



ENTRUST

PKI as a Service

Customer Guide

June 9, 2022



Entrust and the Hexagon Logo are trademarks, registered trademarks and/or services marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.

© 2022 Entrust. All rights reserved.

Table of Contents

1	Introduction to PKIaaS	4
1.1	PKIaaS capabilities	4
1.2	PKIaaS operation	8
1.3	PKIaaS governance model	10
2	PKIaaS use cases and setup instructions	12
2.1	Using ECS Enterprise UI to purchase and manage PKIaaS CAs and certificates	12
2.2	Automate certificate issuance and management using a Certificate Enrollment Gateway (CEG)	13
2.3	Use and manage PKIaaS CAs and certificates through the CA Gateway API	14
3	Ordering and setting up PKIaaS	16
3.1	Placing an order	16
3.2	Activating your Entrust Certificate Service Enterprise account	18
3.3	Activating your Entrust TrustedCare account	24
4	Creating and managing CAs in ECS Enterprise	26
4.1	Checking PKIaaS Inventory	26
4.2	Managing CAs	26
5	Configuring and using the CA Gateway API	37
5.1	Creating and downloading CA Gateway API credentials	37
5.2	Accessing PKIaaS via CA Gateway API	38
6	Configuring and using Entrust Certificate Enrollment Gateway (CEG)	40
6.1	Adding and managing CEG	40
6.2	Automating certificate issuance with Entrust Certificate Enrollment Gateway	42
7	Creating and managing certificates in ECS Enterprise	48
7.1	Creating certificates	48
7.2	Downloading certificates	50
7.3	Revoking certificates	50
7.4	Reporting, alerts, and notifications about certificate activity and expiry	51
8	Managing certificates with Entrust Certificate Hub (Optional)	52
8.1	Certificate Hub	52
8.2	Connecting your CA	52
8.3	Dashboard	52
8.4	Reporting on certificate activity	52
8.5	Ad-hoc exploration	53
8.6	Expiry notifications	53
9	Obtaining support	54
9.1	Authorized contacts	54
9.2	Entrust Certificate Services Support	54
9.3	TrustedCare portal	54

Appendix: Certificate profile reference	55
Signature algorithm constraints for all profiles	56
CA & VA (OCSP) certificate profiles	57
S/MIME Secure Email certificate profiles	59
Smart Card certificate profiles.....	60
Code signing certificate profiles	61
CEG-Intune certificate profiles	61
CEG-Private SSL(ACME) certificate profiles	63
CEG-WSTEP (Active Directory) certificate profiles.....	64
CEG-SCEP certificate profiles	65
CEG-MDM Web Service certificate profiles	66
CEG-CMP certificate profiles	67
CEG-EST certificate profiles	68
V2G certificate profiles	69

1 Introduction to PKIaaS

Entrust PKI as a Service (PKIaaS) provides certificate issuance, management, and status services at the scale, speed, security, and simplicity required of modern business. PKIaaS provides preconfigured certificate profiles to secure use cases through turnkey approaches, solving customer problems while making them straightforward and simple to consume.

- **Scale** – Modern use cases require more, and shorter lifetime, certificates. Entrust PKIaaS is a high-performing, cloud-native system that grows as required with nearly limitless capacity, with Entrust experts at the operations helm. As a next-generation service built on today's technology, you will always have the capacity you need—when you need it.
- **Speed** – The speed of business is changing. Your PKI needs to operate fast and where you do business. Entrust PKIaaS deploys and expands within minutes, giving you a quick solution to secure your business use cases. You can even create new Issuing CAs in minutes to handle the next generation of use cases.
- **Secure** – Maintaining your security posture matters. Entrust PKIaaS gives you the assurance you expect from Entrust, providing you with dedicated root and issuing CAs and protecting your keys in our Tier III data centers, secured by Entrust nShield HSMs running at FIPS 140-2 Level 3.
- **Simple** – As deployments diversify and use cases grow in complexity, they pose a management challenge. With our PKIaaS, Entrust manages the PKI so you don't have to. Use cases are simple to deploy and adaptable so they won't block business. PKIaaS fully interoperates with other Entrust PKI products such as Entrust Certificate Services cloud service (ECS), Certificate Enrollment Gateway (CEG), and Certificate Hub.

PKI as a Service leverages 25+ years of Entrust PKI innovation and technology from a hybrid cloud model. It allows customers to scale on-demand and drive capacity while maintaining simplicity by reducing the number of services, applications, and software they need to run on their premises.

1.1 PKIaaS capabilities

This section describes the PKIaaS CA capabilities. It covers three broad areas: Certification authority instantiation, certificate issuance, and certificate status checking.

1.1.1 Certification Authority instantiation

PKIaaS capabilities for CA instantiation are:

- Dedicated online root CA
- You have your dedicated Root CA with a Distinguished Name (DN) of your choice. You select this DN as part of your CA order submission. Entrust asks that the organization component of the name reflect your company.



1.1.1.1 Issuing CAs

Each customer may have one or more subordinate Issuing CAs. Your first subordinate Issuing CA can be created after you create your Root CA. You may add more Issuing CAs later.

1.1.1.2 Secure CA key management

All CA private keys are stored in Entrust nShield Connect XC high HSMs FIPS140-2 level 3.

1.1.1.3 CA key and signature algorithms

The following CA key and signature algorithm pairs are supported.

CA key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

NOTE: NIST recommends that RSA2048 not be used after Dec 31, 2030. See: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf>

1.1.1.4 Validity period

CA validity periods are 20 years for Root CAs and 10 years for subordinate Issuing CAs.

NOTE: Currently, PKIaaS does not allow CA validity period change. This feature will be enabled in future releases.

1.1.1.5 CA creation time

CAs are provisioned in ~60 seconds in an automated process triggered by your request submission using the ECS Enterprise UI (described in [Creating and managing CAs in ECS Enterprise](#)).

1.1.2 Certificate issuance

PKIaaS capabilities for certificate issuance include the following.

1.1.2.1 Subscriber certificate profiles

Entrust establishes the certificate policies and tunes them to specific use cases. PKIaaS captures these use cases in pre-defined certificate profiles, documented in the CPS, and listed in section [Appendix: Certificate profile reference](#).

You must purchase an enrollment service (Certificate Enrollment Gateway) to get access to the corresponding profiles. For example, purchasing an Intune Enrollment Service bundle will give you access to Intune profiles.

Subscriber certificate profiles	Certificate Enrollment Gateway (CEG) integration
	N/A
CA & VA (OCSP) certificate profiles	
S/MIME Secure Email certificate profiles	N/A
	N/A
Smart Card certificate profiles	
Code signing certificate profiles	N/A
CEG-Intune certificate profiles	Supported
	Supported
CEG-Private SSL(ACME) certificate profiles	
CEG-WSTEP (Active Directory) certificate profiles	Supported
CEG-SCEP certificate profiles	Supported

1.1.2.2 Subscriber key algorithms

PKIaaS supports RSA and EC subscriber certificate key algorithms. PKIaaS is validated to sign certificates that use the following algorithms for their public key:

- ECDSA P-256
- ECDSA P-384
- ECDSA P-521
- RSA 2048
- RSA 3072
- RSA 4096

1.1.2.3 Validity period

The certificate validity period cannot go beyond expiry of the issuing CA. The validity period value defaults to 3 years if it is not specified in the request.

1.1.2.4 Enrollment by CSR

All certificate issuance requests are completed through CSR format. The calling application is responsible for generation of the certificate's private key.

1.1.2.5 Subject Alt Names

Subject Alt Names (SANs) are supplied in the request separate from the CSR. API requests to PKIaaS support the "subjectAltNames" field of the request.

1.1.2.6 Extensions

Certificate extensions are supplied in the request separate from the CSR. Use the API field `optionalCertificateRequestDetails.extensions` to supply extensions.

1.1.2.7 Proof of possession (POP)

The proof of possession check validates automatically that the caller has use of the private key. The POP check is always performed during certificate request validation.

1.1.2.8 Certificate issuance rate

The certificate issuance rate is limited to 10 certificates per second per customer.

1.1.3 Certificate management

The following certificate management functions are available.

1.1.3.1 Certificate actions

PKIaaS certificates support the following actions.

- Hold, also known as Suspend
- Revoke (supported by ECS Enterprise UI).
- Unhold

The following revocation reasons are supported.

- affiliationChanged
- cessationOfOperation
- certificateHold
- superseded
- keyCompromise
- unspecified

1.1.3.2 Search by serial number

PKIaaS supports search by serial number using the API.

1.1.3.3 Events API

PKIaaS supports the Certificate Events API described in the [CA Gateway documentation](#).

1.1.4 Certificate status checking

The following certificate status checking functions are available. The Certificate Revocation List (CRL) is always enabled, and you can enable or disable OCSP in the Enterprise UI.

1.1.4.1 Certificate Revocation List (CRL)

PKIaaS publishes Certificate Revocation Lists (CRLs). They are valid for 7 days.

The CRL is updated:

- Automatically, every 24 hours
- When including the "publish now" option on revocation requests to the API—this option results in the issuance of a new CRL within 15 minutes.
- When revoking an end-entity certificate using the ECS Enterprise UI or the Entrust Certificate Enrollment Gateway (CEG)—this type of revocation also results in the issuance of a new CRL within 15 minutes.

The issued CRLs have the following settings:

- CRL Extensions crlNumber, invalidityDate, expiredCertsOnCRL
- CRL signed with the CA key
- Full CRL issuing
- CRLs up to 10 MB
- CRLs may be configured by both roots and issuing CAs

1.1.4.2 OCSP

The online Certificate Status Protocol (OCSP) supports:

- Nonce extension
- Archive Cutoff extension
- Multiple OCSP certificates per request
- Signed/Unsigned requests
- Delegated keys
- OCSP may be configured by both Roots and Issuing CAs

1.2 PKIaaS operation

This section contains a summary of PKIaaS operational procedures. See the PKIaaS Certification Practice Statement (CPS) for details.

1.2.1 Physical locations

In the US region, Entrust has implemented physical data centers near Dallas, TX and Denver, CO, with failover between the two centers.

In the EU region, Entrust has implemented physical data centers near Munich, Germany and Frankfurt, Germany, with failover between the two centers.

Cloud-based components use multiple availability zones for high availability, and a second region for disaster recovery.

1.2.2 Access control and trusted roles

The computing facilities hosting the CA Cryptographic Module and Activation Data are in the Entrust Tier III, SSAE-18 datacenters. Only personnel in Trusted Roles have access to these facilities.

The room containing the CA key material is designated a two (2) person zone, and controls prevent a person from being in the room alone. Alarm systems notify security personnel of any violation of the rules for access to a CA.

The CA Private Keys are backed up, stored, and recovered only by personnel in Trusted Roles using dual control in a physically secured environment.

Personnel in Trusted Roles must undergo background investigations, be trained for their specific role. They do not have the ability to change the product code.

1.2.3 CA Key management

PKIaaS generates CA keys in response to a customer request to provision new CAs. An API-based process generates CA key pairs within hardware cryptographic modules in a physically secured environment.

1.2.4 Audit logging

Significant security events in the CAs are automatically time-stamped and recorded as internal audit logs. Audit logs are archived periodically. You can see the basic audit logs in the Enterprise UI using the Reports function.

The Entrust Security Information and Event Management (SIEM) system constantly monitors the audit logs. The operations and security teams review the alerts generated by possible policy violations and other significant events.

1.2.5 Disaster recovery

To mitigate the event of a disaster, PKIaaS utilizes:

- Two data centers with highly available HSMs
- Secure on-site and off-site storage of backup HSMs containing copies of all CA private keys
- Database replication between primary and secondary regions, maintained in real time.

- Daily database backups within both the primary and secondary regions and weekly backup of critical data to a secure off-site storage facility

1.3 PKIaaS governance model

Defining the governance model for an enterprise-level PKI is a long and challenging process involving teams across the organization. To save you time and expense, and to ensure that you have a proper PKI, Entrust provides a pre-defined set of policies and practices governing these PKIs. These policies and practices are fully documented in the PKIaaS Certification Practices Statement (CPS) at:

<https://www.entrust.com/-/media/documentation/licensingandagreements/entrust-pkiaas-cps-lq.pdf>

See the following sections for a summary.

NOTE: See [RFC3647](#) for a general description of the policy and practices framework.

1.3.1 Entrust responsibilities

Certification Authorities

Entrust organizes your PKIaaS CA hierarchy into a root and one or more issuing CAs. Thus, your PKI environment is comprised of the following CAs.

- The root CA serves as your PKI trust anchor. This CA is a dedicated root CA for your company alone to use. Root CAs are not shared. You define the common name of your root, though we do ask that it have a naming relationship to your company so that we can support you more easily. Your root CAs will issue certificates to your Issuing CAs and OCSP services.
- You may have one or more issuing CAs. PKIaaS will support any number of use cases (and associated certificate profiles) on one issuer, or you can split the responsibility to multiple issuing CAs. You will define Registration Authorities (RAs) that can issue certificates for all use cases supported by the issuing CA, so if you wish to have some division of responsibility, you may want to set up more than one issuing CA. These Issuing CAs are subordinate to your root. The issuing CAs issue certificates to or for Subscribers.

Policy Authority

Entrust is the Policy Authority and is responsible for overseeing and setting policy and practices as applicable to the operation of the Certification Authorities.

Operational Authority (OA)

Entrust is also the Operational Authority (OA). Entrust manages all root and issuing CA systems hosted and operated on your behalf, as part of PKIaaS. These systems issue and manage certificates, Certificate Revocation Lists (CRLs), and OCSP responses. As the OA, Entrust is responsible for all the operations of the CAs per the CPS.

1.3.2 Customer responsibilities

Registration Authorities (RA)

In PKIaaS, you and your company are the Registration Authority (RA). The RA is the person or entity that decides whether to issue a certificate in response to a Subscriber request. RAs verify the identity of Applicants and submit certificate issuance requests on their behalf. They are responsible for the Applicant registration, identification, and authentication processes.

You will typically use software applications, such as the Entrust Certificate Enrollment Gateway, that interface with the PKIaaS API to perform your RA tasks.

Subscribers

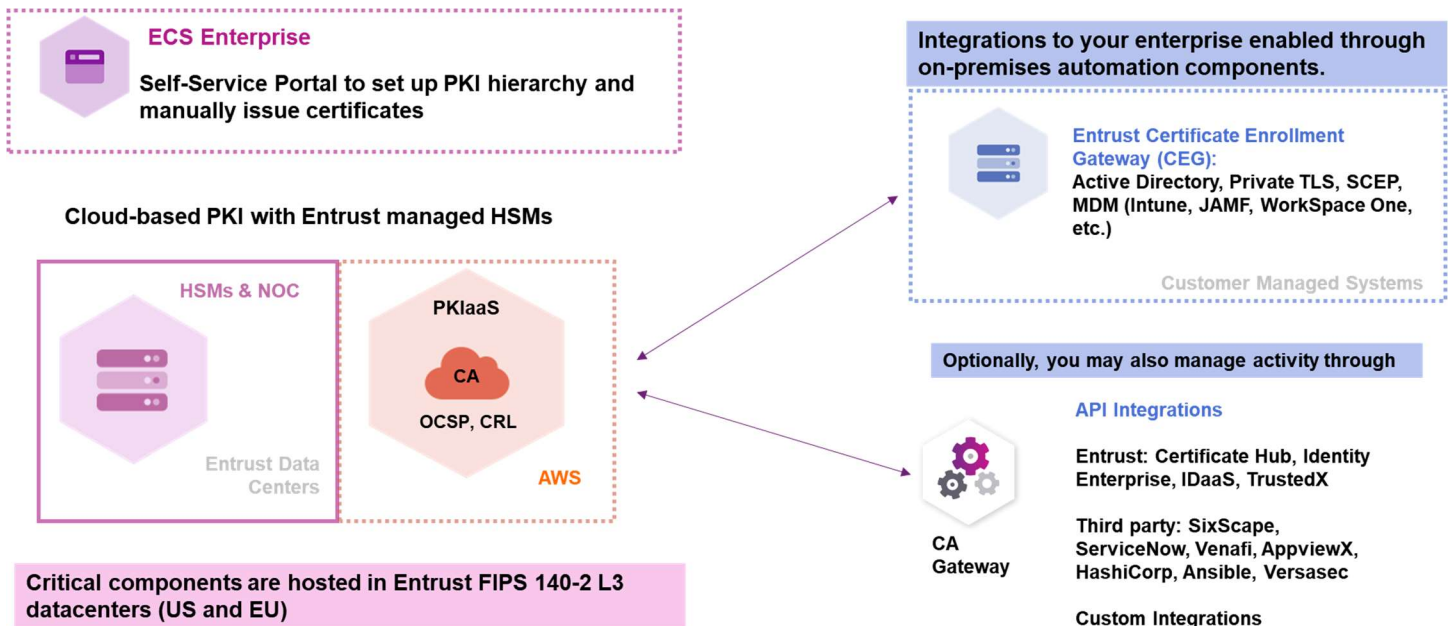
Subscribers are the end-users and entities that request and use certificates. Typical examples of Subscribers are employees/contractors and their devices, enterprise servers and infrastructure, and IoT devices. You, as the RA, are responsible for determining who may be a Subscriber and determining which people, entities, and devices may receive certificates.

Relying parties

A Relying Party is an entity that uses a certificate, to verify an identity, for example. PKIaaS is tuned to support enterprise-level privately trusted certificates. It is your responsibility to assure that Relying Parties perform the necessary certificate validity and status checks. PKIaaS supports both CRL and OCSP checks.

2 PKIaaS use cases and setup instructions

At the highest level, PKIaaS has the services shown in this conceptual model.



There are three general use cases for PKIaaS:

- 1 Use the Entrust Certificate Services (ECS) Enterprise UI to purchase and manage your private PKIaaS CAs and certificate inventory and manually create end-entity certificates.
From Enterprise, you can also view and manage the end-entity certificates issued using any of the three approaches listed here.
- 2 Automate certificate issuance and management using Entrust Certificate Enrollment Gateway (CEG) to automate PKI use cases such as Active Directory (WSTEP), Private TLS (ACMEV2), and Intune Mobile Device Management.
- 3 Use PKIaaS CA Gateway API to manage CAs and certificates directly, or integrate with third-party or other Entrust applications for various use cases such as Entrust Certificate Hub and Private S/MIME Secure Email solution.

2.1 Using ECS Enterprise UI to purchase and manage PKIaaS CAs and certificates

PKIaaS CAs and certificates can be managed in the ECS Enterprise cloud application. As part of your PKIaaS purchase, you will automatically be granted access to Enterprise. You will receive an email containing instructions for registering and logging in.

To use ECS Enterprise to manually create and manage PKIaaS CAs and certificates

- 1 Purchase CA licenses and PKIaaS certificate licenses. See [Ordering and setting up PKIaaS](#).
- 2 Activate your ECS Enterprise account. See [Activating your Entrust Certificate Service Enterprise account](#).
- 3 Create Root CA and Issuing CA. See [Creating and managing CAs in ECS Enterprise](#).
- 4 Create certificates. See [Creating certificates](#).
- 5 Manage your PKIaaS CAs and certificates. See:
 - [Creating and managing CAs in ECS Enterprise](#)
 - [Creating and managing certificates in ECS Enterprise](#)

2.2 Automate certificate issuance and management using a Certificate Enrollment Gateway (CEG)

These implementations require the purchase and installation of a Certificate Enrollment Gateway (CEG). Entrust offers a variety of CEG protocols to cover all common cases.

These are the currently available Certificate Enrollment Gateway protocols you can add to your Issuing CA. The available protocols are determined by the services you select when creating the issuing CA.

- Enrollment Gateway for ACMEv2
- Enrollment Gateway for Intune
- Enrollment Gateway for WSTEP
- Enrollment Gateway for SCEP
- Enrollment Gateway for MDM Web Service (MDMWS)

To set up a Certificate Enrollment Gateway

- 1 Purchase CA licenses, Enrollment Service Bundles, and PKIaaS certificate licenses. See [Ordering and setting up PKIaaS](#).
- 2 Activate your ECS Enterprise account. See [Activating your Entrust Certificate Service Enterprise account](#).
- 3 Create Root CA and Issuing CA. See [Creating and managing CAs in ECS Enterprise](#).
- 4 Add CEG Service to Issuing CA. This is done in the ECS Enterprise UI. See [Adding and managing CEG](#).
- 5 Download and install the Entrust Deployment Manager (EDM) and the CEG. See [Installing and deploying CEG](#).
- 6 Automate certificate issuance with CEG. See [Automating certificate issuance with Entrust Certificate Enrollment Gateway](#).

Here are some examples:

Intune

1. Install Entrust Deployment Manager (a Kubernetes cluster) on your on-prem environment
2. Deploy CEG software on Entrust Deployment Manager
3. Configure Intune protocol with PKIaaS on CEG software.
4. Configure the Intune portal (create Intune credential and load it into the CEG).
5. Deploy the Intune application to the employee devices.

MDM Web Service (MDMWS)

1. Install Entrust Deployment Manager (a Kubernetes cluster) on your on-prem environment
2. Deploy CEG software on Entrust Deployment Manager
3. Configure MDM Web Service protocol with PKIaaS on CEG software.
4. Configure the MDM vendor portal (create MDM credential and load it into the CEG).
5. Deploy the MDM application to the employee devices.

Private TLS/SSL(ACMEv2)

1. Install Entrust Deployment Manager (a Kubernetes cluster) on your on-prem environment
2. Deploy CEG software on Entrust Deployment Manager
3. Configure ACMEv2 protocol with PKIaaS on CEG software.
4. Install the ACME Client you chose.

Active Directory / WSTEP

1. Install Entrust Deployment Manager (a Kubernetes cluster) on your on-prem environment
5. Deploy CEG software on Entrust Deployment Manager
6. Configure WSTEP protocol with PKIaaS on CEG software.
7. Configure your Active Directory.
8. Create an enrollment service for the CEG.
9. Add certificate templates.
10. Configure the Group Policy to control what users and devices are eligible for certificates.

7 Manage your PKIaaS CAs and certificates. See:

- [Creating and managing CAs in ECS Enterprise](#)
- [Creating and managing certificates in ECS Enterprise \(optional\)](#)

2.3 Use and manage PKIaaS CAs and certificates through the CA Gateway API

You can use PKIaaS through the CA Gateway API to manage CAs and certificates directly or through integration with an external application, either Entrust or non-Entrust.

To set up to use PKIaaS through the CA Gateway API

- 1 Purchase CA licenses and PKIaaS certificate licenses. See [Ordering and setting up PKIaaS](#).
- 2 Activate your ECS Enterprise account. See [Activating your Entrust Certificate Service Enterprise account](#).
- 3 Create Root CA and Issuing CA. See [Creating and managing CAs in ECS Enterprise](#).
- 4 Create and download the CA GW API credentials. See [Creating and downloading CA Gateway API credentials](#).
- 5 Integrate with supported applications. Here are some supported Entrust and non-Entrust applications.

Entrust Applications

- Certificate Hub
- Identity Enterprise
- IDaaS
- TrustedX

Certificate Lifecycle Management Software

- Venafi
- AppViewX
- KeyFactor
- ServiceNow

SixScape

- Uses SMIME service

Key Vaults

- HashiCorp
- Microsoft Azure

Other non-Entrust applications

- Ansible
- Versasec

Custom Integrations

- Customer-specific

- 6 View and manage your CAs using ECS Enterprise. Issue and manage your certificates, either through the integrated application, if applicable, or use the API directly via Swagger or any API client:
 - See [Accessing PKIaaS via CA Gateway API](#) [Creating and managing CAs in ECS Enterprise](#)

3 Ordering and setting up PKIaaS

Follow the steps below to order and set up your PKIaaS account.

3.1 Placing an order

Your Entrust Sales Representative usually helps you place the order based on your business needs. Alternatively, if you already have an Entrust Certificate Service Enterprise Account with eStore access, you can also place the order yourself.

Orders for PKIaaS generally consist of three items:

- One or more PKIaaS CA bundles
- One or more Enrollment service bundles
- Certificate licenses (minimum 100)
- ECS Enterprise

3.1.1 PKIaaS CA bundles

A PKIaaS CA bundle includes:

- A root CA license
- An issuing CA license
- An OCSP service license (that you can optionally enable for the issuing CA).
- An external Root CA license (which allows you to sign a PKIaaS issuing CA as explained in [Adding an issuing CA under an external root CA](#)).

You should purchase CA bundles based on how many issuing CAs you need.

PKIaaS only charges for the issuing CAs. Root CA, External Root CA, and OCSP licenses are free for each issuing CA purchased.

You can validate and track your inventory using the ECS Enterprise UI (see [Checking PKIaaS Inventory](#) for details)

Product	Account Inventory		
	Total	Used	Remaining
PKIaaS Certificate	100000	0	100000
PKIaaS External Root CA	99	0	99
PKIaaS Issuing CA	99	15	84
PKIaaS OCSP Service	99	14	85
PKIaaS Online Root CA	99	6	93



3.1.2 Enrollment service bundles

Each enrollment automation use case, such as WSTEP, Intune, MDMWS, Smart Card, Code Signing, S/MIME, SCEP, and ACME (Private TLS/SSL), is provided as a service bundle that you can order. Each service bundle gives you a pre-configured certificate profile set to enable per issuing CA. See [Appendix: Certificate profile reference](#) for details.

As explained in [Subscriber certificate profiles](#), some use cases require Entrust Certificate Enrollment Gateway (CEG).

3.1.2.1 Enrollment service bundles for Certificate Enrollment Gateway use cases

When purchasing Certificate Enrollment Gateway for your use case, you get:

- Access to trustedcare.entrust.com for downloading the Entrust Certificate Enrollment Gateway software.
- An enrollment service license per issuing CA to activate a use case on Entrust Certificate Enrollment Gateway (named "Enrollment Gateway for xxx"). See [Adding a Certificate Enrollment Gateway to an Issuing CA](#).
- A corresponding pre-configured certificate profile enabled per issuing CA (named "PKIaaS xxx Enrollment Service").

For example, a PKIaaS Intune Enrollment Service Bundle includes:

- PKIaaS Trusted Care Access (see [Activating your Entrust TrustedCare account](#))
- Intune Enrollment Gateway
- PKIaaS Intune Enrollment Service

Inventory view in ECS Enterprise:

Account Inventory			
Product	Total	Used	Remaining
Intune Enrollment Gateway			
PKIaaS Intune Enrollment Service			

3.1.2.2 Enrollment service bundles for non-CEG use cases

For the Private S/MIME, Code Signing, and Smart Card use cases, you get:

- A corresponding pre-configured certificate profile set to enable per issuing CA

For Example, for a PKIaaS S/MIME Enrollment Service Bundle, you get **Private S/MIME Enrollment Service**.

Inventory view in ECS Enterprise:

Product	Account Inventory		
	Total	Used	Remaining
Private S/MIME Enrollment Service	100	8	92

3.1.3 Certificate licenses

Each "normal" and "held" certificate requires one certificate license.

- "normal" means certificates issued but not expired, suspended, or revoked.
- "held" we mean a suspended certificate.

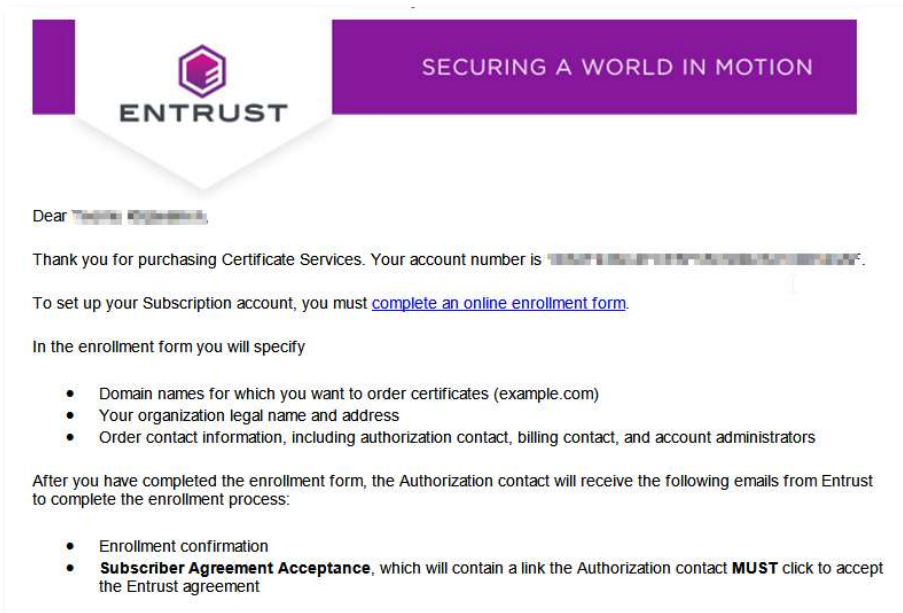
A revoked or expired certificate returns the license to the certificate license inventory. You should purchase certificate licenses based on the certificates you want to issue.

3.2 Activating your Entrust Certificate Service Enterprise account

Follow the steps below to activate your Entrust Certificate Service Enterprise account.

3.2.1 Receiving the Entrust Certificate Services new enrollment email

If you don't have an ECS enterprise account yet, you will get an enrollment email to register an account after our order management system processes the order.

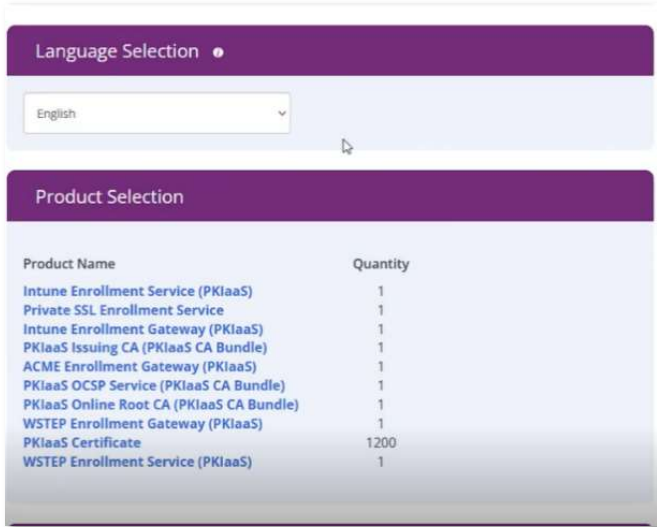


3.2.2 Completing the online enrollment form

When receiving the Entrust Certificate Services new enrollment email, complete the online enrollment form as explained in the following sections.

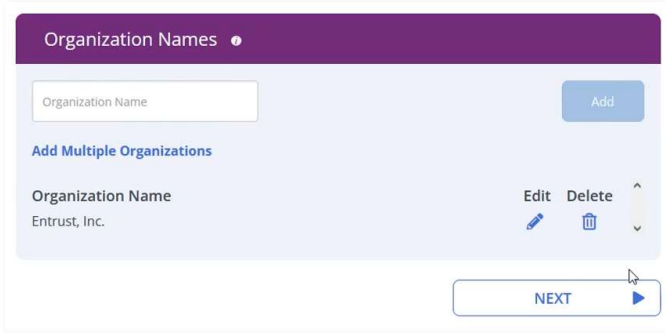
To complete the online enrollment form

- 1 Click the **complete the online enrollment form** link on the enrollment email.
- 2 Review the order.



Product Name	Quantity
Intune Enrollment Service (PKIaaS)	1
Private SSL Enrollment Service	1
Intune Enrollment Gateway (PKIaaS)	1
PKIaaS Issuing CA (PKIaaS CA Bundle)	1
ACME Enrollment Gateway (PKIaaS)	1
PKIaaS OCSP Service (PKIaaS CA Bundle)	1
PKIaaS Online Root CA (PKIaaS CA Bundle)	1
WSTEP Enrollment Gateway (PKIaaS)	1
PKIaaS Certificate	1200
WSTEP Enrollment Service (PKIaaS)	1



- 3 Enter your organization names and click **NEXT**.



Organization Name

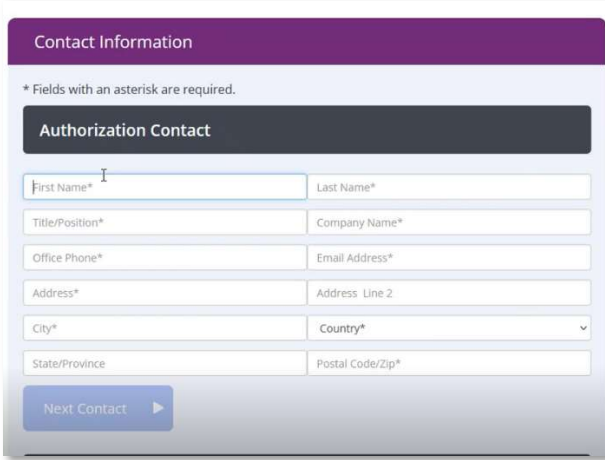
Add

Add Multiple Organizations

Organization Name	Edit	Delete
Entrust, Inc.		

NEXT

4 Enter the authorization contact information.



Contact Information

* Fields with an asterisk are required.

Authorization Contact

First Name* Last Name*

Title/Position* Company Name*

Office Phone* Email Address*

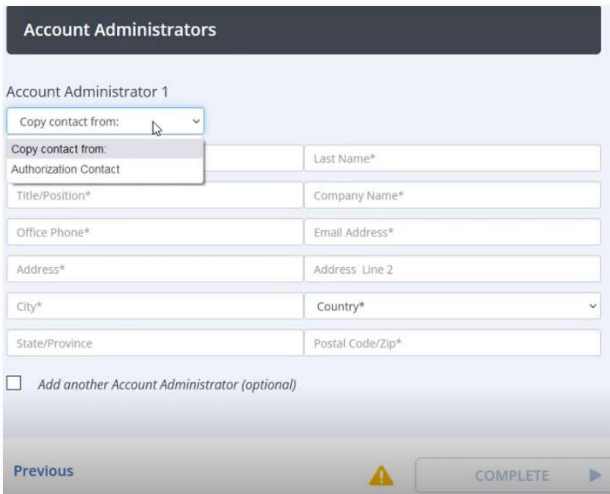
Address* Address Line 2

City* Country*

State/Province Postal Code/Zip*

Next Contact ▶

And the information for one or more account administrators.



Account Administrators

Account Administrator 1

Copy contact from: ▼

Copy contact from:
Authorization Contact

Last Name*

Title/Position* Company Name*

Office Phone* Email Address*

Address* Address Line 2

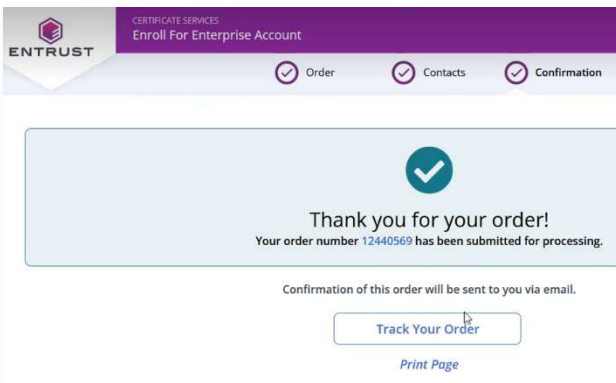
City* Country*

State/Province Postal Code/Zip*

Add another Account Administrator (optional)

Previous ⚠ COMPLETE ▶

5 Click **COMPLETE** to complete the registration.



ENTRUST CERTIFICATE SERVICES
Enroll For Enterprise Account

Order Contacts Confirmation

✔

Thank you for your order!
Your order number 12440569 has been submitted for processing.

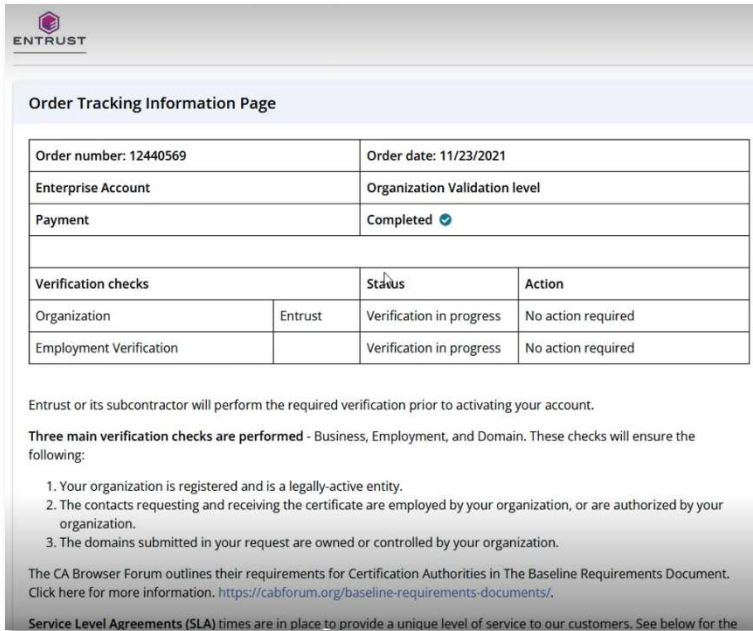
Confirmation of this order will be sent to you via email.

Track Your Order


Print Page

3.2.3 Tracking the activation status

Entrust will conduct organization and employment verifications before activating the account. This process usually takes 1-2 business days. To track the verification status in the **Order Tracking Information Page**, click the **Track Your Order** link provided when completing the registration form.



The screenshot shows the 'Order Tracking Information Page' with the following details:

Order number: 12440569	Order date: 11/23/2021
Enterprise Account	Organization Validation level
Payment	Completed 

Verification checks		Status	Action
Organization	Entrust	Verification in progress	No action required
Employment Verification		Verification in progress	No action required

Entrust or its subcontractor will perform the required verification prior to activating your account.

Three main verification checks are performed - Business, Employment, and Domain. These checks will ensure the following:

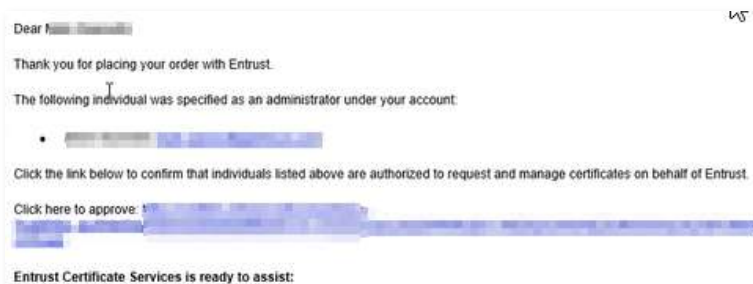
1. Your organization is registered and is a legally-active entity.
2. The contacts requesting and receiving the certificate are employed by your organization, or are authorized by your organization.
3. The domains submitted in your request are owned or controlled by your organization.

The CA Browser Forum outlines their requirements for Certification Authorities in The Baseline Requirements Document. Click here for more information. <https://cabforum.org/baseline-requirements-documents/>.

Service Level Agreements (SLA) times are in place to provide a unique level of service to our customers. See below for the

3.2.4 Accepting the Entrust Certificate Services subscription agreement

As part of the verification process, the Authorization Contact of your organization will get a verification email to review the account administrator's info, and a link to accept the Entrust Certificate Services subscription agreement.



The screenshot shows an email with the following content:

Dear [Redacted],

Thank you for placing your order with Entrust.

The following individual was specified as an administrator under your account:

- [Redacted]

Click the link below to confirm that individuals listed above are authorized to request and manage certificates on behalf of Entrust.

Click here to approve: [Redacted]

Entrust Certificate Services is ready to assist:

To accept the Entrust Certificate Services subscription agreement

- 1 Click the link provided in the verification email.
- 2 Review the subscription agreement.
- 3 Click **I Agree** to accept the subscription agreement and complete the account verification.

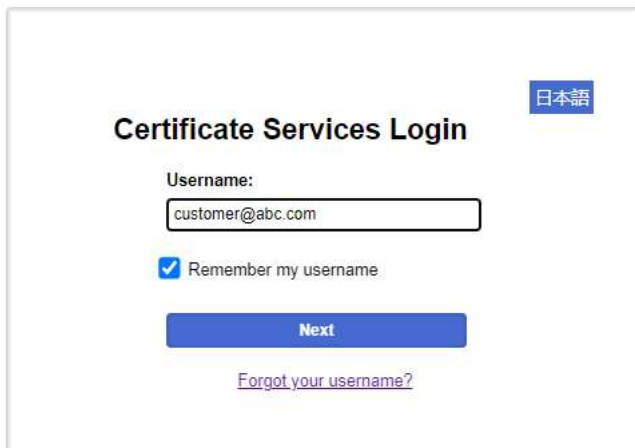
3.2.5 Registering the Entrust Certificate Services administrator accounts

After your account is verified, all new account administrators will receive an email containing instructions for activating their access to Entrust Certificate Services Enterprise.



To activate an Entrust Certificate Services administrator account

- 1 In your browser, open ECS Enterprise at cloud.entrust.net/EntrustCloud
- 2 Log in with the username and temporary password provided in the registration email.



Certificate Services Login 日本語

Username:

Remember my username

Next

[Forgot your username?](#)



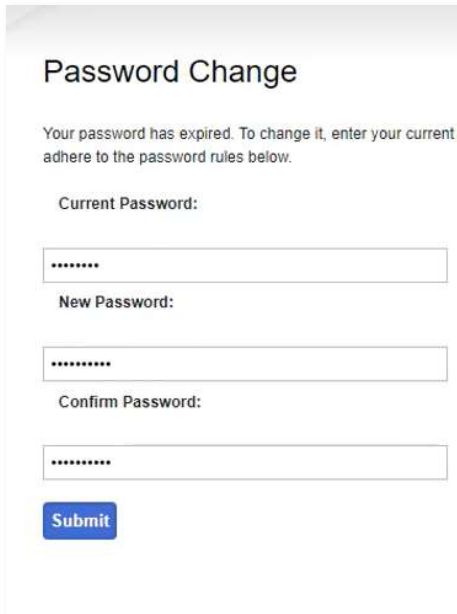
Certificate Services Login 日本語 [ES]Spanish

Password:

Log In

[Forgot your password?](#)

- 3 Replace the temporary password with a password of your choosing.



Password Change

Your password has expired. To change it, enter your current password and a new password. Please adhere to the password rules below.

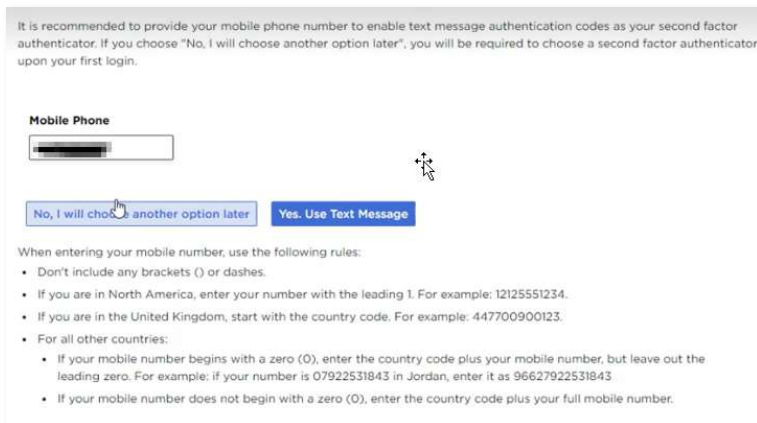
Current Password:

New Password:

Confirm Password:

Submit

- 4 Enter a mobile phone number for setting the two-factor authentication.



It is recommended to provide your mobile phone number to enable text message authentication codes as your second factor authenticator. If you choose "No, I will choose another option later", you will be required to choose a second factor authenticator upon your first login.

Mobile Phone

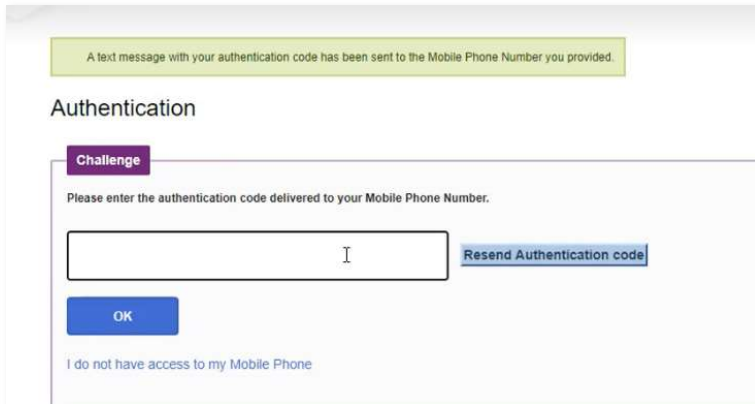
No, I will choose another option later **Yes, Use Text Message**

When entering your mobile number, use the following rules:

- Don't include any brackets () or dashes.
- If you are in North America, enter your number with the leading 1. For example: 12125551234.
- If you are in the United Kingdom, start with the country code. For example: 447700900123.
- For all other countries:
 - If your mobile number begins with a zero (0), enter the country code plus your mobile number, but leave out the leading zero. For example: if your number is 07922531843 in Jordan, enter it as 96627922531843
 - If your mobile number does not begin with a zero (0), enter the country code plus your full mobile number.

- 5 Click **Yes. Use Text Message**.

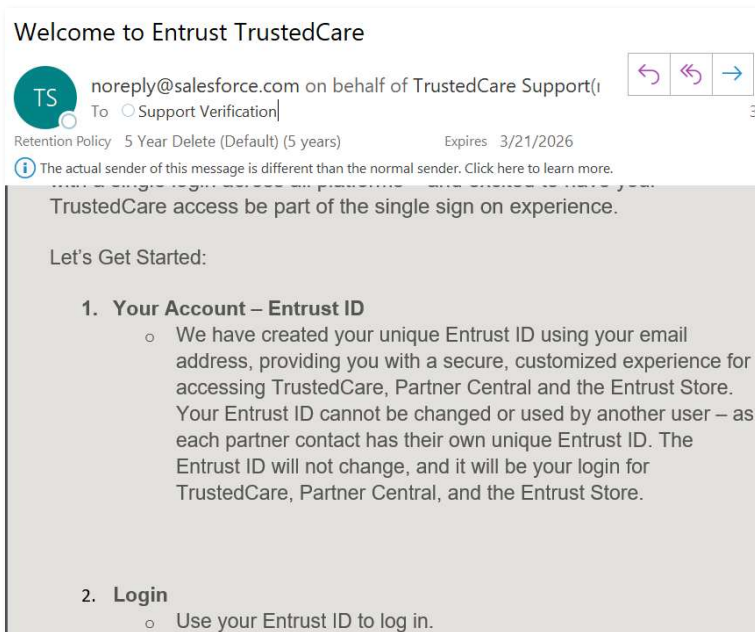
6 Enter the authentication code sent via SMS to the mobile phone.



You will need the username, password, and a second-factor authentication code to log in to ECS Enterprise every time.

3.3 Activating your Entrust TrustedCare account

If you are a new customer and you currently do not have access to Entrust TrustedCare, you will receive an email with instructions to set up your TrustedCare login at trustedcare.entrust.com.



If you have also purchased Certificate Enrollment Gateway, you should also receive an email from Software Distribution SoftwareDistribution@entrust.com to notify you that you can access the Entrust CEG software on TrustedCare.



SD Software Distribution
To: Email@Gsa
Received: Friday, 5 Nov 2010 (Default) (5 years) Reply: 10/14/2010 Read: 10/15/2010

Dear **[REDACTED]**,

Thank you for licensing Entrust software and continuing with the 'Layered Security' approach to enable success within your organization. We appreciate your business.

You have licensed the following Entrust software:

CERTIFICATE AUTHORITY ENROLLMENT SYSTEMS AND CONTROL CAPABILITY WITH ENCRYPTED CERTIFICATE ENVIRONMENT

You can download Entrust software using the following link:
<https://trustedcare.entrust.com>

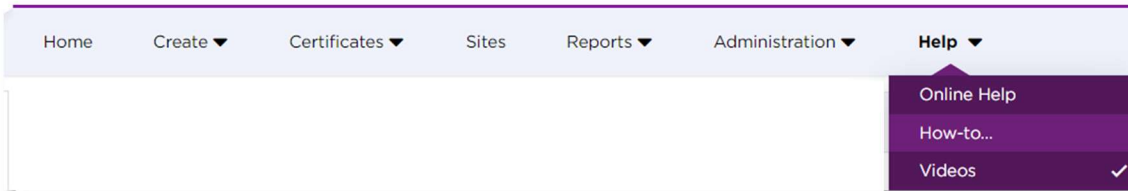
For any support issues please contact Entrust Support via telephone:
Platinum Customers: 1-877-754-7878 in North America or +1-613-270-3700 elsewhere
Silver & Gold Customers: 1-877-754-7878 in North America or +1-613-270-3715 elsewhere
Email: support@entrust.com

Now you are ready to create your PKI hierarchy using ECS Enterprise, including automating your PKI use case using Certificate Enrollment Gateway, if desired.

4 Creating and managing CAs in ECS Enterprise

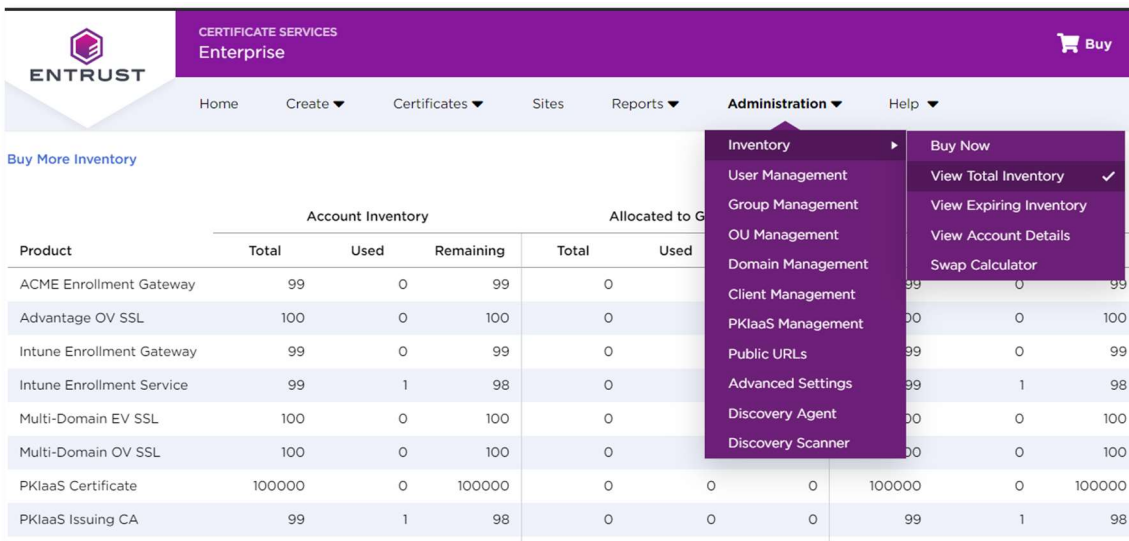
This guide focuses on the high-level PKIaaS user experience using Entrust Certificate Services (ECS) Enterprise. You can find tutorials describing other helpful administration features such as managing service inventory, managing users, reporting, and alerts by reviewing the [Entrust Certificate Service Online Help](#) and watching the training [Videos](#).

You can access these resources under the **Help** drop-down menu on ECS Enterprise.



4.1 Checking PKIaaS Inventory

After you are logged in to ECS Enterprise, select **Administration > Inventory > View Total Inventory**.

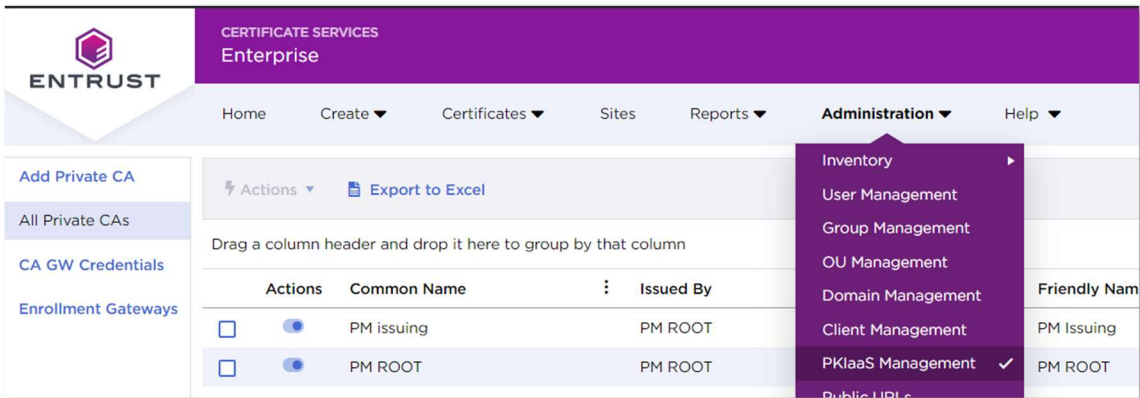


Check that you have all the required licenses as discussed in section [Ordering and setting up PKIaaS](#).

4.2 Managing CAs

Select **Administration > PKIaaS Management** to start creating your CA hierarchy.

WARNING: Before creating a CA, please ensure that you have enough inventory.



The screenshot shows the 'Administration' dropdown menu in the Entrust Enterprise interface. The menu items are: Inventory, User Management, Group Management, OU Management, Domain Management, Client Management, PKIaaS Management (which is checked), and Public URLs. In the background, a table of private CAs is visible:

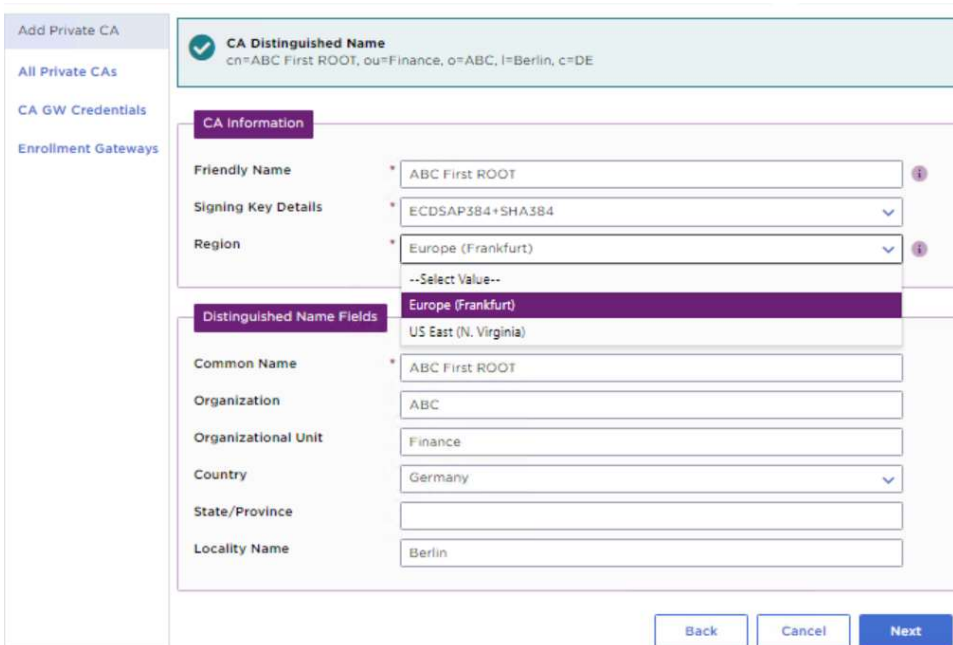
Actions	Common Name	Issued By	Friendly Name
<input type="checkbox"/> <input checked="" type="radio"/>	PM issuing	PM ROOT	PM Issuing
<input type="checkbox"/> <input checked="" type="radio"/>	PM ROOT	PM ROOT	PM ROOT

4.2.1 Viewing private CAs

The private CAs view is the default view of PKIaaS Management. You can see a complete list of all private CAs you have created, if any. Whenever you create, update, or remove a CA, you will be taken to this CA grid view to check the updated CA status.

4.2.2 Setting up your PKIaaS deployment

This section describes how to set up your PKIaaS employment by creating your root and issuing CAs in the ECS Enterprise UI.



The screenshot shows the 'Add Private CA' form. At the top, it displays the 'CA Distinguished Name' as `cn=ABC First ROOT, ou=Finance, o=ABC, l=Berlin, c=DE`. The form is divided into two main sections: 'CA Information' and 'Distinguished Name Fields'.

CA Information:

- Friendly Name: ABC First ROOT
- Signing Key Details: ECDSA384+SHA384
- Region: Europe (Frankfurt)

Distinguished Name Fields:

- Common Name: ABC First ROOT
- Organization: ABC
- Organizational Unit: Finance
- Country: Germany
- State/Province: (empty)
- Locality Name: Berlin

At the bottom of the form, there are three buttons: 'Back', 'Cancel', and 'Next'.

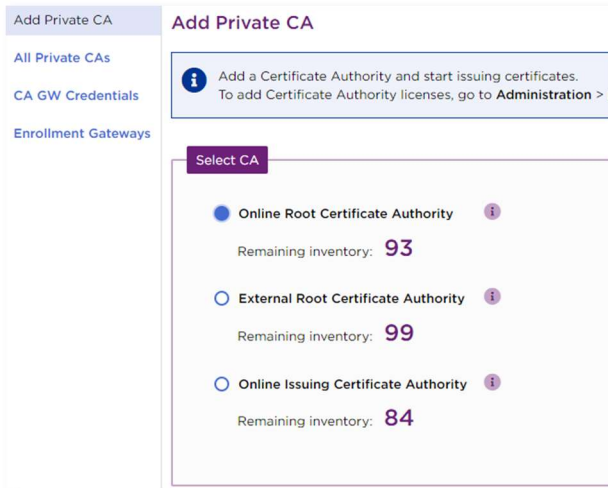
4.2.3 Adding the PKIaaS root CA

This procedure describes how to add the root CA of your PKIaaS CA hierarchy.

NOTE: Alternatively, you can add your own CA as explained in [Adding an external root CA](#).

To add the root CA

- 1 In the side pane, click **Add Private CA**.
- 2 In **Select CA**, select **Online Root Certificate Authority**.



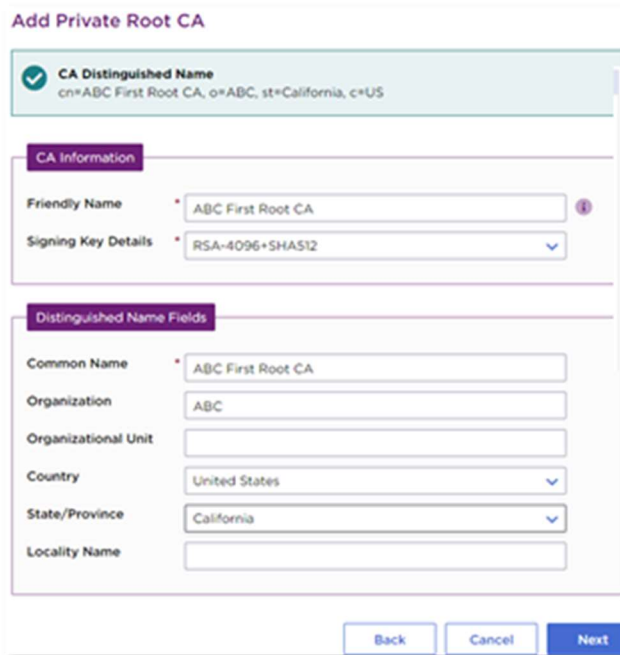
Add Private CA

Add a Certificate Authority and start issuing certificates.
To add Certificate Authority licenses, go to **Administration > Licenses**.

Select CA

- Online Root Certificate Authority** i
Remaining inventory: **93**
- External Root Certificate Authority** i
Remaining inventory: **99**
- Online Issuing Certificate Authority** i
Remaining inventory: **84**

- 3 Click **Next**. The CA information screen appears.



Add Private Root CA

CA Distinguished Name
cn=ABC First Root CA, o=ABC, st=California, c=US

CA Information

Friendly Name * ABC First Root CA i

Signing Key Details * RSA-4096+SHA512

Distinguished Name Fields

Common Name * ABC First Root CA

Organization ABC

Organizational Unit

Country United States

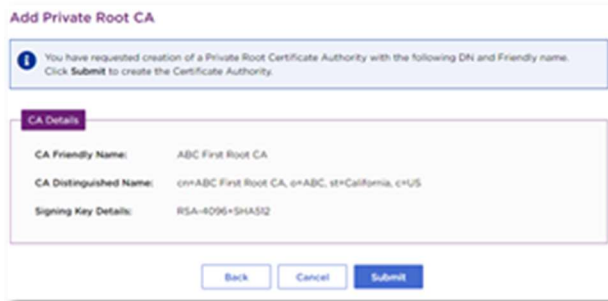
State/Province California

Locality Name

Next

- 4 In **Friendly Name**, enter an informal name for the new Certificate Authority.

- 5 In **Signing Key Details**, select one of the algorithms described in section **CA key and signature algorithms**.
- 6 Fill the **Distinguished Name Fields**.
- 7 Click **Next** and review the CA information.



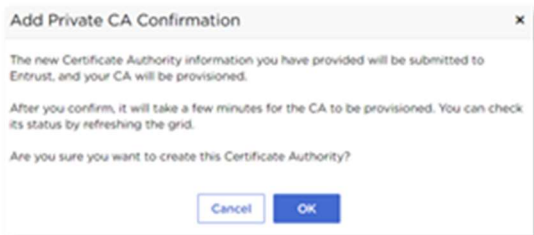
Add Private Root CA

i You have requested creation of a Private Root Certificate Authority with the following DN and Friendly name. Click **Submit** to create the Certificate Authority.

CA Details

CA Friendly Name: ABC First Root CA
 CA Distinguished Name: cn=ABC First Root CA, o=ABC, st=California, c=US
 Signing Key Details: RSA-4096+SHA512

- 8 Click **Submit**.
- 9 In the confirmation request, click **OK** to start the CA creation process.



Add Private CA Confirmation

The new Certificate Authority information you have provided will be submitted to Entrust, and your CA will be provisioned.

After you confirm, it will take a few minutes for the CA to be provisioned. You can check its status by refreshing the grid.

Are you sure you want to create this Certificate Authority?

- 10 When the CA creation is complete, check the CA details in the CA grid view.
- 11 Refresh the grid. You will notice that the status changes to **Active**.

Actions	Comm...	Issued...	Root	Friend...	Valid From	Valid To	Status	
<input type="checkbox"/>	<input checked="" type="radio"/>	ABC First Root CA	ABC First Root CA	<input checked="" type="checkbox"/>	ABC First Root CA	Sep 27, 2021	Sep 22, 2041	Active

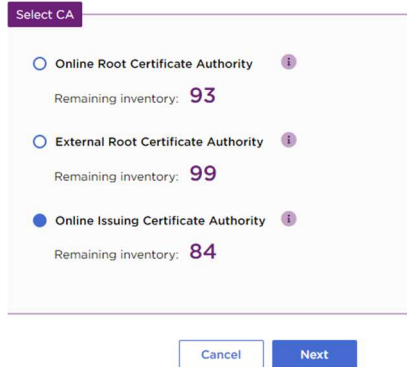
4.2.4 Adding an issuing CA

The following procedure describes how to add an issuing CA under the CA created in [Adding the PKIaaS root CA](#).

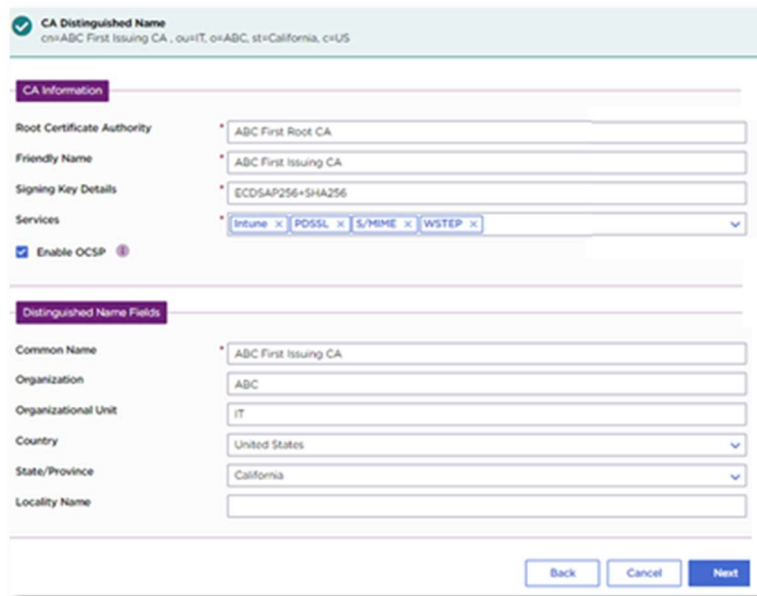
To add an issuing CA

- 1 Navigate to Add Private CA.

2 In **Select CA**, select **Issuing Certificate Authority**.



3 Click **Next**. The **CA Information** screen appears.



4 In **Root Certificate Authority**, select the CA created in [Adding the PKIaaS root CA](#).

5 In **Friendly Name**, enter an informal name for the new Certificate Authority.

6 In **Signing Key Details**, select one of the algorithms described in [section CA key and signature algorithms](#).

7 Select **Enable OCSP** if you want to use OCSP for this issuing CA.


NOTE: You cannot change this setting after provisioning the CA.

8 In **Services**, select a service to enable the corresponding pre-configured certificate profile sets.

- If you plan to add a Certificate Enrollment Gateway to this CA (see [Adding a Certificate Enrollment Gateway to an Issuing CA](#)), add the service corresponding to the Certificate Enrollment Gateway type.
For example, you should add the WSTEP service to an issuing CA before adding Certificate Enrollment Gateway for WSTEP.
- If you plan to use the CA Gateway API (see [Accessing PKIaaS via CA Gateway API](#)), select the service that matches the application you will implement.

NOTE: Each selection will consume an enrollment service license.

- 9 Fill the **Distinguished Name Fields**.
- 10 Click **Next** to review the CA information.



CA Details

Root Certificate Authority:	ABC First Root CA
CA Friendly Name:	ABC First Issuing CA
CA Distinguished Name:	cn=ABC First Issuing CA, ou=IT, o=ABC, st=California, c=US
Signing Key Details:	ECDsap256+SHA256
Services:	Issuance, PDSGL, S/HOME, WSTEP
OCSP:	Enabled

Buttons: Back, Cancel, Submit

- 11 Click **Submit**.
- 12 In the confirmation request, click **OK** to start the CA creation process.



Add Private CA Confirmation

The new Certificate Authority information you have provided will be submitted to Entrust, and your CA will be provisioned.

After you confirm, it will take a few minutes for the CA to be provisioned. You can check its status by refreshing the grid.

Are you sure you want to create this Certificate Authority?

Buttons: Cancel, OK

- 13 The newly created CA will show up in the CA grid view with a **Provisioning** status.

Actions	Common Name	Issued By	Root	Friendly Name	Valid From	Valid To	Status
<input type="checkbox"/>	ABC First Issuing CA	ABC First Root CA		ABC First Issuing CA			Provisioning
<input checked="" type="checkbox"/>	ABC First Root CA	ABC First Root CA	<input checked="" type="checkbox"/>	ABC First Root CA	Sep 27, 2021	Sep 22, 2041	Active

- 14 Refresh the grid. After about 60 seconds, you will see that the status changes to **Active**.

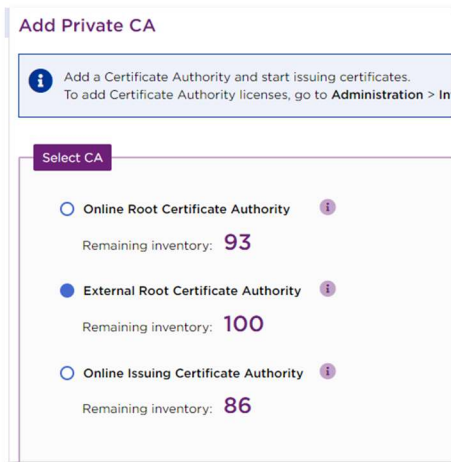
Actions	Common ...	Issued By	Root	Friendly N...	Valid From	Valid To	Status
<input checked="" type="checkbox"/>	ABC First Issuing CA	ABC First Root CA		ABC First Issuing CA	Sep 27, 2021	Sep 25, 2031	Active
<input checked="" type="checkbox"/>	ABC First Root CA	ABC First Root CA	<input checked="" type="checkbox"/>	ABC First Root CA	Sep 27, 2021	Sep 22, 2041	Active

4.2.5 Adding an external root CA

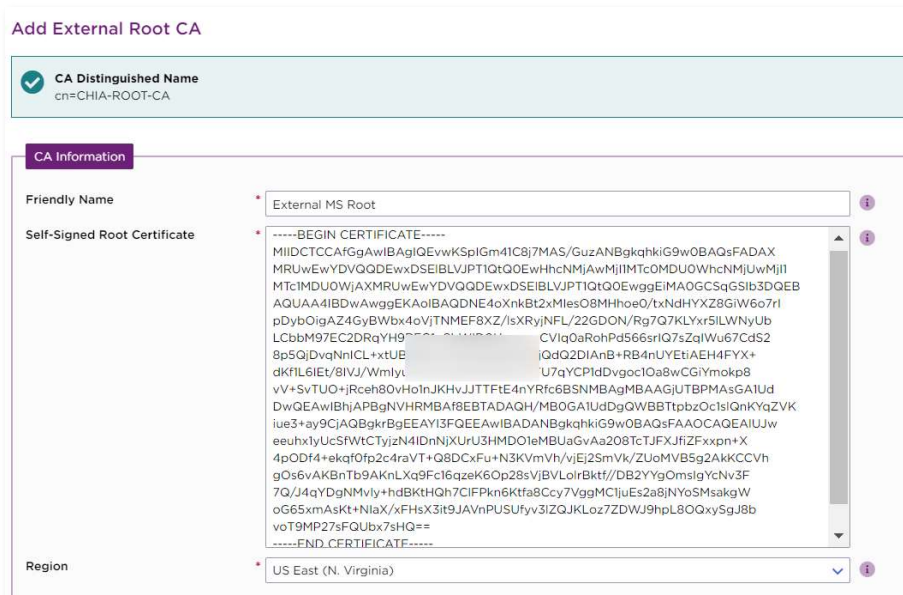
If you want to leverage PKIaaS issuing CAs while maintaining the root of trust within your organization, PKIaaS allows you to sign an issuing CA using a non-PKIaaS root CA you owned. For this use case, you must add your external root CA certificate in ECS Enterprise before adding an issuing CA (as explained in [Adding an issuing CA under an external root CA](#)). This procedure describes how to add root CA that you own.

To add an external root CA

- 1 In ECS Enterprise, navigate to **Administration > PKIaaS Management > Add Private CA**.
- 2 In **Select CA**, select **External Root Certificate Authority**, and click **Next**.



- 3 Click **Next** to fill in the external CA information.



- 4 In **Friendly Name**, enter an informal name for your CA.

- 5 In **Self-Signed Root Certificate**, paste the DER encoding of the external CA root certificate.
- 6 In **Region**, select the geographical region where the CA resides.
- 7 Click **Next** to review the external root CA information.

Add External Root CA

i You have requested import of an External Root Certificate Authority with the following details. Click **Submit** to import the Certificate Authority.

CA Details

CA Friendly Name:	External MS Root
Serial Number:	12FC0A4A92069B8D42F23ECC012FC6BB
Subject DN:	cn=CHIA-ROOT-CA
Validity:	From Feb 25, 2020 to Feb 25, 2025
Signing Key Details:	RSA-2048+SHA256
Region:	US East (N. Virginia)

- 8 Click **Submit**.
- 9 When the CA creation is complete, check the CA details in the CA grid view.

Actions	Friendly Name	Common Name	Issued By	Root	CA Type	Valid From	Valid To	Status
<input type="checkbox"/>	External MS Root	CHIA-ROOT-CA	CHIA-ROOT-CA	<input checked="" type="checkbox"/>	External	Feb 25, 2020	Feb 25, 2025	Provisioning

- 10 Refresh the grid. You will see that the status changes to **Active**.

<input type="checkbox"/>	External MS Root	CHIA-ROOT-CA	CHIA-ROOT-CA	<input checked="" type="checkbox"/>	External	Feb 25, 2020	Feb 25, 2025	Active
--------------------------	------------------	--------------	--------------	-------------------------------------	----------	--------------	--------------	--------

4.2.6 Adding an issuing CA under an external root CA

The following instructions describe how to add an issuing CA under the CA created in [Adding an external root CA](#).

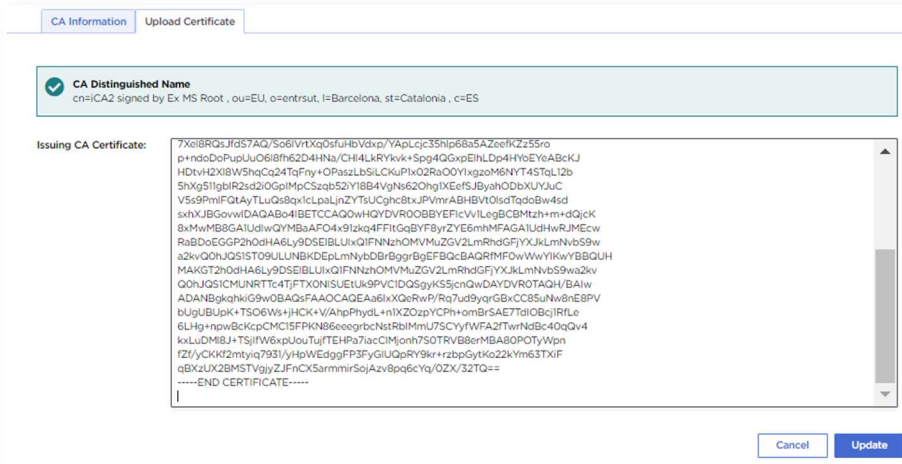
To add an issuing CA under an external root CA

- 1 Add the issuing CA as explained in [Adding an issuing CA](#). In the **Root Certificate Authority** field, select the CA you added in [Adding an external root CA](#).
- 2 When the CA creation completes, check the CA details in the CA grid view.
- 3 Refresh the grid. You will notice that the status of the new Issuing CA changes to **CSR Ready**.
- 4 Select the new issuing CA in the grid and select **Actions > Download CSR**.

⚡ Actions ▾ **📄 Export to Excel**

	Friendly Name	Common Name	Issued By
Download CSR	CA2 signed by Ex MS Root	iCA2 signed by Ex MS Root	CHIA-ROOT-CA
Upload Certificate			
Remove			

- 5 Process the downloaded CSR with your external root CA to issue a CA certificate in base-64 format.
- 6 Select the new issuing CA in the grid and select **Actions > Upload Certificate**.
- 7 Paste the signed certificate base-64 text in the **Issuing CA Certificate** box. Make sure to include the complete BEGIN CERTIFICATE and END CERTIFICATE lines.



- 8 In the CA grid, the issuing CA status will change to **Updating**. Refresh the grid; the issuing CA is ready to use when the status changes to **Active** (usually takes about 60 seconds).

4.2.7 Deleting a CA

This procedure describes how to delete root and issuing CAs. Note the following conditions:

- Before deleting a root CA, you must delete all issuing CAs under the root CA.
- When you delete an issuing CA, you also delete all the certificates you issued from this CA.

After deleting a CA, the CA license returns to inventory, generally within 24 hours.

WARNING: CA deletion is not reversible.

To delete (remove) a CA

- 1 Navigate to **Administration > PKIaaS Management**.

- 2 Select the row of the CA you want to delete and select **Actions > Remove**.



- 3 Review the information on the confirmation request before confirming the deletion.
- 4 In the CA grid view, the CA status becomes **Deleting** while the deletion is processed. This usually takes about 60 seconds.



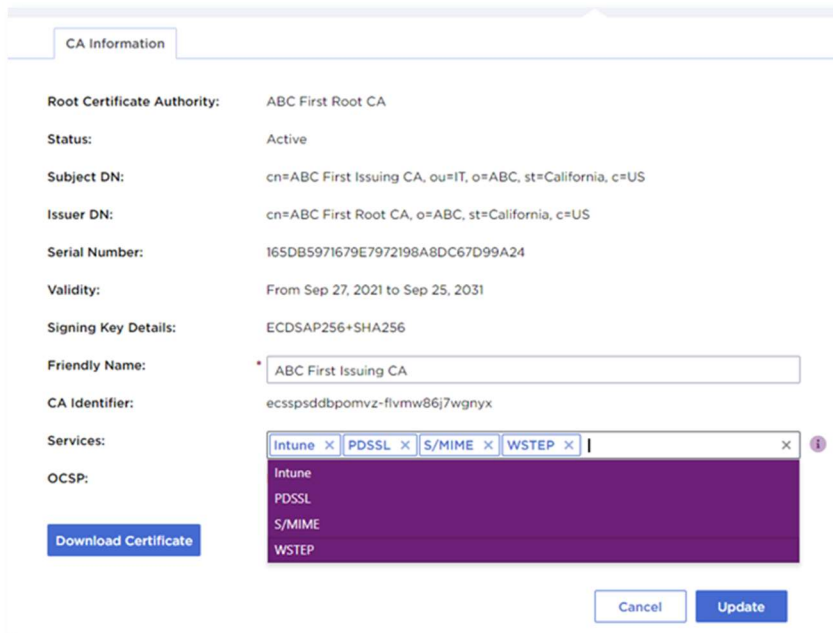
- 5 Refresh the grid. You will notice that the deleted CA is no longer listed.

4.2.8 Changing CA services (pre-defined certificate profile sets)

This procedure describes how to add or remove the services exposed by a CA.

To change the services on a CA

- 1 Navigate to **Administration > PKIaaS Management**.
- 2 Click a CA row in the grid to open the CA details.
- 3 In the **Services** field, use the multi-select drop-down menu to add or remove services.





4 Click **Update** to finalize your changes.

5 Configuring and using the CA Gateway API

Entrust offers a standalone CA Gateway service that works with PKI services such as Entrust Certificate Authority, Entrust Managed PKI, and Microsoft CA. The CA Gateway instance described here is hosted with PKIaaS and is used only with PKIaaS.

This section describes how to create and download credentials and certificate for the CA Gateway API.

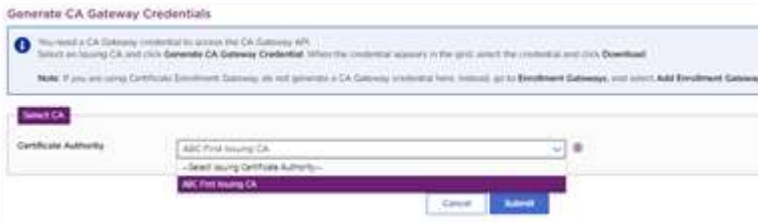
5.1 Creating and downloading CA Gateway API credentials

After provisioning the Issuing CA, you can generate credentials to connect to the CA Gateway API.

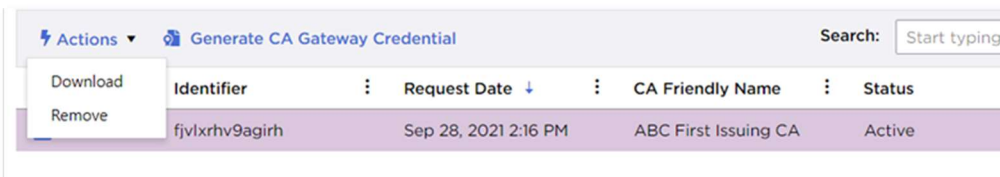
NOTE: If you purchased the PKIaaS S/MIME Enrollment Service, you need to download the CA Gateway credentials to integrate your issuing CA with our SixScape (Entrust partner) secure email solution. Please work with your assigned Entrust Tech Service Consultant to implement the SixScape solution.

To generate and download the CA Gateway credentials

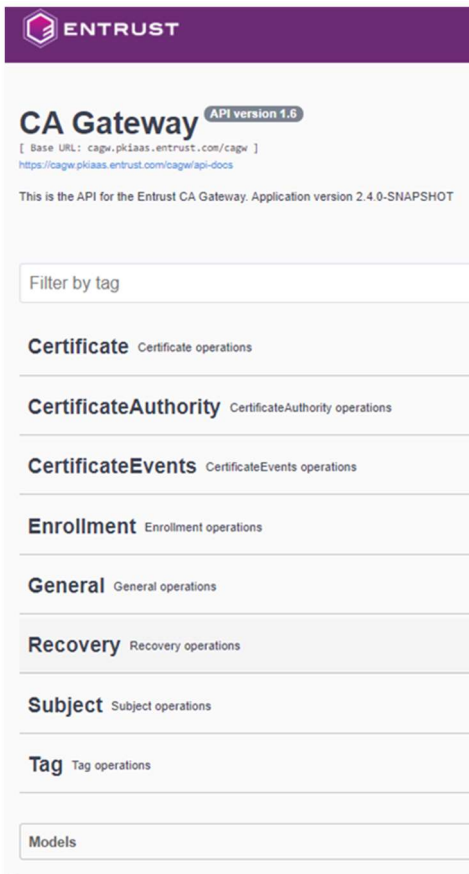
- 1 Select **Administration > PKIaaS Management**.
- 2 On the left side pane, click **CA GW Credentials**.
- 3 Click **Generate CA Gateway Credential**.
- 4 Select an issuing CA from the list of existing issuing CAs.



- 5 Click **Submit** and accept the confirmation request.
- 6 The credential will appear in the grid with **Provisioning** status. Refresh the grid to check completion.
- 7 When the credential status is **Active**, select the credential row, and select **Actions > Download**.



Identifier	Request Date	CA Friendly Name	Status
fjvlxrhv9agirh	Sep 28, 2021 2:16 PM	ABC First Issuing CA	Active



You can also integrate the PKIaaS CA Gateway API with the following services:

- Entrust: Certificate Hub, Identity Enterprise, TrustedX, IDaaS
- Third-party: SixScape, ServiceNow, Venafi, AppviewX, Ansible, Versasec
- Key Vaults: HashiCorp, Microsoft Azure Key
- Your custom applications

6 Configuring and using Entrust Certificate Enrollment Gateway (CEG)

In addition to the root and issuing CAs and the CA Gateway Credential, you have the option of adding a Certificate Enrollment Gateway, which allows you to add automation of your certificate processes.

6.1 Adding and managing CEG

Select **Administration > PKIaaS Management > Enrollment Gateways** to view and manage Certificate Enrollment Gateways.

NOTE: The Certificate Enrollment Gateway documentation is available on Entrust TrustedCare.

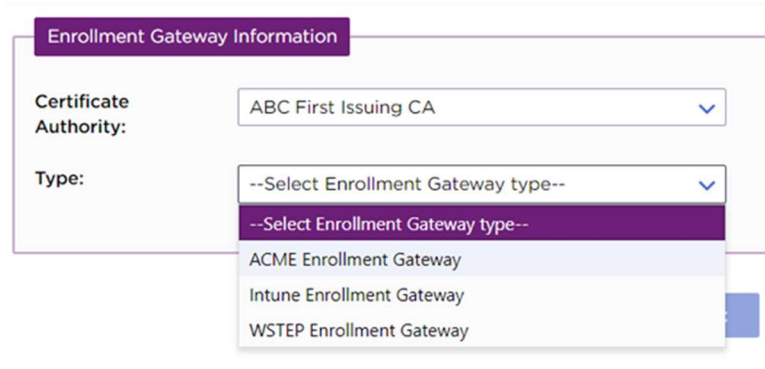
6.1.1 Adding a Certificate Enrollment Gateway to an Issuing CA

If you need more than one of any type of Enrollment Gateway, you must attach the additional one to a different Certificate Authority.

NOTE: You can only add an Enrollment Gateway type to a CA once.

To add a Certificate Enrollment Gateway service to an Issuing CA

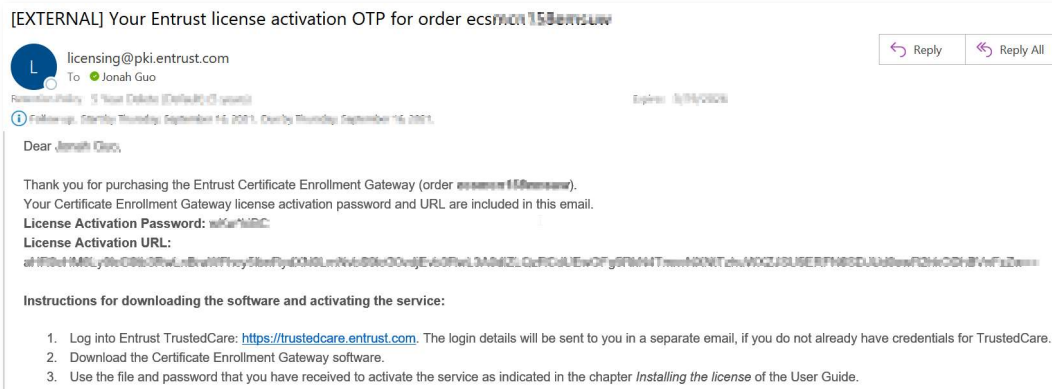
- 1 Select **Administration > PKIaaS Management > Enrollment Gateways**.
- 2 Click **Add Enrollment Gateway**.
- 3 On the **Add** screen, select the Issuing **Certificate Authority** and the Enrollment Gateway **Type**. The **Type** list only includes the Enrollment Gateway services you enabled when you added the Issuing CA.



The screenshot shows a form titled "Enrollment Gateway Information". It has two main fields: "Certificate Authority" and "Type". The "Certificate Authority" field is a dropdown menu with "ABC First Issuing CA" selected. The "Type" field is also a dropdown menu, currently open to show a list of options. The first option is "--Select Enrollment Gateway type--", which is highlighted in purple. Below it are three other options: "ACME Enrollment Gateway", "Intune Enrollment Gateway", and "WSTEP Enrollment Gateway".

- 4 Click **Submit** and accept the confirmation request.

- The first time you add a Certificate Enrollment Gateway, you will receive an email containing license activation information.



For security reasons, the One Time Password (OTP) is only valid for 14 days from the issuance date. Please activate your Certificate Enrollment Gateway software before then.

- If the person managing the Enrollment Gateway is a different administrator, please forward the email as required.
- If you no longer have the original activation email or try to activate the software after 14 days, contact Entrust Support to resend the activation email.
- If you have activated the software and need to reinstall Certificate Enrollment Gateway software, contact Entrust Support to reset the license. You will receive the reset license via a new email.

The license activation OTP email is sent only for the first Enrollment Gateway added. No additional authentication is required for the addition of subsequent CEG protocols, including those added to other Certificate Authorities in the account.

6.1.2 Deleting a Certificate Enrollment Gateway

WARNING: In the current release of ECS Enterprise, removing a Certificate Enrollment Gateway removes ALL Certificate Enrollment Gateways from ALL Certificate Authorities in the account. Certificate Enrollment Gateway licenses return to inventory within 24 hours.

To delete (remove) a Certificate Enrollment Gateway

- Select **Administration > PKIaaS Management > Enrollment Gateways**.

- 2 Select the row of the Certificate Enrollment Gateway you want to delete and select **Actions > Remove**.



6.2 Automating certificate issuance with Entrust Certificate Enrollment Gateway

User enrollment and certificate issuance can be automated using the Entrust CEG that matches your application.

6.2.1 About Certificate Enrollment Gateway

Certificate Enrollment Gateway is a next-generation virtual appliance that simplifies customer deployments and operations through centralized configuration, easy-to-distribute components for disaster recovery, load balancing, self-monitoring, and restart.

After you have associated your PKIaaS CAs with your Certificate Enrollment Gateway licenses on ECS Enterprise (as explained in [Configuring and using Entrust Certificate Enrollment Gateway \(CEG\)](#)) In addition to the root and issuing CAs and the CA Gateway Credential, you have the option of adding a Certificate Enrollment Gateway, which allows you to add automation of your certificate processes. Adding and managing), you can start the integration to automate the PKIaaS certificate issuance.

6.2.2 Installing and deploying CEG

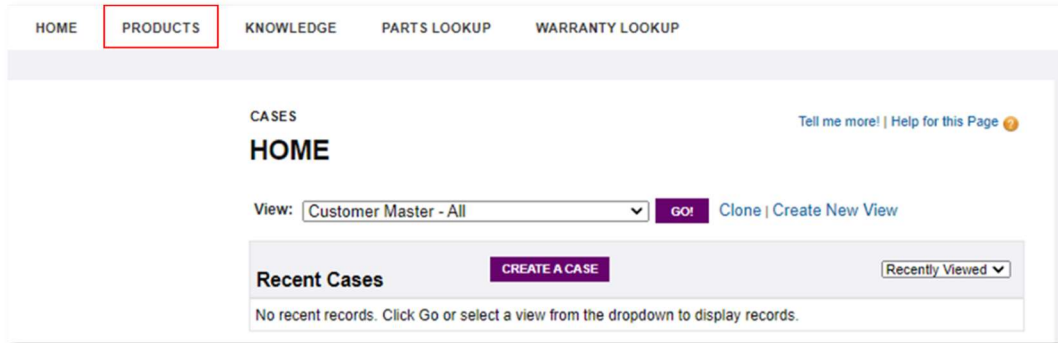
First, you need to install and set up the Entrust Deployment Manager (free of charge with Certificate Enrollment Gateway purchase). The Entrust Deployment Manager provides a clustered platform for installing and running Certificate Enrollment Gateway.

NOTE: If you have any issues during the integration, contact your assigned Entrust technical service consultant or the [Entrust Certificate Services Support team](#).

To download and install Entrust Deployment Manager and Certificate Enrollment Gateway

- 1 Log in to <https://trustedcare.entrust.com>.

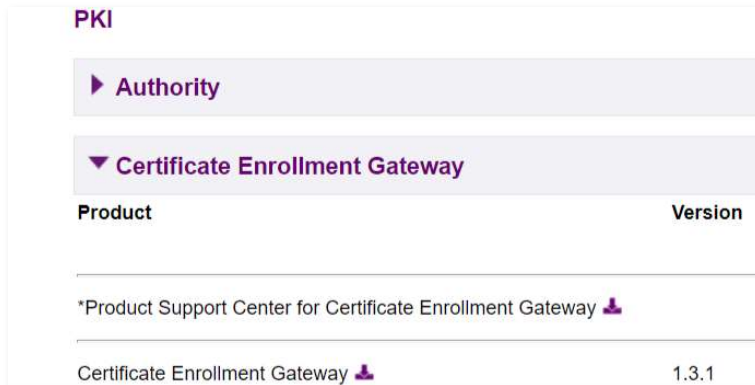
2 Click **PRODUCTS**.



3 Navigate to the PKI section.

4 Click **Certificate Enrollment Gateway**.

5 Select the latest version.



- 6 By default, you will have the **Software Downloads** tab open with a **Related Software** section listed below.

CERTIFICATE ENROLLMENT GATEWAY

Version 1.3.1

SOFTWARE
DOWNLOADS

PATCHES

DOCUMENTS

COLLATERAL

SERVICE
MANUALS

Content Title	Platform	File Type	Size	Posted Date	Digest	
WSTEP PowerShell scripts	Windows	ZIP	20.92 KB	12-15-2021	MD5 SHA-1 SHA-256	Download
log4j Mitigation Script	Windows	SH	1.70 KB	12-15-2021	MD5 SHA-1 SHA-256	Download
CEG Software		GZ	192.11 MB	12-15-2021	MD5 SHA-1 SHA-256	Download

RELATED SOFTWARE

Product	Version
*Product Support Center for Entrust Deployment Manager	1.0
Entrust Deployment Manager	1.3.1

- 7 Open the **Entrust Deployment Manager** page in a new browser window/tab and download the Entrust Deployment Manager Software.

ENTRUST DEPLOYMENT MANAGER

Version 1.3.1

SOFTWARE
DOWNLOADS

PATCHES

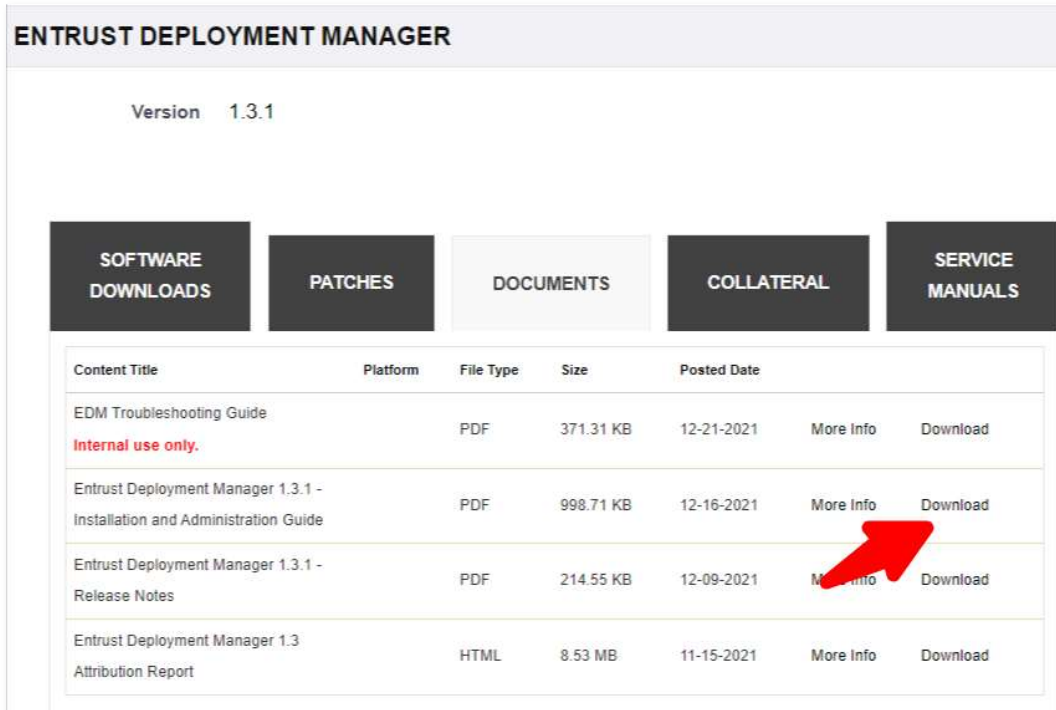
DOCUMENTS

COLLATERAL

SERVICE
MANUALS

Content Title	Platform	File Type	Size	Posted Date	Digest	
Diagnostic Report	Multi	GZ	4.34 KB	12-16-2021	MD5 SHA-1 SHA-256	Download
Entrust Deployment Manager Software	Multi	GZ	1.29 GB	11-15-2021	MD5 SHA-1 SHA-256	Download

- 8 Click the **Documents** tab and download the Entrust Deployment Manager x.x.x - Installation and Administration Guide.



ENTRUST DEPLOYMENT MANAGER

Version 1.3.1

SOFTWARE DOWNLOADS **PATCHES** **DOCUMENTS** **COLLATERAL** **SERVICE MANUALS**

Content Title	Platform	File Type	Size	Posted Date		
EDM Troubleshooting Guide <i>Internal use only.</i>		PDF	371.31 KB	12-21-2021	More Info	Download
Entrust Deployment Manager 1.3.1 - Installation and Administration Guide		PDF	998.71 KB	12-16-2021	More Info	Download
Entrust Deployment Manager 1.3.1 - Release Notes		PDF	214.55 KB	12-09-2021	More Info	Download
Entrust Deployment Manager 1.3 Attribution Report		HTML	8.53 MB	11-15-2021	More Info	Download

- 9 Follow the guide to provision a clustered platform and move to the next step when you are ready to install Certificate Enrollment Gateway (referred to as an "Entrust solution" in the guide).
- 10 Go back to the **Certificate Enrollment Gateway** page.


11 Download the CEG Software.

CERTIFICATE ENROLLMENT GATEWAY

Version 1.3.1

SOFTWARE DOWNLOADS | PATCHES | DOCUMENTS | COLLATERAL | SERVICE MANUALS


Content Title	Platform	File Type	Size	Posted Date	Digest	
WSTEP PowerShell scripts	Windows	ZIP	20.92 KB	12-15-2021	MD5 SHA-1 SHA-256	Download
log4j Mitigation Script	Windows	SH	1.70 KB	12-15-2021	MD5 SHA-1 SHA-256	Download
CEG Software		GZ	192.11 MB	12-15-2021	MD5 SHA-1 SHA-256	Download



12 Click the **Documents** tab and download the Entrust Certificate Enrollment Gateway x.x.x Documentation Suite,

SOFTWARE DOWNLOADS | PATCHES | DOCUMENTS | COLLATERAL | SERVICE MANUALS

Content Title	Platform	File Type	Size	Posted Date		
Entrust Certificate Enrollment Gateway 1.3.1 Documentation Suite - Issue 2.0		ZIP	3.52 MB	01-07-2022	More Info	Download
The Documentation Suite contains the documentation for Entrust Certificate Enrollment Gateway.						
Entrust Certificate Enrollment Gateway 1.3.1 Release Notes		HTML	18.00 KB	12-15-2021	More Info	Download
The Release Notes provide information about new features, fixes, and known issues for Certificate Enrollment Gateway.						
Entrust Certificate Enrollment Gateway 1.3.1 Attribution Report		HTML	1.89 MB	12-15-2021	More Info	Download

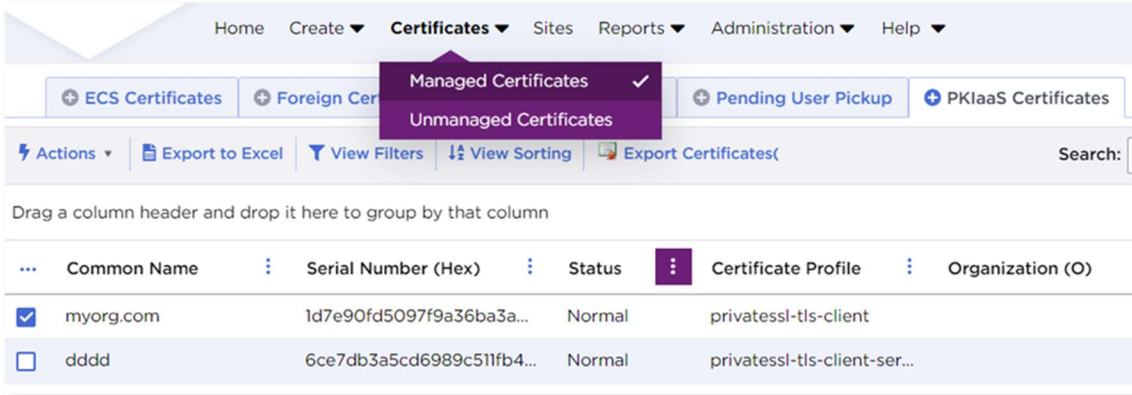


- 13 Unzip the file and follow the instructions in the Deployment Guide to deploy the Certificate Enrollment Gateway software. Follow the individual integration guide to set up the purchased enrollment use cases.



7 Creating and managing certificates in ECS Enterprise

Log in to ECS Enterprise and navigate to **Certificates > Managed Certificates > PKIaaS Certificates** to view and manage the PKIaaS certificates issued by your private issuing CAs.



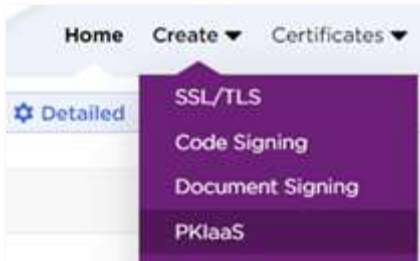
...	Common Name	Serial Number (Hex)	Status	Certificate Profile	Organization (O)
<input checked="" type="checkbox"/>	myorg.com	1d7e90fd5097f9a36ba3a...	Normal	privatessl-tls-client	
<input type="checkbox"/>	dddd	6ce7db3a5cd6989c511fb4...	Normal	privatessl-tls-client-ser...	

7.1 Creating certificates

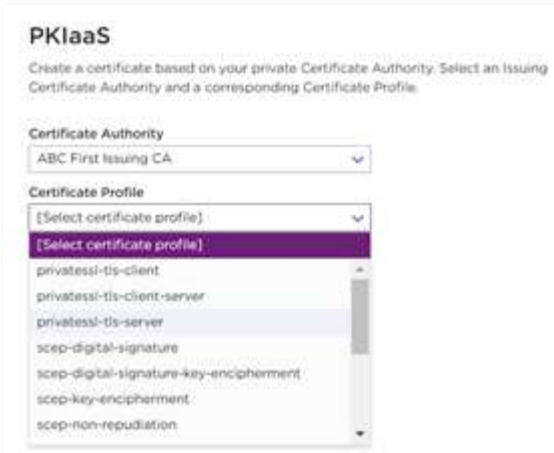
Issue a certificate with one of your private issuing CAs.

To create a certificate

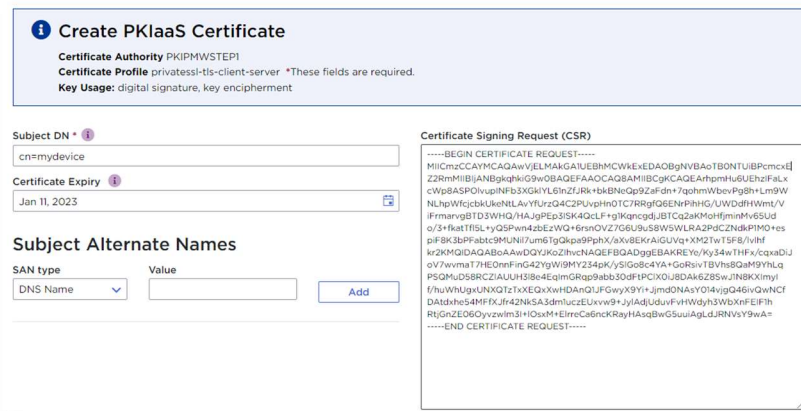
- 1 Select **Create > PKIaaS**.



2 Select the Issuing **Certificate Authority** and the **Certificate Profile**.



3 Click **Next** and fill in the certificate details.



The required certificate details vary depending on the certificate profile previously selected. The certificate expiry is 23:59:59 on the expiry date you select, calculated for the time zone set in your browser.

Because of Daylight Savings Time (if applicable) and the time zone set in your browser, you may see a discrepancy between the actual certificate expiry date (the one you set) and the expiry date you will see in some system viewers or parsers. The Windows System Viewer, in particular, does not handle Daylight Savings Time correctly.

4 Click **Submit** to issue the certificate.



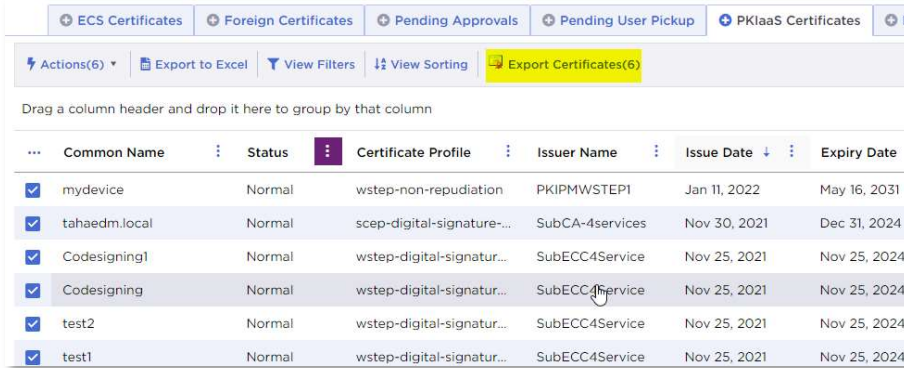
5 On the certificate issuing confirmation page, click the **Download** link.

7.2 Downloading certificates

You can also download one or more certificates later, from the certificates grid.

To download a certificate from the Managed Certificates grid

- 1 Go to **Certificates > Managed Certificates > PKIaaS Certificates**.



...	Common Name	Status	Certificate Profile	Issuer Name	Issue Date	Expiry Date
<input checked="" type="checkbox"/>	mydevice	Normal	wstep-non-repudiation	PKIPMWSTEP1	Jan 11, 2022	May 16, 2031
<input checked="" type="checkbox"/>	tahaadm.local	Normal	scep-digital-signature-...	SubCA-4services	Nov 30, 2021	Dec 31, 2024
<input checked="" type="checkbox"/>	Codesigning1	Normal	wstep-digital-signatur...	SubECC4Service	Nov 25, 2021	Nov 25, 2024
<input checked="" type="checkbox"/>	Codesigning	Normal	wstep-digital-signatur...	SubECC4Service	Nov 25, 2021	Nov 25, 2024
<input checked="" type="checkbox"/>	test2	Normal	wstep-digital-signatur...	SubECC4Service	Nov 25, 2021	Nov 25, 2024
<input checked="" type="checkbox"/>	test1	Normal	wstep-digital-signatur...	SubECC4Service	Nov 25, 2021	Nov 25, 2024

- 2 Select one or more certificates on the grid.
- 3 Click **Export Certificates** to export the selected certificates in DER format as a ZIP file.

7.3 Revoking certificates

You can revoke issued certificates to invalidate them before the expiry date.

To revoke a certificate

- 1 Select one certificate on the grid (you can only revoke one certificate each time).
- 2 Select **Actions > Revoke**.
- 3 Select the **Reason for Revocation** and click **Confirm**.



Revoke

Certificate Profile: wstep-non-repudiation

CA Friendly Name: ABC First Issuing CA

Issuer Name: ABC First Issuing CA

Subject DN: o=xyz

Expiry Date: Sep 28, 2024

Serial Number (Hex): 5c4e2bf0d33745a2bfbba6bc97290aa5

Reason for Revocation: (Please provide a reason)

Revocation Comments:

After you confirm, it will take to Revoked status. You can click **is column to update**

- 4 The revoked certificate will disappear from the **PKIaaS Certificate** grid view because the default filter only displays active certificates. Select **Status > Filter > Select All** to display the revoked certificates on the grid.

...	Common Name	Serial Number (Hex)	Status	Certificate Profile	Organization (O)
<input type="checkbox"/>		5cae2bf0d337d5a2bfbba...	Revoked		yes
<input type="checkbox"/>	test	700266e08c47ada410e6...	Revoked		t
<input type="checkbox"/>	anyrog.com	5824d6cbf4b789f7fe633...	Normal		
<input type="checkbox"/>	myorg.com	1d7e90fd5097f9a36ba3a...	Revoked		
<input type="checkbox"/>	dddd	6ce7db3a5cd6989c511fb4...	Normal	privatesl-tls-client-ser	

- ↑ Sort Ascending
- ↓ Sort Descending
- ☰ Columns
- ▼ Filter
 - Select All
 - Normal
 - Revoked
 - Held
- ☰ Set Column Position

3 items selected

7.4 Reporting, alerts, and notifications about certificate activity and expiry

Reporting, notifications, and alerts are available from **Reports > Report Center**.

Reports can be scheduled (**Reports > Report Schedule**) and you can program alerts based on certificate state, for example (**Reports > Alerts**).

You can define reports based on the information your business needs, such as daily certificate issuance, revocation, and renewal activity.

You can also set up expiry notification thresholds and email addresses in **Administration > Advanced Settings > Notifications**.

8 Managing certificates with Entrust Certificate Hub (Optional)

You can view and manage your issued certificates through the Entrust Certificate Hub product. Certificate Hub is not part of the PKIaaS offering and requires a separate license.

8.1 Certificate Hub

To use Certificate Hub, configure your PKIaaS issuing CA as a Certificate Hub Authority and Source. You can request a CA Gateway credential (see [Configuring and using the CA Gateway API](#)

Entrust offers a standalone CA Gateway service that works with PKI services such as Entrust Certificate Authority, Entrust Managed PKI, and Microsoft CA. The CA Gateway instance described here is hosted with PKIaaS and is used only with PKIaaS.

This section describes how to create and download credentials and certificate for the CA Gateway API.

Creating and downloading CA Gateway API credentials), and then use the credential to connect to Certificate Hub and perform any of the functions below.

8.2 Connecting your CA

Connect your issuing CA as a Source. The URL will be the relevant one listed in the Issuing Certificates section above ([Creating and downloading CA Gateway API credentials](#)). Once you set this up, Certificate Hub will check with your CA every 15 minutes and pull in any issued certificates through CEG or other applications. It will also update for any revocations.

Optionally, you can also connect your issuing CA as an Authority. The URL will be the same. Connecting your issuing CA as an Authority will allow you to revoke certificates and manually issue certificates for other applications supported by the certificate profiles assigned to your CA.

8.3 Dashboard

The Certificate Hub dashboard provides a quick overview of all activities.

8.4 Reporting on certificate activity

Certificate Hub provides a reporting engine that lets you define report content, format, and automated scheduling. You can use this capability to define reports based on your business needs, such as daily certificate issuance, revocation, and renewal activity.

8.5 Ad-hoc exploration

The Certificate View allows you to filter and display certificates from your PKIaaS CA or any other CA that you have connected. Certificate Hub's "Single Pane of Glass" view gives you enterprise-wide visibility of all your PKI activity.

8.6 Expiry notifications

You can define expiry notifications to let certificate owners know that certificates are about to expire and need to be renewed. Such notifications are valuable in some scenarios, but if you are using Certificate Enrollment Gateway to automate the issuance and renewal of certificates, notifications may be unnecessary. You may find that weekly reports of certificates about to expire is a better way to monitor that the overall system operation is working.

9 Obtaining support

As a customer, you will receive a Welcome Guide from Entrust Customer Support. This guide provides more details about getting support on all your purchased products.

9.1 Authorized contacts

Entrust is dedicated to the security of our customers and partners. Because of this, we limit support to listed and authorized contacts.

9.2 Entrust Certificate Services Support

Product and Technical Support: ECS.Support@Entrust.com

Sales: <https://www.entrust.com/contact/sales>

Phone Support:

- North America: 1-866-267-9297
- Outside North America: 1-613-270-2680 or [Toll-free Support Numbers for Customers outside of North America](#)
- The availability of the support team depends on your service plan: Silver vs. Platinum. See [Entrust Certification Solutions Hosted Support Schedule](#) for details.

9.3 TrustedCare portal

Entrust provides a comprehensive service and support program through its [TrustedCare online portal](#). This portal allows you to:

- Obtain PKIaaS product documentation and online access to information, including frequently asked questions, general documentation, and technical bulletins
- Open support cases
- Check on the status of existing cases
- Download software product updates for components that you run on your premises or in your cloud

Appendix: Certificate profile reference

PKIaaS certificate issuance is always done in the context of a Certificate Profile.

Profiles library	Available profiles
CA & VA (OCSP) certificate profiles	basic-ca-root basic-ca-subord basic-ocsp
S/MIME Secure Email certificate profiles	smime-digital-signature-key-encipherment smime-key-encipherment smime-non-repudiation
Smart Card certificate profiles	smartcard-card-authentication smartcard-digital-signature smartcard-domain-controller smartcard-key-management smartcard-piv-authentication smartcard-piv content-signing
Code signing certificate profiles	codesigning-digital-signature
CEG-Intune certificate profiles	intune-digital-signature intune-key-encipherment intune-non-repudiation intune-signature-key-encipherment
CEG-Private SSL(ACME) certificate profiles	privatessl-tls-client privatessl-tls-client server privatessl-tls-server
CEG-WSTEP (Active Directory) certificate profiles	wstep-digital-signature wstep-key-encipherment wstep-non-repudiation wstep-signature-key-encipherment
CEG-SCEP certificate profiles	scep-digital-signature scep-key-encipherment scep-non-repudiation scep-signature-key-encipherment

Profiles library	Available profiles
CEG-MDM Web Service certificate profiles	mdmws-digital-signature mdmws-key-encipherment mdmws-non-repudiation mdmws-signature-key-encipherment
CEG-CMP certificate profiles	cmp-digital-signature cmp-key-encipherment cmp-non-repudiation cmp-signature-key-encipherment
CEG-EST certificate profiles	est-digital-signature est-key-encipherment est-non-repudiation est-signature-key-encipherment
V2G certificate profiles	v2g-supply-equipment v2g-user-identity

These profiles are defined within the PKIaaS service and referenced by name in the certificate issuance requests. See CA Gateway documentation for the API details.

Signature algorithm constraints for all profiles

All PKIaaS profiles support the following key and signature algorithms.

Key algorithm	Signature algorithm
ECDSA P-256	ecdsa-with-SHA256
ECDSA P-384	ecdsa-with-SHA384
ECDSA P-521	ecdsa-with-SHA512
RSA 2048	sha256WithRSAEncryption
RSA 3072	sha256WithRSAEncryption
RSA 4096	sha512WithRSAEncryption

CA & VA (OCSP) certificate profiles

Entrust PKIaaS supports the following CA and VA profiles.

- basic-ca-root
- basic-ca-subord
- basic-ocsp

IMPORTANT: These profiles are not exposed in the ECS Enterprise UI.

See the following sections for the profile constraints.

basic-ca-root profile constraints

The basic-ca-root profile sets the following certificate values.

Field	Value
Issuer	Self-signed
Validity period	Less than or equal to 20 years
Subject	No constraint

The basic-ca-root profile sets the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA=True
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Never present
Key Usage	Yes	digitalSignature, keyCertSign, cRLSign
Extended Key Usage	Yes	Never present
CRL Distribution Points	No	Never present (not applicable)
AIA	No	Never present
OCSP	No	Never present

basic-ca-subord profile constraints

The basic-ca-subord profile sets the following certificate values.

Field	Value
Issuer	Customer's root CA
Validity period	Less than or equal to 10 years. The subordinate expiry cannot exceed the root validity.

Field	Value
Subject	No constraint

The basic-ca-subord profile sets the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA=True, pathLenConstraint=0
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Key Usage	Yes	digitalSignature, keyCertSign, cRLSign
Extended Key Usage	Yes	Never present
CRL Distribution Points	No	Always present
AIA	No	Supplied when the customer enables OCSP on CA creation
OCSP	No	Never present

basic-ocsp profile constraints

The basic-ocsp profile sets the following certificate values.

Field	Value
Issuer	Customer's root CA
Validity period	30 days
Subject	No constraint

The basic-ocsp profile sets the following request extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA = False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Key Usage	Yes	digitalSignature, keyCertSign, cRLSign
Extended Key Usage	Yes	OCSP Signing
CRL Distribution Points	No	Always present
AIA	No	Always present
OCSP	No	No check

S/MIME Secure Email certificate profiles

S/MIME Secure Email profiles only differ in the Key Usage (critical) and Extended Key Usage (non-critical) extensions.

S/MIME Secure Email profile	Key Usage	Extended Key Usage
smime-digital-signature-key-encipherment	Digital Signature Key Encipherment	TLS client authentication 1.3.6.1.5.5.7.3.2 Email Protection 1.3.6.1.5.5.7.3.4
smime-key-encipherment	Key Encipherment	Email Protection 1.3.6.1.5.5.7.3.4
smime-non-repudiation	Digital Signature Non-Repudiation	Email Protection 1.3.6.1.5.5.7.3.4

All S/MIME Secure Email profiles set the following certificate values.

Field	Value
Issuer	Customer's subordinate issuing CA.
Validity period	Less than or equal to subordinate expiry of the issuing CA. Default to 3 years if not specified in the request.
Subject	No constraint.

All S/MIME Secure Email profiles set the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA =False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Subject Alternative Name	No	No constraints
CRL Distribution Points	No	Always present
AIA	No	Supplied if the customer enables OCSP when creating the CA

Smart Card certificate profiles

Smart Card profiles only differ in the supported Key Usage (critical) and Extended Key Usage (non-critical) requests extensions.

CEG-CMP profile	Key Usage	Extended Key Usage
smartcard-card-authentication	Digital Signature	No constraints
smartcard-digital-signature	Digital Signature Non-Repudiation	No constraints
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
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)
smartcard-piv-content-signing	Digital Signature Non-Repudiation	No constraints

All Smart Card Certificate profiles set the following certificate values.

Field	Value
Issuer	Customer's subordinate issuing CA
Validity period	Less than or equal to subordinate expiry of the issuing CA. Default to 3 years if not specified in the request.
Subject	No constraint

All Smart Card Certificate profiles set the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA =False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Subject Alternative Name	No	No constraints
CRL Distribution Points	No	Always present

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA

Code signing certificate profiles

The codesigning-digital-signature profile sets the following certificate values.

Field	Value
Issuer	Customer's subordinate issuing CA
Validity period	Less than or equal to subordinate expiry of the issuing CA. Default to 3 years if not specified in the request.
Subject	No constraint

The code-signing-digital-signature profile sets the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA =False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Subject Alternative Name	No	No constraints
Key Usage	Yes	Digital Signature
Extended Key Usage	No	1.3.6.1.5.5.7.3.3 (Code Signing)
CRL Distribution Points	No	Always present
AIA	No	Supplied if the customer enables OCSP when creating the CA

CEG-Intune certificate profiles

Certificate Enrollment Gateway Intune profiles only differ in the supported Key Usage critical extension.

CEG-Intune profile	Key Usage
intune-digital-signature	Digital Signature
intune-key-encipherment	Key Encipherment
intune-non-repudiation	Non-Repudiation

CEG-Intune profile	Key Usage
intune-signature-key-encipherment	Digital Signature, Key Encipherment

All CEG-WSTEP profiles set the following certificate values.

Field	Value
Issuer	Customer's subordinate issuing CA
Validity period	Less than or equal to subordinate expiry of the issuing CA. Default to 3 years if not specified in the request.
Subject	No constraint

All CEG-WSTEP profiles set the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA =False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Subject Alternative Name	No	No constraints
CRL Distribution Points	No	Always present
AIA	No	Supplied if the customer enables OCSP when creating the CA

CEG-Intune profiles also support the following non-critical extensions in request.

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
MSTemplateName	1.3.6.1.4.1.311.20.2

CEG-Private SSL(ACME) certificate profiles

Private Certificate Enrollment Gateway SSL certificate profiles only differ in the Extended Key Usage non-critical extension.

SSL Certificate profile	Extended Key Usage
privatessl-tls-client	TLS client authentication 1.3.6.1.5.5.7.3.2
privatessl-tls-client-server	TLS server authentication 1.3.6.1.5.5.7.3.1 TLS client authentication 1.3.6.1.5.5.7.3.2
privatessl-tls-server	TLS server authentication 1.3.6.1.5.5.7.3.1

All Private SSL Certificate profiles set the following certificate values.

Field	Value
Issuer	Customer's subordinate issuing CA
Validity period	Less than or equal to subordinate expiry of the issuing CA. Default to 3 years if not specified in the request.
Subject	No constraint

All Private SSL Certificate profiles set the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA =False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Subject Alternative Name	No	No constraints
Key Usage	Yes	Digital Signature, Key Encipherment
CRL Distribution Points	No	Always present
AIA	No	Supplied if the customer enables OCSP when creating the CA

Private SSL Certificate profiles also support the following non-critical extensions in request.

Extension	OID
CertificatePolicies	2.5.29.32
ApplicationPolicies	1.3.6.1.4.1.311.21.10

CEG-WSTEP (Active Directory) certificate profiles

Certificate Enrollment Gateway WSTEP (Active Directory) profiles only differ in the Key Usage critical extension.

CEG-WSTEP profile	Key Usage
wstep-digital-signature	Digital Signature
wstep-key-encipherment	Key Encipherment
wstep-non-repudiation	Non-Repudiation
wstep-signature-key-encipherment	Digital Signature, Key Encipherment

All CEG-WSTEP profiles set the following certificate values.

Field	Value
Issuer	Customer's subordinate issuing CA
Validity period	Less than or equal to subordinate expiry of the issuing CA. Default to 3 years if not specified in the request.
Subject	No constraint

All CEG-WSTEP profiles set the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA =False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Subject Alternative Name	No	No constraints
CRL Distribution Points	No	Always present
AIA	No	Supplied if the customer enables OCSP when creating the CA

CEG-WSTEP profiles also support the following non-critical extensions in request.

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

CEG-SCEP certificate profiles

Certificate Enrollment Gateway SCEP profiles only differ in the supported Key Usage critical extension.

CEG-SCEP profile	Key Usage
scep-digital-signature	Digital Signature
scep-key-encipherment	Key Encipherment
scep-non-repudiation	Non-Repudiation
scep-signature-key-encipherment	Digital Signature, Key Encipherment

All CEG-SCEP profiles set the following certificate values.

Field	Value
Issuer	Customer's subordinate issuing CA
Validity period	Less than or equal to subordinate expiry of the issuing CA. Default to 3 years if not specified in the request.
Subject	No constraint

All CEG-SCEP profiles set the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA =False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Subject Alternative Name	No	No constraints
Extended Key Usage	No	No constraints
CRL Distribution Points	No	Always present
AIA	No	Supplied if the customer enables OCSP when creating the CA

CEG-SCEP profiles also support the following non-critical extensions in request.

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
MSTemplateName	1.3.6.1.4.1.311.20.2

CEG-MDM Web Service certificate profiles

Certificate Enrollment Gateway MDM Web Service profiles only differ in the supported Key Usage critical extension.

CEG-MDM Web Service profile	Key Usage
mdmws-digital-signature	Digital Signature
mdmws-key-encipherment	Key Encipherment
mdmws-non-repudiation	Non-Repudiation
mdmws-signature-key-encipherment	Digital Signature, Key Encipherment

All CEG-MDM Web Service profiles set the following certificate values.

Field	Value
Issuer	Customer's subordinate issuing CA
Validity period	Less than or equal to subordinate expiry of the issuing CA. Default to 3 years if not specified in the request.
Subject	No constraint

All CEG-MDM Web Service profiles set the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA =False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Subject Alternative Name	No	No constraints
Extended Key Usage	No	No constraints
CRL Distribution Points	No	Always present

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA

CEG-MDM Web Service profiles also support the following non-critical extensions in request.

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
MSTemplateName	1.3.6.1.4.1.311.20.2

CEG-CMP certificate profiles

Entrust Certificate Enrollment Gateway CMP profiles only differ in the supported Key Usage critical extension.

CEG-CMP profile	Key Usage
cmp-digital-signature	Digital Signature
cmp-key-encipherment	Key Encipherment
cmp-non-repudiation	Non-Repudiation
cmp-signature-key-encipherment	Digital Signature, Key Encipherment

All CEG-CMP profiles set the following certificate values.

Field	Value
Issuer	Customer's subordinate issuing CA
Validity period	Less than or equal to subordinate expiry of the issuing CA. Default to 3 years if not specified in the request.
Subject	No constraint

All CEG-CMP profiles set the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA =False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey

Extension	Critical	Value
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Subject Alternative Name	No	No constraints
Extended Key Usage	No	No constraints
CRL Distribution Points	No	Always present
AIA	No	Supplied if the customer enables OCSP when creating the CA

CEG-CMP profiles also support the following non-critical extensions in request.

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
MSTemplateName	1.3.6.1.4.1.311.20.2

CEG-EST certificate profiles

Entrust Certificate Gateway EST profiles only differ in the supported Key Usage critical extension.

EST profile	Key Usage
est-digital-signature	Digital Signature
est-key-encipherment	Key Encipherment
est-non-repudiation	Non-Repudiation
est-signature-key-encipherment	Digital Signature, Key Encipherment

All CEG-EST profiles set the following constraint.

Field	Value
Issuer	Customer's subordinate issuing CA
Validity period	Less than or equal to subordinate expiry of the issuing CA. Default to 3 years if not specified in the request.
Subject	No constraint

All CEG-EST profiles set the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA =False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Subject Alternative Name	No	No constraints
Extended Key Usage	No	No constraints
CRL Distribution Points	No	Always present
AIA	No	Supplied if the customer enables OCSP when creating the CA

EST profiles also support the following non-critical extensions in request.

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
MSTemplateName	1.3.6.1.4.1.311.20.2

V2G certificate profiles

Vehicle-to-grid (V2G) certificate profiles set the following certificate values.

V2G profile	Key Usages	Extended key usages	Validity
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

All V2G profiles set the following certificate values.

Field	Value
Issuer	Customer's subordinate issuing CA
Subject	No constraint

All V2G profiles set the following certificate extension values.

Extension	Critical	Value
Basic Constraints	Yes	cA =False
Subject Key Identifier	No	160-bit SHA-1 hash of subjectPublicKey
Authority Key Identifier	No	Matches subjectKeyIdentifier of the signing certificate
Subject Alternative Name	No	No constraints
CRL Distribution Points	No	Always present
AIA	No	Supplied if the customer enables OCSP when creating the CA