMPCZJo27R3IX3MADXkfy2yv8phqPRB1z38wSB1FtKK
Xwim+51v5o+lv6ybnYs6AZOVPfWe2O+9ANW0HjMTV8ztNHtVeSnfciZVS6k1u2UT
GJGef5VRulKELJQj0qx+qGohTYlVm9TFE4iaxlJZ95mf+fWPCLClhHiFdGmpz2cf
m8ZOYhZaoYm96Rf5WI+D+QqqDpQMcX9BNV1a5R4g/cI3YzHlqlNvHC61ajxBPLS8
DbGhES/aVYWUl3NuEgrnc+Di4BKkPhKU9qZRJAV9RLnVjQTocjgakNswMvp3Kuu/
gHSqaWyFex+UUts3Nlu3r+7yUC5EldzwTq+Jn+U7ILRqs2wohnFnjg3cABxXV7ii
7F4qOPoTZhtWP+4KykFqcggTPoV5clkqJTri8AOxv4qsIQHrzgNCAARxy6iZUXq+
x1siqMQcgllK2MnQ74X8Cj4KyJsEez2cGSevPzFDjPOhTmNlBn90o6iV77mDENhP
234OoF5bb0W+oAAwDQYLYIZIAYb6a1AIARgDggnHADCCCcIDggl1AKvPDX74lkdl
Rsb6enWuUrxmTor2Z0iaTem4kK+zMg3esL5iuoDxug+/rTBI/IMzXVpDm2Y9i+cH
riIDr3t3KKh/YCxv/tGLK+ieqEZaun8IYXe17bHbEbTZtBVZat2Tzr932Jy5+pWZ
```

```
6yW7lhfUTQ0N+cXwLH1bm2N+qP0jvZYXpnYGdIAnlFfm9BU0cCWAKKcr9WULIWE7
HlEXOj1jmPHu+inx/qgPvVyer1tq/kBz5q1ereKmB74gxOnsqkdwKAYaktpTJJng
1bUz6/HfDArXIQpiGKq1Jp/aKabU4wQhavAsevLbqaspl/QymwZkv0PYk2rWZ/TC
wzIwAMPeP80nk90RE0BvmXPj4wCK7tkOX4SXh6l2wm1Pw8bquDQVLkud11rqeGyQ
vaxJfKZ6ULAITKHXYmiFTmicFLh2ryEb93dTi97nzq90KFLINjkrznlbDomSKh+1
e6rs1XnBVt2OFsTeE/dsptExPu859goDpVtbdi8h1gaRvkLH78S3PxMdNgdN1Uje
YyFJosdDoPtAJIiq521PQLuOjWrQvAqPUZbFkX3I0ftgOgTKVKosIF2+QChsHC68
S0tFgzvNQDT8f9+yi0ubrSLZ34WzZxZ5O2Vwralp+GR1FzAjw5dTYynUtJdzvGX7
zTr8nDlsloYjv+tS2kuVoc70SQifeT6d0I2cQMGbqMVtbCqhfI/ZxaTwO4WHu3NU
uIfctKewUT4R00mHwvflOLsKikDnwGb+CEJTPttRw2Le4bEpfNWy6U1vuS25kiuk
cfINpx2u8g4jEV5W3eH6EWE0TWp/w7D4Iz/ihmGPfEOhLkSStBCR8UHhzoL5ziAD
LGJAAT/FG3NNRP5arPhaklXYeg4JQL4Cc8AgsgLHslrj3AlZrLM97rNPYi984IjS
dUKy6x7UFulX/nQtpaebw9o/n65/Wl4n0h2SKGgiogt7zu2dJoV65hGI2KvCsvZf
9aF4ovyJf02mAomErcuFSPghhG/JDeUtP0jr3UUhbk8L3Wp8PqhuDBaUFQJvm4R1
7uf/QzvGTrfjZ3/+iZ4S3I43gOzIxziWpk9jPttSEWLxcDTvlxUJOAQFrLws8L/q
VtHLEuT952HxgAy2oyWAVpryS9/hHwQ/jrvNLyAtpyaxi/xdqx0lBaTgQhdA1B06
YFZyoPdthzoGALomzbA4AAbx6j8q2Ms1tBYrCSb0+o5jDui4b4uUsPBQ8zKQ1Q5F
FPxFzqnUHm+cunQNuu0j6bmq6XoJza5JpCAidraybqfQKvdkq/Xmakspxs3r1WsG
Qr0LskBuEaKjxBTTQ2QG7Ku/an6xq7A43Vjx5qSlAvAoZeoTLOPOqhTa+hSUxQ/a
Jl7DqUrGILgAKDUI0mWQkEkbVI48/ivB4a/C9OOsmAX5FeayvJTd03oGIfpFh29K
6+19kBwdZ6vu6CHJV0LfiNrdd+LBAAcCn9alGT+0W5ylLOMNGyMXWFoA1UwxCPRM
ZBTG5KMcDIbqY4/5VmIeiTuAKDzD5ck1Zs2/wyykoLfLH59skKRaP6UbmOacWBIo
f0xn+hzHgUDccAYMvjkPNXAx/vB7O2QFdp/Iwfgo6mHpTiVT/oxlTsSTiBiwHWC3
e57kSDaMXtppWAomEkAu5PNsBqgV/3GfrQgBXAvoJv/Cn09kQ5G+oY6bCKsQr9ox
qsjjHLminrStVkbdx0WTrPQKFVQHL1Y98OSfoi6g2z3O6sAMtIw/IH/dgVI36nbW
u7vE5vHiaAcsNGrmedlq0jq3QA92mWudMYFVl7DptSpUPqkfWO+gH3IHq23ZAcvQ
xdil/niu3vqlzEM2Pd0mjX0EM4Qhx+bhKLFn6vEy4LXBaQ3jEI5+qMVZ1+ZBY+xy
gGXoKwB6WU5jX+tclWn+p8R0FhyQhHSsYR9EYPnJKlCaWL0Kt8jTBe9Oa0kx02hk
DUhM0obuDv6EUqSIgIhXXFnxmOl0QwjPJzn+LW01bBNN+7JuA0AKd0lFDl58wNGf
uES8hFc9zmFhD38cmQLt4C0J3lFu+YNyAeTvyTv5nmzhqxF3hnMT/gULfSc6Su5K
o1FHGiqfjktU+5iA32D6RB4W+sAF9vccHKVra2TPiZUeGvlyVBNT4wtAdVbvcrrr
U0Kp/fOH4sIu9YBgeb2MceRBiP8LRgccMRsmVcPFyGuiEEPqs4mOceD3vD6sRvdb
zYCwUD0jhEgVGGYI7UaDYsZr1l0zQsXhDfAUiNePFkbEDz8sdgzSSLpwS97GTE5C
0cI093IYjvYIQw9krfuKAiS/V7jP+J/bjpVncubzJbynLhWCdq1z5yv53EEz/bgA
lKe5dEuZxuXFVlloI+zZB7/m+m7ociIsZkovPddFibx3upaPC4g/TyOTBkaqRex7
pGazoTW8UTPjB04/qfE+/AZPhYTsr11oNNdgcbx4okQBQv3lRADgGumn3ewThaZ9
GfLvF32Stf/5qNQStUKCbUGwZIOU9CU+tnToQuiDlepW5dK8fXk/Pc5T8hWGA+10
zWFoJd1vDsw5AdR/Ux/Ryw1SWUvCEeeqeXLAUnv//t68nYK0dld9mPnK5TuEBaWH
BZxohIbH3P51p7E8tIjZHZ2NWUQTWY3Sd/D5GIgTZAuau0/5QoE5w8Kqx6l/xQV4
XswStgJCeFopFfqclDGx7La2VcWAT+XN9UrEJ8lR2cExqoN8z5MhLM4gPyVkZTuO
FpVVNtd3rwKhvhWQm24/qZlZu16K/zfaSvH2WunZ3CHyajVQEN6mG+Vnhn9p4TA7
0lW1JVTVCCEcSJBrfOzKwrsFRWes0+gPrInODpr1mXhNPSLsHMth6Uzzv5FY/g6H
+etb/h3SwMvWsdbvV4LHX4BIUNduWWzAl8OJXcAzVg89e78LFlp2hTr6EIDg002d
endVCy3nZpM1nloNI4yzXK/NFRdzJpaZlSkb3h5lRpGXVSPhO54AgT6rtSkRj3nj
+dckRP7NHM6zGR/+94VHkD8XjeHsN9DxT2c3fFg1ctfrpBuFBlsrU3Kr6j1XJZlt
Bfa3hOWiJTXuUz2Abynmj9sT+lzzkdF1Dr7zfI2eitTL410gPL1EQ2ceIqoPoWIY
eecr+FKcQkoIf6Lo9JD9g7chtnesnKjjBCwyYGmAs7S3uMPW4eL1/B01b3d7gIiP
nMXP3wgNF01gcIeWqcnc/gNJWF1sjKfFztUAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAQHCgyA0cAMEQCIF23GlOP8gk76vJtzMxvJ9k+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
ZKM2PFIfmp8mnFb0oCQUDoUS+891HsrMFALd93pynT3sOyRtFa6eCcg/+Ff5xJJN
NlvRLAEUDo9NGtn1r5DaAjOuLIHqIAnJMvTS6liyrDldWcp9CA2hiuxBehU6fjUm
a9t4muP55GGWCzRrzKUW8BJ7+8sfnp5JrdnQdfyt/hwfTG0O4uszdgNJoPM+4Nki
Tkcz9ukJecV7rwOq88RJU7kNwCBjCO9nc365sX83nqiVCEb/uQtcfrKT+wdp8GTL
twF6omx3wQsdGVOko1THOvY2wPhyMrtdWvwzQn4KZLtMVe870Z0HaqimUdm9LcP2
sqV9pT1ZvDTHWHDAaakLXIWuAMdoiAFnPvaDx7Hh6ptFvw5GAAl0GJzPU/5TgvQN
21HzxKOSgCz6+BX56/wjs3Zn2o7i6wwG5TAUg0PbG4otv74Rs/ZhiMpWSzRW+QQS
TQgICgAtNCcfezhZoEP+Khn7fO7N3sxC8+iQWIkr9E0+3CkTJkyLkKMx9lh0cssU
SR/bSdKpotyy8st5BlUu4G96gMreaecmRMAoDe491ED3yHmKWnOk3wQHSxMVU1dT
fxor2vIhTUqT4auT82WN9qzPb0uJil1foTokvC9RGGXqChJ1OOGh40h6IeDMEB7C
q8XR1oJ7LoR4BFMac/qXd4Op+AS8FKKf7bZh7AK7vSdmOdfapQOUVEWMHEEYdV8k
sP7UWYBnPy9CXr2upMUh6kuu6nt7mni23KRBZYqEiKe3f0D+tRC7BQBDG2gJgtR9
y3HO4A3roaOpYn4cvlwHsaexYF+i0SyO/9IOlKRukAjy3vfafwkT9Qw7O/CuPqjW
JH/oAwHo9jc4I/oUrTc3DPVxSxGsU6ZwI26vx+UQeISVRjLjld4qVvem0KMc23Tg
Ojc+H1zd+riJixn8HP8NJI/a/4vz7KwQc/qeiw7yZOCgfKQHNfyoTcwuu0XF/K5s
diS0kmNCGMS+fXVwZjelSryVrYO8OSV+Hr0T8bN9CQxPMwAJnMDIIbvqZMUUwUYS
dsQAGMB1u7+c+PrygwWazUdULNq+ZaaozgcfP9xe90JG2FbwfW9fhG7b7QdByFT1
QxyewWKUTF615NhVkBGuIIo3zQ7LIRxPvfSnMDugmlt4cka1tEunquWlFpq4cDIH
DG0EblsmWG3W8U5OVTzb0STcKjsakI52yEwLNvVBakTFZoZeGxHh941WNK5A3Olw
fFVZmOcYWrCB61JNITN0MKH6ZhG6XmEomwfYAsIVsRujVItIyZzPH+1MbMkoo1+s
yru/P6PeD9axpi3iOKiUb/FTLytPKy2SbVPYZOMPCZJo27R3IX3MADXkfy2yv8ph
qPRB1z38wSB1FtKKXwim+51v5o+lv6ybnYs6AZOVPfWe2O+9ANW0HjMTV8ztNHtV
eSnfciZVS6k1u2UTGJGef5VRulKELJQj0qx+qGohTYlVm9TFE4iaxlJZ95mf+fWP
CLClhHiFdGmpz2cfm8ZOYhZaoYm96Rf5WI+D+QqqDpQMcX9BNV1a5R4g/cI3YzHl
qlNvHC61ajxBPLS8DbGhES/aVYWUl3NuEgrnc+Di4BKkPhKU9qZRJAV9RLnVjQTo
cjgakNswMvp3Kuu/gHSqaWyFex+UUts3Nlu3r+7yUC5EldzwTq+Jn+U7ILRqs2wo
hnFnjg3cABxXV7ii7F4qOPoTZhtWP+4KykFqcggTPoV5clkqJTri8AOxv4qsIQHr
zgNCAARxy6iZUXq+x1siqMQcgllK2MnQ74X8Cj4KyJsEez2cGSevPzFDjPOhTmNl
Bn90o6iV77mDENhP234OoF5bb0W+
-----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+anyacVvSgJBQOhQtygHOyvaO5rHa5fPZoxjx1e6w/2fVfo4+E
3uqJBXk+cRPHhqKNGv/26ezD7LS3F+b1A/P4iNjk0C3DHUUMFw2/WeBqIn1xIQ35
lm91h8VIMh68BhIEX4HbL1RC8M7A5gywSBIIKYiQCeMSKczEBKIUUZg2hQmHScpE
UKPIZOMyRISYAAuAKWGULUlGYcmgQFK4ANsSURFBUhsykII2IpDCgdAEjRFFKcvG
bBGVRdsiJlICRQGTbAQJCBgyIhqVEVkEhNJEhkAScAopCAq5jYEgUgqxbSGmBBiU
KWQETpsgMEqYQSIDLVswSgqjhFO2jCMIZsIYkeTAKNMAbYrCTAg0KBoQLZAogSO3
YNu4aVxEJgu5kYEojsuwDRAJaEMGEARGgRAHZZw0JMk0jEJASSGnZZOmSEM4EhyZ
```

```
kQs0CoC4ReSyaFiCSUA4BdEEMGDEhSHDjROGiNyCEAm3Qdq0SSJGiMoSJUOELIAI
ARhATdwQDcgoacHCEQqYgOCycSCwhJkUKgCVKBtIBeAEQIAyiQCwbOCmhJE4bmMw
aaI2gMgQBgzBDcJAZYNCcgEpClNECoEEYEhCARCXcUQwEuCYjBqgbYImAVmwcMQA
gtikIVDGgIIkDJCAgBJBSZIAUEkmUCElgtlGbpE0USM2jVgUKdMCIErCkYwCbhyS
kVAYYJgUZmQWDhA1IJMWAdw0gUnEbQlIjMwiYaK2bUpIZiMWDMS2KWAWScMARBhG
IckShFyIjRqiQAElThmlJcO4JKG4bJuYTUHCDBuCiBIjKhAjCduGCQQSMUHEiFEy
SFGicBSDBJFGQCFJRokmIqKEYCHHaCQCjBgUTeKiLAw1iICkDSQyINiyQeGGJBIg
EaNITIAyUBQRRhupaaMCjkgohYkoaRIVahslgSCjYcA2JhG4CNQAIVyyKYQoUBI5
gFQ0btBIhhEWKZA0JCIEUpMIDFk0hgSkTBmJMJAUcIwSMZMgZQIhaVkibgEIbKSw
gAEmTkmWBBylUIEIUIiYQAgQAhIlhuNEbJHCTBEwTcoWRBKGEAozaqGQDRNDSprE
ZQDBiYjIKMgCZZyoLCSncVgwUQkVbCLHSNq2jCRFRoMCRhujkcsoKAjGTAJFUYQQ
iAuIDaSQBdlIKdvICJCyhaGSBcgCaa3JyIu/8HR3n+5neE6TuMyTB8nTCJyk/6Y0
KidBTsm5I+LNguG/4MEm6SdmHZfeU4QR8LQVSwDVEI84SAFzKpB/zwRHANrZ0DOx
JYVHwHv0b26Jyu0jvhmUJMWvs7Kxq/WnthiAjuvqSfQXvJlSGh38z6SUytNuG97g
+Sjo6As441A30ygTGYypeVSfXycTVtOvZb4yKeCx0ioTTyph8+GF1kusxumooEqD
GktF4jOk5k+0cm3tRi5b4Z7own4t629fblPpB9mP7qOzjt9C6TZoLwQkjuj30Ih9
/FkEN6hrP1B2BAPT+MpaeC2NwB8oBBU+u/OF5r4Wc1WSjOXlNBKhOwchg95Oryy7
XlL9jpUo587NParE8zR233YuQGCh1ivKNnZVqQkiD67XrH9yyaWf/9AwmQcPYuQm
LgznjM7soPVyi1ZeZ3lsMzwOrSmeSM2qkhTzdIFPDXTZcwWPH30vdkZKDcvmAyDL
dDVSCtzYOumTWZSZy3FKvyjJ70i787HnLTC8StDrgh2MZEUlcSwKXUIMmW3zn/2U
hq72j7Lbw6zktSs65KR1dquGOs+NLwAqbIp1tu8IhB2Fdd4P2YhD1BRGrJrqzPlB
CCNznhvMQk7WLI9/jiUolGAuFedcaEl5+VwxTd9nUTCVpkzXvCIcO5B6Al4nuNi3
KmEb92vLLm+ms0xZ8+spe2umZanD0oPTr66me25vHsGxJRAQQzjw4N01gEUcx5Lq
6hgE4/jEM9vT4PFZ2K0GXqu5L8iyAP5deccLA5UFlJXWyeH2ZEn+R7/HFwZ4bzjc
tKkDl++g0vG6eKeXH1gYypvLvFfheIqg+xsvI/ryS+x+Ameh6jjSpMaJuaXtEhNZ
Uc4eU/lRVyQe+g9oGHs0b+mMAJ6NuwjDWbav13jfeehEzt/BX/2W9ECYVyM9xFP4
MzhUzq/7FaG4dYk51s56vB33U8Eq9QNc7OI1Qz/0HOYjCQnhWu2hFpDW5VH9wQAO
XCkKI4Jl7GkpdVzJ7asVLDhc0gz9QEliLQy7GjEJHhdNKfJje8xr39UzjIUSW8GV
5dzYY2nN0YPDjz/j9Fqwc6kkcBGWJ/fy7u8O7Ar3ZJm01nnEpxrUmenMBv8yt47B
MFuwPD2RqK+wq94F47R22ilfcSVG5s1wWipYEPxtBWCzyvhe5ayykrd4z67zntAV
prD8uK3yFzbghEKNiDv+5R3FmdWLZeRr6Wql8MkTaROzLul4JuJ4xgoumBqx8EOG
/STpQg3hNoy8r8PnRJumERasB5kGKzSjU5vDYVk8e+r4XBaLTQxQiUmTrzXupXLv
2SjvV7Fy1q1DnVf04EnGBqjZzm3qgc7XxSra80oz3NeoW4Jp2P2/fJ+P60JgGHX/
SVsrwxFldtBeTmGA8wcVywkHGiVlTsGQIPM3wFD4mOD15XFVgQPvVrDWyvNr9fSg
7EhQT/BDQP3/Gv4/nuwFG84EHfs0a/rwmURLMsiS0fSjYs+FwvNfrnPOLTsYGDCh
q9eefka0hlPaYX/zwphWQetZo6OUsSQeX3IWMF9k17BFw95Y9Stb76MMoe8iXVDE
UXmFBf1cPCX9TDBk01PjiB2mEUV5L0ygiIZBGSn09xg+sB7EgOCo3GwxobXDpJT2
bV3Svs66CnSZYSkjzm086MRHEM/Agq6InWjJ/QyxJJ2iD5P71PU2r5g4VtgDwi8m
XYxZ0X3eCFHGgpRYRNkyuZBV1sdiilYE3Ej52HOAbKdfsW/Kclbw4PX7VEi8WfQl
ZjX8hMAyI8orgzCvv40f/W2OCeg0lnNUbsAdJGgJaYn0B1DYnJ1Ar9Tcy1ScTnGA
1MhP93Zy85WjnO26PL9v7veyprxFMyzj/S+oCIXwygveXB/7mC6UiaXbVgBh6zX9
Zhg2dBUe/eoZecnn0JjsDMWevvs1PD+TLXpFy6hAF6Trd+841jajoN9bYvQib3cS
nCMv+SlV2oQHyH1ubFi1A7dLhbg5de7+gEJlDB+eR+Q8bbjp0FnepMZ0ivi0ykVz
F8gIhSF/PSzPQXsLzlR2+/s4OevL+SAnsYOFb8cn6IQCS4TdXuvDKGqjuDrrBTq7
hqGmP1SZPsSsEEszIgZlrhRM86ISGdic0svUCpXDeZ/IFM1RAjvmpce/6+fQJU9R
5LEBz206GCs232X6dpLbUIudb7gALPx4Z8qARtWrPITeSp7nfsS7Pqwp4d7hLm7o
EFGPZxeIBHkwdwIBAQQgo/4BafVr5YW93S3cgyzCmvyHmwFyBXyR3Dosv86fkfyg
CgYIKoZIzj0DAQehRANCAARxy6iZUXq+x1siqMQcgllK2MnQ74X8Cj4KyJsEez2c
GSevPzFDjPOhTmNlBn90o6iV77mDENhP234OoF5bb0W+
-----END PRIVATE KEY-----
```

MLDSA44-RSA2048-PKCS15 (2.16.840.1.114027.80.8.1.32)

Use the following CSR and keys to test the MLDSA44-RSA2048-PKCS15 explicit composite algorithm with the 2.16.840.1.114027.80.8.1.32 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-----
MIIRQDCCBqYCAQAwSzEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECxMGUEtJSHVi
MSYwJAYDVQQDEx1NTERTQTQ0LVJTQTIwNDgtUEtDUzE1IFNhbXBsZTCCBlAwDQYL
YIZIAYb6a1AIARYDggY9ADCCBjgDggUhAEhgcjlCjE3jlKB8jHMLD7skD0+mGM4e
44uwa+K+EFgg73ljO1vp2HBIuBEik5tEVAvL+/x/Dep1dAGeAXkTTvplSNADfxIQ
YmUQwcYNGWYEdpwfWSFE8QS9sQurD5Gbi4dvNWFbxeLVpR5uUal5cN9Oe4xqy4iA
pnh+nOkg0DM1oUD0FIOMzNMkf9KkcK4r5gP3v7bdCATdTuQsWR1KWboeE2WD9CSf
dvlEm3ENcpi2/VtAhlnsihFAp8MfkWn+txe/5FvzsN5gZyKyiznR4a4anpH4XGFY
8dIu8Xv+mgZDWJ9kwQ5VeXY90I8lKYL2puk+FmkB85z53CZ6Jz0QNsnferqqLoqC
e2YEk5Rl+sjJs8R5Ax+OQ0dugFV1NmojQheU0AXcGoxdFjEjZ+ssaCed41JadFW6
hLX9oc/weWsLs8Q3WygdRW4LgV9OQQf7thYShSdxAPdT+ZrXH7bLNdSfsqX7H6Pj
humfSRDOSqyVpMgsBBCKybBZCaihk5TXaZl5+HxMw1d2kjfjtqoxL5UA4bo443wA
dJNOSGfSu4C4vl1hNcM7msHUuSR9bgm8uiiLaydiAaB9/NCMMVMOQmO0aK01eJIm
K1do3r4QJkS1XgASIDJhgVVXfHsLB4xRocLIoYoJX/t9pGJJUlCW18o+GE+iWSGl
skGndiIxE/7afaDMwA1SxrI+lG6xs3og66mSULQ0395VkbNHLOjiShj+zhAtgB/6
7fSc2RDGKC5jxMhqzNCD/A5N4qTHv3e1pd7Nv3FDH2S1qsM4hrUBtRi5SqNdLtwS
cVgM2W+3K1PKEVIRGNcomUqreqD9iXH6lInSvZg17WjwBvckj0lkgnGMYkZ1wXFY
Bswa9aiNyGQ6XOT/SjqQM4nfJ1fNyrU2JTfGP6vTeYB1smsotCE5i5mWWfCSmquh
FuhsWlexJZamjTvGtZ/BGikzraPopytxodcvsndx/m6JE+lexV21AfM3rPJMMTae
oONoru/dbOS2kzEXxBvG7KdCDqyiO8AiwjW9HnmuiBmreLdpNDIGHHFiVXp6pw5A
G/qkfAtrRL4fv/YZTC4evEOykohWSDVC+SAbPp2jV+0DdTHCty0UT+CpWBncpGkp
plod5MRbLTsklj3kuytC0AKZuv/e9SAaQz7oDCFHSi+f0H0s3mcLhenk69UmklbI
IdRUPvQxFpZAPAcq7sreJ96AnW/0XrrEorB1ACN/yUOGkcPH7BvW5TeMhMmfM2QW
tmFolzLVXrdmlzrBxFjejHKc09p1up8PND6c+LGDfWmgEslD+2jBEinsoRcsFis9
T4JD8FIb5COHY9KJmSbjwua4MmTjNUTHTq2WoRMNcp36eIdSj0Boo86hfSPtn9lL
XCrpyDGrAKMI3JUG6Gp3+VtdKx88IjxOECBCYU+gFzrJ2urNFNFWc7ZZVrfjn6wA
/HFV/nrSdGZU71gbaxdS52hM9Xa75BvDO1SVjJLsF2bbhccq5njUTCVU8PewznOi
fcv6ALz5urx6t9aLuFAdCeAWcxr6mekrmn4NUlDa5MVry7O6OiORhJ2WgCbZa5yr
cL2CI8ONagnI4owNesXf6xNkJeWSh6MacqTOu1DNdUMolEpsgKcENENVXJsZO4Is
Axbj5UXR0gFUqwlDsgsHTBCNb5At8Q2uTgEEcFlqucXqRMyN5tp+r8WV97pE2c1i
Fr1KZfJEC4Wm3jE+54CbbV/34t/z5nOU+0HrFG57qzWUGKdF3IkoMk8DggEPADCC
AQoCggEBALrTY9cC4IAZklXeHzCfWGuAWVZsKzPXmmqs/jEexm/ENZA4HJyRIMRf
M+59xBe+mQJxnBm0pFbOtwJfRQuckt1KqkMGJ8bqjUBKZYBkk8FHMsLKlpQ79k8A
5mYovneBimZqPmd8s/oTkDrBGA+7fBBkONmblgrvuGIKF9QH6jatUgwpPK/zJ8Gn
sEiTs0n4UvnROcIRD+qnTK6vIrqIz/z7YZF2C7i3fv5QeZe7o2dfLeecSyYw0tr+
Hr/UogFISx9t0axm2Bl4lWhaW43o99HMpE1ENq597Fgpy3SXqrqWbrCWCVhzRpOT
6icAFVba8LYd5iUGTHeDKkTkR/lcfPkCAwEAAaAAMA0GC2CGSAGG+mtQCAEWA4IK
gwAwggp+A4IJdQCjZCaK9+jleELvqjpwbiAZstekD30ui8JvVy6OXPRLceH2fg1k
YoWzpBCYSM/VJrCNnXzswUrhcmGds88EYwmce5JDQsLK/8NPihTq06urGqqxKucv
```

y+joajEEyU4CSKy+TDJdSXCbWWYpGd1fAgxJMFnr3JVy38Yif1oD5/Oo6ljpr2WO
34cm9KF7YcPCFyG/unlhTGZQ+KBe8n/hh9U4ZjAH+UG0JMV+LUcAE0MYSfQkybhY
kbaF6yzzWE+kWA7mIfsGM0GmpBGT8cLr68lmfbkUWdUBhuI6vqKmzgsIISHx6Cp3
c6yXKeIvAqEIcOWnAtHqeLUnsKMLmIkcnNoYokCId876t3e0W6oHf4JxU6GAqDjE
Ty4UB9pslTg3K0OhezcdziHkWz0eBcpLuJjOQwTPqScoXrw4Hbo28YI+GTJr/c5t
+0WrJA+Jy2uaCznnKD6LGRH0RyIV1bVLaqiBUZJJufmSalepjfDnTEeH4aUqq23a
gw7NCIeqt7Nc7tAczrYhndknBiRWTTwMBzFaNUHhYN9JUXprH4QjKV2FGpNYAaSk
9HKxNRnIDaNsw3J0g5gCpSSxxvQ8viPP8zzAKB/yJ6w9N2Ku+giT+abm/feaZIue
H1HMzKnQzyo+iOmeq7P3pRLbegbLXMktKHDjSBwGqYP+SA7P/YLXkA0Lo6ev2gja
yjzABptkP1EvYl/BQwc4muTMd0oDj2xvYLSngRXEyY5yxdqSvHouePf1Ja9LtF6p
ZqS/T98EklG1LWIljVfEUtV7fnkJd+WBtywyr0vNUAhskP2avPeto9K/MujicbP4
xc4k+tn3/ZKZPKHcehF1h/nqyWcqH228ETaDXE7SqVRN7lsWoZ0/R8Hn8tnvjgY4
eb7bNPaCC1llhxN+AbzB7wNB7qLdn9c7OQWhYQ+J3zuiqBjTtTdfZVWiibSp1E+X
Ze0C6hWzamHYSwTD5IQ7tdgy0MLyBrXSsVSs/ERNC7p1a5HRfmbFuo58vd/cUhXA
63Y0Lp53+6U66mDLC8qOc02gq7vlt5LqjqDvZSG4UN7h09WNbNcY9uTMmphRGKAD
Pdh/0b8Ru6NfBDLPW90OqMTlM3hSjzUdu5/w1HgcdWbHPlFQePD6OG/LmBH0yW5D
SpvrE6XVlWFSvN1YjC/cXCm3Zb6iavgRKPxIsWxvTGKG2ss7/tSxAkwUJminD05S
MfGD4GsMoN0I/zyN8mXhTaIuBeMUnCTqNe4qhsrINE9OfrPhcfpyeNON3dT3NIMx
ID4MNMjc82V6EUREluwF8TSYmBbx/JTfpcTDxhZrFWU1vdPdOCp+LsjPUaj2rNIe
FIMHHoEKcpGV9b/wM9qOhRtRxem3lRcLBBIzh8cxQq/XeizV2pNPATqR0yf/buv6
uEhxL6nVzQYJoscnuiBOkrV/nU/wEJrZT4pHEEucnapYiQRgkZpcrGmjy7DpXBJC
ZFAuyKIfUHo+rKRk9y08FSzfRb9VvRBVFWdNUGNMIRDzahEAzRHabSHBbmrdmiE8
fJMy2iC+GuZW5uUtv8HIEGnRWV2JFXXoIJzTuoaZ8Q/rCE8KtA04YIjPjtFEJ3cb
hOhqi+QFUdgMDnCFaYI877lrhHSy9ztcp6szKuJzkqQI2u4nDYxLfFIvAewVmNro
qomr5NECCeLLQymz4J5ZjrTxjzxiq8FsiheEJOErZ6B4gKqvLJhOl/LWAnvTX9WA
BxFjWPL/WkYExDbO3NSL3RFpSBmS2eW0q7I4GO0i70hFsZhh7UTF1/7guU7N5BKz
OeH5pjZCCZglwVc0WOfQQbPXuZFt1ZeP52nxUcSoPTQ8/1dO2xXu2oAkbF66/Lwt
2qgt12mLEhgHO7D5TZkGoZSd2z8jCD8MskU/sZQJ6Xx8lD/qJNVmW8C6qMhLmS8e
9yCyocsnrU4n4uv5UMqAHKlin8s5cR0aAieyYtqSlHb+Eq9JaYWzszTo3gbmPJLA
pKTs3BCVeYsfOIlspPHrlV+GcbWBSo7cFIcsY2oTn3m74UQak2im3ERnz8rWlIxL
ez77s/vi4PnoSi9fcWlvst4wZJ4I7gY/DfKE9sd+4cjmPhKOrM2PO8yXBsNNE01e
RZWfwB2+0se0WoFW4f4B8X3z1JGqQ0Qwp7PjXdwfKDOJ0753j/hAA3yR40F9GrnI
H8kCGpUY1ogMDPMFHi0Nd2dhey8Or2H2tZqHeSGY6/PoVSqIPToLQWVTrp8gnd25
++gcyZDzGR0CusC03C8htOx3qrtGQUDU6TIJueupZkPe9jAQmL7pIVsUbGUZVgJT
iEHFjXlhR5hCMHO+Uz0eKxljOsyabLM4Ha6SwcEmWznl9Q/fna+PmddZVrfHo5o1
orwXF1mPMVi5UKyCZh4t4HhPmmQAMVPiBb+dbA5lX4cOBZmc8ad9857Aq7P42DjD
CGhZUHQ53oGGM5ysKSF4sXcWbCzKOkEHVwsuAhA3dk6x65GIc/5MnUosb38AUscg
ahoYTVDswKcODWzr4KcUQPlXASu3Ek7DEivLkNxzj1gonQ8KB05u/RRY+bh/Hgwe
L+GepEHzJbcWDHFAXopGVsB9Ztmw6Bk2dulKY1AgNodC4bvyvfky7h0LEEnKKeZv
smypS0N02HU1oEkUJQdt6Ks3dS6S1wNw3O9Pqy4JDGcLSpWfLUECISXqM3OID8O4
SIltOnu9AqENDET7B7wqIvyvM/z5mnT3FJVAEdLToXsLxdEH53txDWmo3oNlYBmE
RtdEuMZ8TWzoWpUcHtUo/gAlYxOBhdc/qrm3u2RDfP1rG3wJlf9CiDX0zjF1n+ZB
Ykv9QYlf72+xYcJckAoTF3wauufE/34SZ6qaoM9PRF0LJKlBdWinl7YW+qVcO+I+
B88fZ5n3iUOe6+TVonPfR7jogrYTw7n0LfXIySsVMsnKazdW8sWvWNMlTD30bY3/
C7HLu5u8jzsB7MoODtfwRblcx4rxw8xfYmqsTNJ7Q4DGaJqFNYa+sRTxkW3jFN+W
UDZL2uAGvZRZljFy3zlz8akhJ/NJwvdaYtRtJChyLKGi+zDHW4pEq3F0Uy+8VKCk
wqjsnGRYwgz0KTgm+Uvim0cNWZTl6it3gcVmhs2kfxZEv4s1Ls4AbY+6LBAwRk5o
e4OGi626vuvx8xguP1pxdaXL3P4OLjxSU1xpiJmbsrPHycrY2+Tm6v4AAQMFKzVm
Z2lte4ePkp7H2d7j5vT6/gAAAAAAAAAAAAAADxkuRQOCAQEAuCI9+M3YV5pwqipS
NaHOqk1x1+yH3nT14Qziq//pXhGbSEWcXu8nOqmk+u1aL7aDpBGxIDZ6/sI/m07Y
ZKIvQeuxf7PKs/NmqPo85JTHRr2G1V9+1iE2PFitYBq8EYWilsWh/LQdSAY/l+ea
fyYn1XhbFQ/OE8cJrS5mK22UQSMbnTibyRBgE+7BjPtEBK3KTPKBFom5Z7i3bGDF
o6rJmez5hJ+yYp7yuZUVCKoyqKk8RcIga+3QwPlwpbgTriWOp1oJFLBCLOeskSAj

```
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-----
MIIGUDANBgtghkgBhvprUAgBFgOCBj0AMIIGOAOCBSEASGByOUKMTeOUoHyMcwsP
uyQPT6YYzh7ji7Br4r4QWCDveWM7W+nYcEi4ESKTm0RUC8v7/H8N6nV0AZ4BeRNO
+mVI0AN/EhBiZRDBxg0ZZgR2nB9ZIUTxBL2xC6sPkZuLh281YVvF4tWlHm5RqXlw
3057jGrLiICmeH6c6SDQMzWhQPQUg4zM0yR/0qRwrivmA/e/tt0IBN1O5CxZHUpZ
uh4TZYP0JJ92+USbcQ1ymLb9W0CGWeyKEUCnwx+Raf63F7/kW/Ow3mBnIrKLOdHh
rhqekfhcYVjx0i7xe/6aBkNYn2TBDlV5dj3QjyUpgvam6T4WaQHznPncJnonPRA2
yd96uqouioJ7ZgSTlGX6yMmzxHkDH45DR26AVXU2aiNCF5TQBdwajF0WMSNn6yxo
J53jUlp0VbqEtf2hz/B5awuzxDdbKB1FbguBX05BB/u2FhKFJ3EA91P5mtcftss1
1J+ypfsfo+OG6Z9JEM5KrJWkyCwEEIrJsFkJqKGTlNdpmXn4fEzDV3aSN+O2qjEv
lQDhujjjfAB0k05IZ9K7gLi+XWE1wzuawdS5JH1uCby6KItrJ2IBoH380IwxUw5C
Y7RorTV4kiYrV2jevhAmRLVeABIgMmGBVVd8ewsHjFGhwsihiglf+32kYklSUJbX
yj4YT6JZIaWyQad2IjET/tp9oMzADVLGsj6UbrGzeiDrqZJQtDTf3lWRs0cs6OJK
GP7OEC2AH/rt9JzZEMYoLmPEyGrM0IP8Dk3ipMe/d7Wl3s2/cUMfZLWqwziGtQG1
GLlKo10u3BJxWAzZb7crU8oRUhEY1yiZSqt6oP2JcfqUidK9mDXtaPAG9ySPSWSC
cYxiRnXBcVgGzBr1qI3IZDpc5P9KOpAzid8nV83KtTYlN8Y/q9N5gHWyayi0ITmL
mZZZ8JKaq6EW6GxaV7EllqaNO8a1n8EaKTOto+inK3Gh1y+yd3H+bokT6V7FXbUB
8zes8kwxNp6g42iu791s5LaTMRfEG8bsp0IOrKI7wCLCNb0eea6IGat4t2k0MgYc
cWJVenqnDkAb+qR8C2tEvh+/9hlMLh68Q7KSiFZINUL5IBs+naNX7QN1McK3LRRP
4KlYGdykaSmmWh3kxFstOySWPeS7K0LQApm6/971IBpDPugMIUdKL5/QfSzeZwuF
6eTr1SaSVsgh1FQ+9DEWlkA8Byruyt4n3oCdb/ReusSisHUAI3/JQ4aRw8fsG9bl
N4yEyZ8zZBa2YWiXMtVet2aXOsHEWN6McpzT2nW6nw80Ppz4sYN9aaASyUP7aMES
KeyhFywWKz1PgkPwUhvkI4dj0omZJuPC5rgyZOM1RMdOrZahEw1ynfp4h1KPQGij
zqF9I+2f2UtcKunIMasAowjclQboanf5W10rHzwiPE4QIEJhT6AXOsna6s0U0VZz
tllWt+OfrAD8cVX+etJ0ZlTvWBtrF1LnaEz1drvkG8M7VJWMkuwXZtuFxyrmeNRM
JVTw97DOc6J9y/oAvPm6vHq31ou4UB0J4BZzGvqZ6Suafg1SUNrkxWvLs7o6I5GE
nZaAJtlrnKtwvYIjw41qCcjijA16xd/rE2Ql5ZKHoxpypM67UM11QyiUSmyApwQ0
Q1Vcmxk7giwDFuPlRdHSAVSrCUOyCwdMEI1vkC3xDa5OAQRwWWq5xepEzI3m2n6v
xZX3ukTZzWIWvUpl8kQLhabeMT7ngJttX/fi3/Pmc5T7QesUbnurNZQYp0XciSgy
TwOCAQ8AMIIBCgKCAQEAutNj1wLggBmSVd4fMJ9Ya4BZVmwrM9eaaqz+MR7Gb8Q1
kDgcnJEgxF8z7n3EF76ZAnGcGbSkVs63Al9FC5yS3UqqQwYnxuqNQEplgGSTwUcy
wsqWlDv2TwDmZii+d4GKZmo+Z3yz+hOQOsEYD7t8EGQ42ZuWCu+4YgoX1AfqNq1S
DCk8r/MnwaewSJOzSfhS+dE5whEP6qdMrq8iuojP/PthkXYLuLd+/lB5l7ujZ18t
55xLJjDS2v4ev9SiAUhLH23RrGbYGXiVaFpbjej30cykTUQ2rn3sWCnLdJequpZu
sJYJWHNGk5PqJwAVVtrwth3mJQZMd4MqRORH+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-----
MIIOzgIBADANBgtghkgBhvprUAgBFgSCDrgwgg60BIIKBASCCgBIYHI5QoxN45Sg
fIxzCw+7JA9PphjOHuOLsGvivhBYIMBKoaAl8odQ8Tfy17mXe7+bXrKtMkaLkFsk
TQirgQzxjBv8b2YNfj480CV8rMYUc+/qQGd3IfcR8QI7WbiIcuSTrRw+ePenVgmv
LLtcSf1eXh/lpp3YSgaFmEUxriavCOI2EArIiMkgSlqogRuzaFkQKcGGiUw4iAy3
ZAtCkgMVTlHEaOISSZBIgKRERhFGbBgIEeLAjYkmLmGQLKKGIYyIUBSGCGPGTRQh
UtyShQAkihiUKQNJaogEbRu1ASRBkSMhMAJEJUwCRMEWBVGUKSMmJQlCTdgYTNsm
ckIGReNEIsHEIdwQTEsAkpE4ihJDQkqYSGEIaOKkIZgwaNtCkNG0hBoBjRHIUNkw
JQC5AAGwcJMGMMyCUYswQUCQQROhCeEGjJuQiQK0AZkoUhLDARmxTBOCjMFCQQpH
EkAwMMOATAQziFg0TROlcAHGKZNAbQknSiMTTRAAMBMyUVMyIQQDDFkYQgqkhcsg
KcCoheNGUtIYjYw0TIkSKiOAadkIYFmYABIkYJmQSRSzAASCaEpGQdpAhECYMJC0
KKBEUJJITNqkANmUBEnISIigKNFEiiEmCtCSTeM0TRuBUeHAgYOUbQgiIkAQcpSC
LAsBSUkScECgSQBHIcjAABsUMVu4UJSGMVxIAszIEKMYjEGGQAEyLOQmJlkIkBAx
kAnCZRxJAWA0aAtDbRyZQdkSbJGESYMiisEEjARGiREkbZGyLUAGYNoEKNMUEgIS
BJzAEYFIIMyCJQijRJm4kKE2RhPADEzERGAITZEwYBrJcQIohGBCcGQUMRgxLlu2
gdE4aRKUUdg2TkLIJQAigIrEYAI2ZYKACBIjSAuRaRkGBBxAQJvCCVwoIlAEZYgg
QtMmcMw0YJRAJiKmUKI2YtGYZBSgicOERApJEYE0DUg4ZUMAalAyhmMWQQiCCOSo
DQkojSQ1BSOZiRI5RZCiJKIkTQyjiBkScchCCMMEjcyEjMzGjZgQYsgkAqE4bqII
bBSjSSOhgNqEgBKiMCQZIpkCIss4INQkhFigKQQQgOMWaFEoBgAFYVuYJZy2CFOm
TEpAKlSAkSQAJIOUIMoUTVskIBoWakJGEEhCIINEEcggjYyyAWOUKaOwSUkQQSNG
blSmCMygBAE2DYgUUAAiapkoYEmmadwyAg4ewD0Tg5N+Ex6+hUDyltu1tQnGeOPR
jzpDuDD0ZUi7kzeUebbZSff5EPrFrx53iyA1NHQ9y6sjSHBCrU9hO4F3Cy3dxzWq
5HQibiNiwIJOXu3NvBIIBL5U5UozAS5eyffheGcO0gtmD3mP89vhPCbYE0xjzOrs
El12BcxBnDRDPNphtnkWVzrDtFbASv0uOwi14HXYGTZaQufiECLUUsD3s0pC2/Ji
0qsQSncvQuS2mbMKfUOXeb734rNognmAqD7uaKwqqP26McTZJO0QEA5eItOkcRZf
tRNbZMXnEDLJilps9XjWlA+ORhF5qgo8yv6s0bNn9Sjf/wAsg/BlhIILR/CEgTQn
XdYmlJDuTexqaTUtu7EA3tVm/mhn9xIqcKbVepoySzqDEhz39eQrn3/q9RJiM9mY
pvWnAODb3k5KnFMS1JOj68ssoCYjuBeV5ereAPKQHW9YSeffjG17xijfv9Z5XHHG
lorvqUSRiyzU0fKtv5Kj7cKozmfYxmRDodiYg8upvv3frAMy/9xyr0/dDhoeN9uO
rY0MhipdOhtwekubyG5tjdIrzFr8bZ/Vw54geJ2ZKPmkBowqcwSGHtKlYQC0Deaa
fDPvrLnYb+WzaKiu1pLPrJj1rM9C4SGOeBs4kaW9/c1mzKzmdOVnFBtBC1L5MwVO
xNHQEii0zQeGY9gwlqCIpJxRxfFBwvf0FbKzB2aYyW4d6EGb/+6m2YiK/Tw1xwbq
EBMnvKnb+gKYf1uk6h9X6JBTWrA1BPGTI4xUVDHQsBXBuGIPBFRBaH/97UxQBgHL
LwMqwocRr13BKGo7Yomy8ZdaPbKQASuwdzmw0xI1QpgpcNx8TP6KHmDqG9KYVrMx
8EDK3s42TD6Kas/gBy5XtXchtZ8AXE/MQ3ODzThKlgwtPSyGrQrj2FyOEKL56S+d
xfKrR93Dtw/g8ujkImPCIW0bOA1GpmbmJnmcApdCYW8rIGDkAANtzdZJfy3jFv8U
to2qzytU/C7i0fnGSuJjpqNvIfS0Boz9Pou1NKawLBnV/UJZl9hENkz8gy3MCkU2
qMUoGTmZWyPDeYIXSmzMbuSkqVv7BzP463VFcJ2i2bUiW1f+qhs46EuO0zix+USb
gfupeGaCzMEinUM0tVGcqmdPV0WSbrpFzz27XoMIweE34AgoQatXB5GksXUMC2qT
VW6WCTH1xecpI0xarBC4uGc0g4YfL9sGwBGBHZLJ3GV0+rUx2bT19x7uLYOFTErg
vYVeniWR6joChK5Iu3XsQISn/T1RG1olfl6Jd582XojI3JZwJwXNZFJR/nrAqHFH
gUzJKX1F5zxqsofPKyiNepLr7MXcgZDzQFJmA8WhU+saYSK2qw8806tdUFFWOMEP
zwWXjZ8GcHgmXNb+tl7McV2p9lXrALwTfvFU9aLN4jf1EyN+ZsebCtUsTBfPvtan
tQWibdh8+e6T6NhcorcaOXJ8b78HVNfa8uQhH4VGjEcHKDggOPmFH1IsVqAX1X2I
xauel4Yoc9sapAj5N39I0J+hspThJUrscsx7KcGaGtvihHRrPzgkcBHj420MyrGy
4+7IYWtYrZN1w4yTbdPSoxx2C/pYQ0h+CEJ60/nPIqQOt3IuiqEa2H0lxhl054Ka
2d412oNFLbOWhwgYu9u08N/sHzRsE6fL7VSOnvp++lN+ME9HFl+VrVs+kHednSDU
Fl+s4MDu+RUZO3IorZMTxbRRFlftBUXDBMNxeiiwjktMxdHSyInrYGe+XHt9+vJh
yvuZt0ZwOgTmadlnvpd6ikFg/J6DAw3q/WKg8FL613QLcO+a44ciApQAp2ux7aZX
bDK95YrjLHhl81rdMQzpQS7oJNksObVUd6btYuySUUtJhWanYg4KiEbNEAwWyjq7
gjr7qT7q+0uTrrTkGrbmnwuaZyJN65+f1KjLaQSxwZ8owLrMd/Bv+zRF5qq8myF/
mGZtEZyd7mfs8AsR365HTttJGaSzYQEBB8GkfOJDoP/YqyvAF2m/TYwFRs3RLxwe
```

```
c5P6YP3RXV0lKCnWTlbiFUyzrf/Z5KWgXWDGwV2cBs17KL59e0K2T9PMPT3pirh5
32c2DoiYYTNgUgsv0AzUkQ1PXSka939LUm00LZLfa/2Ikr5a18TK+oZ/7HNp7PjI
/BPnvinreimOmUQVy0esIMq82mwG9pGxxKIHvYPmKW8HqzRUawoGnguXc79xyMCU
cdwJ85FcBIIEqDCCBKQCAQACggEBALrTY9cC4IAZklXeHzCfWGuAWVZsKzPXmmqs
/jEexm/ENZA4HJyRIMRfM+59xBe+mQJxnBm0pFbOtwJfRQuckt1KqkMGJ8bqjUBK
ZYBkk8FHMsLKlpQ79k8A5mYovneBimZqPmd8s/oTkDrBGA+7fBBkONmblgrvuGIK
F9QH6jatUgwpPK/zJ8GnsEiTs0n4UvnROcIRD+qnTK6vIrqIz/z7YZF2C7i3fv5Q
eZe7o2dfLeecSyYw0tr+Hr/UogFISx9t0axm2Bl4lWhaW43o99HMpE1ENq597Fgp
y3SXqrqWbrCWCVhzRpOT6icAFVba8LYd5iUGTHeDKkTkR/lcfPkCAwEAAQKCAQBD
w4b0JwP9EslkQeP4Q+PTYkOFOEjXTf2hccvlTy9UvMtc2y1tkKpc79crSwzEPArN
ux2OqVnubp4syxeFJa6Te5CULPhiixLe3d1BG7oIIeYEh2zkqXcmosHvDho/yInF
qgWmjbHOJChtVzp+Alf2rhN8wpVCtD6huN15t8E5QTaq8g6Z6uZiuS+10cv0dcVS
x3I46lWa0tIyyV+T/tjzmC+dMKLzQd7kirWxRS1J4iselQnTV606tVqpsapVKkY3
ZjoP778Nj0HWcDRwDuYnzx3o7IF5NEXNW6Cwonzz2x3MnNbkZM4pr21pNikZhWdf
yG4ZPuX7dfvWIM1iGD29AoGBAMGMG1gv6dRMSz163OxikcPAcj99Fwzc3IsgtELy
gqJwsjgkrSoy62xMZ4/i9NU7ri+1I59arjaKrG/6f64HuOnDAgJy48EVwhvO/6aQ
LVecBUJwO/xgUbV4Ai/X1UklFyb9C/kUIIwM6rMnaI2ffSYi4Cu5j+KagsdFxJYl
n/A/AoGBAPccDWbtzcSQILSuGaoMw0EWBHiqkcIfkVgSg1ymG0weHPN6EktrZzn8
91opJEGjyX5NWaPVDqkrFTgaHbHfunx4nxlp2OlcD9MbZQlFE6RcBKRMr2AvPuNy
57DYyUGro20Nd8hK1MYx3fDfLjktpDw5D2C8SYCohcCHH74zyETHAoGAIHuaLz/D
V60CR6wyHb4hRqAqzHr6/l6m6PaxKjc3M3oEfyWwpk9rcX6VNvHZM1xTzI/zDZCT
gnXdoOGCwjtrjlf7I1wS21oCfNZN06+I3JZDz7W0a5PiwrkEbPElS6Rc8V8wvjnh
iH+2eCDaDELDJz5dLxlyi45w+m68IpLn99MCgYEA3iQevC/9Mb4rWKHGOoN8p68G
V/9mRu+f9l+2LXy5v2S2u/46IgisZInPRwMDL+rwgRVCBzDKHDO5wJRhq3ynpau9
wtfPgoEbTLksy/eIH9IE7jpt0fbG/ytVszo/OkT1Blz8GFeFDaLYlOfdItOv99+H
vnulS/6zNo+CbrcYSxMCgYEAlOlO5bhwjtfyt9iGIYfHij3Vphe+yZKCHxHnLOHT
8a9uKKKoeGkklZEhPaB+O0AGxys/8XdTpsShe4kf466C5wzh5LaBwgMQenqOhLxz
xmLVKtFpNSTWblQJpP1XYQwSuZ1BReE+qrXwTXWkxaLcGN+KJv8qX8pvvjjZEFaL
frg=
-----END PRIVATE KEY-----
```

MLDSA65-ECDSA-P384 (2.16.840.1.114027.80.8.1.38)

Use the following CSR and keys to test the MLDSA65-ECDSA-P384 explicit composite algorithm with the 2.16.840.1.114027.80.8.1.38 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-----
MIIV6zCCCHMCAQAwRzEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECxMGUEtJSHVi
MSIwIAYDVQQDExlNTERTQTY1LUVDRFNBLVAzODQgU2FtcGxlMIIIITANBgtghkgB
hvprUAgBHAOCCA4AMIIICQOCB6EA5PRGIp5KNxOpfWTCrQ7xkuIB5m+KWFVyuwqy
FyDYULnMf0qcZ/6sIf008tzKZVzjaTLQTB8boJGKdg6cOVURJtrE/qiTA6Ro7tAg
FVASwBcKdqLLhf52R57aDtLkJlNharrtanM/N/v1dB8InwiRbh2V8ZtC0tEmTB76
nDIlYKQfH6Crs4dZWpdDin+pqSPaH9y9eFoByI64aFOeW7fIOnR1d+uWdrPABsc8
```

```
6OlV0SV4+shVy6xdH+niq/GXD1l+4dy9tuz8Zbq84oRy/en31/uhqs3BOPLDWkiV
TOZU6TEfvubwRDMEhUokMmXbudMoz6E85ff2t42uKTWEyD/RV6yPsqT6sb4ywlsy
8RAKtMNWRg3nA5fuxyyhkeEfR69z8PYF8cLgWCSec8X9oNbGOt8bAjx5ouTDYwvA
MArFpMHpJwJWNZ26xMKWhG5Es7jwZS6Hqxyse5OX0h6Wl0BJ+qehjvO3ucFxgTI9
mjfbGyDtie8KkGr5sp9CptV/DgGgUc0qbcrD0bDz6YE2UF/rejZI1nFSQQQ94WLz
FYRFaQcPJvSLleSZ86z4Fk/ZxGfHGTaWjI9Pho4WlFaPCn9Yz88ElOjJDJFyQU76
BV85PUObaHV3xBRttVoOXxxzIm+K/1OyWL9NKlxbcMsnzdNyiX1zyKzQ9/McNrOJ
8ek1/PsHRdMa7QebgUbGS3GOrqtn2Sl1h5jCWu/ZPoL+q6ZVwAbw86z5jux8prRV
3Ct2aMGGhLRcFFgcCqUytPu3/uHWktPpbhTJIElDYAihGF56eZhsXlsoGPgtKbJG
4yZ7o+AjmcSN2qjppgd+Ow3wwghznIHMd8LfcxO3T7n9oKTDFGVLX2F8OHeHQkUw
a9h9D7PJ4gZRHk66bUNGu3uF8lmfjyyYjs2iw6LLVcpLNQRKpTVDeRYXWltR5vVi
5+A4S8SL5RLkKCaDLQAzm+HCgDVFwMY0QWiQ6fHVQJool1FAwzph3f+2WdZI0WZk
NIXk780K4O2/mIq4wGeIMU67MK6RpCs1mIb8zfzvoxg4uBE2/7fO1tbIRBu9qmSa
BiHYFruZEn/6L4AQiFC/nGXO2cYMM9EiTEsataMp8A14HXKcLwWobZ6tTsF0j0G1
AyEaXVcsBrfcXwiLCBeLjhtP7WizrfGOq3GhD4IJCEIVNdZ8Luqz4Rs6gON/wUOH
bIB44+vsQeilheltFNWKckOutHIo+sHh1ah/UIpmpvsUTUZ4Hy9aJWT4ayK9sTcB
vktA3vQcTmK5lYE0fQgvgOppTpv4puhi+l2v6qZBCZD6l/kjxDp453/9Vx/UpyI3
Fj/rPztdkUQtB5fkjD6u+dgKNcUs65KSX82wegw5Yzm2DAKiU7tY7ADP5V0ExE4t
ofrymMBUB3hOFzvLFEzuRxdtj0nGlk8/953EJcWM9NkB9qVSrfogve3UM1/dfITF
aLgoQivG/tUK/CqJdfze3JruL86fwt65gwfrMyVj4jGJ0YlIBmAlxBDo2TybiUpm
CfRQBeaolIrEoxBEthDVsjiAyV4+M9olszB5mzkoS1B2lAoeXaf6/b5Ol4xOtyAq
jmLNM/uGutjiFqCDUQrR+mBfX4TZYkyxzzVr9SKB5H+pLg2f2ZVhqaPSRiOduz7Q
dkE7cVbtwKDuUvpj7OjJBIQ2+/7bo/6cJsVNByqZUbHJc2wVbTH616uLXCxw2T9l
jhfdls29LIbiE5yFWsgOxBY0hCDa7myN6jdaqe4L3+s84rSixyc2n+5apMeL4bLk
erDaZUdEeSsgNNLhYd7fGfn2ITC1HgmWsSR2wD+Y7nbbTKFbPBqqMH1EUhiFZzVt
Hz7nSMZlndA5m7n+fyckP1g8FS1SBCnGYUfwljj9IvUfE5LnOHTc1WuCOgSA4g1k
YQY76pOi97ARvkMoBU7AMkH88Qxx/dEjV3qaFT3CgXczEsqixQhrUpQg8pDMuOnp
Szb1Sll9Lg5Hs54XKkyQDmQDiEKvBSsblHq1yXFT6HS0J5s0Wa00CCNGBJg9PAMb
hee6cjOmhQxQyXgvEkn5GZm/BfoIAoNZ4CEcd60PI3lhf5Cn4NXDtXAkw8k/c0Jg
g/vuxAmsZl7f0tnrH9O20adGT4sy6Cu0YDZHb9f54Riu7IXANHXlQSPT5n+2hmaf
KxFERL32dsgINW8vH9+nCXdnPU/sxAOj3sh+xJFrjRApLNVGdLUarkUEIt/+HmOZ
tY7lnmu9CnX1FLbSt+pyqCzChqHcbBNDLdM0n3qwc7RaVfMMst1XPpgFoJDO/Op5
skYVYo9skDpI2qb5Hnp8wVxNthvYlUTryPnKgrPH4aMeIrUbmGK3VXonlbs0EEwb
IMb14+c0PdNeABfDaxeB8M3hTLb02uE3gGtQaRcbDIfj9tRsv82mVY2UkA36g1AR
mQDH5mN44J1QjXUmlyhhmc9ZKWvgpatqpzc3HF8xuMbu3w2LGNsQ9GHAtNzpSWVB
j4Nq50tWR/1gzOA6VQZGTUNgYffsjpKdi4+s2BRSt9/QfINXn3iL1b8DvtG6OLMV
KPfiofNjQOPqtWRte2R2s+2kZ2mxZ6kNtKC3ViYDYS87N+Ph/OSwNw6kxX+MF2ck
HgsE73QDYgAEDRRxuokt5cSSpnX4DHMD2URAzUZlSiUgdOHyR4QlZVdK9lPmN40Q
I1lYx+DAorp5YHM+CkLNoZAl5yUIjzhQtm8DjH6FAcqAw98+9nySeeldvMW3eFw+
uPP/6QUO8M9boAAwDQYLYIZIAYb6a1AIARwDgg1hADCCDVwDggzuAMzUv2fgDb33
H3SjETHos9Pn9MZ/mxoqAKH439KM8XuN45UVgAWOZMNI/VSpPPLWZ9bsDg02eBIX
UGGbIH+2cGXuY62Vodn3zig8Zb3DYxHNO6kv11vPFOplr3lFC8zkiZDzZNTRrs6v
7ri9YLtfbQxFt1cEoisqhfEeyJUcpwcoEfN9aixny8tGNGCD2Jtq5Rnuw1zHdT0A
UqbiA7lrIX9jsQuEBsmDD9qWfX6yQnCTJYr1Jrl9/lTd7finxZ8XthNrUNVXYQEc
yQenJU1fEW2UuZXIm0KkBwDMFfpPMZqwQpgTo1T+RaKNVafvgiPtenW8t2CGzvhq
UJibDXJVl4/JduXFQddUn9wPlRPqhcODD0emBb7kadiQxb6v/1Yqu/QpdOljMFGm
e3DpiJmJ4vxQ9vosP9ynUeZKyQptZpp71dI4oTCqUzQs7o6R0kyxzzmkNUSl2Wo5
XTf7LH7ri/ziWPto7rqBJH0nylM4kM5/nUJoJXdMz7EHONgjJaTInxZDQq1MH8/X
fV7HFXbITabvy2tYZ5YBhSkuv2ggAL4fBS2spDn4vZ19lxY13HR465fY8GrRq1pW
4rwiC0MwHqNGuDRI+y+dmCEIcyortYB5hjpF/Z4rKT4o4QBAOmFHOWjVoffv9MER
QOFFwrC5Pfr09X0ch8eooLENhNf+uwFtIloT6r0bgOD8KFOu2bnlI/MUNzTJanQk
OzwkFZLi1I8BXdX0t4xg1LaU3vr+EVogg+z41v5zqL8JCrnBRdxB6oKonpOK+kGD
dzWoqxZlTIKoLu/z1nVa8yUudjnAVscbwIJrROmnH5RXeXIGFB/uA/Qvzd88n7B1
```

```
2LBKOfz94D0mkKdM+Pe2ITnsTRAQHI3MkKbF0NGtgC1kR134n46/I8L746e1Gkr+
y3cv6rIqIluaXMeW4cK0WiYC7PD1C1a3mJFpDZ7zvCD6z05oRft/VPDEg2fRWdJm
JWGkYwKhPlr4xv77soIqrrtDsyjrXLFKPqXHln8niAqnlecDlLtlNdxNFe3zRoBR
lNrZK6fdD/TZ7IC7GaiNqx1HM/XqQ9UDpoxZMfCzIJLdPCSDoQ8n8WZdxqt/7N5x
sUYXKHvp1GPhcU8cNOG89gddYeVpnxII6B9BB2xW/MVVaeiUomCtlZYYzJeRWyY3
iYOiwYOHYLE6Cm5SdE9RvRmId38X/YulpossgHaEjLiyZ7nKXp+3kARdKHlkXGU9
kaKWryvczfyDi7z8ly23mg4B2WWlNfUcfoUUMWVnn0AmI7KgUFGrvp+i4vJzdyX8
rDcvp5e32vp8a7L0azUn5qDXq305NwSmX3ha9oXaznxkEQgHVbhpVDN3510YJXHx
pO8F8Tr9kKKoMfFxQJ67q6Ljd1km8Y/crtNxcNOKEcHyHWcj7w+pJJG47K+DLxjC
5KnD350YXHMUOeU4FS8ZvW6/ZdVwCAj7w0oBvh15XYn5tUOuMCCYE0+HDlClRzkJ
xprF2uYD5uZ8W6R438K2iAEm2qYW0ezmmj2B/72mtls10QjsZMcnPnUBdn2hwJVX
y5xhJ1MuE0o5Y4mgUcCf/hc0KWq9wd+h8NlIyS9b2wgY2d7HDBXJ2Wzh5hQ3xeJY
E5zyiGwE4mPbvmjaFPucO46TxkV9ZfaSNRNsBtzNHt+RVXP46DDIOowPcyAW3kSo
mUKaUrfuBek9JTpAE48F2Cd6wGsGQmmhR1qX6a9KgPG6ZTQrv0cZPXLgV4I6EfSl
lcwIl4XAsBb+i98uFrO8btDzvPLCK/C7YnBxfi6zLZxO6eKo5owtOnv8VQcUNlOb
IbfV8kL1czBqabvbuu1hiGwcJKSFpqCUfZkVJMryWdVUTxQoKfQRZAC5KNsdVP4J
+rAoWo4vOiBCWXYjG2uJcVOzMSUf86LzbwB6EDli9fez8JKZZy9Rn77s6ptCyAlU
qr/GZXXtzhPtLJ53a3bDT0g6N9JQqfm7uh02z/RaV4qcN76JwEfZRUVT4DwQRSpl
kTonv5wV4JAEoQ5jl9/T4VL7tg6JBx78qCvEbLSMYmrIXNZfVIYXlPde9Q6SALNM
2Q9iEAcLK2yYpqYPLpEX8o5kzQcRDB9O2ScoxTSZgcT2v7Y2S/0QWRCNU4Qb67XI
CXpbN0AUcS1T/iw0+hybfnW+f5znOvnE9Ay8lBGhunvXjorDymthxz/xUl1XmEYI
ZdVzNtRoo++p6vQS4+AmZgogSd5s0sgq+EKfCmGFpjxyIja0C6mG7IFeOZDRNdLE
XiILpuYPugKOc+HGXdOartDUS6xD0JslcUZj1e97QhJca4kuZTgYg03YgRNMLk+O
x7YGdLSfzFZpGCb6YYyz6w2LfyBVfYX7mrrfGwiH0KN0cB6gLvtSDQBHfbOVMxyQ
Bg4Te/EcMbr5f49e7kuJ4s4FCLB2WKw0cf2E3xXUPc6C293lOy0+MB9vBk9LrSl0
xz1aK3pcX5MP0XDJFdQ4r4EZLgfs/uAuSEoPVMQ2jBoF9C1qRfiVkkyalLzFF5la
ZLsgnMNnWEw/FIknN1kMNC6DE0x/vja7Gjx2k9UsZXRgFrlj4QpruCk8U21xPtq5
hOBphsGNqmntodEhVzZjaOFIHu6Snge18P6SCISldH2Byoa85dV++ejKyp71Z6wM
PvwQ/H4NeJMff+4HFDoJm+5OviUjpOOFf0EVEba3TpGFt+9H2YvcGd7fhj1sB6NF
xB9Xn5dzztgtN2UWMKVNfZvieQIFsNd/qL44NQ8hoEpRfSgQEKjylHbPcrchMYx0
NWMkpQgPOTXFHZvGwp505ovpLmdWevsY48a9quZ5k5DaaVpVP5Ps1BgDRMYM5VXj
aeDQ2t1/eBz3OC4JT1HwEnH9Y0DBJ0CSyUGOxl7Q5+sNkDHykQnnW//GCieJ7nQc
v6Gd4zQ9oJEp8xlrI+jZvwN71qvhqs9lXjJ4EYYHO9xkOxX4cEaROQD485FVFPIA
oyiaH8EBhOxpgqprKKQFW+qnIUBXKZNCuVpztVOemPLxoznIDxUjn77yUpE5/DjO
hw9BqlXWjEimD4Jxkh4SwWRGM35jUIbmdZFc7G8k0y8FggGmnxGnqxyNhMWK+iDp
7IcTdhipk8+pu08/XLIGivp2K36LQUMBxnePtfiHfCsY6mnr9uo62x/3B2J4up83
gqDeFrrpgvLJtX+0kWTccfXKpB/e4BXDDXHinjeFyXHigGY8No/T0k5wLsizB4tZ
abR5vj0TRsfpSioL2bLDpOgGYupOiCcjpKqXVCNdET7WQLMVswBEOF7Qk4S9zFil
ktuzssfeHsxg1QLfBSG9Hq6u+5U5nmcP5LQ1Qft7/dLJfJV5uK/FMR9TZENrC63C
J/11Kf4JW+aobt24HhWHK4oHKCLM8hDlMsQMHPtxDnpXgQxkuj/zoCThBblVe5jH
t3LBhBhkaa+b45YCytRFuxeS7gOLNvFak3/9tJJ0r74UHUfQOHZFH6pBZzhrGLqA
gijFdWnYRm8rLhKjbXRo7U1pciJdtjKIRzDb8OVmofOKTbheCd4jBORdP0VIg+1X
i/eyWuVRfgf3jrlq3VqDP2hZk7KCBkG9h4EKIfAcuN42rNIK0zsOLQI8ZqC0rt+c
QX4cgjJ4f9C8POPVK0z5ou49SHNgvDRY03c1eDJ/dVNJZy/PNOBGh0Egj7YlgYG+
v4++hdiOzdGL1xB9CK2HolGCzxOVTmEEBupikEMM8RFLOJE7bUoYst9bGSwn9ZQK
sv/rY+zqzYIbvWRgeFgv/vyrrty5eevwbRAXiO1I1BwfrXgD8F37wRE+iVZOUxpz
NiFsKD9EbXdNazl2v3Ud8A5hLWuQOoGafRKudkDhw/VDncKxJca7XfkG3SEnQ5MD
1K2Z4+3CxEBEu0pXKyG5z6b1dOuS3HBGcYppcbbuEeUrdqBi9BmhEqTmmyeBT8Hn
XmeI+83nATTTMVZ/I8micNUH2MX9XKrKS8zZGYyD3daYuncZEgn/yHGSJ5/WI5kM
XNgN+qG5lB4oYWM/GbGW0q1v/QIm/VnHwkrhen4GCtw+mL9rV/Oka9390+UzhTOM
lARxDuz1QBTpvkawVWMbs7DZf1bzrmj2Os6dk8pjnAkC9FX/Iida+KATdN71N2qg
wWlegrbJSnVKWRhz+gbRzJREV+YMmCcequkFsmzx6J+oVU4zrCBYTHoc/lwveKXP
5QmqhuuGVHbhcH7yM5vTZW/9IRivfMTvhQNQbaCKhb0Li/Z0fTf5mNB3Zbg/P/CF
```

```
/S43dOgJRiTKOcSSb9xLfJ4s6+xF8JDb1b+Q6nALRrCa5srZ5Hosv+6L5ViBuh4S
GQBHERl4jY7/Aygsyk7M6YHuRn9Nx8zuJCxWdXydu9bd8AABEkFSj5+uvdAKCxUe
HycqVm94tw0w7RE/W8ohmAAAAAAAAAAAAAAAAAAAAoUHyImKANoADBlAjEA9rlw
N6BBuj50CpvMgykN9NmHnroRxxKF7tiUXHN9ZWAYVlQvnwYUiOjeozML6og/AjAc
y+jfjSgw/wry/3H9gdnacubdVcb6g7jBxTh9ySZuJNwIBO1Qw0f4zB3/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-----
MIIIITANBgtghkgBhvprUAgBHAOCCA4AMIIICQOCB6EA5PRGIp5KNxOpfWTCrQ7x
kuIB5m+KWFVyuwqyFyDYULnMf0qcZ/6sIf008tzKZVzjaTLQTB8boJGKdg6cOVUR
JtrE/qiTA6Ro7tAgFVASwBcKdqLLhf52R57aDtLkJlNharrtanM/N/v1dB8InwiR
bh2V8ZtC0tEmTB76nDIlYKQfH6Crs4dZWpdDin+pqSPaH9y9eFoByI64aFOeW7fI
OnR1d+uWdrPABsc86OlV0SV4+shVy6xdH+niq/GXD1l+4dy9tuz8Zbq84oRy/en3
1/uhqs3BOPLDWkiVTOZU6TEfvubwRDMEhUokMmXbudMoz6E85ff2t42uKTWEyD/R
V6yPsqT6sb4ywlsy8RAKtMNWRg3nA5fuxyyhkeEfR69z8PYF8cLgWCSec8X9oNbG
Ot8bAjx5ouTDYwvAMArFpMHpJwJWNZ26xMKWhG5Es7jwZS6Hqxyse5OX0h6Wl0BJ
+qehjvO3ucFxgTI9mjfbGyDtie8KkGr5sp9CptV/DgGgUc0qbcrD0bDz6YE2UF/r
ejZI1nFSQQQ94WLzFYRFaQcPJvSLleSZ86z4Fk/ZxGfHGTaWjI9Pho4WlFaPCn9Y
z88ElOjJDJFyQU76BV85PUObaHV3xBRttVoOXxxzIm+K/1OyWL9NKlxbcMsnzdNy
iX1zyKzQ9/McNrOJ8ek1/PsHRdMa7QebgUbGS3GOrqtn2Sl1h5jCWu/ZPoL+q6ZV
wAbw86z5jux8prRV3Ct2aMGGhLRcFFgcCqUytPu3/uHWktPpbhTJIElDYAihGF56
eZhsXlsoGPgtKbJG4yZ7o+AjmcSN2qjppgd+Ow3wwghznIHMd8LfcxO3T7n9oKTD
FGVLX2F8OHeHQkUwa9h9D7PJ4gZRHk66bUNGu3uF8lmfjyyYjs2iw6LLVcpLNQRK
pTVDeRYXWltR5vVi5+A4S8SL5RLkKCaDLQAzm+HCgDVFwMY0QWiQ6fHVQJool1FA
wzph3f+2WdZI0WZkNIXk780K4O2/mIq4wGeIMU67MK6RpCs1mIb8zfzvoxg4uBE2
/7fO1tbIRBu9qmSaBiHYFruZEn/6L4AQiFC/nGXO2cYMM9EiTEsataMp8A14HXKc
LwWobZ6tTsF0j0G1AyEaXVcsBrfcXwiLCBeLjhtP7WizrfGOq3GhD4IJCEIVNdZ8
Luqz4Rs6gON/wUOHbIB44+vsQeilheltFNWKckOutHIo+sHh1ah/UIpmpvsUTUZ4
Hy9aJWT4ayK9sTcBvktA3vQcTmK5lYE0fQgvgOppTpv4puhi+l2v6qZBCZD6l/kj
xDp453/9Vx/UpyI3Fj/rPztdkUQtB5fkjD6u+dgKNcUs65KSX82wegw5Yzm2DAKi
U7tY7ADP5V0ExE4tofrymMBUB3hOFzvLFEzuRxdtj0nGlk8/953EJcWM9NkB9qVS
rfogve3UM1/dfITFaLgoQivG/tUK/CqJdfze3JruL86fwt65gwfrMyVj4jGJ0YlI
BmAlxBDo2TybiUpmCfRQBeaolIrEoxBEthDVsjiAyV4+M9olszB5mzkoS1B2lAoe
Xaf6/b5Ol4xOtyAqjmLNM/uGutjiFqCDUQrR+mBfX4TZYkyxzzVr9SKB5H+pLg2f
2ZVhqaPSRiOduz7QdkE7cVbtwKDuUvpj7OjJBIQ2+/7bo/6cJsVNByqZUbHJc2wV
bTH616uLXCxw2T9ljhfdls29LIbiE5yFWsgOxBY0hCDa7myN6jdaqe4L3+s84rSi
xyc2n+5apMeL4bLkerDaZUdEeSsgNNLhYd7fGfn2ITC1HgmWsSR2wD+Y7nbbTKFb
PBqqMH1EUhiFZzVtHz7nSMZlndA5m7n+fyckP1g8FS1SBCnGYUfwljj9IvUfE5Ln
OHTc1WuCOgSA4g1kYQY76pOi97ARvkMoBU7AMkH88Qxx/dEjV3qaFT3CgXczEsqi
xQhrUpQg8pDMuOnpSzb1Sll9Lg5Hs54XKkyQDmQDiEKvBSsblHq1yXFT6HS0J5s0
Wa00CCNGBJg9PAMbhee6cjOmhQxQyXgvEkn5GZm/BfoIAoNZ4CEcd60PI3lhf5Cn
4NXDtXAkw8k/c0Jgg/vuxAmsZl7f0tnrH9O20adGT4sy6Cu0YDZHb9f54Riu7IXA
NHXlQSPT5n+2hmafKxFERL32dsgINW8vH9+nCXdnPU/sxAOj3sh+xJFrjRApLNVG
dLUarkUEIt/+HmOZtY7lnmu9CnX1FLbSt+pyqCzChqHcbBNDLdM0n3qwc7RaVfMM
st1XPpgFoJDO/Op5skYVYo9skDpI2qb5Hnp8wVxNthvYlUTryPnKgrPH4aMeIrUb
mGK3VXonlbs0EEwbIMb14+c0PdNeABfDaxeB8M3hTLb02uE3gGtQaRcbDIfj9tRs
v82mVY2UkA36g1ARmQDH5mN44J1QjXUmlyhhmc9ZKWvgpatqpzc3HF8xuMbu3w2L
```

```
GNsQ9GHAtNzpSWVBj4Nq50tWR/1gzOA6VQZGTUNgYffsjpKdi4+s2BRSt9/QfINX
n3iL1b8DvtG6OLMVKPfiofNjQOPqtWRte2R2s+2kZ2mxZ6kNtKC3ViYDYS87N+Ph
/OSwNw6kxX+MF2ckHgsE73QDYgAEDRRxuokt5cSSpnX4DHMD2URAzUZlSiUgdOHy
R4QlZVdK9lPmN40QI1lYx+DAorp5YHM+CkLNoZAl5yUIjzhQtm8DjH6FAcqAw98+
9nySeeldvMW3eFw+uPP/6QUO8M9b
-----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
gBVnMxZBNgVTRARSMGM3ASIQaAJQh4YTNoE2V1Ngg0hjZ2GCRkGIZYBYU0MEJWci
RjESEnaFA2BUMGAxVQGIRDAoA0hhAzMCiAV0gzh4BkMWY3IlEhZkJXKCUHURE4Qx
UAdIEWMjNycDNBYyEiaFh2SEAXGDJxYWgTQFdYUQgCICFRFEVSBoFTUUWENDhyZV
gng4QYI4d1dTYnMDJzgYUkIYQQAHYRFjMQEWeBQFEENTIkRIEUhYVnMRgVRiiEJX
gBKHgUCBEFVlBlE3QVMHM0EHUDFlJkQmYBaHVyF3hhMxZEQWdUFmACAANFY2RgBB
AoRicIEVU0IiBAdWJ0JwdDODQxFzSCckNmE2ERRkGDIBCIBxMkUWhAQXJlNwhRQg
iDKFcRhSV1ETVVAhghhGExh0UnBEdmEmVAJnNAREdnQ4gwNoB4h2cSQBYgVAh1Il
VEUXE3J1cAInaEJIZSAxNQFnI3JAIid3UHGHA4I2ISA1ATRnckcUMkNlVjg4c4B1
JBEQKDYAMyUShkBQBwQyNXhSZQd0N1EnMFGBdQQwBRB2QHGCIQMyFWh1U1Myc4gz
AWSIVVMgJGMjVVcgYlgRN1hmRyYlVTRQVIiAUzYUMSUTJRSHYWhUEDhCMDcgdSg2
MSY0ZIY3UTVmMBOHFnUGcVSGhYI1VWZgc1OIhCIiV2EwRgBkJYJwIXRROEgnQBOC
GIM0AHeII0QxBkMGFRgnBwRUVSSIBHglNhI0IUYkBiAAKBEgYTOFhFVUYTIVR2YV
RDYnNmUDUXcYhVYmYUAVghMiIUQ4Q3NnFjdFBXhFdUUwVHQxOChmF4cTYGJhIAVn
chREdyJQcHIWUQJoaAEXhVN4cgdDh1RVeBh3eFYQAnFCUChgBAJ4JFZYYVhziGBl
I1gAQoM2iIgVNEBXhXMXB1dlJQZQR2YHWIMIEXJQg4ZVFCMnRDBDAmQCdScyQzBw
FzdidSABF2Q0EFZCcCFUSCBzEocSUiBxAWcII4VoZEIyFyBWYxcXh1MxMmZyYBMw
BnIkMGQxIkV0iHUQcwd0VjAAMjBwcohGNCEkMgNWJAQBJ4UTMDNXgUhzAERyI1Am
J0c4EBZCEQUHeFNyYyZwQBNXRVVWBXhHIleCGBQ4SHd0JziDcwMRNSYAQ3iBV0UD
hhBhB4VEUjNUQ1RiOEZFgIdgETcyYIYyUmQDcANxhlZ0ZHAQd3N0ByZAeBMCeDeA
Q4YDhQIFhnR3ZiImCAIjNEhVRmBSZBczcYcyVYKIaAiEZgcxBjQEV4aIhQQhhoYB
c1JWdBGHUIhVB0NgdWEgOGRnNXgoMwQ2YEUicncXYQVhUFV4Z3Vyd1R0BwCBIkRC
MyUmWDcnZWRWQShEEkhYaHRngAKFgRBgh0ImMUViBoYHckZmCDM2dgEEUEJ0Rycx
h1FXgANXVYJBiDESd1EFIWhYVWGHBVaHMCcgJUUSdnJCCIFBEYIChFJoUIRCCHCC
hAEIE1AHcnUkVVYWVYUiEDBWVUh1QDIWUFYTg0B1YwVgZSAAckVgOGZXhjI3SDVF
ZgQBZEIUFEV2eINYJGQkVAYSU0AAUCI2YYdXA4hRE0Y0dihhJBIVBDJmZEUhhBcX
EzhVhDAng1hUY1cBYYNRJjECMHQgiCGCQDUiMDBjgCh1d3QGJkMjgUZGQIVYRzSI
FEOIICJUYiMxhUcoQTFSd2YyWEFVhmRYgXQkFgNwRzg3YjYSF2VIYAc3aChneFUn
MEcoYhZGcxJDNoMXBjQ3d2cSNjIxg3NzE3FieAgEhwgWA0godxAmNAAGFkYAFxJi
BhUHRRdVJwcCRXJhKGAHJoVIBnRoJWYVASZHc1QDSDIzJygoJUA+F40nzgs44bUN
fvEqtoO2c6rvsZ6ldZt5IIWlRFzfc+eAwvSzj8PbKlg3UwkMt54yl5I9qvzNbRsj
SNn1MD/KfhUjW4XE9A68d1PAg2Kw5ZQiAj8C32Go+YrNzymRwtmj1wwplyK/thhn
JBFTqsSi5JFr4GydVXnySQqXxSRWYfBILibXecun46W4fgZXuI3Mpodg8oIihXt5
SeRjl3efJmnQsR12BHrtKwN92Yr33WAf2QNbf9kQF3jeQCWYiQrixuc876D2B8m+
Xb4CanpP1Kvcj+i4+Ke5oKdR4gECVj3Jukcq8t9VOx0viL53n0jPT4cpyzcTIQ2S
wqdjh0VxMjB3HaBTu864cdFzw9S5SoD/8BFdlVHL46ulWTWITAp/GZcvn1Fmodwf
```

```
4JuaUamMu4qOJqSrph5l6Z0ewkjf1EvQ3TGsZLKvmQPvWl6BGjDtbNjr+SELGs84
zwwlrLNkNxYmvNtCipqvCWzQDD/JJ4/I0i7PhzQ1R4zDAnQWUvCDu0FlYvjWwZgO
vhU/8PkVgjvnPb9qRHKlA1o1ryeQPKkK04kNeVl6l3AEZiDKIh2O5tRfQqBqpX0l
g/ET5H9+27RtSj3a8gS2iZeL0iE8PRuTn2SeeQ5//shcjWCB3OyWds981R6aD/hG
gU97UpqGHHF5kDkyVrRkci4xTXFY6rrrh99AzY14yrCIbxk/3zApTHl6kYq2iwLM
fhtwMES9ka/gBdSyA2/w6+INm2UjcSABuH0gurSkI+lnBlEOs8NdpbHy7Oin6op+
9j8c006aZrDR05jFxUAEswuVoqnuvWWqM+MPCnqRVxOGQZ5CRhGNKgDsXLcaFAxd
6GoL6cxZVIqlTbqRxrqU11zAvzaiY5Lg0/1zCLgGUMjBU27vxIZWTmKzo5oQxZoU
rnRrw49Ii+W64CJM2sYa/95qRYk2YFLRK3iFMr23pcchP9pP7pDrJBiVlQ+cmsv4
dH5nCJAepAq8AY2cXB3QhiQdLxNiXvLsDuJhTJg+BPD+M8aKIM0gWm75GT8jZTh6
/tRtfeAFXnQUrqn0lLoJ3rpIR27hQURyEUBrn7p+w6HZyZ3PPm7OWq3JoH8aPWgN
21AqLyWYim8jqdvI1WZUGEi2ogcYteQ5zrI4U38r5p1jAkGgxTkj3jZdNAOGzDQr
j2SMpBnkn7KeO9kSaE/O1oLxBBJmwuk7pFEQ3/D+U5giKBjtH0u+QSBcEF31aSll
NGu8O1OSa/MWnAaGmNEB45K6jWQ/wJg7KQpfm/sLL5Ian1qwys9cvVRfivenFowS
fV6yraqRYfilfsIFsDWDPtzR5lhg+EAAw2O2P0CaJKJqINXKtdeXhkifyvaZ3SMV
iV02ctF4EnpY8TVAD+S/AObtIcP8NabgAM/gnDM3UbfT5AZKjVLz+08KvOYig8Xk
Lb5wkk+jUWyY6sbnUVh5LfRr2YO0SEYhM6g4XoWLRAc8kD0icpET0u/5LtQV+J1r
yRXoaDGUS1tBkoyAWE4pFYsOKLROAXDe52IlJhm6ZkK3WxAMzqnSevTnFvnCtjBo
uSq6bFls8+0y4eah0cdFcE4ZoF/Xt0km3JhS17N6U4COVpS8OYYmWDm+N7eGHFFl
qsLC2Omk8DghyMuXTsmQ5hdT2r91zT8iRCdmYeW25lKmLFUY2DenNkOUGXcku5ZE
xX7IPiGC/zsHAnax5nvcz7S6kVB0IWXOn4PrD4XPrGJpGRodSpDtkcRLu1XszwHa
fyJGB+bO8B40klWsm+Q8uRxQTaRz98RcEhZuzUQuH9Wc1nkOyUzXosUR/4AXLrC+
+qGLqEq+WVscXwlCwEuSbCDUgJ4TBJbylrtSS7EHkVMMnRZZuyNut/SHj8bcdVCk
hSNXAQCdsoQmgJwNVhF0638f2TpNdEEExhSrFOipWszy2YwrlP5ycDycD8eu3BN8
l0Wy2Gj03Lf9b3wiJ6crF/XZ+nVSljaXIGsAteMNN3TZRkTqvVFWXxilC7M3tsta
IBj9Lqp+z7eJyiwB6NlAn1PZrnwgynAXF3MTmoDoVJD+/oH/50gExcGL9E0W02sg
LmM9cYmFvEK8xbfAulOLQrdTlWM10ynX+SJeN9AIJ/8XSPbMnbatKi2pxFr+kVv/
eOwayv/6U8s+DE0YYf9ckkNlYspS8UBwfqFPc7Wp+rDlj7IBmHl/6gkwl3eahnxa
tifzi64CpSnXUXs56vG1W2ARuPqqDXIxaDwGbwsWS9rtmOaP73NXwj0MyDnOFI7D
Vq2tWErgx+hZmP54IeSqWdy3ecq7u+ric8lyF9gGLaYMrFW+BShxwUEstwcNqfZR
jnJXXh68RKvdbBpKrvLnjizdKdhK4N8RNJ1COdfYYHFVCAmptw9d0wOMshLCovFM
21uzAD+PFwWDFGpbO9lupDIbLUSkfJ2lXpuf/5E8gTVOVwoAQrXMq+o7UQo7l8U7
iQ/JcW8Es1qCuGXqIxmdymU15kiM4jnAQnZf2cixo+anyH8K6cwj+wyd3yYPw+BB
lgJBz72xio+kOP2WSDqhJm9dxpJo04DPXQcn/i/T5aDckBxKN1tPJMFLjsomN7om
eNvaVpSltJoD5oRPYubt33nymigv6Jh4J16WUyE4aHrvQkRuOftK93zKWFyMOrP0
LcNSBvsLz/NqH3YvD3FnFpEJzWiZ0CILD9fV3BUr5V1YH6RmkwkMsk1CHmJC+dhz
NPvsaEsHbNxe5xZbngeUDhRfKmDfhhM28IJVUvCt+BOlQ56ZoQs8dFSENTpXXv9u
oGj+GfzxBl8O70UApRygyiYEHqbT9W5QRG8/j9dMsRIeLuffhWCG+LQ5L2vxBN0V
0YE2cnkbortxTRISpnk8jFE9BcdSLweO6zBSUv+qZph//39Vvx8YNL1j4PgzvrUS
yvfI97qLzN+F+8pAXOTcetThAmgnQxN35kzsNJp4H0laFf+UIluEzMbEIOASuBPu
lqgGvOKesyiciqr12Qg7rMuDS+SYd/8nCkeAuWg51LCAkdbrRn1oyNWAx5ryoROh
AvmUeZWQ8FY+/uazaIIj9BKDBGVHE7IwwTqmZUefZ7xyDcbUO3vdFqMFCdQ4BnT1
NNIH/SBMRAljFcspIgkoxvLtwa0SqDugHqU8xoHM265cSuLMDHlSlV11aEy7QPRu
YIDLGBLqcLxb0a9DGR8Ve4Ux/1zvdkTN9lr1/F+pF478Yxy0kJgNCkybTFfy1ikc
/dJ+1JarPXj1SS964hSZp30N0njeZpBLRgJKCjfjBM1RmOVGYHbid86BEaX+Yw0y
5R8cEF+0cSABvQN95tuC8wIrnEC6k30aKJcW0J6JCZBQxfXNjXYEgacwgaQCAQEE
MDjt309p164qWqk/V76DiiXxgIfmOQPvAZPjBOepg+C9ZW/Ng+UAjeG2rT9OIZoI
56AHBgUrgQQAIqFkA2IABA0UcbqJLeXEkqZ1+AxzA9lEQM1GZUolIHTh8keEJWVX
SvZT5jeNECNZWMfgwKK6eWBzPgpCzaGQJeclCI84ULZvA4x+hQHKgMPfPvZ8knnp
XbzFt3hcPrjz/+kFDvDPWw==
-----END PRIVATE KEY-----
```

MLDSA65-RSA3072-PKCS15 (2.16.840.1.114027.80.8.1.37)

Use the following CSR and keys to test the MLDSA65-RSA3072-PKCS15 explicit composite algorithm with the 2.16.840.1.114027.80.8.1.37 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-----
MIIYOTCCCaYCAQAwSzEQMA4GA1UEChMHRW50cnVzdDEPMA0GA1UECxMGUEtJSHVi
MSYwJAYDVQQDEx1NTERTQTY1LVJTQTMwNzItUEtDUzE1IFNhbXBsZTCCCVAwDQYL
YIZIAYb6a1AIARsDggk9ADCCCTgDggehAH95+W/h3bdZDShFkwC/NzNTgUPycJO4
nDicyUB1Xi8rp/yN8fNB1T86ZFJ8dUYDBYgVggGjBh9I9BHKFi5T5Y2TevuTeg33
KAnviHaVPeJS8TrU0t20rSHGPyZv1jyITpnX8m0bsoqBP3H9h3QE8xHWYLj90pIK
sS73IUZwkTa2BuIfPbB4cG7puwBBKoUyCpWmJtxkBEUGUR3ykyHoOH8kmhIYjwmw
RjGBIS6jUARxaf7jvdto7phE5PgFO2kKQrJl0tkZCGrrM/r/qWIUZJEudxOrZbmr
aSD36rkZrQ18hVAo2UMqjYCmKCWX5DDoZ/trN238wQC6jOMnhre6nCWOIjn4MPaW
21A/uPyENfU7bSN0XEuK3KM5f7PwNNXQ1AgFKiSL+Yb6cbkvwm6VFxoLEKA3J6Vc
IZms6gWhkwp+BuaH1SqvFB+VRF552hrX9QlRpVNe5RbyGZv2sGqVnloiri7FuIu/
uSwie8XBhV6aoqeyuF68fnOUGoy3moQSHNrFiTFeDfoo7di6hL/9iFtRH52Wz0rN
Y1RXToNQ/HFPhqhRlB5A8H0kfXW9yxe1oAd5p4gIFLfvhlZN+2fBeFgfx9cvwFTl
52y73vvI6f4r+IivDLEky6gnmmPQADzo0EElAsNLHcwiWhBRwn8Lhd9o7u7ONXSd
PMEgfCB2DlJBr1b22OzBCZ2kzxfpxpD27QhslhEvD193fvg0hQk8sKGKE7LkNgfh
4IxPHt3FMXcI9weVkHs9ymzLn3QWK0egfvQebzXl6G9k026jKPBZ719rpqsDUFzX
jGhC29ehoCPfo/aPShWQ4IME/4hfbpJ4k30sUd+tHqceOqe47P1n3xLY5nH/rLMG
6T2KIvdvhgxjnTyM6rAqfFHSa4ZHA+KJhLKCLXGdzbdiWP6jH5uGr8ZAURPS82D3
GoII8E61GCe8kz9EvHRse8mvByR/ExPOCrbhIiBCb5c3dYJewngOYx5H6ohbfeok
l6FpCc7KB7/LfU7KBv1G1RQIyA/8Bgbctz7H1bBJeanDnsYYuRB6U6zMTI+yAYa3
PBuEGAE4MVdjeHwt101ZZP3R6QhsijfC8cpOrMlh9/VXkZ4j9I2G9l4J8UTWij7C
wWKIyDaKkEZysczRCNDIyQLstwl43LAiG9RiA2nDkDAlBCn0fZo79ArRHsN1vR5j
9LCT3kKDksw8FZeY3PGKdrlOTTa+ZDBp6Dik4AdeOOz7Oh70P3QbbB+/YZD+HHmT
P1qiW03Mfy2DDavpK+KUn9Xo+8zNJls4CN/qOU8gDJIeDGrT7/DF9A1arMAJb5I5
6OBeoWAEoVLkDBKajJDGbq1xtFMXutb6tPaIWivyO1WUouWz4tx0vI9sxT2EqXy0
48GjUijKjeiYt4775eIqK+Bkt/vBg7BbjCwcWNNCyN+NPbk3SX0FGYWzagTyrfWk
fFC4s44UHS6rJMOqMfW3OLigGHZJLXi5wlaN2dXaSds45tSf6LuqBp9ih7kHC2L4
55Dr79H+3uN//ZrD6ODYNVNlrNxV0DK1YgDZFaKL2YUH5L6e827ch6/v9G+pS9iG
GIzRKQA8OvG5uVumzC6+uMam/NTd8x2U62NzyipqJPWwhA9mVGdIdOCDy9rU/rg5
lhO8LOXFArcpDN0+ipdDajnu0byDxK15oGOklk06fgsC0GsEJMMjkRwvB/vXRa79
TB35c+AZJ8OovcQNukSQVMJ56xb/+55H6AZEV17kCL5s2pI5WOMLRWLgMWvNkKMs
K/JDapZiS0Z7b16y3iRJ2xtXSbIBPn3y4q8FSuUQq/Fe6u1MOAhJh6noNY74K5OG
iaez9Q42rPaueHmQglMXcjH1joLGDpVCMzGcv1XOfT5UVzpNtVy5Hc+1ZFwzn5DV
wrOj2AcSA9+ev79ANQx6p8EhwAlcdLX5wH072Uy96o1O0TkzHwZOMmKnW+2dcPeX
hM1ANhdMqTez/SMaoN3zQW4JdjWiT5DWrllFX9IulWOEgphq5jSh48cVDFUQR5ZV
bmTcJLWjssuJRyZJuK83piQFuJTl8oK/VkXY4a0H/+YztJNOuoNsXziqsY0OUbuU
Iil5c80Ejt6r5QRpf5jQx/AAf06kMwxcGYKs9bKaSE9ufXi7X4D3DiGp5PJ/vAGK
eZ4nf5I/s7bDxLqV8ybx+/HVU474mkNv5560YybQFQwXI0tiM09DWys1RRQTRBnp
hlGXGl7BWmnghASaWpNsSMk0COrLElcQLqrg1iQ3IQE5+eyS4X+2Z/edadKw24mD
```

```
asdknyYJf5Embum4o+jSSEN1kABTevPI5yIUMPZKrS65AXj0Ef0EYJxskEsCWhod
AofJH1rYYH1P6EMkU5DtK6Ds56drEPZ41wKIHHKWTUz8uOoQiAgUFAKg0qi69IMk
ckvWtZdyFr6JzEULL8ab4Mdp9nlnRUn6Y8Yy22iMF91l+nIHM2EFKJfjafH/2yvu
D2UGPTtT/jNkm30m1vIjpZAZk+HzVfAhJnJtEeyh2mtXvP1fH6qnvLdspaVer3j4
fUS/dLT+GCyKZWTvUyx46913lFO60JQR7Ri4D7WkFsJG5p8ds+3OIc63cnsIlvmt
y8ok8fRFcSX1A4IBjwAwggGKAoIBgQDf2nh7tjyKgeBsQSxCVyUhElo1xfE+I1nS
Q5MBrFO7vhVL1wjK6e7U69HNFvN/46uC810403AESzAjEcAs/8HKf36wP6meOnx9
eA67gWAP6IdnDi4f2thBaDMJVgRzKqx6OFqNeknYT5KtRCyZ9hFxEbRbQkY7bidO
Ci1dW2mXEvoSOxhVqYEeMhLFSB6OH25k5UJQVMPZ5zP2KnZkjknp2yI0qWaegz4r
5rhkwRG2lPa/R2Lfc3AwAd4Ul+rwPnNqfIYjd3LSDOFicszuvTvTp3aVHqDn+oSn
j8BIXDTWOKE19n1/bHDFWarn0tFf/DA0Uoe2S24X11Dsrs14/QOiOVY91odAlWCP
y17g3zBskYDT2MSmjmLEOV/Ptu5fq8iIrAdsewDtXiIG+QF+btyl7AmYSR4SZywD
tWgM9v4aRET+wKUKjpq8RI4Fj0QDWJTZQAVYF6UKyR5efivJ4grZg7SrQRfOv7wV
SQEn06MZZLYeaIyqzkRJA1/wHXJo5hcCAwEAAaAAMA0GC2CGSAGG+mtQCAEbA4IO
fAAwgg53A4IM7gB+VU3W0jM54imd2PLzODAVtMwlXihKgsppR8AafkCUK3Agyc0l
jwYnAcndygW0ueymAfBTSM7bzigTKadD6gmO+wJFPHqfIWP7kpQjYpLXuv5zsNgn
j+A3pDCRBmoWpD9qukD0y2TdykpFbM2A/VCr7OBybWV4DFmrHm7Qrj+61fgsz0k1
AYErA1Ka/YVHZCZ4tGK76PtgBPRCejMorT101MaN8TudyW5Mkvdx0YTMERR0z4lb
3jc5l2bBvA5lzB7DArNtzwNIWf+7LxuivhvhaWGUyfWjQz2Akp3lbd6Z3MJC0Dq4
cCXr9zEfxdsTsKQW1PconkMRk+cyISJ5FU2+8fNUEKYlBTM+gocdfU3sIz4+iLk0
MLiZqhHdID+1oszQRMD6CQLGtwcp/RfyZ/+EFfOx/AKLQZ27u7iFgQyjV3tYbklm
zv76ahCohLud8DgvkH3lrUq3iQt3DD4LLt6pkvto/+oiyogNZRwkJ/cGzgVsJF+x
vaiER+i3JH7kvXs1ZdneN6JgbZoHIUvOAhki0N6s5V5ivxydAueEELIDsoQHwc9l
llspPa4jVfh8NgZ7OzyUw6TQmYx7DHyHW2V9fJlqyjBp5wk0wchXhSRvUiugtvEA
MwZYuMN1RItApTow8/Y6btxHvU9+UUsE/Za/hW2LN//w9dlPYcL3cX9q9scRTIpH
LD8ON9jYYdKFEtLLpg/KHx3s/9PW4dfMRd6o1ya19ZEarFR/B6V3xUYhXj0gR/K3
QPV5JH0ETkLha5qCrP0ZDu3Nf9CFfdu7XWiXpE6viOE1Exm5Qf0KNdaUElRrQ08N
h8GM7/6sJaRDCoBW8bHyLU9Xm+2tAcB3oMXySRkULWimp4vEqC8ki2UrmtMpprMn
TwsrV1KSWlvS/r2DCtVsVU68w/1jkqoMep1DxbED/WjYRkzEmtLBz9fbQxfkMFpT
LOGF9y731TssxvGOgJ5SvlBbXNUQE3sv7lq0CUARAqseMSbQ6a/qcUXDnriDfN8r
KAR/qeTDO/k/Dftz5M9c+DiUQGNC7WblTjHIFPau6KNivAEaPoYGqkFZZcsmN5xS
FR3ZzYInoa3DSOqriOAkyRihe8A/VXpOyppi7JsSsAnRubWYgwBl/Wp3uB1/8Jrl
Z/bcefxV+JT0R9SGcIeM92Rx9qAjUHlW8Qru1bQjdq4iV/Z/IpZvJsuu6eM6nZfc
XVlxLrei8g+dGbzMqfeUt6o8/46LXWcZiszPg+xvBbwCxrU4YeR7b70HW/Fz5vzx
hqpfhFR8pmPBospf8gOEgRReiR9fw6MbAcHojkEyA7x6mF0w+VOgEGXiQRRzF7II
Z63/aUsIj7pFrRDg+g2N2NWm0D7lTa2FPfD7L5gJ4LHtj9EmaqZ18Xxdbz4Tx9LH
Uy44LGiNrcR3YMbDCrcQEnPbZx4AyPA1cSCpkxFguZDzHbQsaCBb9uZYHhANhrYE
48aWei0W9uoDvLCSJWYmpIJgDm1TCyfCDcXvdNVcTDsJfjuBqjkSNUErqi0Qd0Gd
QCmBGBb7r8FcoYgPJw7QZoXKjj3DEkiRUU5bYKpMYBvOu3VvMmIE/mYCuxbeA/0k
Uwp3VDyYGfcBpH4eIAsosgNg4mxX4CZbSn0UmWarNwGZAf3MRuVzNjAZE8DTzJ1S
UeWinj97jz6WXNWioaLXAUN7LO8EW4clEk8ZN7zlSBxuF00b4B15wdsf/lmIn9p1
mcii4OSmEFboqxboak6zAAQVKdyW8wlLshHqnESy1pnWAK8xXupDr7QJAoQVflKP
7CN2kKJ3CfWfOOdVoho9Xj5EDaxMhFltA0du5rMyyi+DERb47kKLTh8hvO5pEScg
uKfoK0qh0HEk2WuFOcTswU8PJzDNtJy0EMbK83C5g7ZGLU3b1QyOq8uVhPD3DSPH
fvKciZG86GpxWMB6zPBl/LEVp3eP/z/tFg0+QM/x0rylNUSSlBgIXpPeaxOCxb1q
VUzVbHFXN6NT+UDCzznURQXcauuA0kF6Ho3QQwsj44mPzKPhE+e0RZzJCa2OBPhR
YCRIxo8GFNSjNl31lLXK6vthCMragf/ZN/FIZ16Gpuz8Hazi7erMEkJuFJh3Tr1y
78YoYPIqPw38CRJZF0YcEmrrqxkS5jaTfag5B3BNRZwmcE1Qmbb59Hj5TRzGwMgS
ntrXf9ekGKv5GFcgxhK45znvVIx3A7qmPsbkTZlrys/Y903u6KT0qQZPj1qzsxoE
ovWOhqifFUcVMQQpnky4bWrmrKp5KU3sBu9UoILhCzd4arP4ni01f6jP3dGkw5ao
OURnh3WVvrqgLXxvd6/voDh5RKVQfib2zuZLX1gl9JAEqc/CdWH+fjJOey9JtBFA
JtG9nExAdNsZ/D9IaOgzVDDDuZmM8/K0gtdd14T1uP7v3SfSsUUBuRgB8oLG8AYs
rLlwgOhwMviLD3qYYAttInuaK9fcnQFvawAAS7ZF6TW+Zwe8CebnT1xf8cLOTvRE
```

```
D5GCxkYhsBrt/uC/60I1aEX6lrqEbOWeQOVcONHJwewzo7PmAbp52LRxmnopH8BN
y9WqLo6J1wcT1amxmZxDMHx5JCguCOg6QM/u9EBBu6OUbyQPst5osSLY+7YXZYvi
s8EbmZUhJUPYtzpvlQ8WqdzpngzWTiWp2xwfqQ9iNWLPrZAdqG897LdNlQb5H5Vi
j+fCOpyV2jN0ReHUc8uOy0W4BkHYhYPThubHXhkzsKyt6lrQ+Uv4vz6RFCNWsTDn
bC2PPY0hOstghB21dDzDIvyHtGHhesrNdxtT2/w45FiLnhurJj6B4carT1+VQgiL
HnNDWcvafk4Woqv7AMmzuR/FCxJ3zx/oS2vhNpgJpWkLeR4m5UWedHcNoF48EfWw
r1ylqfhTCjRokuFbim6uiyHG5EazK8K1EgiuBaxdrrzG0H1voCuK7Nu1Ahm7we7L
y4lgGXNwU1w0g5N+RezJptYV9wZNDEMbA32sMU04kJ8dT7E4smeewhp89lkE7tH4
fWnVoXMTGKxiZWID5F3K89mSEzxLD9IEzVTLMBC2N/uPKiFU1ncKtF9eIeriJA5J
RdDzmkGUUKx0VGd30OCksZZiCQ9Mq/FA9QkUselhNhVU9VLHU+5d2l06UzQt7JUA
i20OPzNuHG6zXD+1K8CvAO6+Rbbg/AAvlVDYmt555dL8OH/31Bb7Tc2d/eLSUCTO
uaWUICnzrs7dsCA6rTnwzASe6+4oQYVUeZm+S1WhaOc97oyp1N9hmbhMhm+sHtTy
J97sYwHMOHRWOHAhVZjhv4i5xHjTbltcqw859177VWj0R0rO1CWlA1YrZKsdY3vH
gfjxvXhuV1SPQNQ767+Nm8iiz75cJ2cM3VhMt7RAVurFwoqOk9pZKzEaLt6fI1Fi
Y6R+IfZ094qO5O3BlfXwHCYjjc5Dof9vKNtQUKnr98PWHakS2O6w3XhqM4gtNjay
CxrWvHTdKJ+Bm0vPaFSiEJgNKUuJRAbkmSfcR0p+mXwoTiOm+GHA1KOK71EXYz2d
xr0tkLRR7auDYmBWe2IT8tcg19Bj1tSYFOK3+lXj9RM7QWPoqPWpAuG41ayURaOM
+01d0uroWQ1PTl6zwzhgR9fU28ml3WVXnvee5ZUPPm2rsBTlhWJuTiUCNGnqvb4K
y/wjjvzi/YFZBYR3cuKkahg9c0TEr+toNH3c9Hl0+bTXLU6fm2V+SeTQ5vs4Fm8g
T/kzaC6Gge8HIRp1JBS0FIvYgaMDi5Ru9v1KM2vLVF3DzHDS2qgpXFpXlQXN5wgt
ztsaYW81qAHOqVdB2QyCyQHypfRhOgjRLujl69AWYYTcwujauy+nujwnMWR+OGEm
O0xPS5S7WhsgkHtdfM4FxlUzWtUcCZeD//Bn+5hdqXg6Gpu+cssN6JCEPtFtZcTz
KbBw80pnKRjjTRIzFqckCT3Y9h9zyUOewK4ju4FiyadlvhF+D2uQqdGecjwxRXBY
Tp5i30pBiPlVtVkto++luhJGQetrtHYge5HFlw4MVZhoOKE1m29I/b9OR8R+GO4r
H6xNqEJzdLArE75MQok0t4XI2mJhR75B+OaXDsDTKwlJQRx7UQbpwNbACBmqw7Uj
UyK9hI2Wswj94napZT4whddSF6jooN1LXDAfOa+lfYuGA7PZ22iF8fMVYiNLYoSH
cobrw2VVH2UuDsJ4KXrF3LfTEAnmosxCUQBqcKz599BLi4ruEqNoGUfFM8BTmRKE
acjzrsYJQwgtsJdHIvqWvv0L9gr4tw9/uwtTruOpabVhto0AFZFRgXKZOJ3EU3dU
AtXhEL7+dJh5tHhzhZomoeN8A8IIraSuS9iUl2zxo/1o9TuQmfdi/pLRiXB1nJ3W
4zKbKX6Qnvv/hZegrL0Jg424/BVeiK26AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAGCA4TGB0DggGBAMkyqcX7oXTRtZOEsIGbXG734y4XTGdkF2WoBoiXwoXvAeFI
g/hWAGX1i3I8VpmwuA7NhrOeT1XCJR6JQY8OHgLmC6AHaPnEhMgGE+0I0rUHvMeD
vRupIoov2VxMSvibeNUKt1o7X/9lYbOMV3T0LKjczRhisGZTZzh40UZODRH4gBHv
uUkdarLV8fTH3iqGrhKjuz2xbBeyU1IYdvQIql2f/2/YWF4lklIz1SJrisn4Leut
vT9jzN8oWhofJa7JT0a6sePTjG3QLntkmNcs9IY1DM66e8ZNUckn/CjK2Zh06uUW
kryg4uOkcS3nS6D/98KcKw++Wgs0VeJLzcEho760l1O+yfX1GCtkWteVufOTMq8N
veuyOhoTMQBX5GTiXuOaUXMPPV0nELHhzmHDyYR4PbMK8Zd8/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
M1OBQ/Jwk7icOJzJQHVeLyun/I3x80HVPzpkUnx1RgMFiBWCAaMGH0j0EcoWLlPl
jZN6+5N6DfcoCe+IdpU94lLxOtTS3bStIcY/Jm/WPIhOmdfybRuyioE/cf2HdATz
EdZguP3SkgqxLvchRnCRNrYG4h89sHhwbum7AEEqhTIKlaYm3GQERQZRHfKTIeg4
fySaEhiPCbBGMYEhLqNQBHFp/uO922jumETk+AU7aQpCsmXS2RkIausz+v+pYhRk
```

```
kS53E6tluatpIPfquRmtDXyFUCjZQyqNgKYoJZfkMOhn+2s3bfzBALqM4yeGt7qc
JY4iOfgw9pbbUD+4/IQ19TttI3RcS4rcozl/s/A01dDUCAUqJIv5hvpxuS/CbpUX
GgsQoDcnpVwhmazqBaGTCn4G5ofVKq8UH5VEXnnaGtf1CVGlU17lFvIZm/awapWe
WiKuLsW4i7+5LCJ7xcGFXpqip7K4Xrx+c5QajLeahBIc2sWJMV4N+ijt2LqEv/2I
W1EfnZbPSs1jVFdOg1D8cU+GqFGUHkDwfSR9db3LF7WgB3mniAgUt++GVk37Z8F4
WB/H1y/AVOXnbLve+8jp/iv4iK8MsSTLqCeaY9AAPOjQQSUCw0sdzCJaEFHCfwuF
32ju7s41dJ08wSB8IHYOUkGvVvbY7MEJnaTPF+nGkPbtCGyWES8PX3d++DSFCTyw
oYoTsuQ2B+HgjE8e3cUxdwj3B5WQez3KbMufdBYrR6B+9B5vNeXob2TTbqMo8Fnv
X2umqwNQXNeMaELb16GgI9+j9o9KFZDggwT/iF9ukniTfSxR360epx46p7js/Wff
Etjmcf+sswbpPYoi92+GDGOdPIzqsCp8UdJrhkcD4omEsoItcZ3Nt2JY/qMfm4av
xkBRE9LzYPcaggjwTrUYJ7yTP0S8dGx7ya8HJH8TE84KtuEiIEJvlzd1gl7CeA5j
HkfqiFt96iSXoWkJzsoHv8t9TsoG/UbVFAjID/wGBty3PsfVsEl5qcOexhi5EHpT
rMxMj7IBhrc8G4QYATgxV2N4fC3XTVlk/dHpCGyKN8Lxyk6syWH39VeRniP0jYb2
XgnxRNaKPsLBYojINoqQRnKxzNEI0MjJAuy3CXjcsCIb1GIDacOQMCUEKfR9mjv0
CtEew3W9HmP0sJPeQoOSzDwVl5jc8Yp2uU5NNr5kMGnoOKTgB1447Ps6HvQ/dBts
H79hkP4ceZM/WqJbTcx/LYMNq+kr4pSf1ej7zM0mWzgI3+o5TyAMkh4MatPv8MX0
DVqswAlvkjno4F6hYAShUuQMEpqMkMZurXG0Uxe61vq09ohaK/I7VZSi5bPi3HS8
j2zFPYSpfLTjwaNSKMqN6Ji3jvvl4ior4GS3+8GDsFuMLBxY00LI3409uTdJfQUZ
hbNqBPKt9aR8ULizjhQdLqskw6ox9bc4uKAYdkkteLnCVo3Z1dpJ2zjm1J/ou6oG
n2KHuQcLYvjnkOvv0f7e43/9msPo4Ng1U2Ws3FXQMrViANkVoovZhQfkvp7zbtyH
r+/0b6lL2IYYjNEpADw68bm5W6bMLr64xqb81N3zHZTrY3PKKmok9bCED2ZUZ0h0
4IPL2tT+uDmWE7ws5cUCtykM3T6Kl0NqOe7RvIPErXmgY6SWTTp+CwLQawQkwyOR
HC8H+9dFrv1MHflz4Bknw6i9xA26RJBUwnnrFv/7nkfoBkRXXuQIvmzakjlY4wtF
YuAxa82Qoywr8kNqlmJLRntvXrLeJEnbG1dJsgE+ffLirwVK5RCr8V7q7Uw4CEmH
qeg1jvgrk4aJp7P1Djas9q54eZCCUxdyMfWOgsYOlUIzMZy/Vc59PlRXOk21XLkd
z7VkXDOfkNXCs6PYBxID356/v0A1DHqnwSHACVx0tfnAfTvZTL3qjU7ROTMfBk4y
Yqdb7Z1w95eEzUA2F0ypN7P9Ixqg3fNBbgl2NaJPkNauWUVf0i6VY4SCmGrmNKHj
xxUMVRBHllVuZNwktaOyy4lHJkm4rzemJAW4lOXygr9WRdjhrQf/5jO0k066g2xf
OKqxjQ5Ru5QiKXlzzQSO3qvlBGl/mNDH8AB/TqQzDFwZgqz1sppIT259eLtfgPcO
Iank8n+8AYp5nid/kj+ztsPEupXzJvH78dVTjviaQ2/nnrRjJtAVDBcjS2IzT0Nb
KzVFFBNEGemGUZcaXsFaaeCEBJpak2xIyTQI6ssSVxAuquDWJDchATn57JLhf7Zn
951p0rDbiYNqx2SfJgl/kSZu6bij6NJIQ3WQAFN688jnIhQw9kqtLrkBePQR/QRg
nGyQSwJaGh0Ch8kfWthgfU/oQyRTkO0roOznp2sQ9njXAogccpZNTPy46hCICBQU
AqDSqLr0gyRyS9a1l3IWvonMRQsvxpvgx2n2eWdFSfpjxjLbaIwX3WX6cgczYQUo
l+Np8f/bK+4PZQY9O1P+M2SbfSbW8iOlkBmT4fNV8CEmcm0R7KHaa1e8/V8fqqe8
t2ylpV6vePh9RL90tP4YLIplZO9TLHjr3XeUU7rQlBHtGLgPtaQWwkbmnx2z7c4h
zrdyewiW+a3LyiTx9EVxJfUDggGPADCCAYoCggGBAN/aeHu2PIqB4GxBLEJXJSES
WjXF8T4jWdJDkwGsU7u+FUvXCMrp7tTr0c0W83/jq4LzXTjTcARLMCMRwCz/wcp/
frA/qZ46fH14DruBYA/oh2cOLh/a2EFoMwlWBHMqrHo4Wo16SdhPkq1ELJn2EXER
tFtCRjtuJ04KLV1baZcS+hI7GFWpgR4yEsVIHo4fbmTlQlBUw9nnM/YqdmSOSenb
IjSpZp6DPivmuGTBEbaU9r9HYt9zcDAB3hSX6vA+c2p8hiN3ctIM4WJyzO69O9On
dpUeoOf6hKePwEhcNNY4oTX2fX9scMVZqufS0V/8MDRSh7ZLbhfXUOyuzXj9A6I5
Vj3Wh0CVYI/LXuDfMGyRgNPYxKaOYsQ5X8+27l+ryIisB2x7AO1eIgb5AX5u3KXs
CZhJHhJnLAO1aAz2/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
RZMAvzczU4FD8nCTuJw4nMlAdV4vKyghwQ0lNcCI6CPEb3CsCXYPOtZAYOCVOTaJ
a/e921VSHvSJE+gqgySrSkpxRiw7P+KR97HESPbmvRtPl//iYwl+0j5Ldr/CJAU+
/95z8W6RPJXXgNa56cisyh4wzsnTcjMghIN3dzchEQVmFXB3ZXh4dgGEMhU1MYAW
EEJzITIRgVMYAIVmVVYGEEARhTUiYXVScRI1NzcSY3hENTZGZzMRAxJoBmATZDhm
GBhnAUZzEAVUQ1aAVhUHd3N4ZUZBMFIIB3MwZVNCgyBUZzcAWBUVhQFWKEBYd2EY
MBIDSEBCBTGHcyRRFESBVWYycFUxN4MjVwAEZgBWdBFWMQV3cVIYIjUCJkY3AkA2
gogUhRQBRoAgJ1djRSU2hBJ1BANnZyI4cEQYWFYjcgAXVHNBEhMBUjGDZiVgaHhW
JoZFVWVIIVJFUFASdVYoNIIiB0RgQVdSIIRlZ1RjYYAyF3U2Iogmd0N0gYJVEUUF
gAJoc2WEcmFzVScBIGRjh1Fic0FQNFJkGAh4N3ETEnM4GAIRhhhzR0cGiAUkVyg0
QVZTE2cEg3RzMwczQUUAJXFXZ3ZoZyFohHNBh4UgJWgHOAJXdwI3AHdAhAaHQzhi
ZhKCBIdTGAY4UxNRQTRlhCI1E2MmUXg3gjNnGHdwUBYAdBMBYFQjIliFMQQWQQVD
EwdjQIhocyAIaIhyQgMyUnYFRlFid1WDZSETJwESiDdiIEdGN1U3NBVIUoQYYhJR
CCN1dEBRVyBVJoM2cgVmUSYEZyYYN0IFByAoGEKEhgNYMTNkeBQiBBKHAycTVlAT
R3FBdnJxdAQwISZmRWKAUARyZ3R3ZkEHIShgUGaIAgUhhiVgGFFQiCGDdERAcyOD
AHcxFDAHB1WFZgIBiCdGQjE4SGWHMUNIaId0ADECc4QzKAZmFnA3JSdReEFIhkNo
iAFiUSQIhlg4GIeEgYNEETYlB1dmSEhHMERnQkFUKEgjJyWGiCQVdCRlBBBUAWgi
Y2hUFlOFY0CGhBUTQRQEIgRiI1iEMWU0E4VjIBEHMWSDJAZCNSiHAIIjIXBWhgZB
A4KBM3KBcHF3hAAFEyJiM2dzdFZjZXgwU4RxNjFYFWREQgFVZ2hBGCIzVyYXJDBh
dRWHQjGIKAMAAmEoNGg4ZhNQEyVAeEBCQVAGhyGGYiQkMBAUYRVkEnEAVnGIVCNh
YTZ1I1EXhEdGZ3IBFSIjUWRxAQEYOFZIOEckFRUTciJVJEgDIiNhNQWAJgVkYTFA
aAE4VQBjGFMQFXBSQQFoZXJHEmhoNkhGg3IBVoUyFwgkGAVHgARwd1WGAHZ4GDgy
gSVQNHgGSBN2hyYhVUBwgHdHhGeGF3OIAldBQXJUJnYTiHV2QgFgEjhRhBOCVwQD
aGFhcFQIUUMWgCNXAGSAKABwNEZ1UTgGcDZAF2SGREhIhINoFEZBNEQxA1hkUwAT
WAVwdodWiINycyRyFkIIdnSFIiFRcQd1VmGHR1E1dDVYdTR4QUcVOIJIIVFTJyEj
VCWFZIiFI3WIeAFVJSQ2JXUSYRQjA0F3dzRmFVZRgmV0QHE1OHgSNIB1J4ZCI0hj
iIYkd3dFKGMBcUEYUkA2JnVlIoJoYwFhg4BDFXIkZ4hiRoMTaIBTOGADJkgwdYKF
VYA0iBQ1FHMzF1cyGGJIc2ZzZlKAeHZGgWAFgyhBiAhUMjNxhzATFgM3MWJjEGVC
ghWHZSZlg3ExAUAFJDIVFgIkRXVlNxAGd0NTYEdGYAMRFVBxUVBhiEJWcUADCHIx
N4YXEDRYRCJWRWBoUCFGeDQlNjczUBCIMAB4QkdEaDgiglQ2ExcoZgMydjcVGFUF
NXJRQWRxcVdxAzcUdkNEOHMoSBFSEidIBQhycUJkFgBlNxI3dnQ4FkYxRyEjJQWC
JUCEYAdTUGUAIyhydGFDVoAAZAWIgxZ1UoQGZyMUREIAdQNHYxVlhIVUg2RjNYYA
R1aDMhBwcBFoEYBiBzKHJWd1M1IkJDWAAEMjNUZGVUNVQIcCCCMIlsGp58wjH1Aw
Z+9PhxPuiiNTkdRgexiB5Uy1AjRsCTWwwBnLDwecADj+G16A5gTN5sqFMRLPhUdw
94Zj6cidUvpYSEH9PAQNdXs8PUEBRORUZeI7wZA0onyHbqNGRwzutjfm8boe0yOv
yJ9GoZdLOdehk1sQBQIygciWINE9eLsoi41UYnm4rdDTysKeAIOq3zBG9w/yU1bu
80OhppqPRZiiOGOhQ5bHwJhUcSozM7leUf+l2JGAcoJe2kfSmWXQ7elJqZdOgdRb
ETIMc9y8AWYa8i8n4SxxLpC5h+i4+FgYv/DKxgspS+qf2plxqy8jV+EIY91md9Fh
jGi78WAf1QXifVR/qO6pDSz0cdHPMBVH/bFbsaQVb72wIXA4zZPY4hSYNi7I78hg
6GDwWy63U+RaDxUiwbcMDTdC6t21GW1lKQdsV8dkAOLZV6/2Dc9YOFTjWt0j/tZ1
pmy4SAsQw1tViutKVrc+pJHigSoCidHF7sM7ab8IK7QoyPTTf15BSfCgmnMV7hN4
xmAgE2aVphPTYibUnai2H6pDPIfWVD3j6oqQbyAd9nWu6gybSNuB1YolbAJLkT0h
qIHghdnPoByYWMFCD5Vcn/bFAgzWCkKUXQtO3kH/HeIWUEoaCpu67Cs4mtwAO9ad
FaZUQQtaBgCvVYA9EGP1eCzyt7vXgQGC+KBIDFgZ05Vn7JQgEHUW+ErnmpqgnHLA
0hBSxxbzhlZjmc73fDMVVQW0llsrVgBwIqZOVWTWv2zp51q+F+UrwUwwTDVPYRPL
bO0tJ6yobuQZ+6Ucji845jlUPAjAZwy7nXLKSlGjMjIe04c+ih1JgbncpK+ZYUHa
c784ZTMgyaUKVgpUGz+SmaIziHTpvM36kS/H+x+3j6tKhVF63IKV3JVNK/6/gXwN
0YKabed8gHlFTp8KpKm0uXcq1dkGUTw2zeQU7DzQ5XALF1QEN/MlTjk7/XF/A6N3
cKCQUTtP9LIEsYV/txcL8/Jer0kz6k/tsD35MpJZKJj239PVOn3grduT6zMY1097
3DIqyNI9K5ARIGiUuxAQoiAUbpdWLAdYxFK36MskBXAat4HTsMEkmBHARMuZXzc1
hpr87MqABTNhwrL7YOgPfDY6FaelLxnWlc0o1uCp9zmH+uyGP4oxazCTijjz5eov
```

```
d1wDfVZZ3WAp62ZQBHg0DRESW30CugAUNyryYQsWv2up6tAw/Hj71tzK4j8UceBC
fPc8gIxvBrOi3GRn0y/S7QYpFX+OMf7OhAcvGrwEe6R8IKytKMUBxAuArB/spkBG
vLXkIpq4an0+NUOSsk7a1rqeiKufIK6EmOhLtOWxlOpdTREsei7DHDQplRmOUEO8
WPcK6Udt3BRoUQH4iuv8fOLXsI6lmvFbBVbL7mcMMj0h35ZlI90cAbVvo5aiZ0F1
k+4yrPLuDtxjzSAMrQ1vSa9Z5kJUePOkNqRojEN5/y4O7sdPOSe8aC/2Ebj6IXBZ
EvsDBAKqXpnNg2/3QIT77FfO+AYJK7QeegiTiBduEbrieRNJjPwQuQDa3kYciDld
tEvM5XhAcBhDIKvk4MyJutC24+qUikx5GlddVVLoxjqKSzgY0SUOO15EVV5NDDcb
n9S2DGr70J1l7EAjqojpgO2yHkzodiIUtWIKfx5uX/KEkDdGSLvFvSxE3kAhbTxk
8BsxcisgmQbgfdaFskSVcV/JqQO7uma0CKXxl7FuVe0zkl7SjTIYt30EZhjkq8hA
CiAGhcBhD48Hi5lOoemRR/kkNMFTRWndlGH8EAQIF+Vb3BdnRPcV4083Sk7iZack
CapszRq2jBoSgxfYyuoNPhQc80sRt3Vi8lDMDauJ9HIn4TzMb+dY+DKKNNCTAJMJ
OjNheCtQpJOvpoRPU5LCBFfBeq5nntbGOxJJtrkM4dgFB2BUqJSDG1a2U4aMd9Zi
rca9pS35TU6LTkm0ZJZnGROVvlCOME4IckKzyYUbRme37UwUK0RRdwJiRoM77XNW
eOzKNLtnLJr4RNB+QR3lvwAD8SePDIqeu2fWkNeSmhhNucmrW+FF0IcMpjrGRGzO
/SUiqudfGZMq+SAFNLj2T/SzRujWntFd1r/jE0XMidzCLVT0MgOBBxKLxUtZEDog
XGq4kGrbAkCRvC2+2nOrm/MLEk0Z1St+TSou0yJ1ZQwlEwzubEgwb4v7orvwCYIP
+slwQVbtDw2SkWoKN2KiPS93bsBFbm9wQn9EN6eNQSyAytiogUjF97ueR1tEvV0W
K/9kXt1co5FwvZ6k9ttipHWoFZLRBNk34kVAFpZOop4FOryPo3WCewfM19MjARch
/DwEMaox1/hQphFDWoepBlEQw9MX9er7tZ3EjXn9Z02o3trsXDFsVN8wy8gWOJSt
P9FmOmEeosUX6xIg+twzJB3YJ4uuVXT9EprO0a9SgKyMH7H+XdIlQpF1XruYSm5l
t0oW7wOi1igdqQCt93qS9yokMiA30bFjo9s8yI1NG4syF7hriQYsKGrITOR/hmmy
Ddh+eNQkhh27tpe53ZwD4pKPPQB6dPVLupnpaCGG8nesGrzoiqpONwft419PIhU3
Ia6U74FHloE/fdA81GVjamLT4icGolSFIqS1CjpRhP6EFYtavXbLv0XSP8RKzfFQ
XqH1pLug9Xciuuu105AHpqdV4Ln8BNKDvuiZRdu+5A6F21QUMZx/+0lRplQERnY0
R7fVubxEmSCfFX/gEW7qtDbNepskncp+816pii3P4AbSQJUA0AmPuzAzJrvaLnDa
VsQHBtXhjjXD7vmKd5Xw9NlmoHrl+X1XdaREQjkNNEZph1MTfYGy2yExtpjW7zk3
V2I4xYe4VmkcDUu3G/MZHwmcohNltD2Rez7DF0JUnldx32OhZdcZyZ2tejzGA5ka
EgNPQCFVKbzRlRDzE3CXYVMF9CxbZlkfIqGGeDxi3ZOlrnpiydTbO19w/rnSVxQT
L8zCFEA0y0L1giBv9TXUQi21srd4guV2FHEq69xCeMV3pZH4xf5sbnAOj99mjIPB
pA2qSujdMmyTRkf+pN11AfIUTYrGhCGl+DkIq5N61YFUijksGZk7W3As+118+JSa
B89vgv2EoFrfRjZy3ct0PvrO1jKgw30nQ9Ww61L+spZF06NG/YQuRVwR2gpaClGa
Vkwpkb0N+ITqqjzo8IlXJT94ruE2DOQ9ImF5sSsGxtBqz4JVcsE+JZp2n+/CeMjy
iDHvg1U3ziV5uZRGMmMPu0IXmkwXRTYd2rlwaYZRRFl3Hw088lagH6sLF5MaYEAn
iXcaC/m7PoYttHr+A4gCFBs2mmknJIQTM3O6nIZ8uHp92TyOi2IEggbnMIIG4wIB
AAKCAYEA39p4e7Y8ioHgbEEsQlclIRJaNcXxPiNZ0kOTAaxTu74VS9cIyunu1OvR
zRbzf+OrgvNdONNwBEswIxHALP/Byn9+sD+pnjp8fXgOu4FgD+iHZw4uH9rYQWgz
CVYEcyqsejhajXpJ2E+SrUQsmfYRcRG0W0JGO24nTgotXVtplxL6EjsYVamBHjIS
xUgejh9uZOVCUFTD2ecz9ip2ZI5J6dsiNKlmnoM+K+a4ZMERtpT2v0di33NwMAHe
FJfq8D5zanyGI3dy0gzhYnLM7r0706d2lR6g5/qEp4/ASFw01jihNfZ9f2xwxVmq
59LRX/wwNFKHtktuF9dQ7K7NeP0DojlWPdaHQJVgj8te4N8wbJGA09jEpo5ixDlf
z7buX6vIiKwHbHsA7V4iBvkBfm7cpewJmEkeEmcsA7VoDPb+GkRE/sClCo6avESO
BY9EA1iU2UAFWBelCskeXn4ryeIK2YO0q0EXzr+8FUkBJ9OjGWS2HmiMqs5ESQNf
8B1yaOYXAgMBAAECggGANkkP0Mh31Ar89qOzbP8fJO8Da2juQOhnvuLeQpic0bme
Bn9GRZcHcSEjBr5bHJeEn0QPRlmYH6JwMQD7/q2jPE1A1tMJejKqv+6efAA64IC+
XVKGAvmaWfo/7jKq75bYrub9prOSNt/NLTGMM2YGAsqNV1gyGfVzmKxFJg+mApn6
hPNJynRJuJ3iCW+c4VBkABnMxBhaSnyUEE1p2qba69hVajnuheBD8neIHf7oIcPs
NqTEKHYhLbM2PP4+XjZ2aKGVCV21TJDnfRNnEdGKmF+Uv3XfItT0SxsizEYBSVhV
7gUA1w27/L7v72Y+xSFvCnIV8hRUz7MEpjDZb2ZaRbA+wJwunqIjzJmBY4PlAsnO
1byfDH63N/jMgy4gD+Wuv9Ad3Qx+xFBMmLNtuKvrx9PQiUqxAXikUMRZ3I9SPu8S
SfQOZqiAjsdH+qBlcSaPpmJ6xPfWkHdXbMMFHljtQXNebtL1U6Ae1Wodd4FZhZbH
+nl4ddB4588r9vJmZLTpAoHBAPb/OGJUZG2n3jPNf5jSj1Izl45vVeuqQJnc9jpp
Pnc8GHcAXC2NGlahE6Z+fBFfS3TmqVLtXIKkpNbv/Qs8p+xdDoYuMH0kp5Vg2fby
df8cH8TXF3XZdAocVgeEkY+MHt44BP0aUmckbprKb5bc7YQScFJoL/u43aLC8t8o
```

```
7GAUR58eLFdZXwU1PkNb07bff8ewSwZd03s1BsnH+RSQ2Te10fszs90hPQyPMraa
UpBwPt2dWC/JINfRmn8YxW7YmwKBwQDoA0sId04T4on88GTZbSfkZkY6RI21Y8lP
zC00/1L3+9Is4bEUjqMlVeNLWHQ+dBslPHk2gMQ3iMdJmqyqYl/+j/iEoR50LZhA
YhQ1LOi1zRucBbT36ixT9T6NHpQP5fRZbvkXBWLac5wM30PL71oC0SLlRuc5XdG/
JoH8am4VuPdZUJs5NaopRCH3QPOyWrCzx7tb6YmFsJrCsSylVmtOxmW0bWPWeG0h
Ofo6q4SUe7J2AaZwJgCxeqVu+5oACjUCgcEA2oYG3ogHqjSAlJhVMWHoxzM5/Rxn
ie7A5N/nQNpoF5mlk3NQGkTibo5oEj+JiN0kpzKD0AiMdlEwPbFp0Q1DDA1wkio/
YBiT48ciUCdHWgMJ4F7kNLHExkU3n8Mb/UJc9QHe+AbXrMVAzdYYUAL6aITftyjS
ewSdoiiUM/fC2WZXz2EknctGFBd9FJ8jeoHWTVedqO5N8o2BifhQWG+mnnFQa8zc
buG/X2M53PA/5+ZG2E8i/HQXiJm69IN3+Y/NAoHARNQFRGOwQ/HmoaTnJiFdvkIg
/1Qq/e62X/fgSWKdSHfqJ+pkUAbom0DZhxaclZJ4IxnHk8WrcBYhmNJL+tfoRmqL
fT0W/bww+JigCg5iktxgHm8K+qj7sYSFo/O4VOcREB79wjiU1N2LI75wLGW7PC6y
vXXFTp1ohd50nV8tfUA8EMD664PiEQ/nS6R3JygEV7EfAetMIt77alqJNhtnBh2R
Om9hONTM+xhqBVGwqSPxE1T1/Tso5X3O6he13eEpAoHAKwQRFxqHKWBJcsibflm0
wwTkE0U1OF0cnSI5p/ZycTkY377UqbMrTbCvrxFKCMWlWmmyBimgkR5twRjs1JMf
hfX+A6T4wGRqQyzr9N3DwR/O+QQcjjneU4WqE0LUXVNMp2znpNP0zHSjj/4R9+Cy
OH/Drh6NrrbbiO6SWZwxE945ZrsROhKjYC849H7yPBsO0pFfbTLfqMAD7IpdrnOV
qHvbduKK2OqpnLsHNHei6Xy/qQJQOoiv/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
MSYwJAYDVQQDEx1NTERTQTY1LVJTQTQwOTYtUEtDUzE1IFNhbXBsZTCCCdAwDQYL
YIZIAYb6a1AIASMDggm9ADCCCbgDggehAPxkh1CJ8pm3VQB+Xmu7WBiVbOasomNa
eaK9sSVV8z/eUHNzKJsVUODK7UrBXeL7if8dhwrojQ1jCepx+z+ViQLV6oRT9Ozn
3Ue8OR3sBDd4S59i/noUmZT0IxjtN5CEati77zpL37LCHQkhRnClv5a+srA+GI4i
wZcWiaNFfLOmrTWOCY7a6bTqBHZ/fAS83KFngyE3YHGTIH0Fbu9odQFRmeZIeeoZ
3FXFpXYGssOhQe2+Gvca74t582DIgb8x+8T2/EshaoGc8rkQDNMLLeJPCnWwyN5L
NCwgzl623jetuqn+MSBQgxXK7jdxg7lIdR+X+WMvu5kDmbPq7F9gK2j3/zYt3myp
rrIgnptHjASdYyEpQ6jH+/gtQoRV8WGjveoBBQ78mBXQRnRWmauZEDnOkvuy9qic
eFBzLZ78cwCirl4NfU2jo0aTwzvPIWwjIF6P0OY6D1wZqkv6GwRM9Yrvqmig3/r+
OKSMw2iEdQu9G565ImKM0hp1diy2EqU5Tqi9wNTW6sqblkXiJLeo5KP2me6GTqdf
7e1wd9x8oG/8Xi2efOwGU0fxJdrDWWev+N4GrQaQnl8OGXpSA/xnNnYSsUOlFiOm
7113pDsZgnFt1od5Rsn+g2PxV1KKn2/YcMVICybtiMdYet2d8Ozf7eeZ0KSnAMK6
uhNMQZ49AbZnHrikiSQEyvEJnmVdHtPRNPd9FbYj9nBqDmlIPa4BAnCKa9r6qd/F
wgM0ecItfMzUyXTK61BgfQmjmmZ2HcQWlhULTlhL4uSlxhhpJr6pBeViKjtMOSFN
t4PwnhaeXKn0IBl04R4IPi9yW3fXefsIoKAm0wrxqw+iSAMmx+GZHP7Unf+e36a/
yKtew6INaqOfYu7QgabfrJjAYd53MEluCJ6wwqOKajYsvoae3gEnhdFrO8ZFEYM8
```

```
muHswqSmgxcLZggig0hEftW/TAqNf9brzOOCftq9c4+hbMf4PtqaAybDq1OD2T/J
E4dzzdJ0k4KPusgXOKlu6eDRptkqTxlJr36Jo8U6yYM50rpy0LhJUBwPiP64SbrJ
Aet93aBdiwQ4y55t3uowlasDpyDf43ljeLkq1/DVA4PtOsRzuR7BCTRdANJk76Jw
EVQQmagE9ljz4uHdiRHec5BgfZiwUEHQoMD0zKCC807vN9JDHZwe1qRKQTM6hgUg
7X7CqULexlA8aZ4wvaDy6LsRKpD08ZCu8lHnGAwRye4tgGRIeK5AbsDjt4IYj71b
f3dpmD/EaoDFV2W3wU9WdezdoezXwou0ORoE1C0BcjsSoslkDbtTvjokIIrk68Hm
QcfS0JgLEyRLAHx+d/Q7E3V8bnKnBixpKPvBSiLOagnFOpatmBjZ6Xb+31EXHPaj
ByLfGFTxoZEQkzRMQgKKdt/73UHVJkZob6Qjt0uhqetYXFlLCeiJ8hDAtj8yEvfJ
0E5wABtt0ZrpwP1L9vZGBSuTHFfK+5gWzX0brt5C5n26arPBmthM4t4kcU9JDtrU
Y3BkSI48EcPlXnO5W53jE8514Qz+Md/D9gVbH59UTMFXzDgaaB6m6VtX4+trcqQ8
EdJLibsw4XlokMG1BbXpUtbASEurRxIh251m4im3jEcCRYUa8llsV9/xaT58yoiU
ox5cWtEEBL9/MjbdsQ9/vtMVND0beT90AqbtIXP9uYRWro1x+GF8tAZZ8bDMlIfL
Th0vWGF1U2vgGUujIlGM6yO9/RuXF0RizlCMvAs2ilcg+vjVCr/CRd5Kz9McF95o
4JayMblX/E/eMV2iSXZ2DX276WeTXAuKtu6CV3CTqP+T6gQUgbkdSwEFUt1bYsnH
wdxTsnNw+N0nPaJEGTSlyt6TweEpWkYeOb2cntCSeVSPhApIsF/cr89J1GGaH3ul
wIGAV7qfQQklBiUHN/DxNqcH9oyXFrnKZqD8j+WJGzBV3RSy3EHIq+MkMdAH/6cN
vXVwvN5c0cOz0ygijSdu+vbNwAIrYbY9HSfJs/+K5qQ7DOOGVJzfbM9JHyGoWUPY
g0acTNVg5gj33BXxpDywlRHAYXs3NpZEkg08CYJY98WUnGJoLRVwc1s/9wSsFIXX
IoAsvpjQ8EgUbq6TIJglei2cA4LbDXJrLEkgYyxbelnkJw/TQ9IEJIiFLEOHhlcp
C1cos7DaG2VaICJ30Rga75e6/ncIZuAYdqlPxKGvjxRWdZh3zUdO9XC03Pl9tQXI
qZVenFdQHvcG25r69czWkt9ISqrUEDvHdPT3B1F0u2/kDYPBeaYmHmTRAUGyGHNR
Xolj/TUOF2Pg02rxE7aWoRSyHtGl2PKR3lj2Yv1L6hVDlwMK49UXDuaESjnzbcFD
DTA26F8f1/Ncr3nw9TTKhNNgu52umUoMJcWNkJVtIpzim3VgDPXuYEP3/nt791BX
kpOLp7WKppUcnjgpARaWyOPdaa2HuMZnucWyqyNBjojO5C/XVASaJ/VaHx1Xhma3
qZEA9keMohpQNBV3/SuHNKLk93KZg92X7WqtaJuyr1v8m580vPx03ZFGgf/Z/the
LecY+a7+YwDFDEpv2lgEVK0/4JWWTmhxL0ak9KbwMg0rrHB/Yw6Wd+p+Ob3SSZ+X
SPDEJ3O7uLgWA4ICDwAwggIKAoICAQDJ663UCqGVlqMpRV/Y7p4Y75wPPIJGZGcx
H+z5tGpaYEa/vvWbbQKzdIj/9kGIZC4eTCYG30ElpHu9h/bVqTdxHO48x2meEyk3
Qw/ZG3t/iQvYb0vuRHPMXwHbrfdKDD8yZux3Jp18VeKMHSXJu2gyigzCSNi/PvlG
sIQVTYZyeibYqXigG5607bLnhCS07rib/GX0VSwA/ibTHlHnuJAOB0Qg0r1UJ49I
Hr7Oi7/ud19k2X1rqK2hDdI6jSlHdAlAflMVa6pDtB7b8B/7P1h+AkP5HJcOTydb
r+kT0NZaXKFC2YRhhKmEucGEgVpmug2aFIXgZv9CTjU8b5BxkvV4QCk2vMZ+Q5K9
q3s3QqEY/g7iVc3x76WpSES4o/es6N8+cKOprumsKn0qACUd3bhG3ttVTwPcaDmA
TQu4vJ0OaBXKn6GUJDoXYS7GlCRwWG4AdEPsZ6T71NHBW/cD82JUWQR5TZGaapGm
VwTDhZ4YPJztMmhvjeNL0hCMInvHzBQI09W6FIEAFh2H9X7phAzcdHZ0M1UpytGR
n9Ra6/brjl6rVfTvP/XTEi3A+LZgDe3Q0gsex5fOmVlClDeQ2iCzHfCPOwWQ0zny
kOxltz8dxNtZTDhHieF9qUi9nlmPjL8at5v9rkWJUlALfjKrSpaCcYXQKcyfR+Sg
8yGk8dUASwIDAQABoAAwDQYLYIZIAYb6a1AIASMDgg78ADCCDvcDggzuAK9Nc53q
TLf3wM9mDpvsNBZLxBILPzGPDqVeqC30VhO7Pg0l6ZTEYOqiVI+fk8amiHh5yml0
pSNZgJ59g4enwO4/0ESdmEaUoIqdHyof1jTeadArC8eYGL8bkWzZgiZy+/BGlAvA
9vpNsac3ymK2RllGwooer+zWwwq0KMFATp0wN4fghSQPFIbEj2V3PCquqCEwtLe0
G+3uHoFG7UYmTbXDiWGgnA+fXW25SCyvduaCWKxaAIXJmY6n1LtejVJOFmsyGSW5
/SJIbTLLjitGwkfDwv9lDpGEQiRD2eT7I13x7de387JGXzvDovE9g8b23WhO2qEu
bMbGDxaLi6RI8Qe/6gIicoREb/LGuGlaplbs77GyQal6sdAylLKD5P00b9T6N1ap
Tq+0JC7FStGY5Ap1xAn9J92aG/Hp1wwg7m/VCHvQFd0FRyNMflYYx23wN2UnajmM
OWzlddzFtnicATJ0U1qqbiM1OkVdI2+V3by/bonZRcCRh/t0opDOfL1/wz5Av40r
Y34Qo4fLyyBxaGxJJSC556ilG6I+Xi7YBdMA6v+FTpwmhIp+w+j/Gca4+9eUdYPC
7cNF/aWvPCM1Um4rTv8yF9JG9W/f930t83/BKN4BcAvMGn5/u9S51NqTnGY/bMYC
GK8cJiT/qeXqqzgu9Q5o4WPRmQGbQElsTxnpA0ZHnI/GCd7ZYWaBw1Jiq8oHTQVW
4NmxkmOv3NonXobEyE+ccv/T9/QVOajTO2qidRc/5Si4VFqwZEHq156jHAoKCxOr
EcjpjXkBO4laDHC3AksmbsikkqLDnTTLCXYQtO1OIAKOKdkp9jNfgSvPyLPglQaX
49B7PUXLeDw0VeKYcGs06tiLwcsWp2mlzFvVRSrUyd8ZQk9jTVBhnAFazBGo5k1Q
pYRV4Df9EZoikSWCJ/z4vnnnmtrZ3fH8qAd6W0Uy5XsS/4anW6tevcWgBd78uTum
```

```
ny1Upc0FaTUp7UEbDEg2KJo7d824rM41tH8keHHAijQAcdvZaFUEO5Ra9QptMjQF
UFep+wS/UITd+6iqzt+dvIu3e02KqFaB17TNzN23FoWAs3gLrJ07z3EQOCkl9csB
1dheReQlNhB7tEkqMtjt9ayymxPD4c3NZHM9Sozsr4GB/VEKhlleMsGAllr94/BH
lYblXYlbII7IjqlXOAulaGrK7QKEK26Fd7DmsKEc6V0329Icm0zwdA8yNEdXQG++
uQXcnoD7tqpZSDiYjzjgpVbgDzwfMTEYpJzeU2S8HYhJ3j+P+2fWnDERNDx1Pj7L
/NMaJVy7nd3VbeGGips8qdP+9bGnY8elS0u/8KRUmlX7rLa8duvVo9XP6zvRnDNs
N8U1J14uFWuoeVW/urlsYHPmZRv7VSCF5hGAzyqPcEDVh963OtL2pFHllf9LXpBX
ep/2yG5FBPqnQe8ApZF2WmDYCRWtn+u+DsRdZr1ucwmu51MHByluc9XW/j6pdNBp
fz2lq6phxFxAIXn7no0Jm6oKo5CsTtE3OgVn13HRJeyuZdSQ9FvSmFkhMWOEUdRy
gFkSxcw7bnxVD65H0UNSyuv8dVI+WJZcrEtfSb/m1iOrhKtM9H1AC9zPTcGEqe6I
lBsFaA19pvn8i6ryOWdIqf+KGUVvxonFmA4v29Jt6iQrFpfvB08uqXogeDlioE+3
jkhDBBI7vyLKmBiC1yDSOho2vC0v7nomqCpXD46OKs8Ka54Ux+JbivoZk8K+5YSZ
6pzuEOIjerYy86l65v9OLgwnmhrbewF9PC2wGusuilZzRkFb/0O1lBlfV7/nzL/N
7a3cWQYPgn5HcvxchGGVzMuIMnWOikFG1XN28BIU0n/y9Cvk2+V6a6j8dBsD62p3
mLQtA4EQEmvA+JeivzP/+XzPdGXv/fVju91HHO9keNKdIr0NWWd6iWN/OwtQZW/x
7StNYV6lVJhbHMdOvu3GxhWCEmLKT2WW+KXgTwT3kfRYCL9wYTRSfPtv9ZYEadYZ
Pwrd1BJwBrxQ/RmqudHE+ufNRx8rigR4UjWDpm5cE3E4HeZY4ceGKugi2+WUup+D
bySFuxYzwTyCzweoUhviNuM+SKRXWlqRs2pNvjSls+Kdkv5+A8tx1DU1N7rBE/2l
yPsATe2BoXXSkeO4e9DAReNVgK+Mh8485YdD1naOdi5rc8Q3bDjqbDyfhW2DvTKQ
cijRgeHPA44TyqTafTv8kL2L6aHU+Dt1ku6Yq5sQxhuK/585nH6BPAaKC4FNXpl3
x8ZjwyZ7IOsfNx22DyXblPXwyByALjQF9xPrUzRavnMkhc/V9ePzhdJOKlF7xMTw
g+2m+gI9MczD+x6tMHfVLALM6aUaua8fJMI6iUt/Kcwnlwf2wnw8Vm1HkUzmIcMF
585D7xY8YxWFRn2U7wUJhnE5nfjg3IMjmJRZE5Fx2tzCOO/bkqlWHyY3isDTPNyH
/U+PVmQpBe15cNgFm3G5H6eWpzv6QHzqfzLiUpV4aTy+ZnkkwAB1z7p5FGHB5zI1
C9DWCG0ESBAnseUhZkV34frs5R7gLye8xVSNhufkpW/D9WZo/V8F+h23dRmWL1ba
B0mlURVXhLPJxPgUDoiHjMmlpYAxGhPCDnik/Dk093N72AQNuvnMIaZ9rA4iQriW
ShwKyFWvYkrhN11cIJbzvLwbrOrqTxSCx+xMKjO+jgMJo8xMIqJbMSHaVnRxrZnJ
x2yyJWQ4kbrEOoepMJQuJvVunI5G1tmBEglzKCq8uEvUYaOe16+qR9FANG+sHa15
HSnMIEmWu3y3aSdgtTZS9Q6mn+iT0B3vZ53WglfpTV30JNk74DQ9pAhCNNoUq/Nc
8267hNDBFQ4ZoykBgXq5pCU3Nzy8g3nEIMNGpbYvxW8PDdyZ2h0OVGQAMYh66CgN
v2TW9qYeqYUGM0Whl3/MjbsLhPS3g1Gz67iWtfPGl1TrBRbm2kk6tGJIlRP3L/4u
RMlgAt1usZSNFPNfwSbFaUxqabduET1tFkmWk1Oou3xWi7nxHOK+Ie5AVMJuGXTm
RiKPdFYDPtbmrktdCrcHUqVpyfxMqeq/lLUx3Og53dHHeAvISQJZrlAldbrio7MY
82TILcLWPKetBt/CQSwjDf+kw1ZQnjy8Z33H/udkgudDIr0MDDBUrsbzvCuUACi4
TbY3tmy3NNR02yLLZV3XsHhjv2g/l/cRqeXGJnS5l7WLDy+ObEllbtj21QrHP2WE
quFm4U+4mdRzDbeSl0U4L/lWipwxZ/RG6tAfCd853iSxwaLlOZWVgcL7LP+ORrGP
foBJzroOuVHp0g0jFP200qncEV5mfBhlDrtVIUjvz9PMznR0g3ZdLU0cI1TSsWZo
LbvQg4o4cW2qUrcO3pEtNuxSqN4bYrjneM8RVlZl76CppmFWg8UNCBHcK4oHO3Vg
ljLOs2o04Bi1QUfum4nRCFF7G1QLb9TdAEViggDNW/QDqzZ9FfxvFNkRLehB8HpF
5/7HVJFBsV73wtwMEznUdP8FBErxOp9VqGMUfu9YseYmaOl6QDw4Y+CiHzqSWE6C
LgooK/qSdc7+5q+SwRMGuoBHdU0EIfSfgVMWDEzt8ollc1fQcG7X/nY3DE8x8uFf
+uca9EcHVe9jck5yb5gPGYaFdw9lXzJLSy4PsoRGEOSEKV6MPAexkd1nUDs2JIvN
6VZyXoXjYVAG4KM28OaHU9k/SrcO1eb3tpe585xBpRxRsWMJ3YQiDBcKljKqYH6N
V4NDHvs5YpKxyVDOP7EL5Ro2c85reUsIm4mK+0WhNnorKenKM1moQ7ubxLk9m1cQ
+92nQ7bTx8sl0BQOwE+0EY8I8Cljk/6sefBODuyBah64AlDNxYmVdEb7n1Pf1VG/
65sB9p2CwuzxR0mLITFYaGmeuX34h5sRKPrvejJJo8PEoh9lBLQBBMn3xFeUBZ1w
OTxpwiBz5HNboaWwUC+bYVd4BozRsCc/DFGSUB4VFVr/SReNYOyo73QtIAdOcZfq
HOReCdfAH0jJp++BvOXmLOCAgBkGf31VLn7f6nwUwS85y8FjpIFlYEvN4kpViIYE
UtD5FGCDlZ++8xrapn4lxVLSscX+/8ToOfk/9C62vZUIjHmmYknnIeS/dYuMELXZ
HJ8ku16XuIXYQZ90b68lI6T+OKA/Fsavhh0aWim5TzbJtUer4uQK3ZFckL3OPkFl
mWp3wJr2Bccfb6k3vZv/SvWx15kMMSyoJ8YDP6hbvO7eAduok4P7KisvMLFXN/fb
rB8VozmUN1PCaE2sWSUcHF7KKG6H02dSNQF3AhijGq4iLRsvnxPfxZjBhyc0cIsX
IyJZoXZZSzvhg++jhy7KuWUARLmQO8Sr8tkvDDQ5PWQDJzlBr7XIzdzoGDhGvufs
```

```
DVmEj8TQ8WWsxuMIF1SAnJ3DxdPa9wAAAAAAAAAAAAAAAAAUPFRwgKwOCAgEAsz57
EUlgZTAx9SQ4anltbmPglj856iuJg0rWWMsCwUzs5dANULLVP1xRYrH6doDPislt
TTlkf33bF5ths8PF2XhA8jO0dG9FEwVsxjmu0ud1ufb7pqmB/V8rh5zNtrjS8tvl
CkDeIYZcRh71ttDGOfYl8oPlBTtF6Km3SYsaOdgFog60aVqP87xWM+psXB6Pb95j
+ytRhg2930BJrAs9xAUBcxEbwwdo2KnYqcfZiwgfYGyJFb021pzxcb4d+NtAB3ru
VCUf1m6RMm2Q1fGEXP73lWC5FiBapCiXIJarAaFB7TYP2wApiWX6geeZQlTuZyiy
PN2JDbLL56gKlhIfu/YZ0U+nqruSY0u6ZARftJ62nqXYjGPd8vNUBhcQgzd1LWS9
4xH7XJvjj1Oqtmyzxc652GazQNIhrwtERIlPvEHuxXrYaemOiweiqsVjf+IooYXw
tYh8+JFMADvrInbpQTzl3X1vMjLC61yI+p0Mk/LQq/n99WTjHsVVxkisw+RDId/4
sTDnogujMNM4ZkP/QywYgGy1Z5V5r8sbNtfXflcO8/tc9nuon3Dbd3PIiS51u5Ya
wkHL4Ve/IBhyzCAAELvBwH4wSTbD0yVUOJNW3j5Yng68xMxZqg5DFDb0JbDopPfI
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
GJVs5qyiY1p5or2xJVXzP95Qc3MomxVQ4MrtSsFd4vuJ/x2HCuiNDWMJ6nH7P5WJ
AtXqhFP07OfdR7w5HewEN3hLn2L+ehSZlPQjGO03kIRq2LvvOkvfssIdCSFGcKW/
lr6ysD4YjiLBlxaJo0V8s6atNY4JjtrptOoEdn98BLzcoWeDITdgcZMgfQVu72h1
AVGZ5kh56hncVcWldgayw6FB7b4a9xrvi3nzYMiBvzH7xPb8SyFqgZzyuRAM0wst
4k8KdbDI3ks0LCDOXrbeN626qf4xIFCDFcruN3GDuUh1H5f5Yy+7mQOZs+rsX2Ar
aPf/Ni3ebKmusiCem0eMBJ1jISlDqMf7+C1ChFXxYaO96gEFDvyYFdBGdFaZq5kQ
Oc6S+7L2qJx4UHMtnvxzAKKuXg19TaOjRpPDO88hbCMgXo/Q5joPXBmqS/obBEz1
iu+qaKDf+v44pIzDaIR1C70bnrkiYozSGnV2LLYSpTlOqL3A1NbqypuWReIkt6jk
o/aZ7oZOp1/t7XB33Hygb/xeLZ587AZTR/El2sNZZ6/43gatBpCeXw4ZelID/Gc2
dhKxQ6UWI6bvXXekOxmCcW3Wh3lGyf6DY/FXUoqfb9hwxUgLJu2Ix1h63Z3w7N/t
55nQpKcAwrq6E0xBnj0BtmceuKSJJATK8QmeZV0e09E0930VtiP2cGoOaUg9rgEC
cIpr2vqp38XCAzR5wi18zNTJdMrrUGB9CaOaZnYdxBaWFQtOWEvi5KXGGGkmvqkF
5WIqO0w5IU23g/CeFp5cqfQgGXThHgg+L3Jbd9d5+wigoCbTCvGrD6JIAybH4Zkc
/tSd/57fpr/Iq17Dog1qo59i7tCBpt+smMBh3ncwSW4InrDCo4pqNiy+hp7eASeF
0Ws7xkURgzya4ezCpKaDFwtmCCKDSER+1b9MCo1/1uvM44J+2r1zj6Fsx/g+2poD
JsOrU4PZP8kTh3PN0nSTgo+6yBc4qW7p4NGm2SpPGUmvfomjxTrJgznSunLQuElQ
HA+I/rhJuskB633doF2LBDjLnm3e6jCVqwOnIN/jeWN4uSrX8NUDg+06xHO5HsEJ
NF0A0mTvonARVBCZqAT2WPPi4d2JEd5zkGB9mLBQQdCgwPTMoILzTu830kMdnB7W
pEpBMzqGBSDtfsKpQt7GUDxpnjC9oPLouxEqkPTxkK7yUecYDBHJ7i2AZEh4rkBu
wOO3ghiPvVt/d2mYP8RqgMVXZbfBT1Z17N2h7NfCi7Q5GgTULQFyOxKiyWQNu1O+
OiQgiuTrweZBx9LQmAsTJEsAfH539DsTdXxucqcGLGko+8FKIs5qCcU6lq2YGNnp
dv7fURcc9qMHIt8YVPGhkRCTNExCAop23/vdQdUmRmhvpCO3S6Gp61hcWUsJ6Iny
EMC2PzIS98nQTnAAG23RmunA/Uv29kYFK5McV8r7mBbNfRuu3kLmfbpqs8Ga2Ezi
3iRxT0kO2tRjcGRIjjwRw+Vec7lbneMTznXhDP4x38P2BVsfn1RMwVfMOBpoHqbp
W1fj62typDwR0kuJuzDheWiQwbUFtelS1sBIS6tHEiHbnWbiKbeMRwJFhRryWWxX
3/FpPnzKiJSjHlxa0QQEv38yNt2xD3++0xU0PRt5P3QCpu0hc/25hFaujXH4YXy0
BlnxsMyUh8tOHS9YYXVTa+AZS6MiUYzrI739G5cXRGLOUIy8CzaKVyD6+NUKv8JF
3krP0xwX3mjglrIxuVf8T94xXaJJdnYNfbvpZ5NcC4q27oJXcJOo/5PqBBSBuR1L
AQVS3VtiycfB3FOyc3D43Sc9okQZNKXK3pPB4SlaRh45vZye0JJ5VI+ECkiwX9yv
z0nUYZofe6XAgYBXup9BCSUGJQc38PE2pwf2jJcWucpmoPyP5YkbMFXdFLLcQcir
4yQx0Af/pw29dXC83lzRw7PTKCKNJ2769s3AAithtj0dJ8mz/4rmpDsM44ZUnN9s
```

```
z0kfIahZQ9iDRpxM1WDmCPfcFfGkPLCVEcBhezc2lkSSDTwJglj3xZScYmgtFXBz
Wz/3BKwUhdcigCy+mNDwSBRurpMgmCV6LZwDgtsNcmssSSBjLFt6WeQnD9ND0gQk
iIUsQ4eGVykLVyizsNobZVogInfRGBrvl7r+dwhm4Bh2qU/Eoa+PFFZ1mHfNR071
cLTc+X21BciplV6cV1Ae9wbbmvr1zNaS30hKqtQQO8d09PcHUXS7b+QNg8F5piYe
ZNEBQbIYc1FeiWP9NQ4XY+DTavETtpahFLIe0aXY8pHeWPZi/UvqFUOXAwrj1RcO
5oRKOfNtwUMNMDboXx/X81yvefD1NMqE02C7na6ZSgwlxY2QlW0inOKbdWAM9e5g
Q/f+e3v3UFeSk4untYqmlRyeOCkBFpbI491prYe4xme5xbKrI0GOiM7kL9dUBJon
9VofHVeGZrepkQD2R4yiGlA0FXf9K4c0ouT3cpmD3Zftaq1om7KvW/ybnzS8/HTd
kUaB/9n+2F4t5xj5rv5jAMUMSm/aWARUrT/glZZOaHEvRqT0pvAyDSuscH9jDpZ3
6n45vdJJn5dI8MQnc7u4uBYDggIPADCCAgoCggIBAMnrrdQKoZWWoylFX9junhjv
nA88gkZkZzEf7Pm0alpgRr++9ZttArN0iP/2QYhkLh5MJgbfQSWke72H9tWpN3Ec
7jzHaZ4TKTdDD9kbe3+JC9hvS+5Ec8xfAdut90oMPzJm7HcmnXxV4owdJcm7aDKK
DMJI2L8++UawhBVNhnJ6JtipeKAbnrTtsueEJLTuuJv8ZfRVLAD+JtMeUee4kA4H
RCDSvVQnj0gevs6Lv+53X2TZfWuoraEN0jqNKUd0CUB+UxVrqkO0HtvwH/s/WH4C
Q/kclw5PJ1uv6RPQ1lpcoULZhGGEqYS5wYSBWma6DZoUheBm/0JONTxvkHGS9XhA
KTa8xn5Dkr2rezdCoRj+DuJVzfHvpalIRLij96zo3z5wo6mu6awqfSoAJR3duEbe
21VPA9xoOYBNC7i8nQ5oFcqfoZQkOhdhLsaUJHBYbgB0Q+xnpPvU0cFb9wPzYlRZ
BHlNkZpqkaZXBMOFnhg8nO0yaG+N40vSEIwie8fMFAjT1boUgQAWHYf1fumEDNx0
dnQzVSnK0ZGf1Frr9uuOXqtV9O8/9dMSLcD4tmAN7dDSCx7Hl86ZWUKUN5DaILMd
8I87BZDTOfKQ7GW3Px3E21lMOEeJ4X2pSL2eWY+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-----
MIIZEwIBADANBgtghkgBhvprUAgBIwSCGP0wghj5BIIPxASCD8D8ZIdQifKZt1UA
fl5ru1gYlWzmrKJjWnmivbElVfM/3vzIMDJj/jhAQULdbvoeMgtBaid5tSg3WcLk
8l8IcmU2ZE5b6ONubqwP861lxrmK3+3PB2T4tpLLRsGQXGSuHa3yDhjBzOfpc/K+
bYEW/sMZEplxr0VgZLMaJVpRnvwOenYWMUBYZgFBFgUlQyAhAAg0Y4E2EUAEVnQB
JxhQABFXdFMyJWSGQmFgdgUWFiUARSJ1dXUzRiJUE4MQBWh1NDR3EwgCgSGIJnY2
IhgmUnN1RnQhECNVZjgUF4KFEHiCNEaIYzAzAGMUJkIhQ4ciJRaFMQBEYhUWMTVS
BGCDF4BGdjQCJTeIZiASgGVlAGBodzIjhXUxhIEmEXVDF0ZYaDMFUEUDOIKDgndI
MnR2gzeCJBRzSDBACDKBI4WEgxNCYGQWSCMYRkZwg0QkMnQmQiQiRYYSV0hFeCdE
AxGDNXczUjUYEwFjGCAhIFREA4VFaEFkWDYCFxNSh2RkQAJngAgHeEhARCYHBIQx
hXNCQAgUCDMyZwMDNUWAN2dlYRF3YhE2eFE3AxIBFFhjhRcnh3VQAHdxURBiQxVi
dDGGNQABVzEgRwEyCEJCIlhhIxYCJHFHR1JRGBgHRShACINUMoMDOBJYZihmISgC
AVUQglJ4SGJlM4UYcyACSBFCIAEhVjRBNAckAyhQEAaHVkdnBmUIcodkcXKDGFgg
MBYhJhEEA3YXeEB1N0BnUmYxBChgUDVoBEU4I3dGiAhUgWRXUhNXUlRIREVxRDSI
YTSFVQFhBQCAEIQjJWYXIRYYg0dzMUAkYzQyRgaCAlZEgwd2MCOAZHJTMWQhUQRn
OBcwcFI2Q0YSNUNwVRVGMjRiIDJIiERhMWVUdDZAGEVBYFAVh0NXRjMFUWN1NmFF
dQM4ZDgARmMncISHZ1UyQ3ACUlZlFRGEclA0FiMkJRARRoICJ1NQCBRgNhOEhmJl
UFdSVAhRNDZBKAZQFgVTeCMYdBhUBxNhYwKHA1cjQnJhZlJhaBgDM4dmQDVkdzUw
cwcFMiFBFSgXUHcFg0JEBBETgmYUUER0QmSDMVKAdgRVc0Q4dXIAhGVUAoWHgHcQ
NFcyMiIVOHMxBVFQQWRhJoZBZkYCM2QRMiYlZUeDVhBhWDFhAGRVeFMihQMHIWgS
FlUxBHBwRmZTIlBHOCOGcDgViAYDFldXdHACSBVXMXQQYDFWc3NoMCUHAlJwR3UV
ISYIA3gwAURXMAEkUQQBYnZTWAUmUnBgZCFHNxg1B0FHdlRyGDAng0IRJzQnZlER
BDB2EmdCQzITCANTZURhFmhoJWFGEUURBhBSZgNGEIFDd3g2VYAoY0CHVWJEAFZI
ZRgCARJlJAR2aGYxY0ImOCMngFWCVIAxh2gSCAVXSDMYhYNxSEEnCIAkUzFVBFAW
```

```
GCRjBXR4gCSBgndkYgKBB3VxSANDEAY0YHRiITc0gVgwWCVEQGRXUghBdmVYdVdI
IlVHYjhhN0Y3clBxcUBkYAJgMiKAKFYRJTBzSCUDUWgTdnRQhHNydQhQgxdgFTEH
MjcxQAOBWBVQI4E1IDJQdhE0JBY1AxKAVwiEIyhCNWR4gyY1ABZQRHI4JlcRVUE2
BhRVFYVIAnNFdSOANlaDQ4OGNQVnRHEBBjEQUWMShxKHQhVUgBJwV3VhNmZxVyOA
c2cYUkaFFRaFWBUAhyRwdmE3aDAwJUh1FDVkh4UzYjJHYlYAiFhwYjY2aEVXV4JV
aAdkETJ4FVBEJhWDKAZkN1iHFmMTFHNoURVxIYJzMwNnYiWGQlJDVnKHAWYRQxE0
R0KIg1QgQAhlQjRGFxVCZncHBCIFEldCdzAoZhQIRIQgECcEaEGECHRmNAdiJiFS
FYg0BzIgNDMDEiEBZFVFcTRHaBeDYgIIRWBINTAWU4UkERgjBRFWVGdQFSQXYgMY
U0N4VoAkFnMjhkJQInVkImJCdoZUExWBgnAwECY2JxWHAiKBBWgxBRaBRDUhKFUj
djJDA4VjAYJyGDBHgIJlZydSFDAEJFF2h0eDJwMVQkg2dzQEh3B5FeWdj82jWr71
N7Gv+X09RN4dV+FTn2TSH9GDk+cbLdvC3EcMrLMb3ndkcwTaOVZ+K4CeH2GOQuVP
AKaY90TUULrfibos91PLLr5bfwV0WkMdX6G4j6Wm5IgNA+MEotDNZkh7ehAHZkxK
5XZua6G6kvY6ZyH/+7wtUbzqaxUdDffTCY/lRIHRgzIkIR9OOsaR2T2qggN3cB7o
3vW67CE0zylOj+P5kMZt66KfMjEc97ELdTifq861q7f5WdEKwunjPAk+cXAAT/7z
Q/opERRYkkX4dQnsdQyf6SANT6AFbU1+Wxan54dW+N32iLu/g7DnAzN1/U0JLgrR
uBWkqW51og5HZ8TcPnHYidmNXdUHiLQ/YmYlci6vpdkrGR/dK0qaLg8X3qF8dg8p
zFPpKlzE05hcxq2Ir1OEJM6x7fkTaDwpgPzDBBz3ZP5Y2VqYfWFTnn8YuF+bCxUw
m1h648pMTkVfaI9ti8rt62orOmRUMzxfRDX0jf7acpwpGqeWmHiHNNhm2rTvHhCW
t/1RAsr7te7WvriLAOTZ5y0ZKwiGAjx5yvUMTi7rUrEu2oSVaoW5Pfxxiz19LJxk
YLXlmdC9hYd+EVmSdElWzR92E/GE23rLpAVKXPJDhQyzMJZBFtP3GF94tDpBjBBW
6u16U9ne2AgzUzxIjYLPShPZ7FXvsxwxmHKAAILsIIVIYwRtisVZkbMgAm3zhFwF
4kfPFUtfKgP4vDBfyyBjux7sT6dsRpcMMDC3T8IvfwWNykCqLH3ypSQ9kEorOdzF
mdkDWylJuGtdAX/SNIwDvvesB2EG+l1axz0gEcfOA7o0Cq2xUrZzCtZXPteuw+Ic
KtiW2Y2epLy75aa1QsZx6ycd7kcEtMC76qmc5TSKlJ8XoVKpjs5lc2R5JmtRLk8v
2vKJEilnCRsoc/yIwQGUehCKfhxCwHdnC4hy6n0zYVY5VUrkBPE5yGs2LJ/9Nccg
7zZLlYIT2DJ0S1sVdZrr6bnm4u5bXzg+ONGQYuO/SiNBcju45rJtCLOZQN25TRqz
Rz7MpnA7+rMKzSTml8P7ZHOymUUX3nX90abBApbXvA8q4u6Y81Nqfd6c59CEgXIE
F+VLLOM3zGxj/g2Lfy+6NBoJqp9TrEBgohS/57CpZTm/MDcn7HJMGgL2M1dYQE0X
gO3FdmODdmhjX9SLf2t5lYXamOm9mFgPWMS0pNTiiPStsaI+nyfxOGZkIYA5kuoS
S0/S+cu9VdIeQk+huedJ9kYpyXIdKEY9j0l1qtRPsWCLBPCg7V7T87Axr+DE9L9Z
tEag1ZQK/Lc8uvZ5KGOF/5JjgTga6fmfmadYp0kZFs69ldXsOvAe9i8Uy/YMpdKM
C+QemMHwizSnRs1ihLSHUT+OJd2EldItjZ3NNcNs0OSDlJzrXw0HEYHxfTPVVwbA
1R1LH/mXV5W/NYcTGIAMWbKt/Ks3mfZTXIpGKq+iRfzrlOfuRemfSxkWV8yMK3uS
Z2vU4yCqpYCXxTM4WfZYP0GrPw/RD7OqNOrYjgCbLXkrjigctfIZA++PiYDl6MM9
bB+L4dq6I/1kxBbnSwgm3WV2moj+AcNl7re/h7ywLbtH1zdYrWQbTgZINYRvgj4T
+d2UdWuzVvd2oBCbRZbfNzxBLAMv/zP/9TZ2X+OfrDwJ98+bui5da+xWVocQqYxf
bNoA2b01QfbxyH21JPoiSWIxku24MTUQ2BakdJpXBjwQcnwam29kxzHehBunPIem
pTzTjmTZLATfVU0oj+eFU1eGb9UOW8wsTGnozw/h9ZL+CzVYcjhDu0HoSPAb/9Sv
Suc0KENh9QSFXnbOz8R3WzmKSDtCktKJ5YmnWTi5BIVd6aw87P2eIbjoCBNH7ioF
bYMf82UMDcFmpmidn2QhioBNd96dOf+B39jf+5sR3D7N0iTOPQrVLZnncLqEyYNY
bTQLdLEY17kZcYZzh4uFeaTAU99AETYXafYyBDi0K4WmQYc70z9VH7bbsaCNVlXh
s13ckkStQL2rCjdnrcZvdyme/dKOKq7nLyiH7Oiy7LeW5cUdCcXjQ+8XudtGzNOv
5XolOFqDut4hwaojPjaQr82ztYliIhhWov/qKTexDZ7N3JvjoZe43PfqB4sTSnDc
dNdBDic9ubN2cz4V7cKSjiEAP2InRZGml6ldhYBunR/g0rpAG/Eq4zTSfpFm+rSz
JYkS/J+lVqRN1yFCULwXDZJqcrYkTqG4B5HdLuRwXcXVd3A9P7vwETpq9ecaBLwb
AwzKYxibSy6r04onpnUugNk0Xghwuob9YHbPsgdApUaLOFrGf63iTiC2RZdeN4CX
rX9tougX61U6mF/e7WNlTiSiurzGlASPvYYLDZuM19Iqhqth8GA0dWT7ynMexV5Q
PEl4QJv1ZNUgEkpz7ktu4lKkWnMh37v6nhe0NLQ8RI0p7fBdnjYdpd47jOvIpJsN
bboyotaINK7X4EYsWyNj2Uhr4RNuVJeh2OoUkCFsK8Ms8cgDU3IxN4wa4V7PGUKo
y+rUs3d37+A1DwmJq34uir38Iv60fv42N5xJUDtcwPd5BEBZ78WUj5/dvMGjgnuB
HzJgcf/m9yUvdvIzFXOzjnEQIhvwWED0Yk7vZID9+xT+j3dhqsmb1f1gUjv4kk9U
p/OL9St5qYamIFvitTIAuI6PVuv2sEyrcmfOlPr50Oi6um5Q4oBorxE6CAzjhYEe
tIO5UNs3pgmQ9QtT5WkQCOzrNe5m3pZ7JZ2uEr4umrPh71g243xZad+T9hdl4AMA
```

```
VPvdELg/d4ze2rcuHrvFFw/hoA0w6u4EFmAddmPtEANuWjHWPAGgTdR9MCzwnCxQ
+QHU1zHxZIzXaWdXn0WR/L6wG3UmmmAw48r/tGnnMCG/HJjpzIXfMMtD0mKr0ArG
/5G82VORP3NCM4z3YeugTPudzCXXfBelhMlsGU0aUFOFtj9AelU6EorxgVvJ4IVR
tjGWSXei/kce6mlYJm+N0ovDUDemaLXXBbQgsWfehWiQMgzBbHmFlyHCaULBM0G9
CF6plKmrhRDRpOKoElTOqgu2f6B5d+peNhdwhES8gDfl92jNvnhfzZEkg9Rs8Yy0
ZNdM097t1xK3x2FN6z2wh7IUK2doR3YHWH7NV6OdmQKxaUYSxsrKk6XxmAzVMkjC
lezObzldYwfpl1EeTxqYhWCZalAIs4ng/pbOxs9CHDJr2u4yE1xXHdwCC7dsfsWi
FNGy+50FpIioV5GGAbC2WS0qPF3Qk3URJlKqDb49OBK3bx9OvOgCwi7SP0nQfSFG
ah/Jq66J4H6KyCvCvgEvBjn8eUrQRdh8ajrBEc1nvF1ddwAY0XIEggktMIIJKQIB
AAKCAgEAyeut1AqhlZajKUVf2O6eGO+cDzyCRmRnMR/s+bRqWmBGv771m20Cs3SI
//ZBiGQuHkwmBt9BJaR7vYf21ak3cRzuPMdpnhMpN0MP2Rt7f4kL2G9L7kRzzF8B
2633Sgw/MmbsdyadfFXijB0lybtoMooMwkjYvz75RrCEFU2Gcnom2Kl4oBuetO2y
54QktO64m/xl9FUsAP4m0x5R57iQDgdEINK9VCePSB6+zou/7ndfZNl9a6itoQ3S
Oo0pR3QJQH5TFWuqQ7Qe2/Af+z9YfgJD+RyXDk8nW6/pE9DWWlyhQtmEYYSphLnB
hIFaZroNmhSF4Gb/Qk41PG+QcZL1eEApNrzGfkOSvat7N0KhGP4O4lXN8e+lqUhE
uKP3rOjfPnCjqa7prCp9KgAlHd24Rt7bVU8D3Gg5gE0LuLydDmgVyp+hlCQ6F2Eu
xpQkcFhuAHRD7Gek+9TRwVv3A/NiVFkEeU2RmmqRplcEw4WeGDyc7TJob43jS9IQ
jCJ7x8wUCNPVuhSBABYdh/V+6YQM3HR2dDNVKcrRkZ/UWuv2645eq1X07z/10xIt
wPi2YA3t0NILHseXzplZQpQ3kNogsx3wjzsFkNM58pDsZbc/HcTbWUw4R4nhfalI
vZ5Zj4y/Greb/a5FiVJQC34yq0qWgnGF0CnMn0fkoPMhpPHVAEsCAwEAAQKCAgBi
mtj0Z4ypBDsBeINp6H0EKF7Jgf8MaROLhc+v0U7ue32RPaurDvz2rb4JYTR3apSq
7vzS9ktWGpDi6Xa8uDn+3uXogGkvbKP//JvMpgMVMNO8Cf3GiV8TOoIpyTatznU+
I8zuEsltYnOTgNhnP0GPDKNWbUSLgDEzOBgIXyd81/IIdBoX9eT27e0j6gAS61Dz
u7n+K2mlwncrOe89fX+7mgjHDqKuafMqgPkk3FIKHflTwnHhFSpVL+6t8SlrX1r1
R7tDBqTLEzbOqOC1TSXlwy12hWOu9TB/MdRcfOtwjTOi9Z4UETjHO/8ouhJvgAQM
bmFCSIn200JkFQcwr1d3VrTpGzSUHBnZQhTPo3u9ul0Tqy2EGvmQgf3i7yJ0UVjk
wQeeNj2zLN2ZRN+ECXa+Uxfa/0bB7M6kqRr73GlXjv+w6B/JwzbZUPx3H68URsjH
Cwu4lMqCMbItnibTiRghcHwh+e0woT4aUsx8Ffuxok1OnVhUxgSihF2HWEp0ABLr
8iznf4Qbdjpjz70RKBGlML/dJIgfWx5NNFmpwb+X5UDxrI6j5Zm2QqOmqZOtlIwY
EKwPCOrKMLb90m2vQjs3KlDFV03xlaGxKhpS62idkj+2HVnW3T5VIVkLnt8sB0sP
SXANXuITApunbVEqIquqDF93uZ4yQ+ckDNjhmxUpIQKCAQEAzwBoTHqFWjyLOT36
F3QiEawBNuERo2QRhd9774hs5JF3YYd/vybLXwXO0+CiPqSrX75gnemxnp6vWA6k
jo5ihhbY+CMiVkPvMdqBcBFvKaJYrUR9jNxfQyTIwUWT9Ci5Rd+dX4jaMeJ9ox75
ts9gDDRge1OsJ8VReaeQVOvvma9CRkfABSAm7vfS1qM2on3jcg8OPDyGUKh/vYzH
xKO4zVzwfApNzEPdNePcZhZWwigTPBnhf0Fr8530lePQYghUUxA8L5I7raw1uL+5
cj5raR2hC3b0fOnWmUoOgkyqt3dJiqy7t8vS7MWBjATnk59RNn++3KaGliIr6JLw
Ze0jFwKCAQEA+bdhz7IDVjQUFSVzwGDBohnhV72fsauRVOsBR7N4TKMYFuoACfd3
3ACBhC+tn5D4LJwnu3ykJt5ZGhtW3UovKN9+HkHszh3cGYaRIVZCshlDV+K0HzLI
TlI0Nc5hYByQq9D6V2+Il8lVz1PlPZyFVNw9aGlPz4ArWu/6H+e8Nk5IQYZ58dli
py4zvmIbVsT4zFquReRsCMDbNql/arKhEcII0EBP9MlBLSCTW2nPUUMo9UoYOTBR
NqoBq/D/qXH621Kd6i4uoHzzDBusxIKwSacxD7Sm+8al0TOInnnI+hVOiCkVfzLj
47ZLCLsw80uwIFvhTHYmwX2JxlWjA1Mc7QKCAQEAuB/OpihdMXSlChecuvvryfhL
ZDsyazl5dLDjFp8s7OqPW8sg0DB7uVv7Ku+moT3rydAXNJ9IBKV1pkfwC3WPIWJ1
P9JQmpb2zktj0wFO9aOYaRaA7qiee6TehTuUbRtEIWjUHMQoATNLOas1x2wSLQjx
wQEeIooa/LEVatQqXXNM6iKsJGMC/pClk5G96S88/plxuhbECj620S3GC5ztpo3C
wzKPHOBIhcTWqF+6cB0hbtY+g+j3UszvX9wx4OEz0GaiglX6i3KgnmK7W2k2NVvL
gd0ff3SoE9WRrkjvmR2b5qPanZPJXB4aKye5rM+Ld4SNisr879IZaFg7SQ5zpQKC
AQAQ13FdVKAs/C4ujuwTmXL1v9EW3c8baHrQw1i+wTfn00gYo4eFJI+M4uvZQm3v
SROzzoRPfMSFapGP1TAylIJBu3ECEWgrLpBdmFnJacvtvw5vqvaC9CXWQm0LA/RF
Syfmrp1zsC4CLq3+4aWgViIX6xKpLBEZ6YcDBxRTeomTEAyHfs5SpVql89PBj1RQ
sdAl2CfQxusSXA9szFmvlISQcgmuIehCliAzLvNBQw2caW8lu+2OTdfsW+Lo+cQE
ZY+JozTLSnoSkNrDgkpQpo/FJ+WDLaflayxbw6H/Li+DzlQRktPEVGZSQUUmPZm7
jus+A3Rad819Vz4nhjcMTlqxAoIBAQCjYdSMOlEot/q8s+wp60sCsnL6BxPqVTsW
```

```
TrMfIguP3edeNkvb1LYnqTwkZxbkkqnzkZTJuLHqgeRy2pdCvPHKVgxnw48osrOV
cyXTtshVG3SVyZw8yqKV8xwh8w4scbkOTlaDivP3bl1ZzCAR9EM/zaLd9EyAOTHL
77M6Ht2qbX6STKVfVH1ZyFMZydrZBroQTx/jBN/u2zwyRhAhCIESNL5JOhOVqeSw
2KB8mPvjwuxg9mn76D2soY1hq9uWU5selv+2CNniS7Xu8Sn7pPBPfnFCD0G5t5F6
M1bYisNGS1nBsAtaMdhHE0X6PEDuYKJ/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
3n0vwn5p0OOUaQ6OxM+agtglkYgLF32ZVOgLYZqzhPhPODaTgcCp01P2gw9vhrWq
snZn6tpE5cwaVrnkKmLWI/4aR17opelT9zfwH7uYVpB0K53h9lDRu8/Lj/bhh414
Q4g+3dxEc7Pw65m1vBRJg3088aWKWDQ/axoAtiMmfac9JpOtdLEej5+8Yh3bNycE
7zN/sjZShZ7sHBlnN2cK6Z8cc/86+SxsWImS6rEgQUs2V+WU9PbhuSJn9in9NbL2
KSm9y9MSTw6Z6NcGOPZ3cCr96l2hgEQVhEuqs31ft8sRBm7uIOA/N0UuCsSek+hk
MwH/WnBmQJL7s7p4wtyvX0JaL6t3MQstp6awihjVc4dFS+cj8Sl8LqLyeuqQ2PbL
TY8P5IF84PNv33aDGiCSLTMKiXquhcuLE5y/O04bDi0hAT2E1r2bCdPtB3qgsIgS
n46mBcJMqdjnqseJ2GhO2hyQ06J5AenvL4JsiAWaJExdm23WfwRnKtTzxF1NrAvx
Jp25k5f57qBbiACzZvP97aZfAu534QwQnW5JlsiVHO53WjpidGTBKkPKhG0I1vtH
O4RqtD5m4Fp70xr7J+BrcmsqonnLGlJN9avUMdeAhcavm0e3wOoa2GmrgSlfDV5d
3Y2VVZQm0k1sGlhLd9xhRircAYgmQjbyaPKZ+dTiDcsRV+9tQqrpXsx9gdQFrKS5
S2zTy3p1KnwbyDCxYMGKXtfVVgrvX22D3uvNMYPpmN4XFix0ot42Lp02L1mrPi8i
IBPgSksljzVeg6wMDKTwxf8eAvL5zKJGan8xhCeUJjCHAzoHU/HtLQwBq5/Yb1G7
8auxz5aQjbAlKSRreknCppyLX7Qr9N3rSSnxO8UDjKSM728w31zj+fD7Hb2x0dOO
Y6DuWcwdH50D9SlUuiv89l4Qt1ksIhV1+6LCKpXg3WBKYZx37IJUrKFaKpt8SCIO
ZpPdF3stI8EzHbJg+KNDcx8xv3/pjQe8mH5fNzF1fwwwhXqJR7qIyHVKqIgHKqQD
mba/WCJXhgGf2DxMxJCQBQn/1uhskM1lBZPw5KuXLy1Paty01XvWcpkOgVH27jXG
SpYEhDlyS9S3jaCXhRpyqKHeu+XqqyJden6HwUgtpd61TmG+++yvA2swmQR1J8o4
qe/x9fAqmrwfP4K8HhL02W5e20pBEBxUTBr2Ycvf+zpb51dPFWSN2bzMqYzCSX1g
91hau1iZ2W2/JEaRfHc1WXhRAB7OD3cdUbWlJTEE4BsYi14KJOD5aglhVmvdUm67
YXDuUUnyJ3alExRmDoLFa2JLTDDKGiQWhhVVfSp2n8avyB70mjHwz8gKM4v9daWz
GLHyApTWYm0Jg2V56B9IXRS6qpJC14JCW7kRig11Cv3HLvUvPt4cdmCGgHsI9DlY
UAZb8nziSrCY3aN645qYzIB0bnd57j3s6aHP/Q5yRIQkEWabA8vUORsHMp70KP58
kumQIcku9Sgr+trksp3HiAIOpCHlSRnDZAoRi6jw1T7PPGB8y3BMaTZMNB1PwdVZ
hDQg+LaxGMAVG/GKxrYbhkQK28Muj+I8LBp4r9ZUwLm6KH/i2mmYc8CjdNiBjYky
hM1AiNFAWzCx9+UHbbhILVwB6hT9tGQQJxmuI8CHdtZw6gYzEcyWhiaYmUDKXQ+q
xTnVblxKcNNDzsstUX/HdHpfsvibCNThKBM8Ci0sWmKcxvMPOU/uUqZlcwOwQ28S
```

```
dT7NyjpY7PWSjKYyukssZoMvyPhcsDEPVhNa+fo0O+mHEg6kmXH3Fdtlu4DPb4qF
b9zAupGB26HIDgVvRYRP9A/JMarJUnOYSupC9kUxyMPGjpeEBcucoBb7u4yLmZpb
i2QF/KfvPNApC9irlXv/vMDMV9yFQhAY8iv0zZc1LaATWDba903xNO9sSSDaDCHz
bLVXlSL5g8oVO1/oO9LLgObQq9jTEU0b6LXpYXTZWvW//SpI8PjiDu2D0BS49sUk
4lsWHPKfOv1+/ThPiQPsHZlgRXToq/ujcoYTHr2/ES59vVsGxdrUwsBy/Y+uMfqo
hpje/vS3JfdfeAWhqq3U+52EK4UEJG1DHWPnsv9KsXLmYFMmi9U2AgrG4L4DzxT9
Pl526/9aVfrsDL+Pj0HZNvM2qJh1iXhbc9EbahRgHpxydkRMlrvRUPuTSp86M+OH
o0dqXniUENo1tOccjnk1FUiuCmNkDCHlK4S2AKeN9D2GMMQsJpZeXXXoLQ09CZ1U
4rQjx9zNqm9EDTMVRfTuEWSpEpQfUcNvB8lIbBINP1ZTDHfrKmuuOtcwShEi1GoC
e0oCVmiNDumwE6jw++gc0d5XzH9OHvJaChnBBCCf73ZybzZrKDRddAUlRLsiGjSF
siZcQMIBpbTGlIyhwvye/NagR+OYHlsuNEyJJOFEGK3xVlsyNJ8y+DJZwz3usZ0f
WZRy4NUZzV6eJCTap6HVmdYMvs4lGd9lWL8i0RC/BQe91vUycVdqSnPkef/d01Xy
bv0O6TLMqsHzH2rbkC3SLMtQOAx7FxEM7y6+0SZ/lCujQoBV14ggBuoFgDtfl2EB
XRs8f/x/z+0t9p+TTXL5yM2953o9Q6aD8tLhXE6GazN1AodTlpu8VsnY4LrBP/yW
4+KuREHj64fKSSv82q6jT3rfbmtW1aSWMVpUe3anLN2gjn/1po3/MAJsa68akIXm
ntn7AjWjURnoKmLxEy64AzFeo9xI1JVL69XaO5DNRMW+JtiTSm+lN8cWjqbdiMNS
eKd37anyX4C74sEbxQM2K101PJMkGci554CGqES4Qgt8fis+26OWWk09N++JSt+B
eKYp5EpRI+drwbsqeqH88GXj6KyGtJET/hUC7nTkEMGVYfYKD63YNA3ozjF8VMle
/ZYQ8l3eX8YbWoocZmR5oWGDgeQ0Y5rYRqI4SbVfIhx6hwJIHBMgjiexX/F73BRP
9JZ32hTpyvg0b6p4zghDPrSOR1Ra5+oCp87mlmh6uVjSXXflbDBXs60UH7UwXTAC
rr9aeR6yMQLtUcIx2CnJqJoBNbG3C5fujc3jeZAWc7r0Wadc6uA204ZKXoE1kNhE
0zqdrmmWZ26m6aNdKJ0+dr/tTODh0OIWkTIACwv1BtVSboMWaevrfAwn/9T1LlHC
4O7HPrQjAFqbqCDJ8aFD7ga0vm/hw5e/LeUMqNp/CCX889m5kJjwXawVsGpRpbrc
GNuKtR+RIbkZSdAh77wzpnRDuPq2EYVOkaqwXxKA8Jq0Knl1JNu5pYJtpngg7dc7
4MvzpcA0nHrZbbnR1fHiDhaK+C4a97MN03ETLOggbKwI/QahYfjBPcF1trLkaMWk
0Wz1YR6jePQn/Fu+Vxd2EVkB+i6enEb9GYQS/lqs/1PzKWrzAdSE6FqJr6eI57Hk
4T+GGkj+UwA4zzv1KerQROQJti5yA2IABCHyu6g4zZjaZQiSolrMkLL0dviU63jg
fyz6sJ9GPLwMC+3GA4YJ7m4xU1Sy0eGU//57s2Yy1xWv4zXThhLYX754ThB0wg4u
kwXzAajU0HOaeuLL5tqFE4kC2cugJbLMpKAAMA0GC2CGSAGG+mtQCAEfA4IShwAw
ghKCA4ISFAApQdDYKr7L9QtCBvYwc5PeOFInevAO+0t1U46xJz84Fb0h6fSLVroN
GRiiTiz/8HV5g0MCj/OQs1BmgEx0gBIhKenMWckAtBF1ySwnb6DdScEF3aG3dMX5
SNNYq7fpH6WttJQtCKmu6QoPgjzsknSPZxFTs/wFknTwxJGDOCz6DWCWUl7dthPP
4IWRbG8ROW1C+wwmZ7+2c+2o8cpMON4IJKmsBQN3UOIRNXurLFDagJ6A3yveem8J
jUGjKD5dCMOf61mEnNjDprbEBkQ8O52UDPrKWtPXRIDyvj4rAFfHSCop3tz0rX9S
2IREtU3RhJCVS19c0sGH027ojVZX9AN3dXdVze47erHB9qWES8vmu0RoBMlEQ1jn
xd3ibLQWwb8H5az/8waoRR48lB+VMkHjnKPXhSBQ9m9UViWmq/WmT5Kc/40u9an7
fVsD61tWQbqU/9J5TGQKdRGkDfxxthnAyDU/5YGy+j5ysVQXjZ815MguwY2yqL8+
nNb2bDjdq148c75VoOXR5KmGAOxIAPAgUVgjKabuIJSQza2kmQgYc0QaDDUQc4zj
Gh7Tnnd49W9uwvs8kwadWeUDftooMmXToYtKMmT2QHGq4hIpFI4+/UrP9Bfr8ZKH
QqJrS3lAO/JooGEGJoAE/8ktG2LY8mwqQvJPWBkxD2qjVdfqT4hOnXrbdl/1E3Qg
s10WTXsdKSZeTP9s9u5IqcYoeQj/4QrEHzq28Izg89664v1BzK0tppH2kCvlo0Hy
Ps/0IKhgCK0viKOoesBO9OyhNXetKBMFDt+Bcfdz+xNGtOgtLMHTK8FCv9JmifXH
V9R0hJQxTDEVncofsw3fsjmduw9dmLimOkqKZasK8zrAQeYZpLMrhidj4+DgAQhI
Kf2NGXuGHWKdvV3xTQx9uTxetdvKZDqR/+ufQu0MIYQJpPJY9Q1XNYs7EWuWQ1F+
UugoXlnUn6glCwuFU45wzUL0BlbWAFEarg8WsMQANNQRDxU7QIJpw+QOu/g9/1cg
ZQMDLxPA2FpLeH4nlFbJAfqGH8FqW3NrdT0T2a1upsWhA+3oMLFMrhMWDuJqKdso
85NEXIjOVo6AGvrkBGcyuqA+Vi4zJ2uxL2zwhhFDb5gMkHrlZxDeiTuIdCALOguj
u8/gz53dNRpwdKa2xPGJNX68/mVMc7cXk73fx7faJ45N25hEHnGta6RR+8D95dPe
DKlfBCAtBybbag0XJzRE8omeKfKz4GMFRGzVfa6lMlHJLRDoFWoun+0TTSMf3C68
X/gYAjVJ1KClmG0D181YEDn5pO76kiRBYa5afYiy0+gY08dwaVQIE7zBrAevVZfi
HwiQByuqTpaPLUAkEL+1pXjxDH4e4K1E6dFSHtfwxdS2KIJgsU7tmiCuJo4Fkqno
dcM3zyZQz2rLAgFIwoiFTmOAuuEEe5aVdJeQlLt/UEjhl76XbV7cpE1vbV/SbJOS
/tNjj6YwrD1Q+kW0GVxMvRiqS6JlKxehyOOkPAGPXnLPOtpmrm0BBqhfr65xS8bn
```

```
FVcsptFfinTM7GZE9G7Wj9A+eHVV2ixFYz2rA1heE7yMAZ2wf+kGHg+ji7Lf5jPE
l1N/mLUUhrAqjqkFSnZshkHquspQfflseCsRA2oMZPri2LjycgOOeayM823CEAMR
AIVIuuK956I848t67yg15V4G/1irg2h9rdw4j29jmh3RxzAwavC6eBuJncyJRkWh
7R/E/kX3K3h0Parlq4Tfupdg+OBiJhsymR0LMLyE953BrpHcsmAg27lbyfW9rchp
Q5BWtNgay3G/auJ4i/YfYhsxTOCtsuEBhLbNjqpN7xvd9E1guAx7SzEzccLEcxjD
+fpVsEizogFtQq7HMCA9mskKibNm4QbDwfSd1/MeKrxy7wFhwINoK5BLuNiXmVMS
xGmCUK74u4AcvvekC1dMktazTz+m/a6MY/mH+5ikIiXQxTq3hC3zDG1ctoEV6aik
VGr2wocqCk0cZN+gHNIXtKvuBh0/UiZtz4SO89g3bytynIPPPiK9np83HMq/eFPg
2BzvMLdi9MJwA3QJquG5l7DZiDIFmRwr/Pc/gZ5iu1LgRPMut+SJJgtnQUpXeaQh
NSOI+zY+tHRfkk/jgsuQ3rbagUCxAZjsqK5UsDL2Srxn+ROOVs95YXhSULhRJfUu
y2W4MNYwZOzjLGkY1lAgK0JKfWWyrD05yH0DRrz4gkuDN26CxXb9fSmMZgwRUTX5
siU3vpPWAhq8pgIslkoSy8vg5RsTN7J64H+ZCzeOWJHQXUKba/cus7iRKcdr6iea
a/xZuKxOzK+wtyibH4W1LQrcWIxH44RJDleToJn/7qGxKvzZ8yz3lLwio/gpGDSI
sosJyrnVUrP2RYj5lNRZS1v07Y2SWPnbwgyubL50szPhejKt/2DntGtLr6mtXVtd
DCn/xpU8O/E5Mw8E2a/y9PbJKAI2/rewak16+Ro1qCBvsCXy57qc0gLoZ97O9UMa
Ehelj4vmOu0xq2+335Vh/r0NIJZD+yc2LR7wGaPTyqWaEYWanqVvtNXFIXZxU6nK
sT8ZHam3ULeEAOZwX0vbLUd8sg8e7AT7+8MJUE+HdxmX0o7qKeAGazrPfDHCks5n
rqf1VMf13bz772MUSiCXzsUBpycDkuYte/D9SQ0sDH/vQOcdBefb3u2VJPUfyD+1
/UHcYZm66bD16dACiLeUW+59GOyjccabdJ4O02eYN/VtxBmM9w35eR9Suam6ZVfH
G2CXFgJU6BBs1Toa4PK9G+tErEcjR36kR1uidooNiaLhs6e3CUyeUppqdvy1t65E
QTxcYOtpg5XyLqdf2IAt9jSxaxeRHk44RPGlTWtb9fEYw+VZRYGuiEIJCyoFoZnZ
KUVsB8YA+9J0dtZLnntU2tKXZ7X1hrLUWPoyRI4uEGo2HxzPUnfPSXSE3d7gTS1w
9Py47lRbTfHwiFOrAH8bDsrR8XDkNGWc03boV2RtPEssNiiQ9GPzaPqt1spTaMwq
uChzfPXuQu5RWE128dC5jZEVIyFo+bOHX3nomcWQT/YZcfRDdzYwmeUNvYnoOoNE
qVKOMDLoSRodeGERv3Dn+H+3q2Psd7I/JSUKZJxcG275qICB6Xnkr6EMMZhDPdCA
g22yIXS4uNLU8AbTKbv7q+8s6cn+MJ+Xku42NY8nTlXg+LyPuXwbCZMLDa5hp/0p
p2fOOKIdfMJXjMwGhLKvgUYyLtHvqZxisHtWjb774lI2swcK3038kiZEexpsQ8yi
6tlvlTZ2bsp3c/Ap9AHbu5DzU7cgxZKEEkNJiW+iOOKTtx1LXnfSt1K6C8NSilae
Iy69uNQ8dtUPXzLnhAwVL+J6lsYnjMPEo/FPvCfPzLeN70Q0ITKxaVcqdib+7KyP
cD5mKjasSdg47Rn1NeNRtCIM1pRszqV27FTpxPExRwFixsfDtTiWOa5QLNm6V1FM
1vjKsm2kanhinZByLy5eO1SV5iuuudyQXNtqEGfA3xKatOkuGUaGXUYDn7HkjL+w
ZJhpnS5C8Pnt3pgrWRDQl1/qFtBPfEjXppbKZ2w3IgVSRk0ZWUVFMB4C73Fp+HQ6
5nh0ZfqvMW6QtZXiOvIkdRvXVciqvj16UMiZPBiVL3DQ2NTnds9deufau4/s0e+L
UWjr/nDyVgcY1/ox2p59siOjet6+FhghQ5uzYRBcehlIp3+2yd7ptcstfLNbn001
SPT/YgTwzlc7SRJ0r4NapgzMZoJRH4QIrbLtOaOssw89fLXKGDAhCykc/qb1VBEH
jet6GW3AEJtIzHqswueAUJNWXiLTyjqg4ZESIoWUCwwjF8QhrWw1iOXvYBTki+lU
nTICEczMx2Z46AQxotl8kYKfRh+bXtP4fm+JsJ5DFl7ni7JWzi15lUApbVKsGbBq
Jz3Lp8n1CGRVftjNt1OtXNx3eS6ioE1PR6Q+F4VEt/g+Alm/FOkVoUzQvq9ioELg
CtQ8DLN9VJuydr13w/symES34jJ+NBx+zaTUD2A6XTZmymeSlKofbgcscG9rHgLp
29bIPTcjFNtDt9+hWeglUouy/1PHqtlCxjGEvLwJPF/Oji/L3MRt2GjYICkkHOon
9C4RwZDR+IE6ThaCNctJ84bvRTw+otciv8S9FDDpKrtzGIKI3UCXQ3YoSf5SFKIs
un2esTUMeQDeQ51/jyfdA2wSY5K4iBLIZNvJLnqm4pTmJX0d6rDrRbL8nf19IobB
oojqDtfT+kNk5xUjCcNv4+heLRYw6qoH5IP0/B+9CP7iQ5Bc29Fh35s3bgmcBWm0
iiRw7GDwTSFlaAa0JRuNMAwon0mwgJjyM16VZOh217DxqNJ/ewANOrERVFqC25j4
BkjIfHeP5s45T4BhrbXGmX+K6kvVkyUzAQ8rHMS5AsTQBPwbEf0SJHFvqQlwdEd1
0jpMHWoBa3qZgK2+0SF0ABsgRBRiDS3Ehb01Jd35seiMFTkzDHdEmzw+ZwSl/XMo
4vB6N9vs7g5uL443KVWyl/kVhTviRghtKHnYYzvlQvY9+fwzRtJSpTPgdNj6uKy+
+fMsk/jfCDfzhAvsSlV78wNDva/KNm/KUdw78d+pvd9ztdLMH+z4IojwyVITTvc4
lukiSqbN1EMa3NUfua9UmuHHWXr62W+qhiBYp7uHKgod5lYx7Mlo2Jn4fWNbva/v
Dv8uKBdAAr7e3N6WD03lY1tC2QsQhk1vQMeFsbz74HJIdQtWkw98cjyA+q0zB+Mj
wdkYymykAjwV5V9IM4optTlIxoJY5M96LtIEw+mg6wfOOwP4tsmL3/mae9VdiQeC
1mPItVGg3qfQamBxTxY7aBY9srzfg8dvasD4U4IWnVNhf4z3r0Cbmo5p9dhRqkew
VJHz9+c/oyFsfVecwBVjygmrow12yYFonB3btszbCiD2yAVAVEf/QurBhwxC2XGo
```

```
sHsJt6HEO2U7/UIohoIlqrRfxChm9rio9PqJT6pMu1/LEPfs1RwidkbdOT64Hgaf
v1F/A8zA5+6qQvATwCnYH845Xv45AFXDBBcJNU2uMb57nF5/uXrojtLtqyg6ouob
hoc26yHMCZmVr8m8EPg13fK5tT+SS4hg+L5c7DwGaMZ6NSd+ufUAA7QO6Sc2nqEc
gFndeY0180Z96BwlsvsR7J4LaIoganbPNEUyFH+alHaYt6VF91Q+41/lYEyG4zmJ
9hcZg8VOMOxoTN+Z0aGPwnmznmFpSv4aNdmq/MavKVcNu0qAQLDYGKDqO3iPoKQI
3jEZSBR68LDmjwoEok4iNIIaU8gBQnNC3cHNk4u1suQqu2YDc2HdKByzfW1VVToP
F8igPbDW2owHYJI0SOYRC7J43UTnkIi7Z0VwquOCzsQgYFyvB9GQlnGTuMmRzKia
sBXsk5YAlnqCFEztcFA2R8JF+fGgYoz5zKMpUhTmhooP7Yu+Pp/kbUyYfDmGa6tG
TzO8QGp1hwuIjYyVP8FebrRHThMSbcRqkMPWbbR1gtu2mY/Fd3zJPLyOyyh+SWXm
No4X+ESMYxailVDfjOiUswH68IVp0hmtjtO4vCZunFhnXWcSoyhGLCxLpUTELXFP
gYr3OgVCxLf5fhQYtM0RkE1yLgmosbXNqVX/k6cjkz1vG0Wazk8M2/m/VDPDKh9a
OtNFA1BiVZ96hWqqgntPb7lhV8ldWoIxdrIJHjsjsAiQWAuXJD9VS1vhpr0edsHy
diR1AN5NXP0EztJYsyzteLC53LKMwCGqYoGtppbPKEg7ravBLoSPJcVDsM6+Anpp
Kp5jZAiSAzkNCMP0Rl3rvyek0P1etxp54bf9r69s1dvOQ9S51gHotjKXe432JP19
pBVZIIjO/LhqOizgb6Pkq94xO72CGiJIYizjgR0F3tPmSpJkuScMMdLuLSw+nAmf
rOjPtQjq2we+HQp60k39w47viGuQQvXsDaOCm0WtX+gqinzKf4TcwcpkkuLYnW/z
kAmgjk2i2Uzu+R596G6j1HE7ielNyALZI79ubLFLY6gkLKm/B5xYlSGZkDoo214o
07dDUybITkxeOUrtJGysB/rCFyxE0MM9lLlMxAO1ujnrW+85bfNyuB1KTmueHzJH
o7y90Q8bstHiGkaktiArOkWDhYfC6yRQWHW7v+cKEBM1Njg/f7G0u8YRs97i9gAA
AAAAAAAAAAAAAAAAAAAAAAAAAAUMERUeJTE2A2gAMGUCMGVHdV0PTO+2u+WuBsjZ
kTlCZ2GVGemFv2ZsrjV2KdikOmkAWAWuG31m80/QDFYqIgIxAKfEWo2lEWa/VQT3
5701G2mackohVuS8fzlOJzEiP8/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-----
MIIKoTANBgtghkgBhvprUAgBHwOCCo4AMIIKiQOCCiEAK7u9rNJO4TTLy7wPSB8H
6ggu0le3IzKk/Lzs3n0vwn5p0OOUaQ6OxM+agtglkYgLF32ZVOgLYZqzhPhPODaT
gcCp01P2gw9vhrWqsnZn6tpE5cwaVrnkKmLWI/4aR17opelT9zfwH7uYVpB0K53h
9lDRu8/Lj/bhh414Q4g+3dxEc7Pw65m1vBRJg3088aWKWDQ/axoAtiMmfac9JpOt
dLEej5+8Yh3bNycE7zN/sjZShZ7sHBlnN2cK6Z8cc/86+SxsWImS6rEgQUs2V+WU
9PbhuSJn9in9NbL2KSm9y9MSTw6Z6NcGOPZ3cCr96l2hgEQVhEuqs31ft8sRBm7u
IOA/N0UuCsSek+hkMwH/WnBmQJL7s7p4wtyvX0JaL6t3MQstp6awihjVc4dFS+cj
8Sl8LqLyeuqQ2PbLTY8P5IF84PNv33aDGiCSLTMKiXquhcuLE5y/O04bDi0hAT2E
1r2bCdPtB3qgsIgSn46mBcJMqdjnqseJ2GhO2hyQ06J5AenvL4JsiAWaJExdm23W
fwRnKtTzxF1NrAvxJp25k5f57qBbiACzZvP97aZfAu534QwQnW5JlsiVHO53Wjpi
dGTBKkPKhG0I1vtHO4RqtD5m4Fp70xr7J+BrcmsqonnLGlJN9avUMdeAhcavm0e3
wOoa2GmrgSlfDV5d3Y2VVZQm0k1sGlhLd9xhRircAYgmQjbyaPKZ+dTiDcsRV+9t
QqrpXsx9gdQFrKS5S2zTy3p1KnwbyDCxYMGKXtfVVgrvX22D3uvNMYPpmN4XFix0
ot42Lp02L1mrPi8iIBPgSksljzVeg6wMDKTwxf8eAvL5zKJGan8xhCeUJjCHAzoH
U/HtLQwBq5/Yb1G78auxz5aQjbAlKSRreknCppyLX7Qr9N3rSSnxO8UDjKSM728w
31zj+fD7Hb2x0dOOY6DuWcwdH50D9SlUuiv89l4Qt1ksIhV1+6LCKpXg3WBKYZx3
7IJUrKFaKpt8SCIOZpPdF3stI8EzHbJg+KNDcx8xv3/pjQe8mH5fNzF1fwwwhXqJ
R7qIyHVKqIgHKqQDmba/WCJXhgGf2DxMxJCQBQn/1uhskM1lBZPw5KuXLy1Paty0
1XvWcpkOgVH27jXGSpYEhDlyS9S3jaCXhRpyqKHeu+XqqyJden6HwUgtpd61TmG+
++yvA2swmQR1J8o4qe/x9fAqmrwfP4K8HhL02W5e20pBEBxUTBr2Ycvf+zpb51dP
FWSN2bzMqYzCSX1g91hau1iZ2W2/JEaRfHc1WXhRAB7OD3cdUbWlJTEE4BsYi14K
JOD5aglhVmvdUm67YXDuUUnyJ3alExRmDoLFa2JLTDDKGiQWhhVVfSp2n8avyB70
```

```
mjHwz8gKM4v9daWzGLHyApTWYm0Jg2V56B9IXRS6qpJC14JCW7kRig11Cv3HLvUv
Pt4cdmCGgHsI9DlYUAZb8nziSrCY3aN645qYzIB0bnd57j3s6aHP/Q5yRIQkEWab
A8vUORsHMp70KP58kumQIcku9Sgr+trksp3HiAIOpCHlSRnDZAoRi6jw1T7PPGB8
y3BMaTZMNB1PwdVZhDQg+LaxGMAVG/GKxrYbhkQK28Muj+I8LBp4r9ZUwLm6KH/i
2mmYc8CjdNiBjYkyhM1AiNFAWzCx9+UHbbhILVwB6hT9tGQQJxmuI8CHdtZw6gYz
EcyWhiaYmUDKXQ+qxTnVblxKcNNDzsstUX/HdHpfsvibCNThKBM8Ci0sWmKcxvMP
OU/uUqZlcwOwQ28SdT7NyjpY7PWSjKYyukssZoMvyPhcsDEPVhNa+fo0O+mHEg6k
mXH3Fdtlu4DPb4qFb9zAupGB26HIDgVvRYRP9A/JMarJUnOYSupC9kUxyMPGjpeE
BcucoBb7u4yLmZpbi2QF/KfvPNApC9irlXv/vMDMV9yFQhAY8iv0zZc1LaATWDba
903xNO9sSSDaDCHzbLVXlSL5g8oVO1/oO9LLgObQq9jTEU0b6LXpYXTZWvW//SpI
8PjiDu2D0BS49sUk4lsWHPKfOv1+/ThPiQPsHZlgRXToq/ujcoYTHr2/ES59vVsG
xdrUwsBy/Y+uMfqohpje/vS3JfdfeAWhqq3U+52EK4UEJG1DHWPnsv9KsXLmYFMm
i9U2AgrG4L4DzxT9Pl526/9aVfrsDL+Pj0HZNvM2qJh1iXhbc9EbahRgHpxydkRM
lrvRUPuTSp86M+OHo0dqXniUENo1tOccjnk1FUiuCmNkDCHlK4S2AKeN9D2GMMQs
JpZeXXXoLQ09CZ1U4rQjx9zNqm9EDTMVRfTuEWSpEpQfUcNvB8lIbBINP1ZTDHfr
KmuuOtcwShEi1GoCe0oCVmiNDumwE6jw++gc0d5XzH9OHvJaChnBBCCf73ZybzZr
KDRddAUlRLsiGjSFsiZcQMIBpbTGlIyhwvye/NagR+OYHlsuNEyJJOFEGK3xVlsy
NJ8y+DJZwz3usZ0fWZRy4NUZzV6eJCTap6HVmdYMvs4lGd9lWL8i0RC/BQe91vUy
cVdqSnPkef/d01Xybv0O6TLMqsHzH2rbkC3SLMtQOAx7FxEM7y6+0SZ/lCujQoBV
14ggBuoFgDtfl2EBXRs8f/x/z+0t9p+TTXL5yM2953o9Q6aD8tLhXE6GazN1AodT
lpu8VsnY4LrBP/yW4+KuREHj64fKSSv82q6jT3rfbmtW1aSWMVpUe3anLN2gjn/1
po3/MAJsa68akIXmntn7AjWjURnoKmLxEy64AzFeo9xI1JVL69XaO5DNRMW+JtiT
Sm+lN8cWjqbdiMNSeKd37anyX4C74sEbxQM2K101PJMkGci554CGqES4Qgt8fis+
26OWWk09N++JSt+BeKYp5EpRI+drwbsqeqH88GXj6KyGtJET/hUC7nTkEMGVYfYK
D63YNA3ozjF8VMle/ZYQ8l3eX8YbWoocZmR5oWGDgeQ0Y5rYRqI4SbVfIhx6hwJI
HBMgjiexX/F73BRP9JZ32hTpyvg0b6p4zghDPrSOR1Ra5+oCp87mlmh6uVjSXXfl
bDBXs60UH7UwXTACrr9aeR6yMQLtUcIx2CnJqJoBNbG3C5fujc3jeZAWc7r0Wadc
6uA204ZKXoE1kNhE0zqdrmmWZ26m6aNdKJ0+dr/tTODh0OIWkTIACwv1BtVSboMW
aevrfAwn/9T1LlHC4O7HPrQjAFqbqCDJ8aFD7ga0vm/hw5e/LeUMqNp/CCX889m5
kJjwXawVsGpRpbrcGNuKtR+RIbkZSdAh77wzpnRDuPq2EYVOkaqwXxKA8Jq0Knl1
JNu5pYJtpngg7dc74MvzpcA0nHrZbbnR1fHiDhaK+C4a97MN03ETLOggbKwI/Qah
YfjBPcF1trLkaMWk0Wz1YR6jePQn/Fu+Vxd2EVkB+i6enEb9GYQS/lqs/1PzKWrz
AdSE6FqJr6eI57Hk4T+GGkj+UwA4zzv1KerQROQJti5yA2IABCHyu6g4zZjaZQiS
olrMkLL0dviU63jgfyz6sJ9GPLwMC+3GA4YJ7m4xU1Sy0eGU//57s2Yy1xWv4zXT
hhLYX754ThB0wg4ukwXzAajU0HOaeuLL5tqFE4kC2cugJbLMpA==
-----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
vA9IHwfqCC7SV7cjMqT8vOzefS/CfklUbLCwYE/8DDeGmIDT+8Eg17JDnQYarvQf
ra1cMcSXm7tXNRp94xuGoEo1CUyIOciLw1xToWS7Dy8A82W7yAgNT4J0FnfcioqC
TKekbVhFMFFYwR5dWjZ9dnMXcyOm0Qm0aUQ2jRgIBhOWAVRASaIIZIIyQNsEBASy
ZeSIjeK0aQo2BUmybeQSbGICbplGglLEjBOFCUSQkEO0EQvAkMmmYFvCcEgwJZEg
bhI3iUwACQOWbBKzcQEQhoCIUWCAQQwJCiQyagizLRkJAJsiASGJQQkBcqQmiRC2
LMlGACTGTWI0kAtIbhxIEpKIkNSQTRPABQQFghQBEclGRRM4CQuRbZsiAQiiYOEY
ZqHGMACCMOCGRAMWAQkZAKGGJBwjEpACjWOiBFOgZRS3DdkIiUJIQEkmcOKohGOI
YNMgThwRDJACMBSwSAGRQcgEaiGXYYoSLhADMhQESosSBpFGLZA0jBEAIAGAUBFE
```

aJxAUiKWcSIBMICCTQSYUCEzQlvCKRuBAFsCEAMkcRiwMaKCUAwkhgGlcAnHjQJA
QQQ3KlsAhMAQUVHCABJFSJE0ZeIGbiAGitEohREDUZICYJnGBNqyRZSwbRsABuNG
cAGTcAKBjYgGZAAVgCNBZiKjEVKIhdTGiQgAShOnYRQzIAAQJAm2DRgWUcLGhNtA
LZSwMZRGgVyGbMOSjZoCIhSFBJmETCIISoAYIFAIJhEBSYgIEAg4ZAlGAOREEQE5
RZPIRETGMcHGkKE2AtTEDBNGcZuYgYGkjNgQMdMGKsK0kNJAcWSEYZsmRguHRRio
MOEoBIGQhRk1MQQhMRyxaUQGQZkoACExKBGShRIpSBMBTdpGjloibhKFEZwkTAgh
ImEgTWE0cuGYDZg0LJySYYMACIM0TAo1gsEgTsBIghQ2CtI0ktqAJFomkgASCcSA
hQG5aRsHTANELdumJCKxEIAyKOMmICRGkGOSUOMoMtQYUUQ2DaKyECKEhdg4YFsI
UJoYCEy0JQomUZtAhgFFJJuEMUqmTdIWbaMiTtrAUUFIQFokMsREEskgIqA4MBun
DQuJgBkohNkWgtO0UOKQDeMCaFPGYaG4kVq2IVtITAIAkYQEAIugJMOCQNgCkMyW
jUK0hMsGBEykTCKoAKOETOKYgAtBItQSghuXBCIJiRGYbMOUDGTCUFISCSMCLiIH
gNgiTFESDJgkSBAGLWCWLMAkEZwoZoNGQpimDCASKAADhgGJIAImQhIAbAsiUqE4
EkqyIIIkCNKSBRgEQAM3Qck4KhypSIKQkKIiCpw4isoyUAjCZUE2bQojYRwzcUwS
TNJAEAGyjVMIRQiXbdQCTcwSBswYEIACStMoUIJCTgvGEBIQKiGjjNykcYDIBIOU
BAQGShMSkhGRjJoEUWOobBpDEgRBLFoYCQECkMmIYASECBkAIhqUiAi1gNiSDMG2
DVMECcEwDEvAIOEwKQxJBghEAJwAbYNCkBCBACHJbaQoYqLAREmwUJxITpsWCQsQ
gQw0cuKEJBiILcSGkNOWLMKyQRO4hdwgClgEDVq4DYEQUBOSEFvIKYLACFEkIJO4
KdMobtO4LVSABckESFKUaeMoEpSCRAkhMoAwCBJIMQwwYcpGMpIgEJuIMQAhAlO2
haKWUcoWjsICkYkkjZK0iQLHcRNASMswRsJEhGOUUUAoTBqmCdzASBM2UBwpQGAW
QNAiYBQzBBnBYFpICAEiksgwaFmyieLCbEsWbdhGEcK4YOKwSNKoQZuyYMwwKCGE
UEMgJYPAbBI2jePIKQq0IIy2QNGyYAOWCNgkkOOmgSKFhRoScFpGRpIYLNQIUVQC
hZugTRuIbUhIRCQJLog2UkKmJODGJcoogoKADYughQQ5MqNABRlGgqKyAeEgSAO3
hYEQcgS5SAu0hZE4hEKiTNlIZIPCjeMGTgMWDSEUkOQwjRGEZBwUSIMSSYFAZmGk
gSQyQhsxkoK4jQRHagwIhGKoKFsmchEHEFQwbNMmTpTELcNGMEuICAk2ZookbGCY
iJsYhVwmRBwmDcQYMQM3CqCwcdi0ETynna4hOgvu6H2su5THKoH4Iq4Bp7W8clYN
FVEZrknpbKJTPBWbTJRrsjxYDC8nZ3DFwgMmTeFHW9Q8OOUT0BSN0qZrrfl5Ju1n
2U3aPgJU9K2VBCWRrtnFTh7au+pD6XHE5RJHk/FqzD7PZeEVz5xHBBZ3UD6hQOni
a+o/N6NOtnH4e1XYAVlLmWzqrndOghmnD7FjaacmOcrh4iA4mex3NedqvUJEIsB7
EGJPpRND0qFti+yDsTqX7yj12ydMrtonfAEk4fCpGJL3ruy+Wd4aYkegzzg/HcPm
Eu/O9jjgR3PPhmxsswmIUIMPT/6cRBlSuGcfMMq5E+xsN5u0jjZRwJBC3Ke3Jlk6
gIxv8ReKIsX+im6ffoK3IZB8GLBIL9FXcJ/IwUY949L0ADZZvGwmfAXJ9X4/u06f
N1HPIM6n4rvNNrwXVh8l3w+L2mW9eks3jrVaG370eBiqiWDx7nL5CJzfx6BM493z
Ca5LRf9RR2sxQbq1qOemqF8IJ1ENthvSdBFZvrRWbu26Sodwz+c5SYysn+bJcVQy
C7YZLlNMCyzhEaw9nE/G4ukAc2NCSftEwQpKl2MfBfbwjyj6+TrHorbBi9jSNW+E
bzPQbKRiKmanfNzEHksptHzdG0mwRsVjlAk4xBvitnPC7YHdTH8AL3Nrn/VD+wqZ
SLZ8EqhlC/a/agkNVVT8n05T4hQ7BgNFhDBWlsGiXzgcsAIwrWMNYUxd4Yp32QDh
4MhCFz08O2ad2VFeVKFEV5TYkUS2YciMpL0urvR4wGbZFktEcy2/YbLZAyDmuN4Y
de28DeRaVvQSa1f65ZOq57f3zdJMOdZ8CcVh5iTwrmSsU38I78/BDpi8dl8E7YLw
CMG69v64+xK92ZH3uvpEfXBsaMhsOuVILtjjdBWjTKldR5jvR4o7yGPT9yl6dH0b
jdvxU1kal76hFtHBKovwr4z8THRSFRzp/WYeSzqxv89CYU1inY2CXo0TuKXB1SjW
KO9qO5RGNWQeVkyngxbroX9D9vfl+uB9Mia4sufltrVobL+ReTPS47XYFU74Uyzy
OtEOtbBk+Gb8Cjljtnzmusu+9bo4r8A6jAOknhImsex11EeaTOvejA92KmrAAsGX
YXtTUk6qAID08CthqSsJEIdK7rOYq0AvHSXIlDd4HsCsbNmj2+NaxB26wly5gTj7
yxLQu/7cm4fEYS1VC5vKm9qD99kVmWxBouth9U0ZEhDN9sdHPe8NexUEqzGvdYNO
9KTfU2HstAglB6h18HXHgPnC4tp/2kjxkV+PKx3WzsGi3AvI7LZRzfdlxOCfIMtR
2iaqqSG4kXoaAt7rVB07kMiAb0V178PIF4XYKFdIGR4MFPkcCmLBwbaKELIXK82D
nR4QzbmSNkh9owBKLy9GLVEs1OewA5DD9RnIp/7EjOBOUgNimRlaI8rd/UHqNjLK
CvBkfQ4OXbZ9d93NK46pDMnrm092/dzbmFeJW4uwuFBQyTFe1P/MsekNFQjuo83D
KltZFkEg7MzM24N5n2uK5bnwOZi5v+9j5Ha9gjdscfJv0orJYShtDdqIoaVh41yv
2JHMGBOsFlYGu/SQrwLd/x0LCjKZYz8Zduj1/un5BSWRK28k896qWl9Spc99rAqp
T4PQ78UCS3jfYqifkr166GFxpKrhvmHOjUZoMnfmwAiRq4mqZdiv/R3ztQ9psVQw
aiKdIMWZv+UFt4VmltYYP9NAlV1SuY9arPH+gPDeBqcYTv33Jqj3SRR+Qj5Fk3wU
vzQWAEGEswJYhLz9EIVL9izPS4/viIBkSgkKbPdVYuQFMnocyrkXgBSJk1yfCgAv

```
95881zhfmrdvFrIJHUApZ00RsMA0ZtMPlvH/Cs7ivb+r1T3qTBsy26wkPdY7f2TB
BlTTIk/3CNf0hgxOXBwNp+hIN64lfbSeuomnDNYUmXj+QoudIpCr1Aj0LYyZ4RES
2d44cw04oozjCZJqDZ/zmfMgUVh3LshfDtf5qk73dFgZvDhpBwChyj6YFkmuQgh7
C9d/8wyuLcSGeXn40At+Iw23wcvSOp4GhtIeW9uJVSt+9dIXEBI6MzHNCy4RGG9R
exFOyfgquLoWAHfTbzIea8ZtLoUYzLUQEFdlC6cpxpZJyuoYN/aO4PEQ5YUjSIsA
YoCPpstcYB+4jEOEIF4wAoX5OK1xwRjTrFug8u4QIE6GVlzM7662y8MzRJoIbfMZ
HJuNp10sg7vkhPDRd9MoxAlSrmQvKptzbfOQFRSRazN0ZPRCFxx5B32zhBeIq0zt
mAueqqlxc7Bmp/VhC1OXx1DCzGUgCvqLV4iiZ1mAjfT61kv+9j41pgKCepgJiLUF
kXH0GBxgG+L9dloRdrsbFaar5/0/ZeW+duaWbey9VJejmfzc/nh0Gz2geVT9AXBv
qUzV2odkdaea+voN83py4RXwv7Hco1W+PMc1ogSWgAqYO9hJiiwXaGlhSd3/FSeY
oWsrdYaEmWb8v9UUp0VWVWOGKgYMlWdOmSghw3j5yobOpeOkp8hmM60kzs4u1sfX
uHesJlmjiZ+ppaxKZig+S5AV4yvlZi95nck3J0JXII6Df9tKa6FQneVHmX4NPHcr
VfJOZmqtL1uscdyJbRI+P/csNZvClt9nTepybZqFq49lWankESybMN5agxh4Yb5l
aj8oWgbXVd0XvXsHAzsXqvd52N0ylCYarc77cE7rii+A5+OLMBdzYcoJ/6lPu0VD
osEm9hGvohXI2p2rReXjGBoe1GJGJOiuBt8VQ0wp+TFVDvWI0Ygg4UpfN/YjAdnf
nVzDLkS4mxjy0ViDGXxmVrMrbfPBmq0E68PIGs8JcPh3BdF2Z0xwM4VHjUWzH/xT
uPga4V93cL9/HaCgTu2S4nojApeV11Rvwm5rShMY0uCM3ix0jj8+EC+yfdC+g8yW
0LVNDPujxO5l9ivZTpfzU+wF7YIs3LF+xxJB1wJC40lWfy5TeSDj4kHchrIfx83q
J1zFtQmoBID8FYo/JbZheC9ozAbsGGds+F0sivrAJbZ+zvr30lTtzSymn2gbkUR+
JOuNYUcmQQP2+uwNdTKh57SXmHT5tnKMat+8NIMD4ni3jucGxenKI4cevMEHkh6A
oOVgTAHbLz+BTl4pW86qtLkY3VSmJxKd0ssOAt9Plhx9j+kyA9mWcSRttLiyOOyl
mmBCz/x20cp8utigkI+w1krlqv/HupmD1hs7qAtlywgZwELHbwZnWoW7fyunPqLW
e1wwPAQnV07PcKZoMcSvwRB3JskxFxOiIgUHZBICoUDtjTApHuTZqWJGLzNhuq0E
CNtsh8vBleKXtWtyXxKdLPuHK9Q15QkqyAUQtwFrzZNY3XnE+EGY0F//rucAZXhq
ptQrbRR9N6t2FoYWrFlnQcQ0uAjS5YqIO2/PsykuSwtbuCt5aHWVaUCc8eUefW1m
kRkiyRnHtEQQyU0oGok/i6pme8PAjJgkHKCjJQ7mBBjDci3TcPxMisVLgVcr9kqD
K/1vm1+Hq3LizLMTPLOR2lmwObIt14bqK3OKUrcAV2wvIStbca3VFhcrp/uSjJUm
1azVhopDOKPqIvFDt+cB0xgaE9fAZaiiyKETuKhk6Qidb18M7InDOtTQxzBHZ6yU
BXv1nXFx7fPoir2i6YIL4GvcptYvlPgHNpCZCZqDgmdynL8rWNAQk51WEfIkizBd
8fRmiHLHKf4DynoirBmpC88HcMpRX0kKvJ2ZNu6qgEuMpA+PpWGrXNLowgKuloQ3
4jDXv6Ek/BZ7bLLMsA2iob7GsW/AKf63mJMe3Rl73nYCPHJZoEISdNsdHu2W5MGc
vQOVTaYO+gyGoQneBK0YxRPzdBzcAsmpFjY8ejrYi55ZceWVHJojq8UxfZghbyH4
CuPWQy3xns009764j14Jlxr/BH1ipuYZFWKYhxdRM7Oa29VDdjFW+4sEUpwUgFjU
olcIos3oXvhGWpsslUa8dbFoBz4wXG8xBkLLPt6Bp7AGyOkAqABIj8bILr/pKejs
a21jnVkTv/xmnbI8djph4VN+wRcv8AQU+uoZebmbPx0hKcgqlaT7geX8lp3gvZQR
6cIvu55FADzYhrTiLiBvFSn/xLIuK1oA+/oX3dQHoM9qUERD2GAAGxY+fkrMZrTt
bxThjev0zqz3YDA65h1FYUIBVtmvI5p4rfwR+AdTNIkrR0N7stt+pkPgG+kXUTY7
BWvrOSv5HfQa4ygkBbYfyD8U/qZMLiM6twrgYhXjnFFYGwpyvtoOEaKOngP0qgc6
zDaYMb46wSBfS20Ea0lcduEce6JvctZpq39HmK4PBn+Lmd1BPHcMyxsQsGkKrvet
hlEWQpXZ22tI1xdPw1RM/4xAIgp3edKS4juMM8k6tuG2tmIlZizU2Ei4UHfQHpUw
iF/nUj6qrtLy8ViA+BetAMrdjsdMXM+XO3o8nPbIm+Ii9c4ziAcEgacwgaQCAQEE
MG8Ju+kdMxlk1Qfi6mVRD7WH7iw04Fgx1Kr0t1eWmVoOyqDigiFz2VgYdBjbebZg
GqAHBgUrgQQAIqFkA2IABCHyu6g4zZjaZQiSolrMkLL0dviU63jgfyz6sJ9GPLwM
C+3GA4YJ7m4xU1Sy0eGU//57s2Yy1xWv4zXThhLYX754ThB0wg4ukwXzAajU0HOa
euLL5tqFE4kC2cugJbLMpA==
-----END PRIVATE KEY-----
```

24 Integration report

This section provides a complete integration report for Cryptographic Security Platform.

- Base installation integration report
- CA Gateway integration report
- Certificate Authority integration report
- Certificate Enrollment Gateway integration report
- Certificate Manager integration report
- Timestamping Authority integration report
- Validation Authority integration report

Base installation integration report

Regardless of deployed solutions, all Cryptographic Security Platform installations share the following integration report.

- Infrastructures supported by Cryptographic Security Platform
- Browsers supported by Cryptographic Security Platform
- SIEM supported by Cryptographic Security Platform
- Cryptographic Security Platform internationalization
- Cryptographic Security Platform upgrade

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 Starting up CSP for the required installation steps.

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 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

Browser	Windows	Mac O
Mozilla Firefox	9 or higher	9 or higher

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

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.

> As explained in Log Server, Cryptographic Security Platform supports the RFC 5424 and RFC3164 implementations of this protocol.

Cryptographic Security Platform internationalization

Cryptographic Security Platform is released in English.

> As explained in Selecting the keyboard keymap, you must set the system locale `en_US.UTF-8` during installation.

Cryptographic Security Platform upgrade

Cryptographic Security Platform 1.3.0 is a greenfield release that does not support upgrading from previous versions.

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.

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
DigiCert CA	Service	Only supports issuing DV (Domain Validation) certificates
EJB Certificate Authority (EJBCA)	Community Edition	
Entrust Certificate Authority (ECA)	10.2	
	10.1.1	
	8.3	Does not support the events API is not supported
Entrust Certificate Services	Service	Supports TLS certificates
Entrust PKIaaS	Service	Requires CSR on enrollment
Microsoft Active Directory Certificate Authority	2019, 2016, 2012 R2	Requires CSR on enrollment
Sectigo Certificate Authority	Service	

Certificate Authority integration report

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 Certificate Authority
- Key types supported by Certificate Authority
- Entrust products compatible with Certificate Authority
- Database management systems supported by Certificate Authority

Hardware secure modules supported by Certificate Authority

See the following table for versions supported by Certificate Authority and other solutions.

Hardware	Client driver	Firmware	Certificate Authority	Timestamping Authority	Validation Authority
Entrust nShield Connect XC	13.9.0 (FIPS 140-2 Level 3 mode supported)	12.60.15 & 12.60.2	✓	✓	✓
Entrust nShield 5c	13.9.0	13.2.4	✓	✓	✓
Epicom	EP990 v1.08-1	—	✗	✓	✓
Thales Luna HSM 7	10.8.0	7.7.1-20	✓	✓	✓
Thales TCT	10.8.0	7.7.1-20	✗	✓	✓

General considerations:

- 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.
- On high-availability installations with a cluster of several HSMs:
  - You cannot use HSMs from different providers simultaneously, meaning that nShield and Thales HSMs cannot coexist within the same deployment.
  - Entrust Validation Authority may experience the Thales TCT limitations described in the *Thales TCT Universal Client Plugin Additional Information* technical note dated May 28, 2025.
  - Solutions using the HSMs must be redeployed after any loss of connection with the HSMs, such as after an HSM reboot.

Key types supported by Certificate Authority

See the following table for the cryptosystem and hash algorithm combinations supported by Certificate Authority to sign certificates.

- The available algorithms on this list depend on the configured cryptographic module.
- 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

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
RSA-2048+PKCS15-SHA256	RSA2048	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-2048+PSS-SHA256	RSA2048	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-3072+PKCS15-SHA256	RSA3072	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-3072+PSS-SHA256	RSA3072	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-4096+PKCS15-SHA512	RSA4096	sha512WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-4096+PSS-SHA512	RSA4096	sha512WithRSAPSS	RSA2048	sha256WithRSAPSS
ECDSAP256+SHA256	ECDSAP256	ecdsa-with-SHA256	RSA2048	sha256WithRSAEncryption
ECDSAP384+SHA384	ECDSAP384	ecdsa-with-SHA384	RSA2048	sha256WithRSAEncryption
ECDSAP521+SHA512	ECDSAP521	ecdsa-with-SHA512	RSA2048	sha256WithRSAEncryption
ML-DSA-44	ML-DSA-44	ML-DSA-44	RSA2048	sha256WithRSAEncryption
ML-DSA-65	ML-DSA-65	ML-DSA-65	RSA2048	sha256WithRSAEncryption
ML-DSA-87	ML-DSA-87	ML-DSA-87	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	RSA2048	sha256WithRSAEncryption
Falcon-512	Falcon-512	Falcon-512	RSA2048	sha256WithRSAEncryption
Falcon-1024	Falcon-1024	Falcon-1024	RSA2048	sha256WithRSAEncryption

Entrust products compatible with Certificate Authority

Certificate Authority for Cryptographic Security Platform 1.3 is compatible with the following Entrust products.

- Certificate Manager included in Cryptographic Security Platform 1.3
- Certificate Enrollment Gateway included in Cryptographic Security Platform 1.3

Database management systems supported by Certificate Authority

Certificate Authority supports the following Database Management Systems (DBMS).

DBMS	version
PostgreSQL	15+

Certificate Enrollment Gateway integration report

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.

- Certificate Enrollment Gateway localization
- Databases supported by Certificate Enrollment Gateway
- Enrollment protocols supported by Certificate Enrollment Gateway
- Entrust products compatible with Certificate Enrollment Gateway

Certificate Enrollment Gateway integrates with Entrust CA Gateway to provide certificate enrollment capabilities.

Certificate Enrollment Gateway localization

The current Certificate Enrollment Gateway release only supports English localization.

Databases supported by Certificate Enrollment Gateway

Certificate Enrollment Gateway supports the following Database Management Systems (DBMS).

DBMS	version
PostgreSQL	15+
Microsoft SQL Server	2019+
	2022+

For information about deploying an external database for Certificate Enrollment Gateway, see Deploying an external database for Certificate Enrollment Gateway.

Enrollment protocols supported by Certificate Enrollment Gateway

See below for details on the Certificate Enrollment Gateway support for enrollment protocols.

- Certificate Enrollment Gateway support for ACME v2
- Certificate Enrollment Gateway support for CMPv2
- Certificate Enrollment Gateway support for EST
- Certificate Enrollment Gateway support for Intune
- Certificate Enrollment Gateway support for MDM

- Certificate Enrollment Gateway support for MS-WSTEP
- Certificate Enrollment Gateway support for SCEP

Certificate Enrollment Gateway support for ACME v2

See below for details on the Certificate Enrollment Gateway support for ACME (Automatic Certificate Management Environment) v2.

- ACME v2 version supported by Certificate Enrollment Gateway
- ACME v2 clients tested with Certificate Enrollment Gateway
- Load balancer support for ACME v2 enrollment with Certificate Enrollment Gateway

ACME v2 version supported by Certificate Enrollment Gateway

Certificate Enrollment Gateway supports the ACME v2 version described in:

https://datatracker.ietf.org/doc/html/rfc8555

ACME v2 clients tested with Certificate Enrollment Gateway

The 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 Certificate Enrollment Gateway

ACME v2 enrollment with Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✅
3	✅
4	✅
7	❌

Certificate Enrollment Gateway support for CMPv2

See below for details on the Certificate Enrollment Gateway support for CMP (Certificate Management Protocol) v2.

- CMPv2 version supported by Certificate Enrollment Gateway
- CSP CA Gateway version for CMPv2 enrollment with Certificate Enrollment Gateway
- Load balancer support for CMPv2 enrollment with Certificate Enrollment Gateway

CMPv2 version supported by Certificate Enrollment Gateway

Certificate Enrollment Gateway supports PKIX CMPv2 (RFC 4210 and RFC 6712) for:

- LTE (4G/5G)
- VPN

CSP CA Gateway version for CMPv2 enrollment with Certificate Enrollment Gateway

The Certificate Enrollment Gateway support of CMPv2 is tested with CA Gateway for Cryptographic Security Platform 1.2.0.

Load balancer support for CMPv2 enrollment with Certificate Enrollment Gateway

CMPv2 enrollment with Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✔
3	✔
4	✔
7	✔

Certificate Enrollment Gateway support for EST

See below for details on the Certificate Enrollment Gateway support for EST (Enrollment over Secure Transport).

- EST version supported by Certificate Enrollment Gateway
- EST clients tested with Certificate Enrollment Gateway
- Load balancer support for EST enrollment with Certificate Enrollment Gateway

EST version supported by Certificate Enrollment Gateway

Certificate Enrollment Gateway supports the EST standard described in:

https://datatracker.ietf.org/doc/html/rfc7030

EST clients tested with Certificate Enrollment Gateway

The Certificate Enrollment Gateway support for EST has been tested with the following clients.

Client	URL	Comments
LibEST 3.2.0	https://github.com/deviance/libest/tree/feature/opensslv3-compat	Requires compiling Uriparser-0.9.8 (https://github.com/uriparser/uriparser) before compiling and building LibEST.

Client	URL	Comments
GlobalSign EST client 1.0.6	https://github.com/globalsign/est	—

Load balancer support for EST enrollment with Certificate Enrollment Gateway

EST enrollment with Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✔
3	✔
4	✔
7	✔

Certificate Enrollment Gateway support for Intune

See below for details on the Certificate Enrollment Gateway support for Microsoft Intune.

- Intune versions supported by Certificate Enrollment Gateway
- Load balancer support for Intune enrollment with Certificate Enrollment Gateway

Intune versions supported by Certificate Enrollment Gateway

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 Certificate Enrollment Gateway

Intune enrollment with Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✔
3	✔
4	✔

Load balancing layer	Supported
7	✅

Certificate Enrollment Gateway support for MDM

See below for details on the Certificate Enrollment Gateway support for MDM (Mobile Device Management).

- MDMWS version supported by Certificate Enrollment Gateway
- MDM clients tested with Certificate Enrollment Gateway
- Load balancer support for MDM enrollment with Certificate Enrollment Gateway

MDMWS version supported by Certificate Enrollment Gateway

Certificate Enrollment Gateway supports the following version of the MDM Web Service (MDMWS) protocol.

- v8
- v9
- v11

MDM clients tested with Certificate Enrollment Gateway

The Certificate Enrollment Gateway support for MDM enrollment has been tested with the following clients.

- VMware Workspace One (Formally AirWatch)
- JAMF Pro
- MobileIron

Other MDM vendors leveraging Entrust MDMWS APIs should work out of the box.

Load balancer support for MDM enrollment with Certificate Enrollment Gateway

MDM enrollment with Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✅
3	✅
4	✅
7	✅

Certificate Enrollment Gateway support for MS-WSTEP

See below for details on the Certificate Enrollment Gateway support for MS-WSTEP.

- MS-WSTEP version supported by Certificate Enrollment Gateway
- MS-WSTEP requests supported by Certificate Enrollment Gateway

- MS-WSTEP domain enrollments supported by Certificate Enrollment Gateway
- Windows products supported for MS-WSTEP enrollment with Certificate Enrollment Gateway
- Load balancer support for MS-WSTEP enrollment with Certificate Enrollment Gateway

MS-WSTEP version supported by Certificate Enrollment Gateway

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

MS-WSTEP requests supported by Certificate Enrollment Gateway

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 Certificate Enrollment Gateway

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 Certificate Enrollment Gateway

The 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 product	Version
Windows endpoints	10+, 2012 R2+

Load balancer support for MS-WSTEP enrollment with Certificate Enrollment Gateway

MS-WSTEP enrollment with Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✅
3	✅
4	✅
7	❌

Certificate Enrollment Gateway support for SCEP

See below for details on the Certificate Enrollment Gateway support for SCEP (Simple Certificate Enrollment Protocol).

- SCEP versions supported by Certificate Enrollment Gateway
- Load balancer support for SCEP enrollment with Certificate Enrollment Gateway

SCEP versions supported by Certificate Enrollment Gateway

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 Certificate Enrollment Gateway

SCEP enrollment with Certificate Enrollment Gateway supports high availability with the following load-balancing layers.

Load balancing layer	Supported
2	✅
3	✅

Load balancing layer	Supported
4	✔
7	✔

Entrust products compatible with Certificate Enrollment Gateway

Certificate Enrollment Gateway is compatible with the following Entrust products.

- Entrust Certificate Authority
- Entrust PKI as a Service
- Microsoft Certificate Services
- Digicert CA

Entrust Certificate Authority

Through Entrust CA Gateway, Certificate Enrollment Gateway is compatible with Entrust Certificate Authority 10.2. This integration supports the following protocols:

- ACMEv2
- CMPv2 (with CA Gateway v3.0.3 or later)
- EST
- Intune-SCEP
- MDMWS
- SCEP
- WSTEP

Entrust PKI as a Service

Through Entrust CA Gateway, Certificate Enrollment Gateway integrates with Entrust PKI as a Service (PKIaaS) to support the following protocols.

- ACMEv2
- EST
- Intune-SCEP
- MDMWS
- SCEP
- WSTEP

Microsoft Certificate Services

Through Entrust CA Gateway, Certificate Enrollment Gateway integrates with Windows 2016 and 2019 Microsoft Certificate Services to support the following protocols.

- ACMEv2
- EST
- Intune-SCEP
- SCEP
- WSTEP

Digicert CA

Through Entrust CA Gateway, Certificate Enrollment Gateway integrates with Digicert CAs to support the following protocols.

- ACMEv2
- EST
- Intune-SCEP
- SCEP
- WSTEP

Certificate Manager integration report

Entrust Certificate Manager allows you to view and manage certificates across your enterprise, regardless of the issuer.

> Certificate Manager uses Entrust 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 Certificate Manager
- Databases supported by Certificate Manager
- Plugins supported by Certificate Manager
- Standards supported by Certificate Manager
- Database management systems supported by Certificate Manager

Entrust products compatible with Certificate Manager

Certificate Manager for Cryptographic Security Platform 1.2.0 is compatible with CA Gateway 3.x (the version included in Cryptographic Security Platform 1.2.0).

Databases supported by Certificate Manager

The external Certificate Manager database must be hosted on PostgreSQL 15 or higher.

Plugins supported by Certificate Manager

Certificate Manager supports the following plugins to extend the native integrations.

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 Certificate Manager

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.

Database management systems supported by Certificate Manager

Certificate Manager supports the following Database Management Systems (DBMS).

DBMS	version
PostgreSQL	15+

Timestamping Authority integration report

Timestamping Authority is an on-premises timestamping solution based on RFC 3161 that guarantees that data, including documents or code, exists at a given time through the generation of digitally signed timestamps. Specifically:

- Proof of the time when a digital signature was applied or validated.
- Prevents code rejection, ensuring that the signature is valid when signing.
- Enables digital signature verification after the certificate used for the signature is revoked or expired.

When deployed on Cryptographic Security Platform, this Entrust solution adds the following to the Base installation integration report.

- Hardware secure modules supported by Timestamping Authority
- Signature key generation algorithms supported by Timestamping Authority

Hardware secure modules supported by Timestamping Authority

See the following table for versions supported by Timestamping Authority and other solutions.

Hardware	Client driver	Firmware	Certificate Authority	Timestamping Authority	Validation Authority
Entrust nShield Connect XC	13.9.0 (FIPS 140-2 Level 3 mode supported)	12.60.15 & 12.60.2	✅	✅	✅
Entrust nShield 5c	13.9.0	13.2.4	✅	✅	✅
Epicom	EP990 v1.08-1	—	❌	✅	✅

Hardware	Client driver	Firmware	Certificate Authority	Timestamping Authority	Validation Authority
Thales Luna HSM 7	10.8.0	7.7.1-20	✅	✅	✅
Thales TCT	10.8.0	7.7.1-20	❌	✅	✅

General considerations:

- 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.
- On high-availability installations with a cluster of several HSMs:
  - You cannot use HSMs from different providers simultaneously, meaning that nShield and Thales HSMs cannot coexist within the same deployment.
  - Entrust Validation Authority may experience the Thales TCT limitations described in the *Thales TCT Universal Client Plugin Additional Information* technical note dated May 28, 2025.
  - Solutions using the HSMs must be redeployed after any loss of connection with the HSMs, such as after an HSM reboot.

Signature key generation algorithms supported by Timestamping Authority

Validation Authority supports the following algorithms for generating the timestamping response signing key.

<key_type>	Description	Post-quantum
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	❌
ML-DSA-44	Module-Lattice-Based Digital Signature Algorithm 44-bit	✅
ML-DSA-65	Module-Lattice-Based Digital Signature Algorithm 65-bit	✅
ML-DSA-87	Module-Lattice-Based Digital Signature Algorithm 87-bit	✅

Validation Authority integration report

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 Validation Authority
- Hardware secure modules supported by Validation Authority
- Signature key generation algorithms supported by Validation Authority
- Database management systems supported by Validation Authority

Certificate Authorities supported by Validation Authority

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

Hardware secure modules supported by Validation Authority

See the following table for versions supported by Validation Authority and other solutions.

Hardware	Client driver	Firmware	Certificate Authority	Timestamping Authority	Validation Authority
Entrust nShield Connect XC	13.9.0 (FIPS 140-2 Level 3 mode supported)	12.60.15 & 12.60.2	✅	✅	✅
Entrust nShield 5c	13.9.0	13.2.4	✅	✅	✅
Epicom	EP990 v1.08-1	—	❌	✅	✅
Thales Luna HSM 7	10.8.0	7.7.1-20	✅	✅	✅
Thales TCT	10.8.0	7.7.1-20	❌	✅	✅

General considerations:

- 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.
- On high-availability installations with a cluster of several HSMs:
  - You cannot use HSMs from different providers simultaneously, meaning that nShield and Thales HSMs cannot coexist within the same deployment.
  - Entrust Validation Authority may experience the Thales TCT limitations described in the *Thales TCT Universal Client Plugin Additional Information* technical note dated May 28, 2025.
  - Solutions using the HSMs must be redeployed after any loss of connection with the HSMs, such as after an HSM reboot.

Signature key generation algorithms supported by Validation Authority

Validation Authority supports the following algorithms for generating the OCSP response signing key.

<key_type>	Description	Post-quantum
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	✗
ML-DSA-44	Module-Lattice-Based Digital Signature Algorithm 44-bit	✓
ML-DSA-65	Module-Lattice-Based Digital Signature Algorithm 65-bit	✓
ML-DSA-87	Module-Lattice-Based Digital Signature Algorithm 87-bit	✓

Database management systems supported by Validation Authority

Cryptographic Security Platform solutions support the following database management systems (DBMS).

Validation Authority supports the following Database Management Systems (DBMS).

DBMS	Version
Oracle	21.3.0
PostgreSQL	15+
Microsoft SQL Server	2019 CU15
	2022 CU13