Entrust PKI as a Service

Welcome to the user guide for Entrust PKI as a Service (PKIaaS), the cloud-based PKI as a service by Entrust.

About this guide

This document provides a complete customer guide for Entrust PKIaaS.

Revision information

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

|Issue|Date|Section|Description |--|--|-- |1.1|Jan 2026|Running Certbot|Document missing parameters |1.0|Dec 2025|Initial release of this document

Other documents

See the table below for other relevant documentation on Entrust PKI as a Service.

Document	URL
Entrust PKI as a Service Product Page	https://www.entrust.com/digital-security/certificate-solutions/products/pki/managed-services/pki-as-a-service
Entrust PKI Terms and Conditions	https://www.entrust.com/legal-compliance/terms-conditions/entrust-pki

Documentation feedback

Complete the form at https://go.entrust.com/documentation-feedback to rate and provide feedback about product documentation.

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

Acronyms

See below a definition of acronyms that may appear in this document.

Acronym	Description
ACME	Automatic Certificate Management Environment
ADCS	Microsoft Active Directory Certificate Services
ADDS	Microsoft Active Directory Domain Services
AES	Advanced Encryption Standard
AIA	Authority Information Access
API	Application Programming Interface
CA	Certificate Authority
CAGW	Entrust CA Gateway
CEG	Entrust Certificate Enrollment Gateway
CEP	Certificate Enrollment Policy
CLI	Command-line Interface
CLM	Certificate Lifecycle Management
CMC	Certificate Management over CMS
CMP	Certificate Management Protocol
CMS	Cryptographic Message Syntax
CN	Common Name
CPS	Certification Practice Statement
CRL	Certificate Revocation List

Acronym	Description
CSR	Certificate Signing Request (PKCS #10)
CSS	Certificate Status Server
CT	Certificate Transparency
DER	Distinguished Encoding Rules
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DNS	Domain Name System
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EEE	End Entity Enrollment
EST	Enrollment over Secure Transport
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
IdP	Identity Provider
JDK	Java Development Kit
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over SSL
LRA	Local Registration Authority
MDM	Mobile Device Management
MDMWS	Entrust Mobile Device Management Web Services
MS-WSTEP	WS-Trust X.509v3 Token Enrollment Extensions Protocol (WSTEP)
MS-XCEP	X.509 Certificate Enrollment Policy Protocol (CEP)
NIST	National Institute of Standards and Technology
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OTP	One-time Passcode
OVA	Open Virtual Appliance
P12	PKCS #12

Acronym	Description
PA	Policy Authority
PEM	Privacy Enhanced Mail
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIaaS	PKI as a Service
PKIX	Public Key Infrastructure X.509
PQ	Post-Quantum
RA	Registration Authority
RBAC	Role-Based Access Control
RDN	Relative Distinguished Name
REST	Representational State Transfer
RFC	Request for Comment
RHEL	Red Hat Enterprise Linux
RPO	Recovery Point Objective
RTO	Recovery Time Objective
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAN	Subject Alternative Names
SCEP	Simple Certificate Enrollment Protocol
SHA	Secure Hash Algorithms
SIEM	Security Information and Event Management
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TPM	Trusted Platform Module
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
V2G	Vehicle-to-Grid
VM	Virtual Machine
WHFB	Windows Hello for Business

Introduction

Entrust PKIaaS is a highly secure PKI that is quick to deploy, scales on demand, and runs where you do business — the cloud. As explained in the following sections, Entrust PKIaaS secures use cases through turnkey approaches, solving customer problems while maintaining simplicity by reducing the number of services, applications, and software they need to run on their premises.

- Capabilities
- Operation
- Governance
- Quotas
- Compliance
- Definitions

Capabilities

Entrust PKIaaS capabilities cover the following areas.

- Certificate authority instantiation
- Certificate issuance
- Certificate management
- Certificate status checking

Certificate authority instantiation

PKIaaS provides the following Certificate Authority (CA) instantiation capabilities.

- CA types
- CA key and signature algorithms
- Secure CA key management
- CA creation time
- CA validity period

CA types

Each customer may have one or more subordinate issuing CAs. You can:

- Create an online root CA and add issuing CAs subordinate to this root CA.
- Add an issuing CA signed by an external root CA â□□ for example, your on-premise Microsoft root CA.

Secure CA key management

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

CA creation time

CAs are automatically provisioned in ~60 seconds after submitting your request.

CA validity period

CA certificates have a default validity period of 20 years for root CAs and 10 years for subordinate issuing CAs. You can select a different period when creating each CA.

⚠ An issuing CA should have a minimum lifespan of 3 years to support some features. For example, to automate Intune/MDM enrollment using an Entrust Hosted Certificate Enrollment Gateway, an issuing CA must have at least 3 years of remaining lifespan when the Enrollment Gateway is created.

Certificate issuance

Entrust PKIaaS capabilities for certificate issuance include the following.

- Certificate profiles
- Subscriber key algorithms
- Validity period
- Enrollment by CSR
- Subject Alt Names
- Extensions
- Proof of possession

Certificate profiles

PKIaaS certificate issuance is always in the context of a certificate profile. These profiles are:

- Defined within the Entrust PKIaaS service.
- Referenced by name in the certificate issuance requests.

As described in PKIaaS subscriber certificate profiles, Entrust tunes the profiles to specific use cases:

- CA Gateway API
- On-premises Certificate Enrollment Gateway (CEG)

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

Validity period

The certificate validity period cannot go beyond the expiry date of the issuing CA.

ℹ The validity period value defaults to 3 years when not specified in the request.

Enrollment by CSR

All certificate issuance requests use the CSR format.

ℹ The calling application is responsible for generating a private key for the certificate.

Subject Alt Names

Subject Alt Names (SANs) are supplied in the `subjectAltNames` request field, separate from the CSR.

Some third-party services like Venafi require to automatically supply SANs using the common names for TLS server certificates. To automatically supply SANs using common names, the privatessl group provides the following profiles.

- `privatessl-tls-client-server-supply-san`
- `privatessl-tls-server-supply-san`

Extensions

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

```
optionalCertificateRequestDetails.extensions
```

Proof of possession

The Proof of Possession (POP) check automatically validates that the caller has possession of the private key.

ℹ The POP check is always performed during certificate request validation.

Certificate management

To manage certificates, Entrust PKIaaS provides:

- The web portal described in this guide.
- The API described in https://api.managed.entrust.com/doc/#operation/certificate-events

Certificate status checking

PKIaaS provides the following certificate status-checking functions.

- Entrust PKIaaS Certificate Revocation Lists
- Entrust PKIaaS OCSP service

Entrust PKIaaS Certificate Revocation Lists

PKIaaS publishes Certificate Revocation Lists (CRLs) with the following settings.

CRL setting	Value
â□□CRL validity	7 daysâ□□
CRL extensions	`crlNumber`, `invalidityDate`, `expiredCertsOnCRL`
Signing key	CA key
CRL type	full CRL
Maximum size	22 MB
CA type	root and issuing CAs

CRL issuance and update modes are the following.

Mode	Period
Automatic	Every 24 hours
Include the "publish now" option on revocation requests to the API	Within 15 minutes of receiving the request
Revoke an end-entity certificate using the PKIaaS UI or the Entrust Certificate Enrollment Gateway (CEG)	Within 15 minutes of the revocation

CRLs are available at the following URLs.

Region	URL
US	`http://crl.PKIaaS.entrust.com/crl/{accountId}/{caId}/crl.crl` â□□
EU	`http://crl.eu.PKIaaS.entrust.com/crl/{accountId}/{caId}/crl.crl`
PQ Lab	`http://crl.pqlab.PKIaaS.entrust.com/crl/{accountId}/{caId}/crl.crl`

Where `{accountId}` is your account identifier, and `{caId}` is the certificate authority identifier.

Entrust PKIaaS OCSP service

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 for both roots and issuing CAs

OCSP services are available at the following URLs.

Region	URL
US	`http://ocsp.PKIaaS.entrust.com/ocsp/{accountId}/{caId}`

Region	URL
EU	`http://ocsp.eu.PKIaaS.entrust.com/ocsp/{accountId}/{caId}`
PQ Lab	`http://ocsp.pqlab.PKIaaS.entrust.com/ocsp/{accountId}/{caId}`

Where `{accountId}` is your account identifier, and `{caId}` is the certificate authority identifier.

Operation

Entrust PKIaaS implements the following operational procedures.

- Physical locations
- Access control and trusted roles
- CA key management
- Audit logging
- Disaster recovery

For the Entrust PKIaaS terms and agreements, see https://www.entrust.com/legal-compliance/entrust-certificate-services-repository

Physical locations

In each region, Entrust has implemented two physical data centers with failover between the two.

Region	Data centers
US	â□□Dallas (TX), Denver (CO)
EU	Munich (Germany), Frankfurt (Germany)

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

Access control and trusted roles

The HSM and Activation Data are located in either:

- A Tier III, SSAE-18 data center.
- A two-person controlled safe located in a facility.

The personnel with a Trusted Role:

- Can backup, store, and recover CA Private Keys using dual control in a physically secured environment.
- Receive alarm notifications on any violation of the rules for accessing the HSM or a CA.
- Are trained for their specific role and must undergo background investigations.
- Cannot change the product code.

CA key management

When a customer requests to provision a new CA, an API-based process generates the CA key pair within HSMs in a physically secured environment.

Audit logging

Significant security events in the CAs are automatically time-stamped and recorded as internal audit logs. Audit logs are:

- Periodically archived.
- Constantly monitored by the Entrust Security Information and Event Management (SIEM) system.

Additionally:

- The operations and security teams review the alerts generated by possible policy violations and other significant events.
- You can see the basic audit logs related to your Entrust PKIaaS account in the Enterprise UI using the Reports function.

Disaster recovery

To mitigate the event of a disaster, Entrust PKIaaS utilizes:

- Two data centers in each region (US and EU) with highly available HSMs
- Secure on-site and off-site storage of backup HSMs containing copies of all CA private keys
- Real-time database replication between primary and secondary cloud regions
- Daily database backups in both the primary and secondary cloud regions
- Weekly backup of critical data to a secure off-site storage facility

Governance

Defining the governance model for an enterprise-level PKI is a long and challenging process involving teams across the organization. Entrust provides a pre-defined set of policies and practices governing these PKIs to save you time and expense. See the following sections for a summary.

- Entrust responsibilities
- Customer responsibilities

ℹ See RFC 647 for a general description of the policy and practices framework.

Entrust responsibilities

In Entrust PKIaaS, Entrust has the following responsibilities.

- Root CA
- Issuing CAs
- Policy Authority
- Operational Authority

Root CA

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 ask for a naming relationship with your company so that we can support you more easily. Your root CAs will issue certificates to your issuing CAs and OCSP services.

Issuing CAs

You may have one or more issuing CAs. Entrust 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 and issue certificates for subscribers.

Policy Authority

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

Operational Authority

Entrust manages all root and issuing CA systems hosted and operated on your behalf, as part of Entrust PKIaaS. These systems issue and manage

- Certificates
- Certificate Revocation Lists (CRLs)
- OCSP responses

As the Operational Authority (OA), Entrust is responsible for all the operations of the CAs per the CPS.

Customer responsibilities

In Entrust PKIaaS, customers have the following responsibilities.

- Registration Authority
- Subscribers
- Relying parties

Registration Authority

In Entrust 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. Specifically, RAs:

1. Verify the identity of the applicants. They are responsible for the applicant registration, identification, and authentication processes.
2. Submit certificate issuance requests on their behalf.

ℹ To perform RA tasks, you will typically use software applications, like the Entrust Certificate Enrollment Gateway, that interface with the Entrust PKIaaS API.

Subscribers

Subscribers are the end-users and entities that request and use certificates. Typical examples of Subscribers are

- Employees or contractors and their devices,
- Enterprise servers and infrastructure,
- IoT devices.

⚠ As the RA, you are responsible for determining who may be a subscriber and which people, entities, and devices may receive certificates.

Relying parties

A relying party is an entity that uses a certificate, for example, to verify an identity. Entrust PKIaaS is tuned to support enterprise-level, privately trusted certificates. You are responsible for ensuring that relying parties perform the necessary certificate validity and status checks.

ℹ Entrust PKIaaS supports both CRL and OCSP checks.

Quotas

Entrust PKIaaS enforces the following quotas and limits.

- Region limits
- Rate limits
- Certificate issuance capping

Region limits

PKIaaS currently supports setting up your PKI in the US or EU regions.

- You can set up your whole trust chain (root CA and issuing CA) in the same region.
- Entrust PKIaaS does not support cross-region trust chains; you cannot use a root CA from another region to sign an issuing CA.

Rate limits

PKIaaS has two tiers of quotas based on your certificate inventory.

Quota	Purchased certificates
Standard quota	Less than 1 million
Premium quota	1 million or more

To protect against burst requests and prevent abuse, PKIaaS enforces a request rate limit based on **10-second** intervals.

Capability	Standard quota	Premium quota
Certificate creation	100 requests/10 seconds	1000 requests/10 seconds
OCSP	100 requests/10 seconds	1000 requests/10 seconds
CRL	100 requests/10 seconds	1000 requests/10 seconds
All others	100 requests/10 seconds	1000 requests/10 seconds

If the number of requests exceeds the allowed rate limit:

- The API access is temporarily blocked
- All requests return a 429 HTTP status code with a "TooManyRequests" error message.

Certificate issuance capping

When the number of active certificates reaches the number of PKIaaS certificates purchased for your account, PKIaaS blocks your account from issuing additional certificates. To issue more PKIaaS certificates, you can either:

- Revoke some of the active certificates.
- Contact your sales representative to purchase more certificates.

Compliance

The Entrust corporation and the PKIaaS solution comply with the following certifications.

- Entrust headquarters certifications
- Entrust PKIaaS data center certifications

Entrust headquarters certifications

The Entrust headquarters comply with the following ISO certifications at an enterprise-wide level.

- ISO 27001 (Information Security Management Systems)
- ISO 27701 (Privacy Information Management Systems)
- ISO 9001 (Quality Management Systems)
- ISO 14001 (Environmental Management Systems)

For details on these certifications, check:

- https://www.entrust.com/legal-compliance/iso-certifications
- https://www.entrust.com/legal-compliance/security

Entrust PKIaaS data center certifications

The Entrust PKIaaS solution is hosted by reputable data centers following the best security practices and complying with security and privacy certifications, including but not limited to:

- Type 1 Attestation HIPAA/HITECH
- SOC2 Type 2

- SOC3
- ISO 27001
- HITRUST
- PCI-DSS

Definitions

See below for a definition of the main PKIaaS-related concepts.

- Agent
- Applicant
- Activation data
- Agreement
- Certificate
- Certificate authority
- Certificate authority certificate
- Certificate profile
- Certificate revocation
- Certificate Revocation List
- Certificate Signing Certificate
- Certification Practice Statement
- Cryptographic Module
- Customer
- Digital signature
- Distinguished Name
- Key pair
- Public cloud
- Object identifier
- Online Certificate Status Protocol
- OCSP responder
- Partition
- PKI certificate
- Public Key Cryptography
- Public Key Infrastructure
- Region
- Registration Authority
- Relying party
- Repository
- Request for comments
- Subject
- Subject Alternative Name
- Subscriber
- Subscription
- Trusted role
- Validity period
- X.500
- X.509

Agent

An agent is a lightweight, stateless virtual machine deployed in your local environment for Automating WSTEP enrollment. Since Entrust PKIaaS is cloudâ□□hosted, the agent provides the required local network presence without requiring the CA itself to be onâ□□premises.

Applicant

An applicant is a person, entity, or organization applying for the issuance or renewal of a certificate.

Activation data

Activation data are values, other than keys, that are required to operate cryptographic modules and that need to be protected â□□ for example:

- PIN
- passphrases
- manually-held key share

Agreement

An agreement is a legally binding contract for PKIaaS comprising:

- The PKIaaS terms of use.
- The PKIaaS schedule.
- The Entrust General Terms and Conditions provided with the PKIaaS Schedule at https://www.entrust.com/-/media/documentation/licensingandagreements/certificate-solutions-general-terms.pdf
- An order for PKIaaS as defined in the General Terms.

Certificate

A certificate is a digital document issued by the CA that, at a minimum, meets the following:

- Identifies the CA issuing it.
- Names or otherwise identifies a Subject.
- Contains a Public Key of a Key Pair.
- Identifies its Operational Period.
- Contains a serial number and is digitally signed by a CA.

Certificate authority

A Certificate Authority (CA), or simply *Authority*, is a trusted entity that issues, manages, and revokes certificates. See below for the supported types.

CA type	Own certificate	Certified entities
Root	Self-signed	Intermediate or issuing subordinate CA

CA type	Own certificate	Certified entities
Intermediate	Signed by a root or intermediate subordinate CA	Intermediate or issuing subordinate CA
Issuing	Signed by a root or intermediate subordinate CA	End-entities (like servers, clients, or software applications)

Certificate authority certificate

A certificate authority certificate is a digital document that verifies the authenticity of the public key owned by a certificate authority. This certificate is essential because it allows the CA to securely issue, sign, and validate other digital certificates.

Certificate profile

A certificate profile is a set of properties for the certificates issued by a CA – for example:

- Certificate extensions like the key usage
- The supported key and signature algorithms

For a CA to issue a certificate, the certificate request must indicate a certificate profile enabled in the CA.

ℹ See Authority certificate profiles and Subscriber certificate profiles for a list of the default profiles.

Certificate revocation

Certificate revocation is the permanent invalidation of a certificate from a specific time onward. Revocation includes:

- Listing the certificate in a CRL.
- Preventing users from accessing the certificate once connected to the central infrastructure.

Certificate Revocation List

A Certificate Revocation List (CRL) is a time-stamped list of the serial numbers of certificates revoked before their expiration.

Certificate Signing Certificate

A Certificate Signing Certificate is a digital certificate used by a Certificate Authority (CA) to sign other certificates.

Certification Practice Statement

The Certification Practice Statement (CPS) states the practices for a CA to issue, manage, revoke, renew, or re-key certificates.

Cryptographic Module

A Cryptographic Module is a software, device, or utility for:

- Generating key pairs,
- Storing cryptographic information.
- Performing cryptographic functions.

Customer

The customer is the entity that has entered into a PKIaaS Agreement with Entrust.

Digital signature

A digital signature is the transformation of an electronic record by one person using private and public key cryptography so that another person having the corresponding public key can determine whether:

- The record transformation was created using the private key corresponding to the public key.
- The record has been altered since the transformation was made.

Distinguished Name

A Distinguished Name (DN) is a unique identifier for locating a subject in an ITU/CCITT X.500 directory. Entrust PKIaaS has no restriction on distinguished names per certificate profile, and all certificate profiles support the following identifiers.

Alias	OID
`CN`, `CommonName`	2.5.4.3
`SN`, `SurName`	2.5.4.4
`SERIALNUMBER`, `DeviceSerialNumber`	2.5.4.5
`C`, `Country`	2.5.4.6
`L`, `Locality`	2.5.4.7
`ST`, `S`, `State`	2.5.4.8
`STREET`, `StreetAddress`	2.5.4.9
`O`, `Org`, `Organization`	2.5.4.10
`OU`, `OrganizationalUnit`, `OrganizationUnit`, `OrgUnit`	2.5.4.11
`T`, `Title`	2.5.4.12
`BUSINESSCATEGORY`	2.5.4.15
`POSTALCODE`	2.5.4.17
`givenName G`	2.5.4.42
`I`, `Initials`	2.5.4.43
`ORGANIZATIONIDENTIFIER`	2.5.4.97

Alias	OID
`UID`	0.9.2342.19200300.100.1.1
`DC` `DomainComponent`	0.9.2342.19200300.100.1.25
`Email`, `E`	1.2.840.113549.1.9.1
`unstructuredName`	1.2.840.113549.1.9.2
`unstructuredAddress`	1.2.840.113549.1.9.8
`JurisdictionOfIncorporationLocalityName`	1.3.6.1.4.1.311.60.2.1.1
`JurisdictionOfIncorporationStateOrProvinceName`	1.3.6.1.4.1.311.60.2.1.2
`JurisdictionOfIncorporationCountryName`	1.3.6.1.4.1.311.60.2.1.3
`TrademarkOfficeName`	1.3.6.1.4.1.53087.1.2
`TrademarkCountryOrRegionName`	1.3.6.1.4.1.53087.1.3
`TrademarkRegistration`	1.3.6.1.4.1.53087.1.4
`LegalEntityIdentifier`	1.3.6.1.4.1.53087.1.5
`WordMark`	1.3.6.1.4.1.53087.1.6
`MarkType`	1.3.6.1.4.1.53087.1.13
`StatuteCountryName`	1.3.6.1.4.1.53087.3.2
`StatuteStateOrProvinceName`	1.3.6.1.4.1.53087.3.3
`StatuteLocalityName`	1.3.6.1.4.1.53087.3.4
`StatuteCitation`	1.3.6.1.4.1.53087.3.5
`StatuteURL`	1.3.6.1.4.1.53087.3.6

Key pair

A key pair comprises two mathematically related cryptographic keys with the following properties.

- A message encrypted with one key can only be decrypted with the other.
- Even knowing one key, it is believed to be computationally infeasible to discover the other key.

These keys are referred to as the **private key** and the **public key**, with the following uses.

Key	Description	Sign	Verify signature	Encrypt	Decrypt
Private	Sensitive key protected by the subject and kept secret	✓	✗	✗	✓
Public	Non-sensitive key disclosed in the certificate	✗	✓	✓	✗

Public cloud

The public cloud is a collection of computing services offered by third-party providers over the public Internet.

Object identifier

An Object Identifier (OID) is a unique alphanumeric identifier registered under the ISO registration standard to reference a specific object or object class. In this document, OIDs uniquely identify certificates and cryptographic algorithms.

Online Certificate Status Protocol

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of a digital certificate. Unlike a Certificate Revocation List (CRL), which requires downloading and checking a potentially large list of revoked certificates, OCSP allows validating the status of a certificate in real time.

OCSP responder

An OCSP responder is a service that responds to certificate status requests with one of three responses.

- Valid
- Invalid
- Unknown

Partition

A partition is a dedicated and secure environment within the PKIaaS platform for a customer to manage and run a PKI. Each partition ensures the customer's data, operations, and resources are separate and protected while supporting scalability and customization.

To create a partition, assign your Subscription to a Region.

PKI certificate

A PKI certificate is a certificate issued according to the PKIaaS Certification Practice Statement.

Public Key Cryptography

Public Key Cryptography, also known as *asymmetric cryptography*, is a type of cryptography that uses a Key pair rather than a single key to secure data authentication and confidentiality.

Public Key Infrastructure

A Public Key Infrastructure (PKI) comprises the architecture, technology, practices, and procedures supporting a security system that uses certificates and public key cryptography.

Region

Each Entrust PKIaaS region defines:

- A legal boundary for:
  - Regulatory requirements
  - Jurisdiction
- A physical location for:
  - Performing cryptographic operations
  - Storing private keys
  - Enforcing dataâ□□residency requirements

Typically, you choose a region based on:

- Where regulated data is required to reside
- The geographic location of your users and devices
- Legal and jurisdictional requirements for protecting cryptographic keys
- Disasterâ□□recovery, auditing, and compliance considerations

Assigning your Subscription to a region results in a Partition.

Registration Authority

A Registration Authority (RA) is an individual, organization, or process responsible for verifying the identity of a subscriber.

Relying party

A relying party is an individual or legal entity that relies on a certificate or any digital signature verified using that certificate.

Repository

A repository is an online system for storing and retrieving certificates and other information relevant to certificates, including certificate validity or revocation information.

Request for comments

A Request for Comments (RFC) is a document series for communicating information about the Internet.

- The IAB (Internet Architecture Board) designates some RFCs as Internet standards.
- Most RFCs document protocol specifications like Telnet and FTP.

Subject

The subject is the individual, legal entity, organization, or device identified in a certificate. The subject holds the private key corresponding to the public Key in the certificate.

Subject Alternative Name

A Subject Alternative Name (SAN) is an X.509 digital certificate extension that allows multiple identities (like domain names, IP addresses, email addresses, or URIs) to be associated with a single certificate. This feature is particularly useful for securing multiple domains or subdomains with a single SSL/TLS certificate, providing flexibility and reducing the need for multiple certificates.

Subscriber

The subscriber is the person, legal entity, or organization that has applied for and has been issued a certificate. Before the identity verification and issuance of a certificate, a subscriber is an applicant.

Subscription

A subscription is a prepaid inventory of PKI products purchased by the customer. To utilize this inventory, you must convert your subscription into a Partition by assigning it to a Region.

Trusted role

A trusted role is a role for employees or contractors with authorized access to or control over PKIaaS.

Validity period

The validity period of a certificate is the intended term of validity of a certificate. This period begins with the later of the following dates:

- The date of issuance stated in the "Issued On" certificate field.
- The date stated in the "Valid From" or "Activation" certificate fields.

The period ends with the earlier of the two dates:

- The expiration date stated in the "Valid To" or "Expiry" certificate fields.
- The revocation date asserted in the CRL. This CRL is published in the distribution point within the certificate.

X.500

X.500 is a series of computer networking standards covering electronic directory services, like:

- Directory access protocol (DAP)
- Directory system protocol (DSP)
- Directory information shadowing protocol (DISP)
- Directory operational bindings management protocol (DOP)

X.509

X.509 is a standard of the ITU-T (Technical committee of the International Telecommunication Union) for public key certificates and certification path validation.

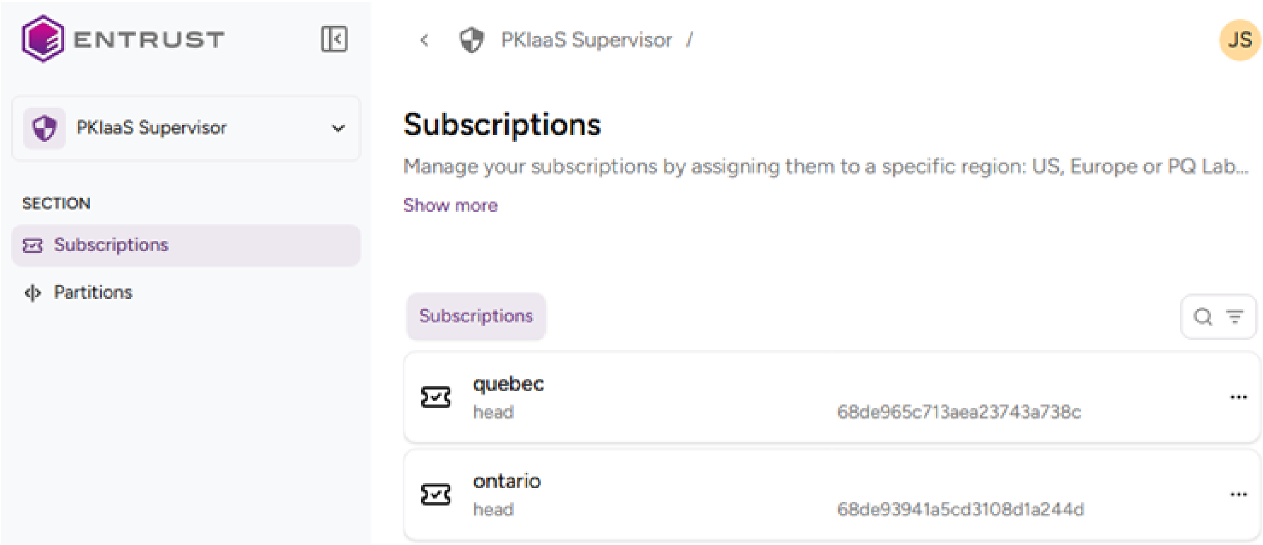
Checking your subscriptions

Log into the PKIaaS Supervisor interface to browse the details of your purchased subscriptions.

ℹ As explained in Definitions, a subscription is a prepaid inventory of PKI products purchased by the customer.

To browse subscriptions:

1. Open the https://super.pkiaas.entrust.com URL of the supervisor interface. Supported browsers are:
    - Apple Safari
    - Google Chrome
    - Mozilla Firefox
2. Authenticate using your username and password.
3. Select your preferred method to confirm the authentication request.
    - Entrust Identity mobile application
    - Token authentication
    - OTP authentication
4. Confirm the authentication request to log into the user interface.

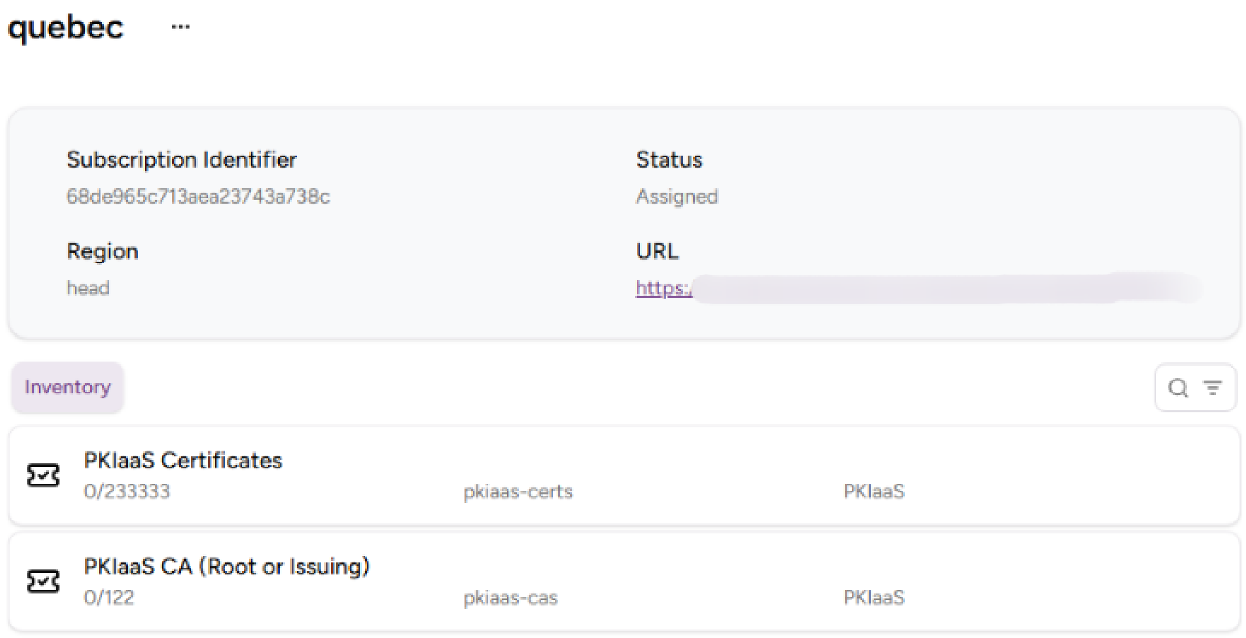


Subscriptions

Manage your subscriptions by assigning them to a specific region: US, Europe or PQ Lab...

quebec head	68de965c713aea23743a738c
ontario head	68de93941a5cd3108d1a244d

5. Click **Subscriptions** in the sidebar.
6. Click the name of a subscription to inspect the following subscription details.
    - Subscription Identifier
    - Status
    - Region
    - URL
    - Inventory



quebec ···

Subscription Identifier
68de965c713aea23743a738c

Status
Assigned

Region
head

URL
https:/[redacted]

Inventory

PKIaaS Certificates
0/233333 pkiaas-certs PKIaaS

PKIaaS CA (Root or Issuing)
0/122 pkiaas-cas PKIaaS

Subscription Identifier

The internal identifier of the subscription.

Status

The subscription status:

- **Assigned**, if the subscription has been assigned to a partition as explained in Assigning subscriptions to partitions.
- **Unassigned** otherwise.

Region

The region selected when assigning the subscription to a partition.

ℹ See Definitions for considerations on selecting a region.

URL

The URL for managing the CAs and certificates of the partition as explained in Accessing your partitions.

Inventory

The number of **PKIaaS Certificates** section displays the number of subscription certificates in, `<issued>/<purchased>` format. Where:

- `<purchased>` is the maximum number of certificates allowed for your subscription.
- `<issued>` is the number of certificates already issued.

ℹ This inventory does not include the certificate signing certificates issued when creating a certificate authority.

The **PKIaaS CA (Root or Issuing)** section displays the number of certificate authorities, `<active>/<purchased>` format. Where:

- `<purchased>` is the maximum number of certificate authorities allowed for your subscription.
- `<active>` is the number of active certificate authorities.

⚠ After Deleting a CA, it takes 24 hours for the CA to be removed from the total number of active CAs.

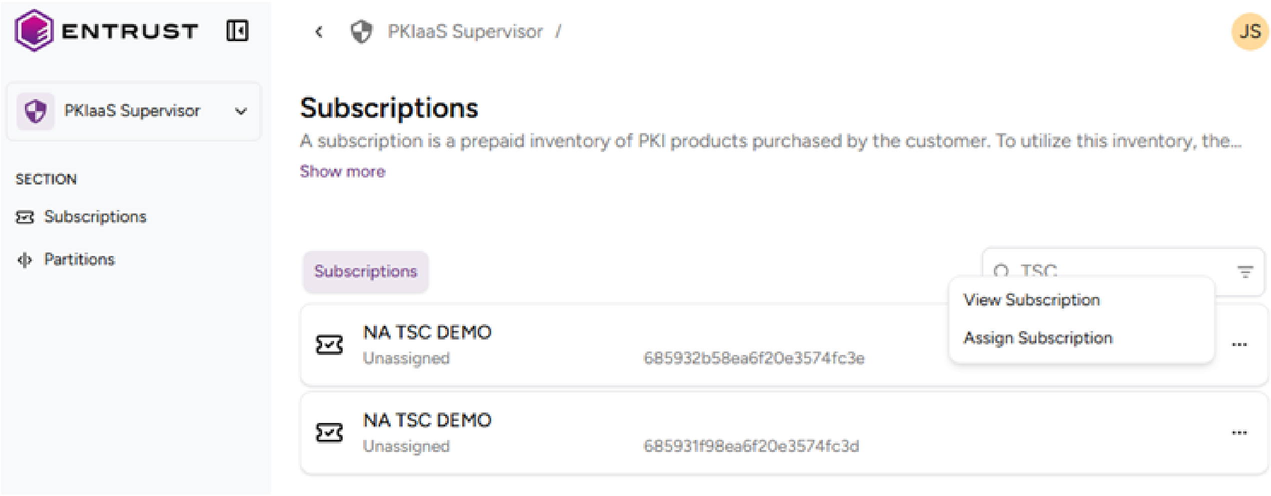
Assigning subscriptions to partitions

Log into the PKIaaS Supervisor interface to assign your purchased subscriptions to a partition.

ℹ As explained in Definitions, a *partition* is a dedicated and secure environment within the PKIaaS platform for a customer to manage and run a PKI.

To assign a subscription:

1. Open the https://super.pkiaas.entrust.com URL of the supervisor interface. Supported browsers are:
   - Apple Safari
   - Google Chrome
   - Mozilla Firefox
2. Authenticate using your username and password.
3. Select your preferred method to confirm the authentication request.
   - Entrust Identity mobile application
   - Token authentication
   - OTP authentication
4. Confirm the authentication request to log into the user interface.
5. Click **Subscriptions** in the sidebar.



Subscriptions

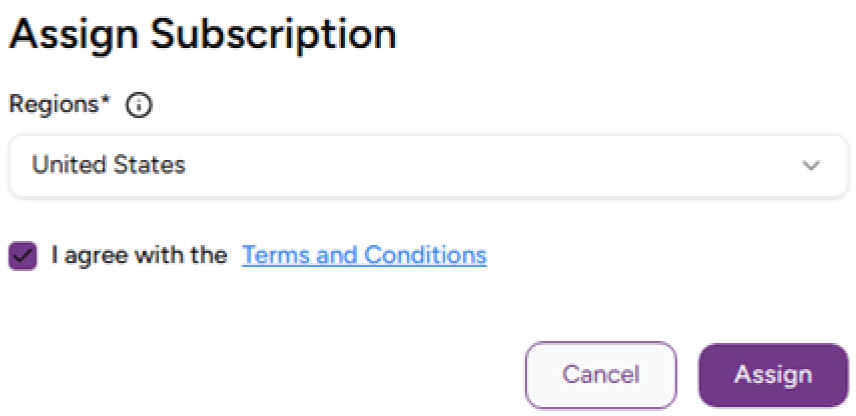
A subscription is a prepaid inventory of PKI products purchased by the customer. To utilize this inventory, the...

NA TSC DEMO
Unassigned 685932b58ea6f20e3574fc3e

NA TSC DEMO
Unassigned 685931f98ea6f20e3574fc3d

6. Click the three dots **"..."** to the right of a partition and select **Assign Subscription**.

7. Select a region in the **Assign Subscription** dialog.



Assign Subscription

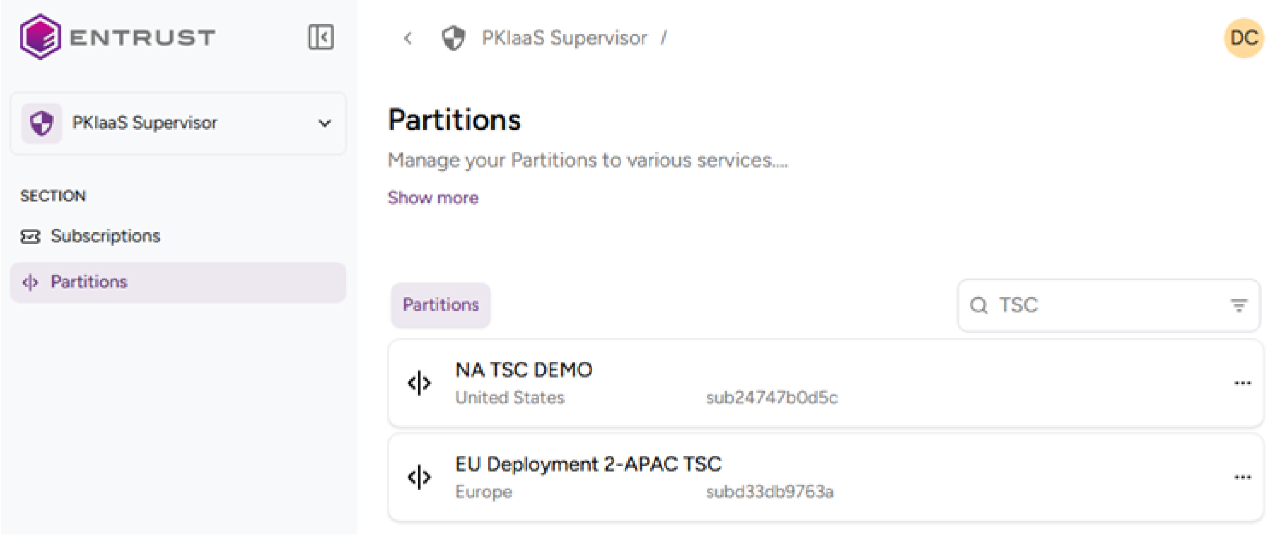
Regions*: United States

☑ I agree with the Terms and Conditions

ℹSee Definitions for considerations on selecting a region.

8. Check the **I agree with the Terms and Conditions** box and click **Assign** to create a partition for the subscription.

9. Click **Partitions** in the sidebar.



Partitions

Manage your Partitions to various services....

Show more

NA TSC DEMO
United States sub24747b0d5c

EU Deployment 2-APAC TSC
Europe subd33db9763a

10. Check the following values of each partition.
    - The label name, which is the same as the assigned subscription.
    - The region selected when assigning the subscription to the partition.
    - The partition internal identifier.

11. Click the name of a partition to manage the partition CAs and certificates in the PKI as a Service user interface.

Accessing your partitions

Log in to the PKI as a Service (PKIaaS) user interface to manage the CAs and certificates of your partitions.

ℹ See Assigning subscriptions to partitions for how to create partitions.

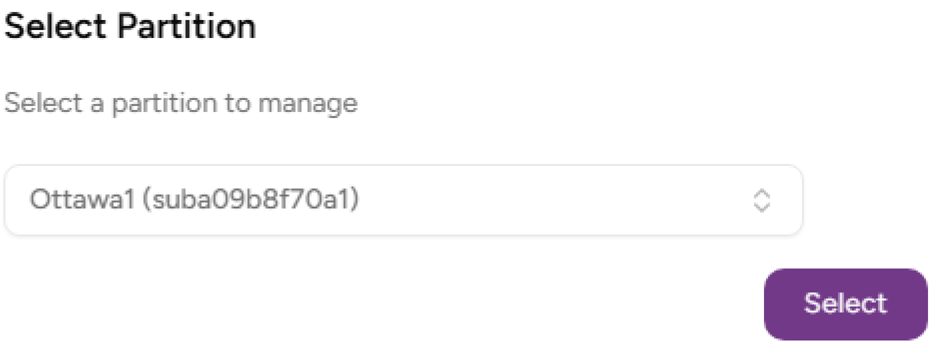
To access a partition:

1. Open one of the supported browsers: Apple Safari, Google Chrome, or Mozilla Firefox.
2. Navigate to the URL of the PKIaaS interface for your region.

Region	URL
United States	https://ui.pkiaas.entrust.com
Europe	https://ui.eu.pkiaas.entrust.com
Post-quantum lab	https://ui.pqlab.pkiaas.entrust.com

⚠ Make sure the URL is whitelisted on your network firewall to avoid connectivity issues.

3. Authenticate using your username and password.
4. Select your preferred method to confirm the authentication request.
   - Entrust Identity mobile application
   - Token authentication
   - OTP authentication
5. Confirm the authentication request to log into the user interface.
6. Select a partition in the **Select Partition** dialog.

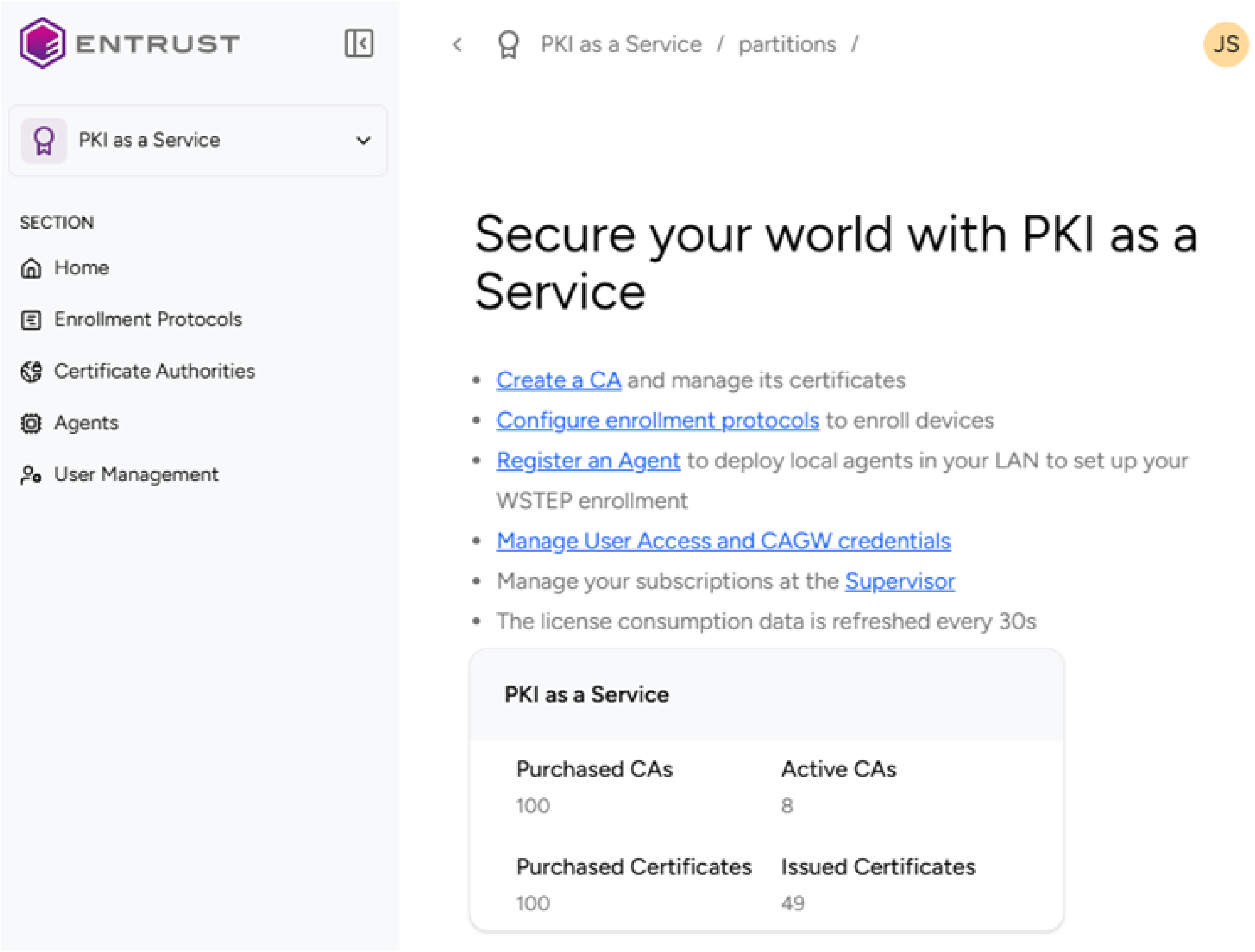


Select Partition

Select a partition to manage

Ottawa1 (suba09b8f70a1)

7. Click **Select** to display the welcome page.



Secure your world with PKI as a Service

- Create a CA and manage its certificates
- Configure enrollment protocols to enroll devices
- Register an Agent to deploy local agents in your LAN to set up your WSTEP enrollment
- Manage User Access and CAGW credentials
- Manage your subscriptions at the Supervisor
- The license consumption data is refreshed every 30s

PKI as a Service

Purchased CAs	Active CAs
100	8
Purchased Certificates	**Issued Certificates**
100	49

8. Under **Secure your world with PKI as a Service**, see a list of the main steps to start up your PKI, with links to the corresponding UI sections.

9. In the **PKI as a Service** box, check the certificate and CAs inventory values already described in Checking your subscriptions.

Managing users

See below for how to manage PKIaaS users.

- Inviting users
- Managing roles
- Role permissions

---

i See Managing CA Gateway credentials for how to create user credentials for the CA Gateway API provided by PKIaaS.

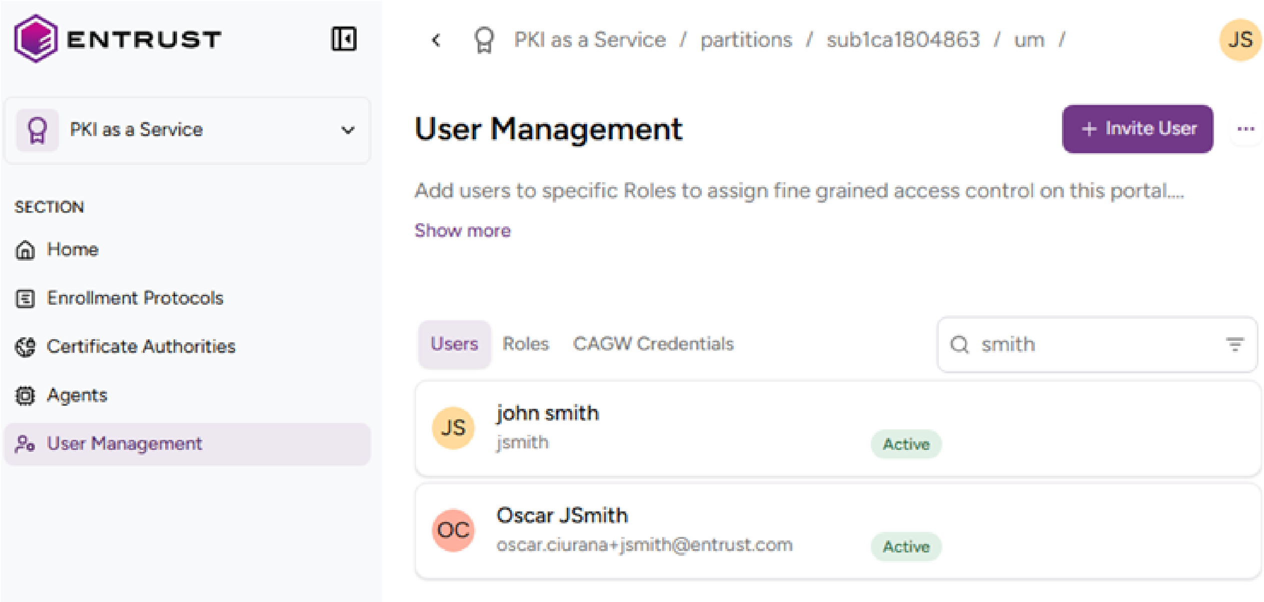
Inviting users

See below for how to add PKIaaS users by sending invitation emails.

To invite a user:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS user interface as a member of the Owners team.

2. Select **User Management** in the sidebar.



3. Click the plus **+** icon to the right of the **Users** tab.

4. Fill in the **Invite User** form fields.

   - The **Email** to which to send the invite.
   - The **First Name** and **Last Name** as they will be displayed in the user interface.

5. Click **Invite** to send an email that includes a link to confirm the invitation and generate PKIaaS user credentials.

---

i See Managing roles for how to grant permissions to users by granting them roles.

Managing roles

See below for how to grant or remove roles from users.

- Adding users to a role
- Removing users from a role

i See Role permissions for the permissions granted by each role.

Adding users to a role

See below for how to add a user to a role.

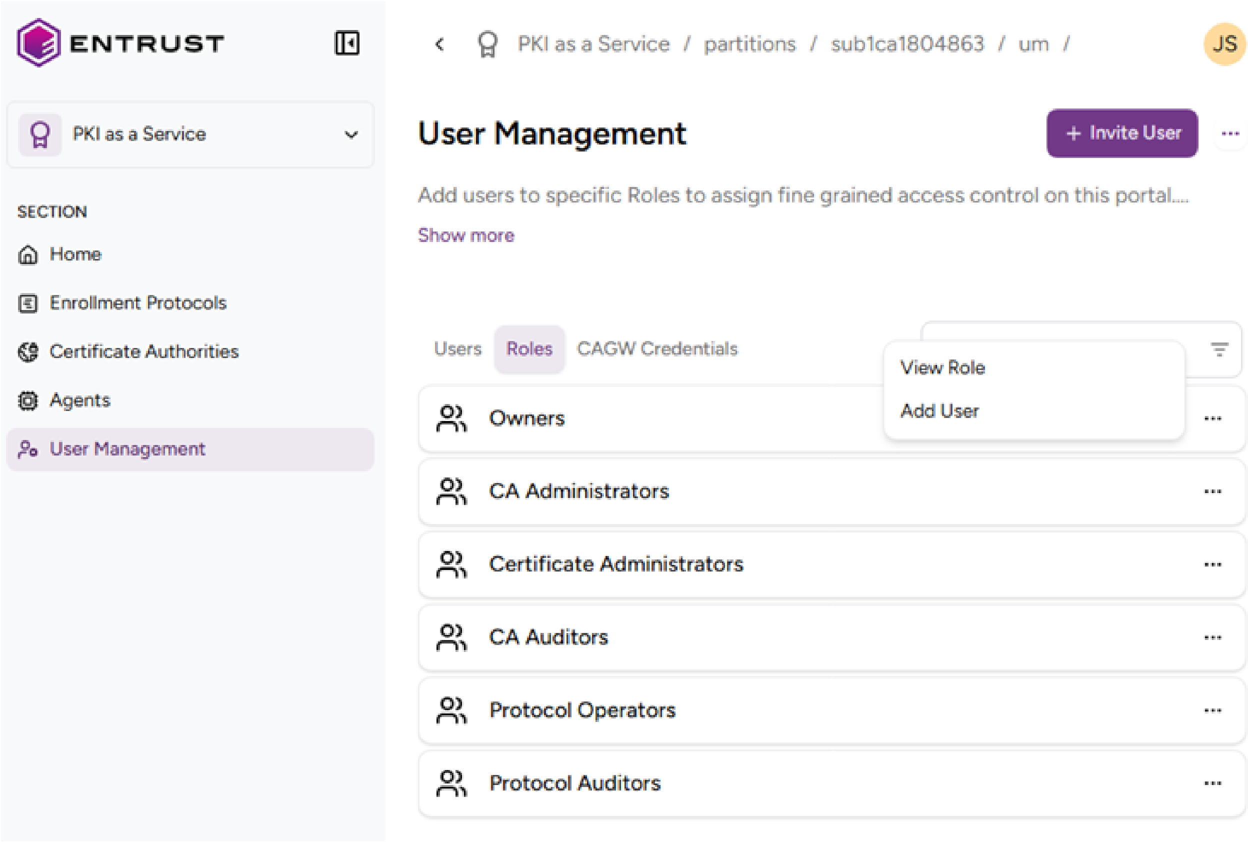
To add a user to a role:

1. Follow the steps described in Accessing your partitions to log in to the PKIaaS interface.

2. Authenticate as a user with the Owners role.

3. Select **User Management** in the sidebar.

4. Select the **Role** tab.



Add users to specific Roles to assign fine grained access control on this portal....

5. Click **ACTIONS > Add user** for a role.

6. Select the user name from a list of invited users.

7. Click **Add**.

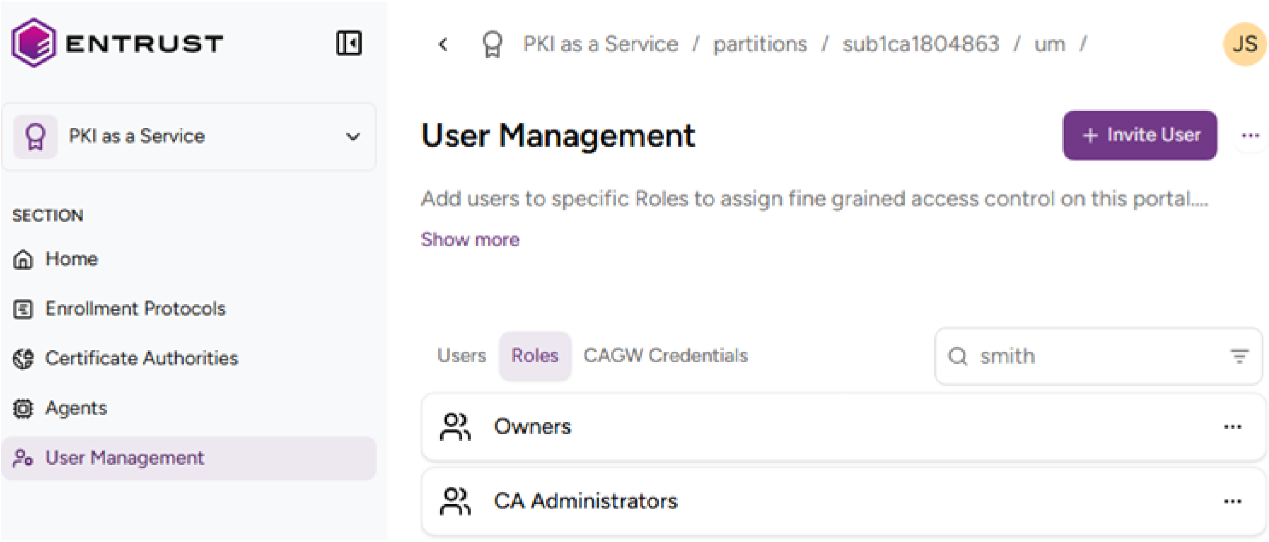
Removing users from a role

See below for how to remove a user from a role.

To remove a user from a role:

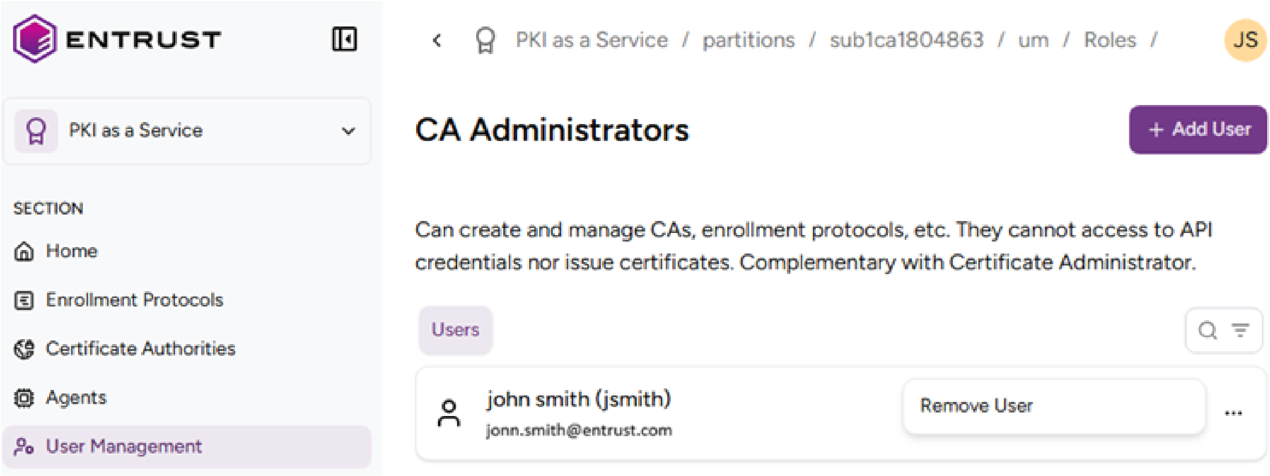
1. Follow the steps described in Accessing your partitions to log into the PKIaaS user interface as a user with the Owners role.

2. Click **User Management** in the sidebar.



Add users to specific Roles to assign fine grained access control on this portal....

3. Click the name of a role to display the list of members.



Can create and manage CAs, enrollment protocols, etc. They cannot access to API credentials nor issue certificates. Complementary with Certificate Administrator.

john smith (jsmith)
jonn.smith@entrust.com

4. Click **ACTIONS** > **Remove User** for the user you want to remove.

5. Click **Remove** in the **Remove User** confirmation dialog.

Role permissions

See below for the list of user roles and the permissions granted by each one.

- Owners
- CA Administrators
- Certificate Administrators
- CA Auditors
- Protocol Operators
- Protocol Auditors

Owners

Members of the **Owners** role can perform all supported PKIaaS operations.

- Subscription management
- User management
- CA management

- Certificate management
- Enrollment management
- CA Gateway management

Subscription management

Members of the **Owners** role can perform all subscription management operations.

Operation	Authorized
Checking your subscriptions	✓
Assigning subscriptions to partitions	✓

User management

Members of the **Owners** role can perform all user management operations.

Operation	Authorized
Inviting users	✓
Managing roles	✓

CA management

Members of the **Owners** role can perform all CA management operations.

Operation	Authorized
Browsing CAs	✓
Creating a root CA	✓
Creating an intermediate subordinate CA	✓
Creating an issuing subordinate CA	✓
Importing an external root CA	✓
Downloading a CA certificate	✓
Selecting CA profiles	✓
Deleting a CA	✓

Certificate management

Members of the **Owners** role can perform all certificate management operations.

Operation	Authorized
Browsing certificates	✓

Operation	Authorized
Issuing a certificate from CSR	✓
Issuing a certificate in a PKCS #12	✓
Changing the certificate status	✓
Downloading certificates	✓

Enrollment management

Members of the **Owners** role can perform all the enrollment management operations.

Operation	Authorized
Configuring ACME in PKIaaS	✓
Configuring Intune in PKIaaS	✓
Configuring Jamf in PKIaaS	✓
Configuring Workspace ONE in PKIaaS	✓
Configuring Ivanti in PKIaaS	✓
Configuring MDM IBM MaaS360 in PKIaaS	✓

CA Gateway management

Members of the **Owners** role can perform the operation described in Managing CA Gateway credentials.

CA Administrators

Members of the **CA Administrators** role can perform the following operations.

- Subscription management
- User management
- CA management
- Certificate management
- Enrollment management
- CA Gateway management

Subscription management

Members of the **CA Administrators** role cannot manage subscriptions.

Operation	Authorized
Checking your subscriptions	✗
Assigning subscriptions to partitions	✗

User management

Members of the **CA Administrators** role cannot manage users.

Operation	Authorized
Inviting users	✗
Managing roles	✗

CA management

Members of the **CA Administrators** role can perform all the CA management operations.

Operation	Authorized
Browsing CAs	✓
Creating a root CA	✓
Creating an intermediate subordinate CA	✓
Creating an issuing subordinate CA	✓
Importing an external root CA	✓
Downloading a CA certificate	✓
Selecting CA profiles	✓
Deleting a CA	✓

Certificate management

Members of the **CA Administrators** role can perform the following certificate management operations.

Operation	Authorized
Browsing certificates	✓
Issuing a certificate from CSR	✗
Issuing a certificate in a PKCS #12	✗
Changing the certificate status	✗
Downloading certificates	✓

Enrollment management

Members of the **CA Administrators** role can perform all the enrollment management operations.

Operation	Authorized
Configuring ACME in PKIaaS	✓
Configuring Intune in PKIaaS	✓

Operation	Authorized
Configuring Jamf in PKIaaS	✓
Configuring Workspace ONE in PKIaaS	✓
Configuring Ivanti in PKIaaS	✓
Configuring MDM IBM MaaS360 in PKIaaS	✓

CA Gateway management

Members of the **CA Administrators** role can perform the operation described in Managing CA Gateway credentials.

Certificate Administrators

Members of the **Certificate Administrators** role can perform the following operations.

- Subscription management
- User management
- CA management
- Certificate management
- Enrollment management
- CA Gateway management

Subscription management

Members of the **Certificate Administrators** role cannot manage subscriptions.

Operation	Authorized
Checking your subscriptions	✗
Assigning subscriptions to partitions	✗

User management

Members of the **Certificate Administrators** role cannot manage users.

Operation	Authorized
Inviting users	✗
Managing roles	✗

CA management

Members of the **Certificate Administrators** role can perform the following CA management operations.

Operation	Authorized

Operation	Authorized
Browsing CAs	✓
Creating a root CA	✗
Creating an intermediate subordinate CA	✗
Creating an issuing subordinate CA	✗
Importing an external root CA	✗
Downloading a CA certificate	✓
Selecting CA profiles	✗
Deleting a CA	✗

Certificate management

Members of the **Certificate Administrators** role can perform all certificate management operations.

Operation	Authorized
Browsing certificates	✓
Issuing a certificate from CSR	✓
Issuing a certificate in a PKCS #12	✓
Changing the certificate status	✓
Downloading certificates	✓

Enrollment management

Members of the **Certificate Administrators** role can only inspect the enrollment configuration.

Operation	Authorized
Configuring ACME in PKIaaS	Read-only
Configuring Intune in PKIaaS	Read-only
Configuring Jamf in PKIaaS	Read-only
Configuring Workspace ONE in PKIaaS	Read-only
Configuring Ivanti in PKIaaS	Read-only
Configuring MDM IBM MaaS360 in PKIaaS	Read-only

CA Gateway management

Members of the **Certificate Administrators** role cannot perform the operation described in Managing CA Gateway credentials.

CA Auditors

Members of the **CA Auditors** role can perform the following operations.

- Subscription management
- User management
- CA management
- Certificate management
- Enrollment management
- CA Gateway management

Subscription management

Members of the **CA Auditors** role cannot manage subscriptions.

Operation	Authorized
Checking your subscriptions	✗
Assigning subscriptions to partitions	✗

User management

Members of the **CA Auditors** role cannot manage users.

Operation	Authorized
Inviting users	✗
Managing roles	✗

CA management

Members of the **CA Auditors** role can perform the following CA management operations.

Operation	Authorized
Browsing CAs	✓
Creating a root CA	✗
Creating an intermediate subordinate CA	✗
Creating an issuing subordinate CA	✗
Importing an external root CA	✗
Downloading a CA certificate	✗
Selecting CA profiles	✗
Deleting a CA	✗

Certificate management

Members of the **CA Auditors** role can perform the following certificate management operations.

Operation	Authorized
Browsing certificates	✓
Issuing a certificate from CSR	✗
Issuing a certificate in a PKCS #12	✗
Changing the certificate status	✗
Downloading certificates	✓

Enrollment management

Members of the **CA Auditors** role can only inspect the enrollment configuration.

Operation	Authorized
Configuring ACME in PKIaaS	Read-only
Configuring Intune in PKIaaS	Read-only
Configuring Jamf in PKIaaS	Read-only
Configuring Workspace ONE in PKIaaS	Read-only
Configuring Ivanti in PKIaaS	Read-only
Configuring MDM IBM MaaS360 in PKIaaS	Read-only

CA Gateway management

Members of the **CA Auditors** role cannot perform the operation described in Managing CA Gateway credentials.

Protocol Operators

Members of the **Protocol Operators** role can perform the following operations.

- Subscription management
- User management
- CA management
- Certificate management
- Enrollment management
- CA Gateway management

Subscription management

Members of the **Protocol Operators** role cannot manage subscriptions.

Operation	Authorized

Operation	Authorized
Checking your subscriptions	✕
Assigning subscriptions to partitions	✕

User management

Members of the **Protocol Operators** role cannot manage users.

Operation	Authorized
Inviting users	✕
Managing roles	✕

CA management

Members of the **Protocol Operators** role can perform the following CA management operations.

Operation	Authorized
Browsing CAs	✓
Creating a root CA	✕
Creating an intermediate subordinate CA	✕
Creating an issuing subordinate CA	✕
Importing an external root CA	✕
Downloading a CA certificate	✕
Selecting CA profiles	✕
Deleting a CA	✕

Certificate management

Members of the **Protocol Operators** role can perform all certificate management operations.

Operation	Authorized
Browsing certificates	✓
Issuing a certificate from CSR	✕
Issuing a certificate in a PKCS #12	✕
Changing the certificate status	✕
Downloading certificates	✓

Enrollment management

Members of the **Protocol Operators** role can only inspect the enrollment configuration.

Operation	Authorized
Configuring ACME in PKIaaS	✓
Configuring Intune in PKIaaS	✓
Configuring Jamf in PKIaaS	✓
Configuring Workspace ONE in PKIaaS	✓
Configuring Ivanti in PKIaaS	✓
Configuring MDM IBM MaaS360 in PKIaaS	✓

CA Gateway management

Members of the **Protocol Operators** role cannot perform the operation described in Managing CA Gateway credentials.

Protocol Auditors

Members of the **Protocol Auditors** role can perform the following operations.

- Subscription management
- User management
- CA management
- Certificate management
- Enrollment management
- CA Gateway management

Subscription management

Members of the **Protocol Auditors** role cannot manage subscriptions.

Operation	Authorized
Checking your subscriptions	✗
Assigning subscriptions to partitions	✗

User management

Members of the **Protocol Auditors** role cannot manage users.

Operation	Authorized
Inviting users	✗
Managing roles	✗

CA management

Members of the **Protocol Auditors** role can perform the following CA management operations.

Operation	Authorized
Browsing CAs	✓
Creating a root CA	✗
Creating an intermediate subordinate CA	✗
Creating an issuing subordinate CA	✗
Importing an external root CA	✗
Downloading a CA certificate	✗
Selecting CA profiles	✗
Deleting a CA	✗

Certificate management

Members of the **Protocol Auditors** role can perform the following certificate management operations.

Operation	Authorized
Browsing certificates	✓
Issuing a certificate from CSR	✗
Issuing a certificate in a PKCS #12	✗
Changing the certificate status	✗
Downloading certificates	✓

Enrollment management

Members of the **Protocol Auditors** role can only inspect the enrollment configuration.

Operation	Authorized
Configuring ACME in PKIaaS	Read-only
Configuring Intune in PKIaaS	Read-only
Configuring Jamf in PKIaaS	Read-only
Configuring Workspace ONE in PKIaaS	Read-only
Configuring Ivanti in PKIaaS	Read-only
Configuring MDM IBM MaaS360 in PKIaaS	Read-only

CA Gateway management

Members of the **Protocol Auditors** role cannot perform the operation described in Managing CA Gateway credentials.

Managing certificate profiles

See below for how to browse and create certificate profiles.

- Browsing certificate profiles
- Customizing subscriber profiles

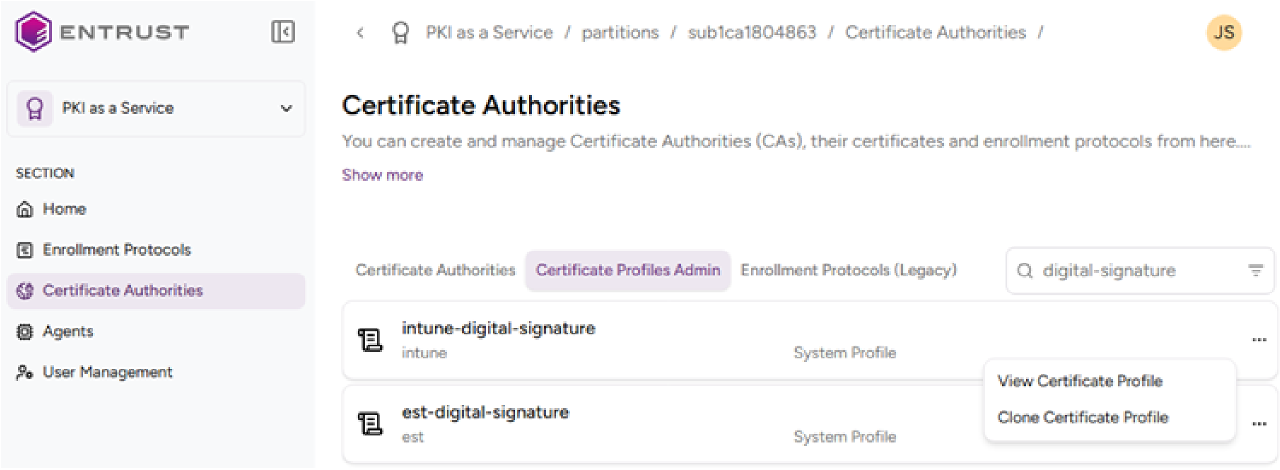
ℹ See Selecting CA profiles for how to assign or unassign certificate profiles to a certificate authority.

Browsing certificate profiles

See below for how to browse certificate profiles.

To browse certificate profiles:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
    - Owners
    - CA Administrators
2. Click **Certificate Authorities** in the sidebar.
3. Click the **Certificate Profiles Admin** tab.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

intune-digital-signature intune	System Profile	...
est-digital-signature est	System Profile	...

4. Browse the list of certificate profiles:
    - A **System profile** is one of the predefined certificate profiles described in Authority certificate profiles and Subscriber certificate profiles.
    - A **Custom profile** is a certificate profile configured by the user as explained in Customizing subscriber profiles.
5. Click the three dots to the right of a profile and select **View Certificate Profile** to display the Certificate profile fields.

Authority certificate profiles

Entrust PKIaaS profiles for issuing authority certificates are organized into the following groups.

- basic
- external
- intermediate
- issuing

issuing

Entrust provides the `basic-ca-subord` profiles for certificate issuing authorities.

- Certificate fields
- Certificate critical extensions
- Certificate non-critical extensions

⚠ This profile is not exposed nor configurable.

Certificate fields

The `basic-ca-subord` profile set the following certificate fields.

Field	basic-ca-subord
Issuer	Customer's online root or issuing CA
Subject	No constraint
Validity period	Less than or equal to 10 years

Certificate critical extensions

The `basic-ca-subord` profile set the following certificate critical extensions.

Extension	Value
Basic Constraints	`cA=True, pathLenConstraint=0`
Extended Key Usage	Never present
Key Usage	`digitalSignature`, `keyCertSign`, `cRLSign`

Certificate non-critical extensions

The `basic-ca-subord` profile set the following non-critical certificate extensions.

Extension	Value
AIA	Supplied when the customer enables OCSP on CA creation

Extension	Value
Authority Key Identifier	Matches the `subjectKeyIdentifier` of the signing certificate
CRL Distribution Points	Always present
OCSP	Never present
Subject Key Identifier	Â«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKeyÂ» as described in RFC 7093 section 2

Subscriber certificate profiles

Entrust PKIaaS profiles for issuing subscriber certificates are organized into the following sets.

- cmp
- codesigning
- esim
- est
- intune
- mdmws
- mobile
- multiuse
- privatessl
- scep
- smartcard
- smime
- v2g
- wstep

ℹ See Definitions for a description of Certificate profile.

wstep

Entrust PKIaaS provides the following Active Directory (WSTEP) certificate profiles.

- `wstep-digital-signature`
- `wstep-digital-signature-key-encipherment`
- `wstep-key-encipherment`
- `wstep-non-repudiation`
- `wstep-non-repudiation-key-encipherment`

These profiles support the following features.

- Use cases
- Key usages

- Request extensions
- Certificate fields
- Certificate extensions
- Distinguished names

Use cases

All Active Directory (WSTEP) certificate profiles support the following use cases.

- CA Gateway API
- PKIaaS gateway
- On-prem Enrollment Gateway

Key usages

See below the Key Usage extension values supported by each WSTEP profile.

Profile	Key Usage
`wstep-digital-signature`	Digital Signature
`wstep-digital-signature-key-encipherment`	Digital Signature, Key Encipherment
`wstep-key-encipherment`	Key Encipherment
`wstep-non-repudiation`	Digital Signature, Non-Repudiation
`wstep-non-repudiation-key-encipherment`	Digital Signature, Non-Repudiation, Key Encipherment

Request extensions

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

Extension name	Extension OID
Application Policies	`1.3.6.1.4.1.311.21.10`
Certificate Policies	`2.5.29.32`
Extended Key Usage	`2.5.29.37`
MSTemplateName	`1.3.6.1.4.1.311.20.2`
MSTemplateOID	`1.3.6.1.4.1.311.21.7`
Smime Capabilities	`1.2.840.113549.1.9.15`
`szOID_NTDS_CA_SECURITY_EXT`	`1.3.6.1.4.1.311.25.2`

Certificate fields

The `azure-firewall-ca-subord` profile sets the following certificate fields.

Field	Value
Issuer	Customer's subordinate issuing CA.
Subject	No constraint
Validity period	Defaults to 1 year if not specified.

Certificate extensions

The Active Directory (WSTEP) certificate profiles set the following certificate extensions.

Extension	Critical	Value
AIA	No	Supplied if the customer enables OCSP when creating the CA
Authority Key Identifier	No	Matches the `subjectKeyIdentifier` of the signing certificate
Basic Constraints	Yes	`cA=False`
CRL Distribution Points	No	Always present
Subject Alternative Name	No	No constraints
Subject Key Identifier	No	Â«The leftmost 160-bits of the SHA-256 hash of the value of the BIT STRING subjectPublicKeyÂ» as described in RFC 7093 section 2

Distinguished names

Entrust PKIaaS has no restriction on Distinguished Names (DNs) per certificate profile. All certificate profiles support the following identifiers.

Alias	OID
`CN`, `CommonName`	`2.5.4.3`
`SN`, `SurName`	`2.5.4.4`
`SERIALNUMBER`, `DeviceSerialNumber`	`2.5.4.5`
`C`, `Country`	`2.5.4.6`
`L`, `Locality`	`2.5.4.7`
`ST`, `S`, `State`	`2.5.4.8`
`STREET`, `StreetAddress`	`2.5.4.9`
`O`, `Org`, `Organization`	`2.5.4.10`

Alias	OID
OU, OrganizationalUnit, OrganizationUnit, OrgUnit	2.5.4.11
T, Title	2.5.4.12
BUSINESSCATEGORY	2.5.4.15
POSTALCODE	2.5.4.17
givenName, G	2.5.4.42
I, Initials	2.5.4.43
ORGANIZATIONIDENTIFIER	2.5.4.97
UID	0.9.2342.19200300.100.1.1
DC, DomainComponent	0.9.2342.19200300.100.1.25
Email, E	1.2.840.113549.1.9.1
unstructuredName	1.2.840.113549.1.9.2
unstructuredAddress	1.2.840.113549.1.9.8
JurisdictionOfIncorporationLocalityName	1.3.6.1.4.1.311.60.2.1.1
JurisdictionOfIncorporationStateOrProvinceName	1.3.6.1.4.1.311.60.2.1.2
JurisdictionOfIncorporationCountryName	1.3.6.1.4.1.311.60.2.1.3
TrademarkOfficeName	1.3.6.1.4.1.53087.1.2
TrademarkCountryOrRegionName	1.3.6.1.4.1.53087.1.3
TrademarkRegistration	1.3.6.1.4.1.53087.1.4
LegalEntityIdentifier	1.3.6.1.4.1.53087.1.5
WordMark	1.3.6.1.4.1.53087.1.6
MarkType	1.3.6.1.4.1.53087.1.13
StatuteCountryName	1.3.6.1.4.1.53087.3.2
StatuteStateOrProvinceName	1.3.6.1.4.1.53087.3.3
StatuteLocalityName	1.3.6.1.4.1.53087.3.4
StatuteCitation	1.3.6.1.4.1.53087.3.5
StatuteURL	1.3.6.1.4.1.53087.3.6

Certificate profile fields

See the table below for a description of the profile configuration fields

ℹ Some fields support both UI and JSON configuration, some do not.

UI field	JSON	Value	Mandatory
Profile ID	--	The unique identifier of the certificate profile, as a string of 2 to 64 characters consisting of lowercase letters and numbers.	Yes
Profile Group	--	The name of the group to which the certificate profile belongs, as a string of 2 to 64 characters consisting of lowercase letters and numbers.	Every profile must be associated with one, and only one, group.
Default CA Types	`allowedCATypes`	The type of certificate authorities the profile supports, as a list of Type identifiers.	Select at least one type.
Validity period	`validity_period`	The validity period for the issued certificates, as a time interval in ISO 8601 format.	Yes
Key Usages	`usages`	The key usages permitted for certificates issued using the profile, as a list of key usage object identifiers. Use the JSON field to add key usages not included in the drop-down list.	Yes
Extended key Usages	`usages`	The extended key usages permitted for certificates issued using the profile, as a list of key usage object identifiers. Use the JSON field to add key usages not included in the drop-down list.	No
--	`allowed_extensions`	The X.509 extensions permitted on request, as a list of the extension object identifiers.	No
--	`ignore_unknown_extensions`	`true` to ignore unknown extensions on request; `false` to reject requests with unknown extensions.	No, defaults to `true`.
--	`ca_constraint`	The basic constraints for the issued certificates, as the sequence described in Section 4.2.1.9 of the RFC 5280.	No

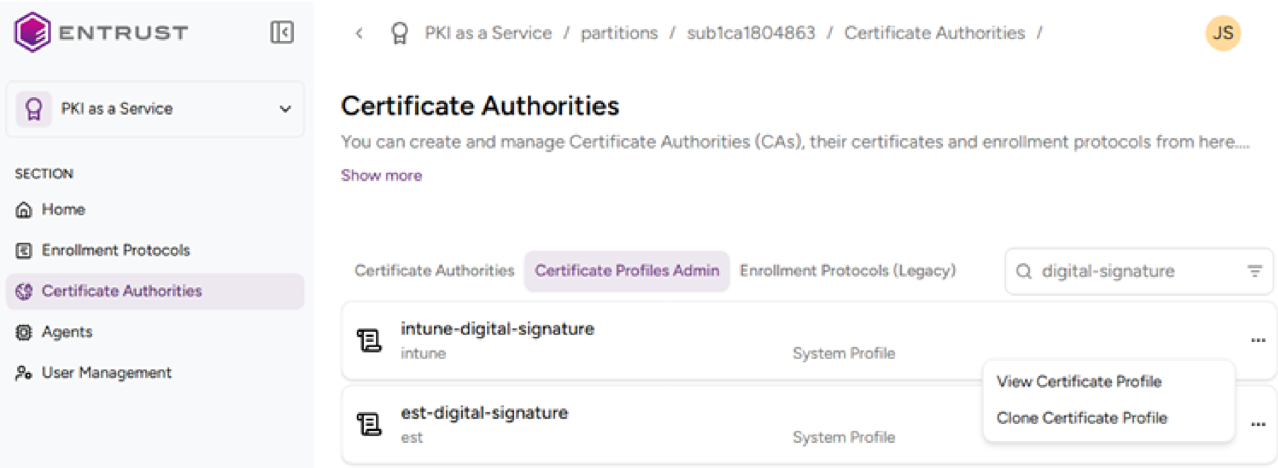
Customizing subscriber profiles

See below for cloning Subscriber certificate profiles to create custom ones.

⚠ Authority certificate profiles cannot be cloned or modified.

To create certificate profiles:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
   - Owners
   - CA Administrators
2. Click **Certificate Authorities** in the sidebar.
3. Click the **Certificate Profiles Admin** tab.



4. Click the three dots to the right of the profile you want to use as a template.
5. Select **Clone Certificate Profile**.
6. In the **Clone Certificate Profile** form, edit the Certificate profile fields. You can:
   - Fill in the UI fields.
   - Toggle the **Edit the Raw Profile Information** switch and edit the profile JSON specification.
7. Click **Clone** to complete the profile creation.

Managing certificate authorities

Create and manage the certificate authorities hierarchy of your PKIaaS subscription.

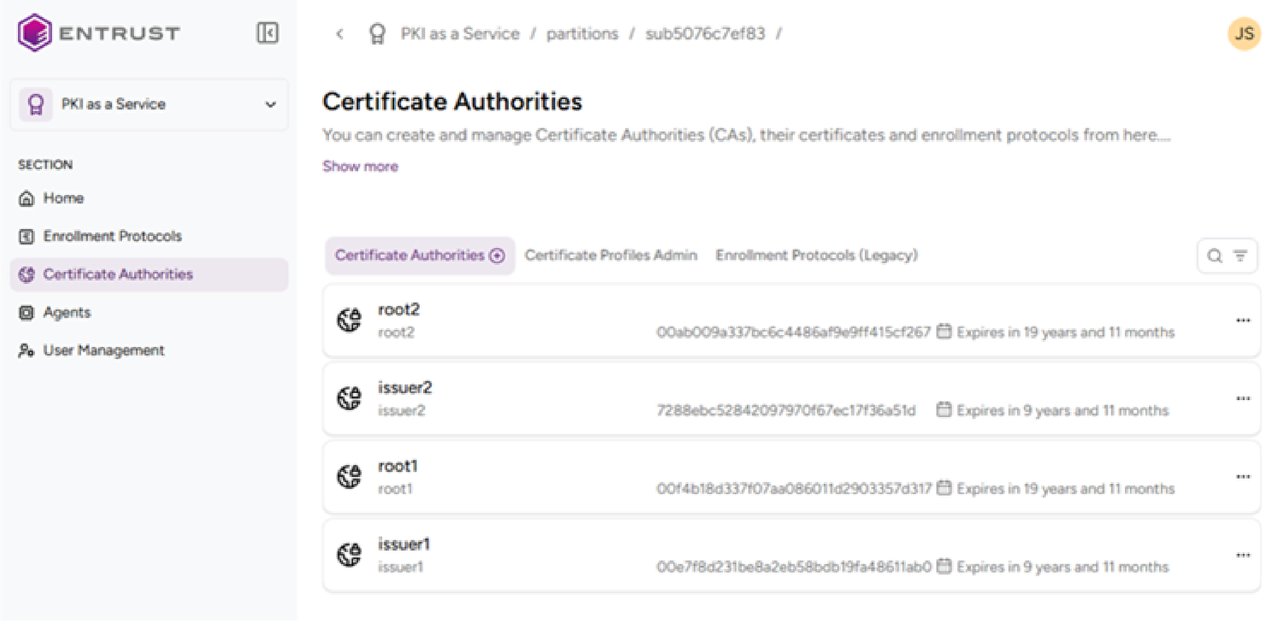
- Browsing CAs
- Creating a root CA
- Importing an external root CA
- Creating an intermediate subordinate CA
- Creating an issuing subordinate CA
- Certifying a CA with an external root CA
- Selecting CA profiles
- Downloading a CA certificate
- Deleting a CA

Browsing CAs

See below to browse and inspect the details of all certificate authorities (CAs) in your PKI.

To browse certificate authorities:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the roles described under Role permissions.
2. Click **Certificate Authorities** in the sidebar.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

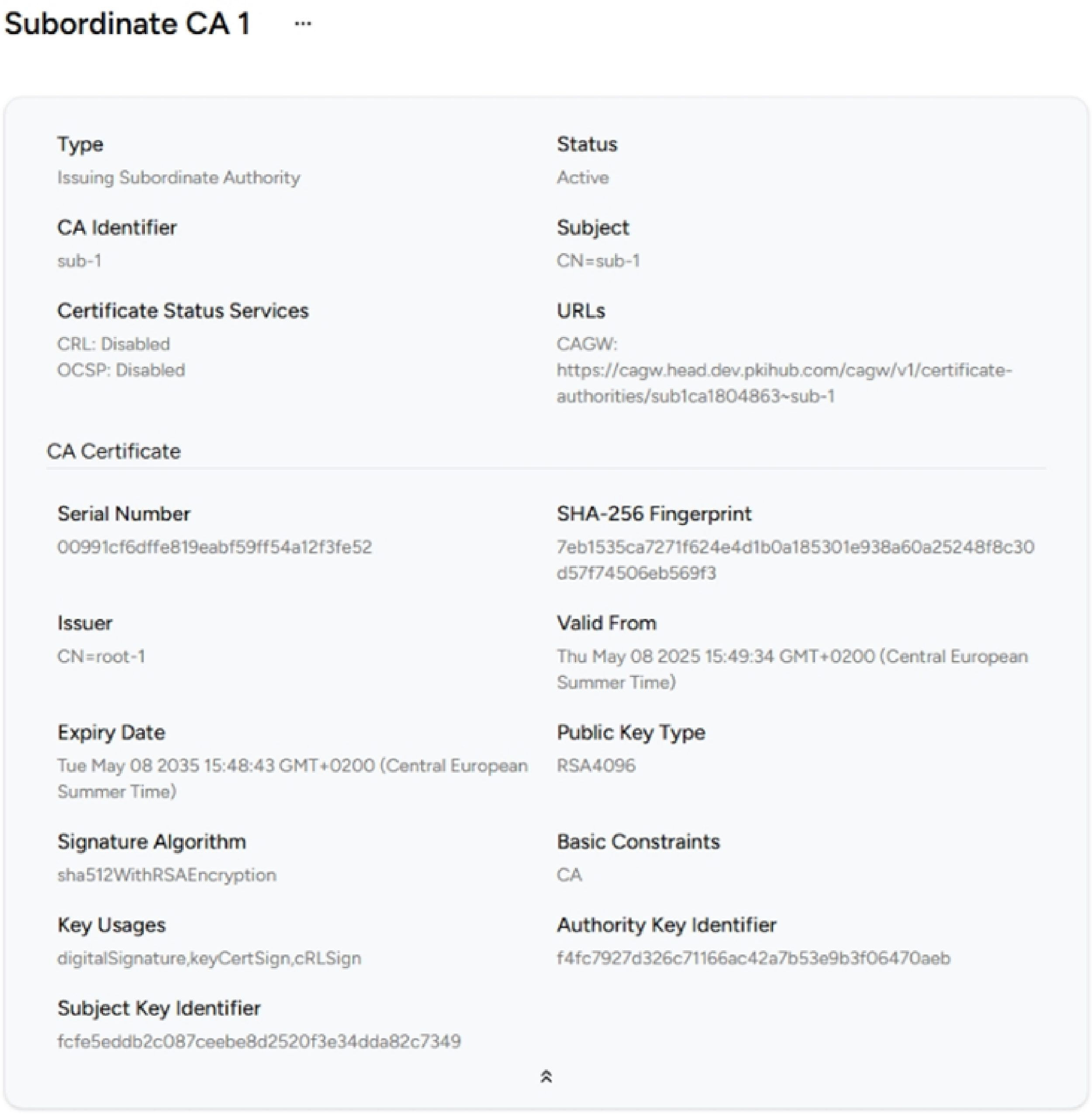
root2
root2 00ab009a337bc6c4486af9e9ff415cf267 Expires in 19 years and 11 months

issuer2
issuer2 7288ebc5284209797Of67ec17f36a51d Expires in 9 years and 11 months

root1
root1 00f4b18d337f07aa086011d2903357d317 Expires in 19 years and 11 months

issuer1
issuer1 00e7f8d231be8a2eb58bdb19fa48611ab0 Expires in 9 years and 11 months

3. In the **Certificate Authorities** tab, click the name of a certificate authority.
4. Click the downwards arrow icon to display the full details of the CA.



Subordinate CA 1 ···

Type
Issuing Subordinate Authority

Status
Active

CA Identifier
sub-1

Subject
CN=sub-1

Certificate Status Services
CRL: Disabled
OCSP: Disabled

URLs
CAGW:
https://cagw.head.dev.pkihub.com/cagw/v1/certificate-authorities/sub1ca1804863~sub-1

CA Certificate

Serial Number
00991cf6dffe819eabf59ff54a12f3fe52

SHA-256 Fingerprint
7eb1535ca7271f624e4d1b0a185301e938a60a25248f8c30d57f74506eb569f3

Issuer
CN=root-1

Valid From
Thu May 08 2025 15:49:34 GMT+0200 (Central European Summer Time)

Expiry Date
Tue May 08 2035 15:48:43 GMT+0200 (Central European Summer Time)

Public Key Type
RSA4096

Signature Algorithm
sha512WithRSAEncryption

Basic Constraints
CA

Key Usages
digitalSignature,keyCertSign,cRLSign

Authority Key Identifier
f4fc7927d326c71166ac42a7b53e9b3f06470aeb

Subject Key Identifier
fcfe5eddb2c087ceebe8d2520f3e34dda82c7349

5. Check the following values.

   - Type
   - Status
   - CA Identifier
   - Subject
   - Certificate status service
   - URLs
   - CA Certificate

ℹ See RFC 5280 for more details on the standard certificate extensions.

Type

The type of certificate authority.

Type	Description	Creation procedure
root	Root certificate authority	Creating a root CA
externalKey	External root certificate authority	Importing an external root CA
intermediate	Intermediate subordinate certificate authority	Creating an intermediate subordinate CA
subord	Issuing subordinate certificate authority	Creating an issuing subordinate CA

Status

The activation status of the certificate authority.

CA Identifier

The identifier assigned to the certificate authority on creation.

Subject

The Subject's Distinctive Name (DN) of the Certificate authority certificate.

Certificate status service

The activation status of the CRL and OCSP services.

URLs

The CA Gateway endpoint for the certificate authority.

CA Certificate

The settings of the Certificate authority certificate.

Setting	Description
Serial Number	The serial number (SN) of the CA certificate
SHA-256 Fingerprint	The SHA-256 fingerprint of the CA certificate
Issuer	The Distinguished Name of the entity that issued the CA certificate
Valid from	The time and date when the CA certificate was issued
Expiry Date	The time and date when the CA certificate will expire
Public key type	The public key algorithm of the CA certificate
Signature Algorithm	The signature algorithm of the CA certificate
Basic Constraints	The basic constraints for the CA certificate (see RFC 5280 for details on basic constraints)
Key Usage	The key usages for the CA certificate

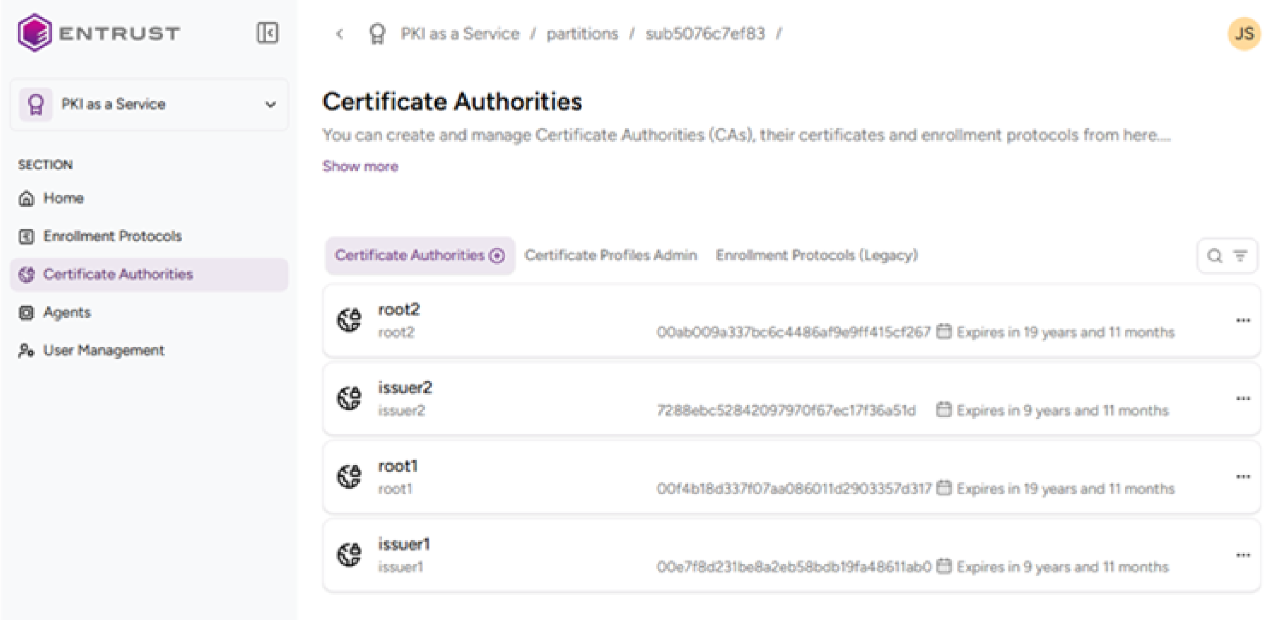
Setting	Description
Authority Info Access OCSP	The URL of the OCSP responder service informing on the CA certificate status
Authority Info Access CA Issuers	The locations from which the issuer certificate can be obtained
Authority Key Identifier	The key identifier of the entity that issued the CA certificate
Subject Key Identifier	The key identifier for the certificate subject
CRL Distribution Points	The URLs from which to download the CRLs (Certificate Revocation Lists) informing on the CA certificate status

Creating a root CA

A root Certificate Authority (CA) is the topmost entity in a hierarchy of digital certificates that establishes trust in a Public Key Infrastructure (PKI). The root CA issues and signs certificates for intermediate or issuing subordinate CAs, which in turn can issue certificates to end-users, servers, or devices.

To create a root CA:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
   - Owners
   - CA Administrators
2. Click **Certificate Authorities** in the sidebar.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

Show more

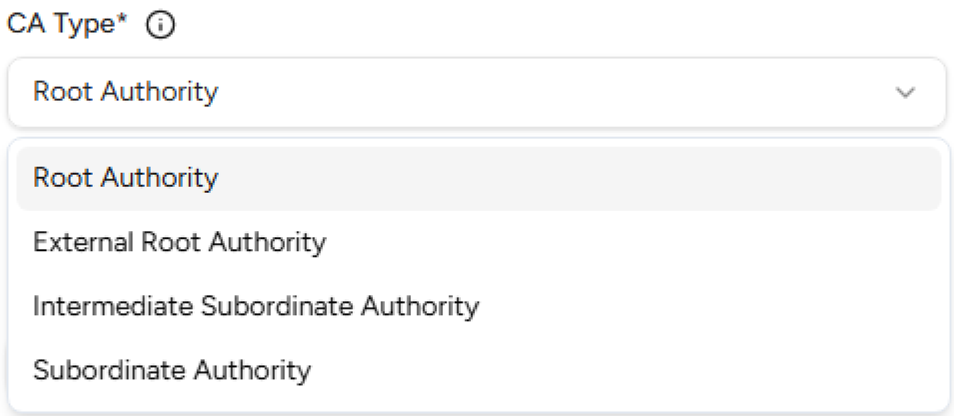
root2
root2 00ab009a337bc6c4486af9e9ff415cf267 Expires in 19 years and 11 months

issuer2
issuer2 7288ebc52842097970f67ec17f36a51d Expires in 9 years and 11 months

root1
root1 00f4b18d337f07aa086011d2903357d317 Expires in 19 years and 11 months

issuer1
issuer1 00e7f8d231be8a2eb58bdb19fa48611ab0 Expires in 9 years and 11 months

3. Click the plus + icon to the right of the **Certificate Authorities** tab.
4. Select **Root Authority** in the **Create Authority** list.



CA Type*

Root Authority

Root Authority

External Root Authority

Intermediate Subordinate Authority

Subordinate Authority

5. Complete the following values.
   - CA Identifier
   - Friendly Name
   - Signing Key Details
   - Expiry Date
   - Certificate Profiles
   - Subject
6. Click **Create**.
7. Check the details of the created CA — for example, the **Serial Number** of the Certificate Signing Certificate.

CA Identifier

Write a unique identifier for the new CA in your PKI hierarchy. This identifier:

- Must be 2-18 characters long
- Can only include lowercase letters, numbers, hyphens ('-'), and underscores ('_')

---

i After deleting a CA, wait 24 hours before creating a CA with the same identifier.

Friendly Name

Write a descriptive name for the CA in your PKIaaS partition.

Signing Key Details

Select a combination of cryptosystem and hash algorithm for the new CA to sign certificates.

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
RSA-2048+PKCS15-SHA256	RSA2048	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
RSA-2048+PSS-SHA256	RSA2048	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-3072+PKCS15-SHA256	RSA3072	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-3072+PSS-SHA256	RSA3072	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-4096+PKCS15-SHA512	RSA4096	sha512WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-4096+PSS-SHA512	RSA4096	sha512WithRSAPSS	RSA2048	sha256WithRSAPSS
ECDSAP256+SHA256	ECDSAP256	ecdsa-with-SHA256	RSA2048	sha256WithRSAEncryption
ECDSAP384+SHA384	ECDSAP384	ecdsa-with-SHA384	RSA2048	sha256WithRSAEncryption
ECDSAP521+SHA512	ECDSAP521	ecdsa-with-SHA512	RSA2048	sha256WithRSAEncryption
ML-DSA-44	ML-DSA-44	ML-DSA-44	RSA2048	sha256WithRSAEncryption
ML-DSA-65	ML-DSA-65	ML-DSA-65	RSA2048	sha256WithRSAEncryption
ML-DSA-87	ML-DSA-87	ML-DSA-87	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	RSA2048	sha256WithRSAEncryption
Falcon-512	Falcon-512	Falcon-512	RSA2048	sha256WithRSAEncryption
Falcon-1024	Falcon-1024	Falcon-1024	RSA2048	sha256WithRSAEncryption
MLDSA44-RSA2048-PKCS15	MLDSA44-RSA2048-PKCS15	MLDSA44-RSA2048-PKCS15	RSA2048	sha256WithRSAEncryption
MLDSA44-RSA2048-PSS	MLDSA44-RSA2048-PSS	MLDSA44-RSA2048-PSS	RSA2048	sha256WithRSAPSS
MLDSA44-ECDSA-P256	MLDSA44-ECDSA-P256	MLDSA44-ECDSA-P256	RSA2048	sha256WithRSAEncryption
MLDSA65-RSA3072-PKCS15	MLDSA65-RSA3072-PKCS15	MLDSA65-RSA3072-PKCS15	RSA2048	sha256WithRSAEncryption
MLDSA65-RSA3072-PSS	MLDSA65-RSA3072-PSS	MLDSA65-RSA3072-PSS	RSA2048	sha256WithRSAPSS

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
MLDSA65-RSA4096-PKCS15	MLDSA65-RSA4096-PKCS15	MLDSA65-RSA4096-PKCS15	RSA2048	sha256WithRSAEncryption
MLDSA65-RSA4096-PSS	MLDSA65-RSA4096-PSS	MLDSA65-RSA4096-PSS	RSA2048	sha256WithRSAPSS
MLDSA65-ECDSA-P384	MLDSA65-ECDSA-P384	MLDSA65-ECDSA-P384	RSA2048	sha256WithRSAEncryption
MLDSA87-ECDSA-P384	MLDSA87-ECDSA-P384	MLDSA87-ECDSA-P384	RSA2048	sha256WithRSAEncryption

Expiry Date

Select an expiration date for the Certificate Signing Certificate of the new CA.

⚠ After the expiration date, the CA becomes unusable unless the certificate has been renewed.

Certificate Profiles

Select the profiles the new root CA will support for issuing subordinate CA certificates.

To select the certificate profiles of a root CA:

1. Select one or more profile groups.
    - See Authority certificate profiles for a reference of the system profiles for issuing authority certificates.
    - See Managing certificate profiles for how to create custom profiles.
2. Click **+** to expand the profiles on the selected groups.
3. Mark the boxes of the profiles you want to enable.

Subject

Enter a value for each attribute of the certificate subject. The resulting Distinguished Name will uniquely identify the Certificate Signing Certificate of your new CA â□□ for example:

```
CN=MyRootCA, O=MyOrganization, L=MyCity, ST=MyState, C=US
```

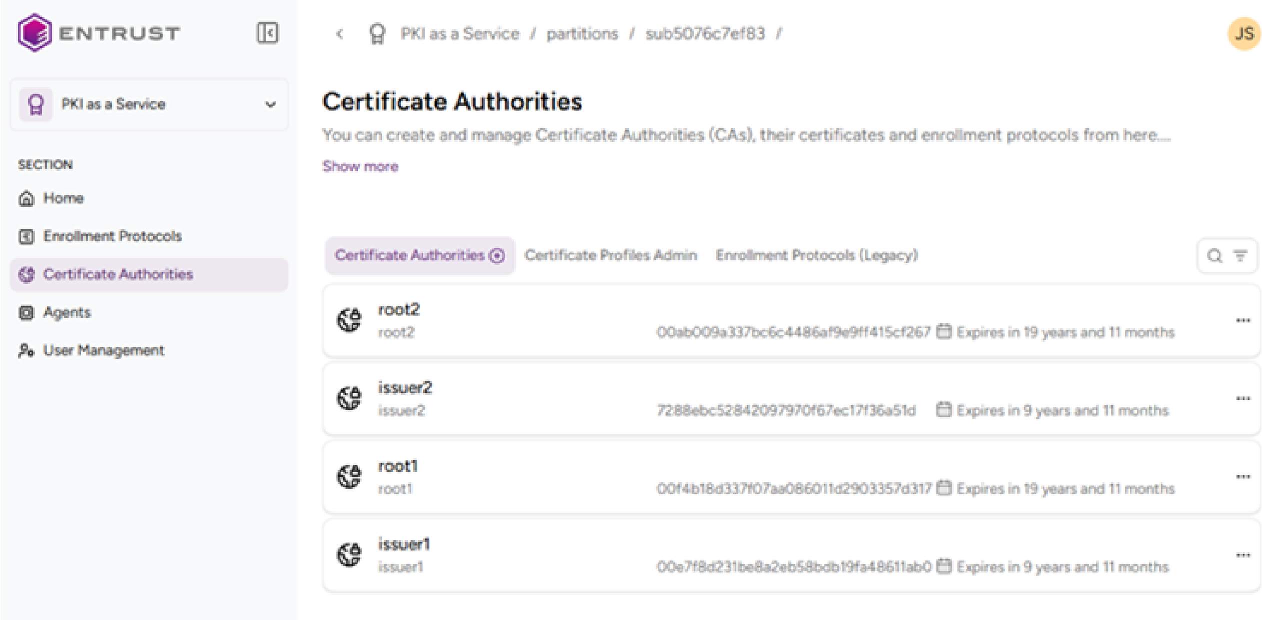
i Only the **Common Name** subject attribute is mandatory.

Importing an external root CA

Instead of Creating a root CA in PKIaaS, you can import an existing root CA.

To import an external root CA:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
   - Owners
   - CA Administrators
2. Click **Certificate Authorities** in the sidebar.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

Show more

Certificate Authorities ⊕ Certificate Profiles Admin Enrollment Protocols (Legacy)

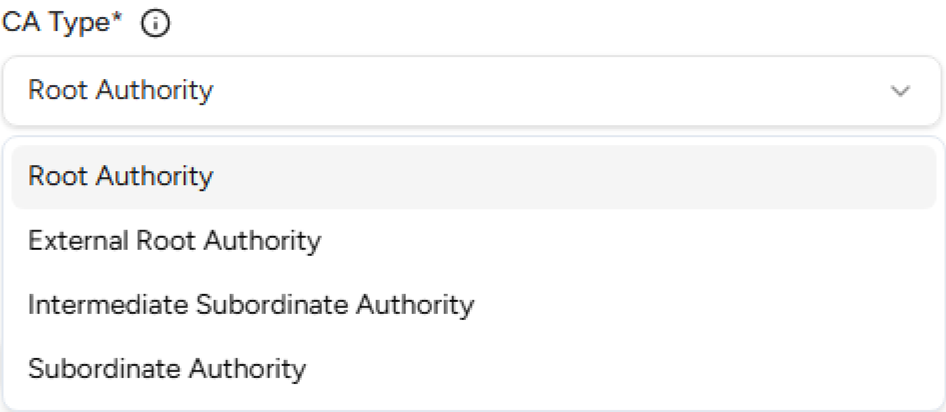
root2
root2 00ab009a337bc6c4486af9e9ff415cf267 Expires in 19 years and 11 months

issuer2
issuer2 7288ebc52842097970f67ec17f36a51d Expires in 9 years and 11 months

root1
root1 00f4b18d337f07aa086011d2903357d317 Expires in 19 years and 11 months

issuer1
issuer1 00e7f8d231be8a2eb58bdb19fa48611ab0 Expires in 9 years and 11 months

3. Click **ADD** in the **Certificate Authorities** tab.
4. Select **External Root Authority** in the **CA Type** list.



CA Type*

Root Authority

5. Complete the following values.
   - CA Identifier

  - Friendly Name
  - Root CA Certificate

6. Click **Create**.

7. Check the details of the created CA.

CA Identifier

Write a unique identifier for the new CA in your PKI hierarchy. This identifier:

- Must be 2-18 characters long
- Can only include lowercase letters, numbers, hyphens ('-'), and underscores ('_')

ℹ After deleting a CA, wait 24 hours before creating a CA with the same identifier.

Friendly Name

Write a descriptive name for the CA in your PKIaaS partition.

Root CA Certificate

Click **Choose File** and select the file containing the Certificate Signing Certificate of the external CA.

Creating an intermediate subordinate CA

An intermediate subordinate Certificate Authority (CA):

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

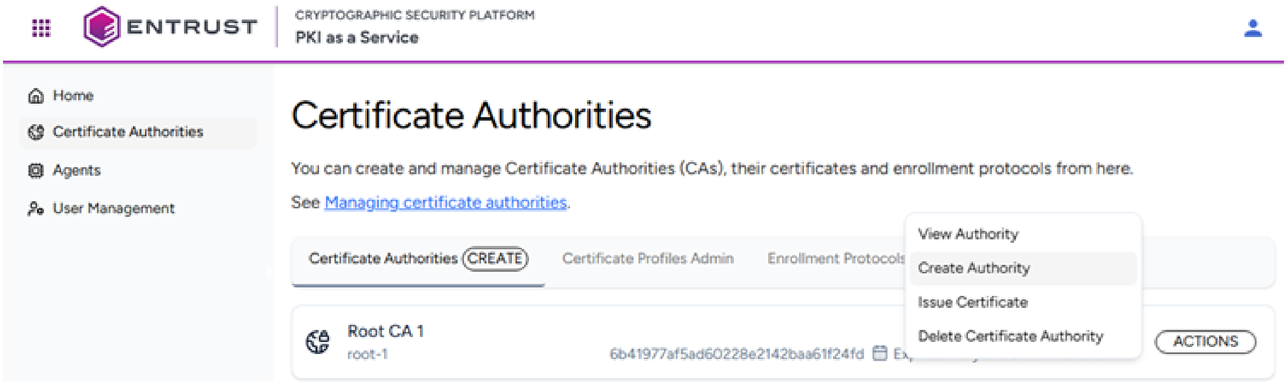
See below for how to create an intermediate subordinate CA.

To create an intermediate subordinate CA:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:

   - Owners
   - CA Administrators

2. Click **Certificate Authorities** in the sidebar.



ENTRUST | CRYPTOGRAPHIC SECURITY PLATFORM
PKI as a Service

Home
Certificate Authorities
Agents
User Management

Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here.

See Managing certificate authorities.

Certificate Authorities (CREATE) | Certificate Profiles Admin | Enrollment Protocols

View Authority
Create Authority
Issue Certificate
Delete Certificate Authority

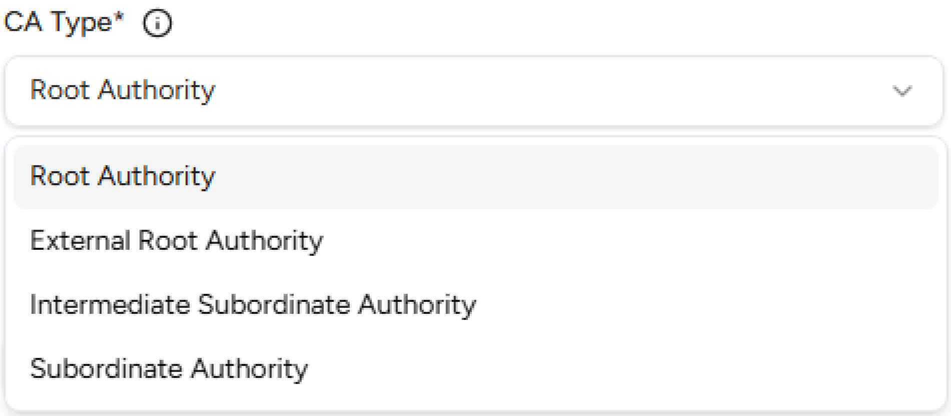
Root CA 1
root-1
6b41977af5ad60228e2142baa61f24fd Ex

ACTIONS

3. In the content pane, select **ACTIONS** > **Create Authority** for either:

   - A root CA.
   - An intermediate subordinate CA (as intermediate subordinate CAs can be the parent of other intermediate subordinate CAs).

   Alternatively, you can click the top **ADD** button and select **Intermediate Subordinate Authority** in the **CA Type** list.



CA Type*

Root Authority

Root Authority
External Root Authority
Intermediate Subordinate Authority
Subordinate Authority

4. Complete the following values.

   - CA Identifier
   - Friendly Name
   - Parent Authority Identifier
   - Signing Key Details
   - Expiry Date
   - Enable CRL
   - Certificate Profiles
   - Subject

5. Click **Create**.

6. Check the details of the created CA.

7. If the Parent Authority Identifier corresponds to an external root CA, follow the steps in Certifying a CA with an external root CA.

CA Identifier

Write a unique identifier for the new CA in your PKI hierarchy. This identifier:

- Must be 2-18 characters long
- Can only include lowercase letters, numbers, hyphens ('-'), and underscores ('_')

ℹ After deleting a CA, wait 24 hours before creating a CA with the same identifier.

Friendly Name

Write a descriptive name for the CA in your PKIaaS partition.

Parent Authority Identifier

Select the root or intermediate subordinate CA that will sign the Certificate Signing Certificate of the new intermediate subordinate CA.

ℹ This field is read-only if the parent CA was selected at the start of the intermediate subordinate CA creation.

Signing Key Details

Select a combination of cryptosystem and hash algorithm for the new CA to sign certificates.

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
RSA-2048+PKCS15-SHA256	RSA2048	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-2048+PSS-SHA256	RSA2048	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-3072+PKCS15-SHA256	RSA3072	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-3072+PSS-SHA256	RSA3072	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-4096+PKCS15-SHA512	RSA4096	sha512WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-4096+PSS-SHA512	RSA4096	sha512WithRSAPSS	RSA2048	sha256WithRSAPSS
ECDSAP256+SHA256	ECDSAP256	ecdsa-with-SHA256	RSA2048	sha256WithRSAEncryption
ECDSAP384+SHA384	ECDSAP384	ecdsa-with-SHA384	RSA2048	sha256WithRSAEncryption
ECDSAP521+SHA512	ECDSAP521	ecdsa-with-SHA512	RSA2048	sha256WithRSAEncryption
ML-DSA-44	ML-DSA-44	ML-DSA-44	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
ML-DSA-65	ML-DSA-65	ML-DSA-65	RSA2048	sha256WithRSAEncryption
ML-DSA-87	ML-DSA-87	ML-DSA-87	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	RSA2048	sha256WithRSAEncryption
Falcon-512	Falcon-512	Falcon-512	RSA2048	sha256WithRSAEncryption
Falcon-1024	Falcon-1024	Falcon-1024	RSA2048	sha256WithRSAEncryption
MLDSA44-RSA2048-PKCS15	MLDSA44-RSA2048-PKCS15	MLDSA44-RSA2048-PKCS15	RSA2048	sha256WithRSAEncryption
MLDSA44-RSA2048-PSS	MLDSA44-RSA2048-PSS	MLDSA44-RSA2048-PSS	RSA2048	sha256WithRSAPSS
MLDSA44-ECDSA-P256	MLDSA44-ECDSA-P256	MLDSA44-ECDSA-P256	RSA2048	sha256WithRSAEncryption
MLDSA65-RSA3072-PKCS15	MLDSA65-RSA3072-PKCS15	MLDSA65-RSA3072-PKCS15	RSA2048	sha256WithRSAEncryption
MLDSA65-RSA3072-PSS	MLDSA65-RSA3072-PSS	MLDSA65-RSA3072-PSS	RSA2048	sha256WithRSAPSS
MLDSA65-RSA4096-PKCS15	MLDSA65-RSA4096-PKCS15	MLDSA65-RSA4096-PKCS15	RSA2048	sha256WithRSAEncryption
MLDSA65-RSA4096-PSS	MLDSA65-RSA4096-PSS	MLDSA65-RSA4096-PSS	RSA2048	sha256WithRSAPSS
MLDSA65-ECDSA-P384	MLDSA65-ECDSA-P384	MLDSA65-ECDSA-P384	RSA2048	sha256WithRSAEncryption
MLDSA87-ECDSA-P384	MLDSA87-ECDSA-P384	MLDSA87-ECDSA-P384	RSA2048	sha256WithRSAEncryption

Expiry Date

Select an expiration date for the Certificate Signing Certificate of the new CA.

⚠ After the expiration date, the CA becomes unusable unless the certificate has been renewed.

Enable CRL

Check this box to enable the generation of CRLs (Certificate Revocation Lists).

---

i A Certificate Revocation List (CRL) is a list of digital certificates that the issuing Certificate Authority (CA) revoked before expiration.

Certificate Profiles

Select the profiles the new intermediate subordinate CA will support for issuing subordinate CA certificates.

To select the certificate profiles of an intermediate subordinate CA:

1. Select one or more profile groups.
    - See Authority certificate profiles for a reference of the system profiles for issuing authority certificates.
    - See Managing certificate profiles for how to create custom profiles.
2. Click **+** to expand the profiles on the selected groups.
3. Mark the boxes of the profiles you want to enable.

Subject

Enter a value for each attribute of the certificate subject. The resulting Distinguished Name will uniquely identify the Certificate Signing Certificate of your new CA â□□ for example:

```
CN=MyIntermediateCA, O=MyOrganization, L=MyCity, ST=MyState, C=US
```

---

i Only the **Common Name** subject attribute is mandatory.

Creating an issuing subordinate CA

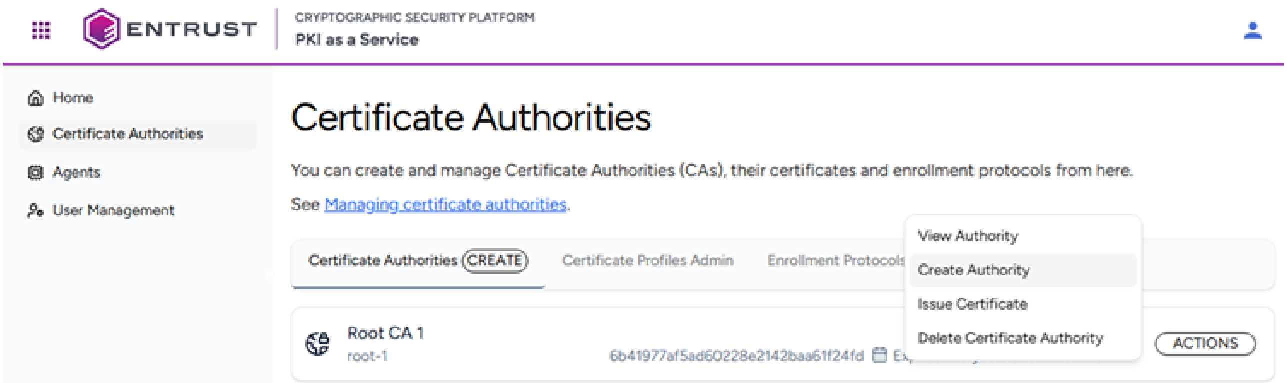
An issuing subordinate Certificate Authority (CA):

- Operates under the authority of either a root CA or an intermediate subordinate CA.
- Issues digital certificates to end entities like servers, devices, or users.

See below for how to create an issuing subordinate CA.

To create an issuing subordinate CA:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
   - Owners
   - CA Administrators
2. Click **Certificate Authorities** in the sidebar.

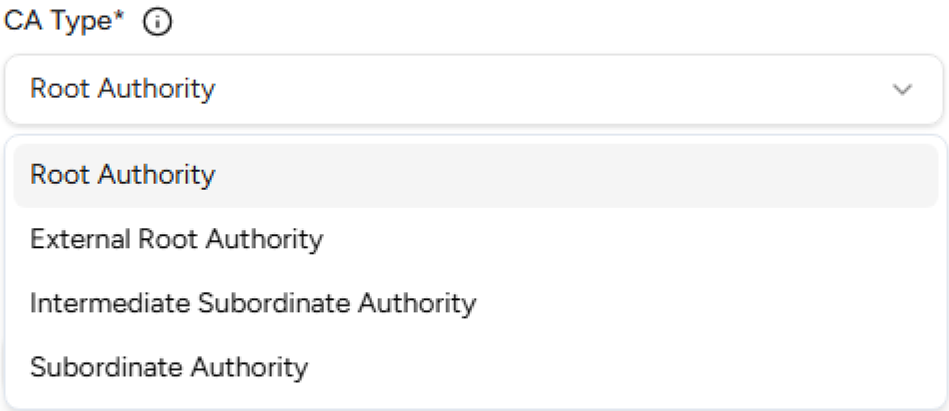


Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here.

See Managing certificate authorities.

3. In the content pane, select **ACTIONS > Create Authority** for a root or intermediate CA. Alternatively, you can click the top **ADD** button and select **Subordinate Authority** in the **CA Type** list.



4. Complete the following values.
   - CA Identifier
   - Friendly Name
   - Parent Authority Identifier
   - Signing Key Details
   - Expiry Date
   - Enable CRL
   - Enable OCSP
   - Certificate Profiles
   - Subject
5. Click **Create**.
6. Check the details of the created CA.
7. If the Parent Authority Identifier corresponds to an external root CA, follow the steps in Certifying a CA with an external root CA.

CA Identifier

Write a unique identifier for the new CA in your PKI hierarchy. This identifier:

- Must be 2-18 characters long
- Can only include lowercase letters, numbers, hyphens ('-'), and underscores ('_')

ℹ After deleting a CA, wait 24 hours before creating a CA with the same identifier.

Friendly Name

Write a descriptive name for the CA in your PKIaaS partition.

Parent Authority Identifier

Select the root CA that will sign the Certificate Signing Certificate of the new subordinate CA.

ℹ This field is read-only if the root CA was selected at the start of the subordinate CA creation.

Signing Key Details

Select a combination of cryptosystem and hash algorithm for the new CA to sign certificates.

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
RSA-2048+PKCS15-SHA256	RSA2048	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-2048+PSS-SHA256	RSA2048	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-3072+PKCS15-SHA256	RSA3072	sha256WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-3072+PSS-SHA256	RSA3072	sha256WithRSAPSS	RSA2048	sha256WithRSAPSS
RSA-4096+PKCS15-SHA512	RSA4096	sha512WithRSAEncryption	RSA2048	sha256WithRSAEncryption
RSA-4096+PSS-SHA512	RSA4096	sha512WithRSAPSS	RSA2048	sha256WithRSAPSS
ECDSAP256+SHA256	ECDSAP256	ecdsa-with-SHA256	RSA2048	sha256WithRSAEncryption
ECDSAP384+SHA384	ECDSAP384	ecdsa-with-SHA384	RSA2048	sha256WithRSAEncryption
ECDSAP521+SHA512	ECDSAP521	ecdsa-with-SHA512	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
ML-DSA-44	ML-DSA-44	ML-DSA-44	RSA2048	sha256WithRSAEncryption
ML-DSA-65	ML-DSA-65	ML-DSA-65	RSA2048	sha256WithRSAEncryption
ML-DSA-87	ML-DSA-87	ML-DSA-87	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	Hash-SLH-DSA-SHA2-128s-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	Hash-SLH-DSA-SHA2-128f-With-SHA256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	Hash-SLH-DSA-SHA2-192s-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	Hash-SLH-DSA-SHA2-192f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	Hash-SLH-DSA-SHA2-256s-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	Hash-SLH-DSA-SHA2-256f-With-SHA512	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	Hash-SLH-DSA-SHAKE-128s-With-SHAKE128	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	Hash-SLH-DSA-SHAKE-128f-With-SHAKE128	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	Hash-SLH-DSA-SHAKE-192s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	Hash-SLH-DSA-SHAKE-192f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	Hash-SLH-DSA-SHAKE-256s-With-SHAKE256	RSA2048	sha256WithRSAEncryption
Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	Hash-SLH-DSA-SHAKE-256f-With-SHAKE256	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	SPHINCS+-SHA2-128f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	SPHINCS+-SHA2-128s-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	SPHINCS+-SHA2-192f-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	SPHINCS+-SHA2-192s-simple	RSA2048	sha256WithRSAEncryption
SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	SPHINCS+-SHA2-256f-simple	RSA2048	sha256WithRSAEncryption

Label	Key algorithm	Signature algorithm	VA key type	VA signature algorithm
SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	SPHINCS+-SHA2-256s-simple	RSA2048	sha256WithRSAEncryption
Falcon-512	Falcon-512	Falcon-512	RSA2048	sha256WithRSAEncryption
Falcon-1024	Falcon-1024	Falcon-1024	RSA2048	sha256WithRSAEncryption
MLDSA44-RSA2048-PKCS15	MLDSA44-RSA2048-PKCS15	MLDSA44-RSA2048-PKCS15	RSA2048	sha256WithRSAEncryption
MLDSA44-RSA2048-PSS	MLDSA44-RSA2048-PSS	MLDSA44-RSA2048-PSS	RSA2048	sha256WithRSAPSS
MLDSA44-ECDSA-P256	MLDSA44-ECDSA-P256	MLDSA44-ECDSA-P256	RSA2048	sha256WithRSAEncryption
MLDSA65-RSA3072-PKCS15	MLDSA65-RSA3072-PKCS15	MLDSA65-RSA3072-PKCS15	RSA2048	sha256WithRSAEncryption
MLDSA65-RSA3072-PSS	MLDSA65-RSA3072-PSS	MLDSA65-RSA3072-PSS	RSA2048	sha256WithRSAPSS
MLDSA65-RSA4096-PKCS15	MLDSA65-RSA4096-PKCS15	MLDSA65-RSA4096-PKCS15	RSA2048	sha256WithRSAEncryption
MLDSA65-RSA4096-PSS	MLDSA65-RSA4096-PSS	MLDSA65-RSA4096-PSS	RSA2048	sha256WithRSAPSS
MLDSA65-ECDSA-P384	MLDSA65-ECDSA-P384	MLDSA65-ECDSA-P384	RSA2048	sha256WithRSAEncryption
MLDSA87-ECDSA-P384	MLDSA87-ECDSA-P384	MLDSA87-ECDSA-P384	RSA2048	sha256WithRSAEncryption

Expiry Date

Select an expiration date for the Certificate Signing Certificate of the new CA.

⚠ After the expiration date, the CA becomes unusable unless the certificate has been renewed.

Enable CRL

Check this box to enable the generation of CRLs (Certificate Revocation Lists).

ℹ A Certificate Revocation List (CRL) is a list of digital certificates that the issuing Certificate Authority (CA) revoked before expiration.

Enable OCSP

Check this box to enable an OCSP (Online Certificate Status Protocol) service that checks the validity status of the certificates issued by this CA.

⚠ This option is only present when creating a subordinate CA and requires a valid OCSP license.

When creating a subordinate CA with OCSP enabled:

- The CA issues a certificate to sign the OCSP responses.
- The certificates issued by the CA include the URL of the OCSP service. See Browsing certificates for how to inspect this URL in the certificate details.
- The OCSP service cannot be disabled.

Certificate Profiles

Select the profiles the new subordinate CA will support for issuing subscriber certificates.

To select the certificate profiles of a subordinate CA:

1. Select one or more profile groups.
   - See Subscriber certificate profiles for a reference of the system profiles for issuing subscriber certificates.
   - See Managing certificate profiles for how to create custom profiles.
2. Click **+** to expand the profiles on the selected groups.
3. Mark the boxes of the profiles you want to enable.

Subject

Enter a value for each attribute of the certificate subject. The resulting Distinguished Name will uniquely identify the Certificate Signing Certificate of your new CA â□□ for example:

```
CN=MyRootCA, O=MyOrganization, L=MyCity, ST=MyState, C=US
```

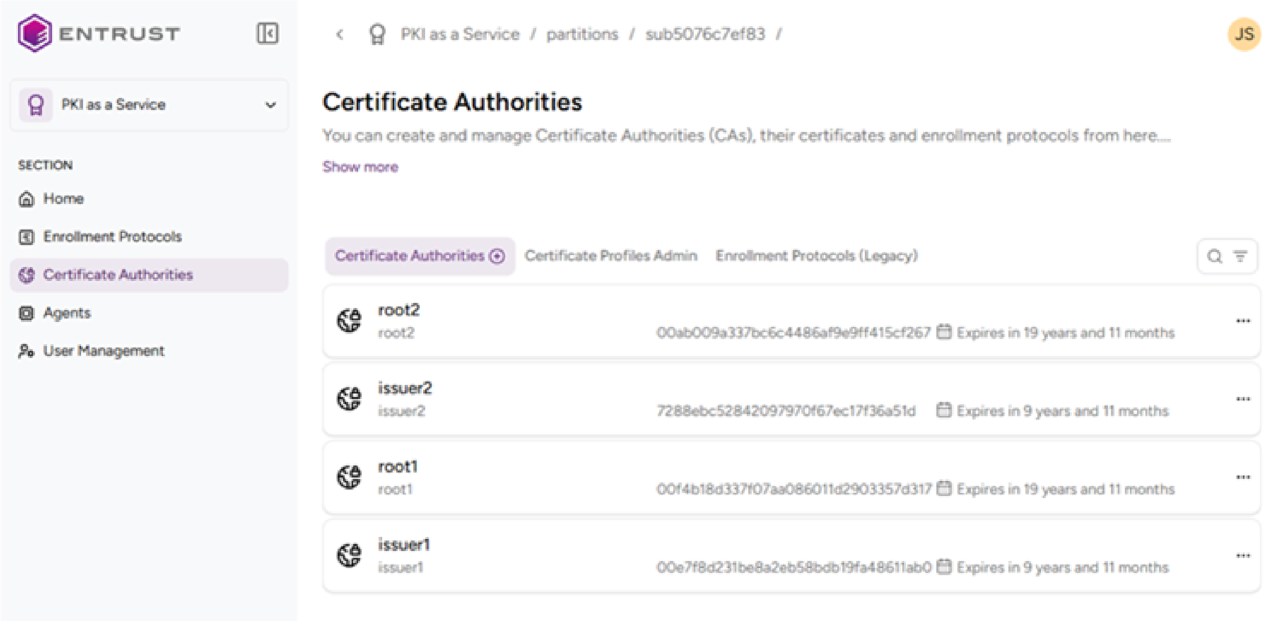
ℹ Only the **Common Name** subject attribute is mandatory.

Certifying a CA with an external root CA

After Creating an intermediate subordinate CA or Creating an issuing subordinate CA, follow the steps below if the parent CA is a root external CA.

To certify a CA with an external root CA:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
    - Owners
    - CA Administrators
2. Click **Certificate Authorities** in the sidebar.



ENTRUST
PKI as a Service
SECTION
Home
Enrollment Protocols
Certificate Authorities
Agents
User Management
PKI as a Service / partitions / sub5076c7ef83 /
JS
Certificate Authorities ⊙
Certificate Profiles Admin
Enrollment Protocols (Legacy)

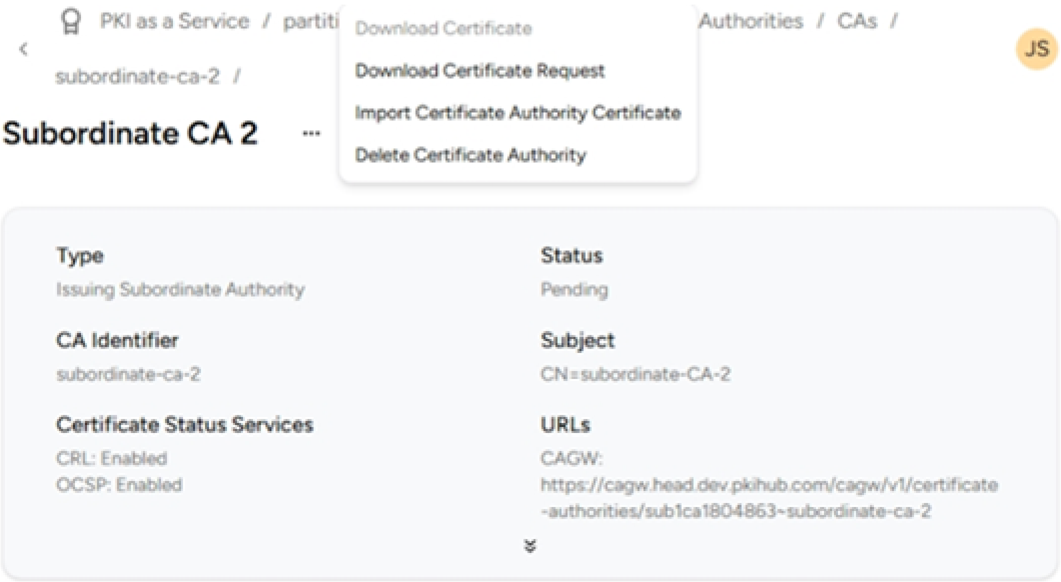
Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

Show more

root2 root2	00ab009a337bc6c4486af9e9ff415cf267	Expires in 19 years and 11 months	···
issuer2 issuer2	7288ebc52842097970f67ec17f36a51d	Expires in 9 years and 11 months	···
root1 root1	00f4b18d337f07aa086011d2903357d317	Expires in 19 years and 11 months	···
issuer1 issuer1	00e7f8d231be8a2eb58bdb19fa48611ab0	Expires in 9 years and 11 months	···

3. In the CA grid, select the name of the intermediate or issuing CA.
4. Click the three dots to the right of the CA name.



PKI as a Service / partiti
Authorities / CAs /
subordinate-ca-2 /
JS
Download Certificate
Download Certificate Request
Import Certificate Authority Certificate
Delete Certificate Authority

Subordinate CA 2

Type
Issuing Subordinate Authority

Status
Pending

CA Identifier
subordinate-ca-2

Subject
CN=subordinate-CA-2

Certificate Status Services
CRL: Enabled
OCSP: Enabled

URLs
CAGW:
https://cagw.head.dev.pkihub.com/cagw/v1/certificate-authorities/sub1ca1804863~subordinate-ca-2

5. Select **Download Certificate Request** to download the Certificate Signing Request (CSR) generated for the subordinate CA.

6. Issue the subordinate CA certificate by signing the downloaded CSR with the private key of the external root CA. Make sure this certificate meets the RFC5280 requirements â□□ for example:

   - The certificate includes the **Basic Constraints** extension with the `ca` boolean set to `TRUE`.
   - The certificate includes the **Key Usage** extension with the `keyCertSign` bit set.
   - The certificate includes other enabled bits, such as `cRLSign` for signing Certificate Revocation Lists (CRLs).

7. Select **Import Issuing Certificate Authority** to upload the subordinate CA certificate.

Selecting CA profiles

After creating a CA, you can modify the list of certificate profiles the CA supports.

i See Managing certificate profiles for how to browse and create certificate profiles.

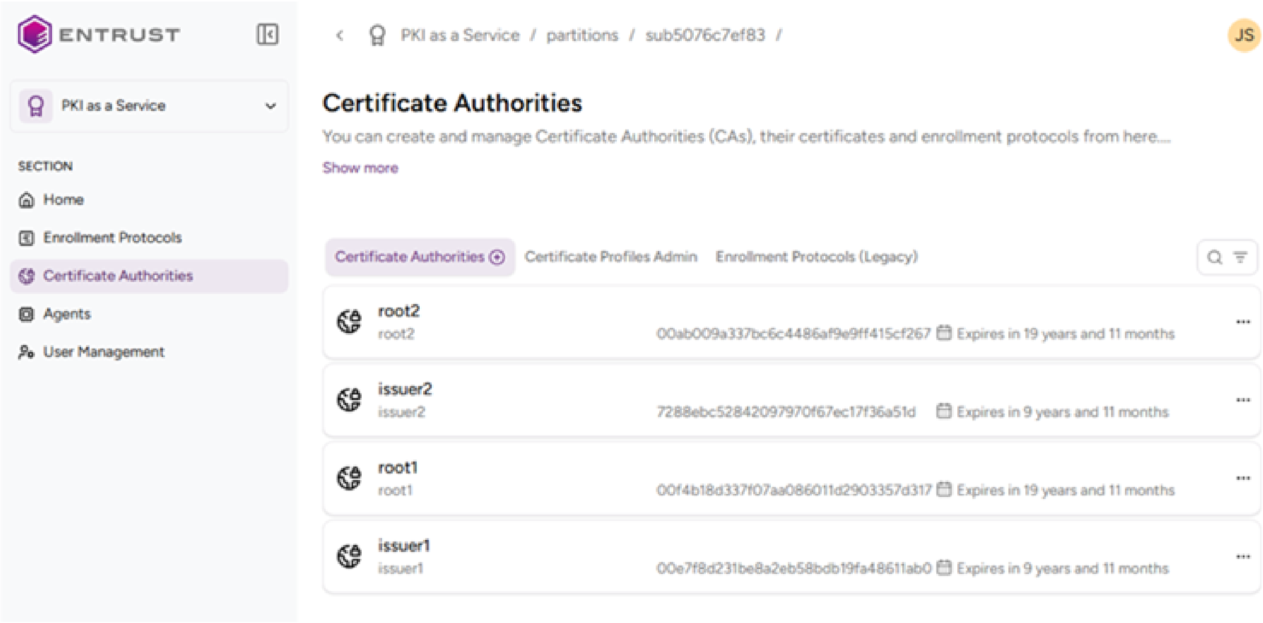
To select the certificate profiles of a certificate authority:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:

   - Owners
   - CA Administrators

2. Click **Certificate Authorities** in the sidebar.

3. In the **Certificate Authorities** tab, click the name of the certificate authority.



PKI as a Service / partitions / sub5076c7ef83 /

Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

Show more

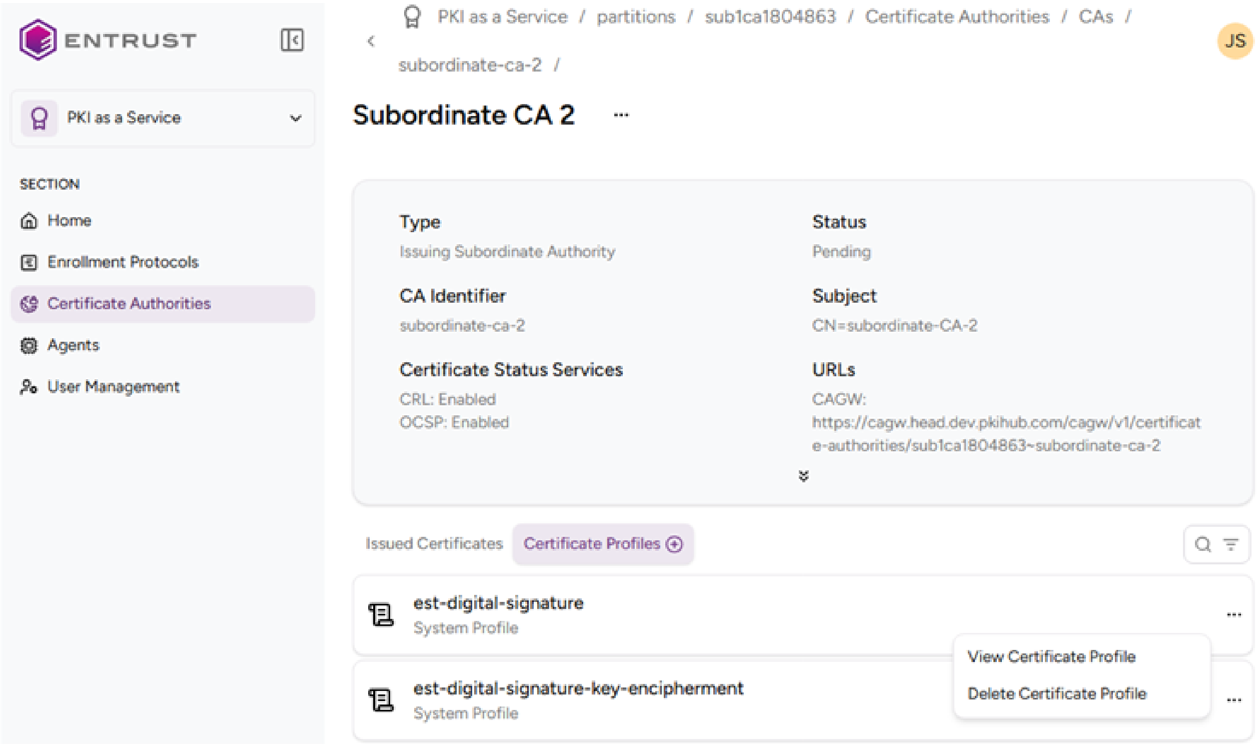
root2
root2
00ab009a337bc6c4486af9e9ff415cf267 Expires in 19 years and 11 months

issuer2
issuer2
7288ebc52842097970f67ec17f36a51d Expires in 9 years and 11 months

root1
root1
00f4b18d337f07aa086011d2903357d317 Expires in 19 years and 11 months

issuer1
issuer1
00e7f8d231be8a2eb58bdb19fa48611ab0 Expires in 9 years and 11 months

4. On the CA details page, select the **Certificate Profiles** tab to list the certificate profiles supported by the CA.



PKI as a Service / partitions / sub1ca1804863 / Certificate Authorities / CAs / subordinate-ca-2 /

Subordinate CA 2

Type
Issuing Subordinate Authority

Status
Pending

CA Identifier
subordinate-ca-2

Subject
CN=subordinate-CA-2

Certificate Status Services
CRL: Enabled
OCSP: Enabled

URLs
CAGW:
https://cagw.head.dev.pkihub.com/cagw/v1/certificate-authorities/sub1ca1804863~subordinate-ca-2

est-digital-signature
System Profile

est-digital-signature-key-encipherment
System Profile

5. You can.

   - Click the plus **+** icon right to the **Certificate Profiles** tab to select or deselect profiles.
   - Click the three dots to the right of a profile and select **View Certificate Profile** for a profile to browse the Certificate profile fields.
   - Click the three dots the right of a profile and select **Delete Certificate Profile** to remove it from the list of profiles supported by the CA.

Downloading a CA certificate

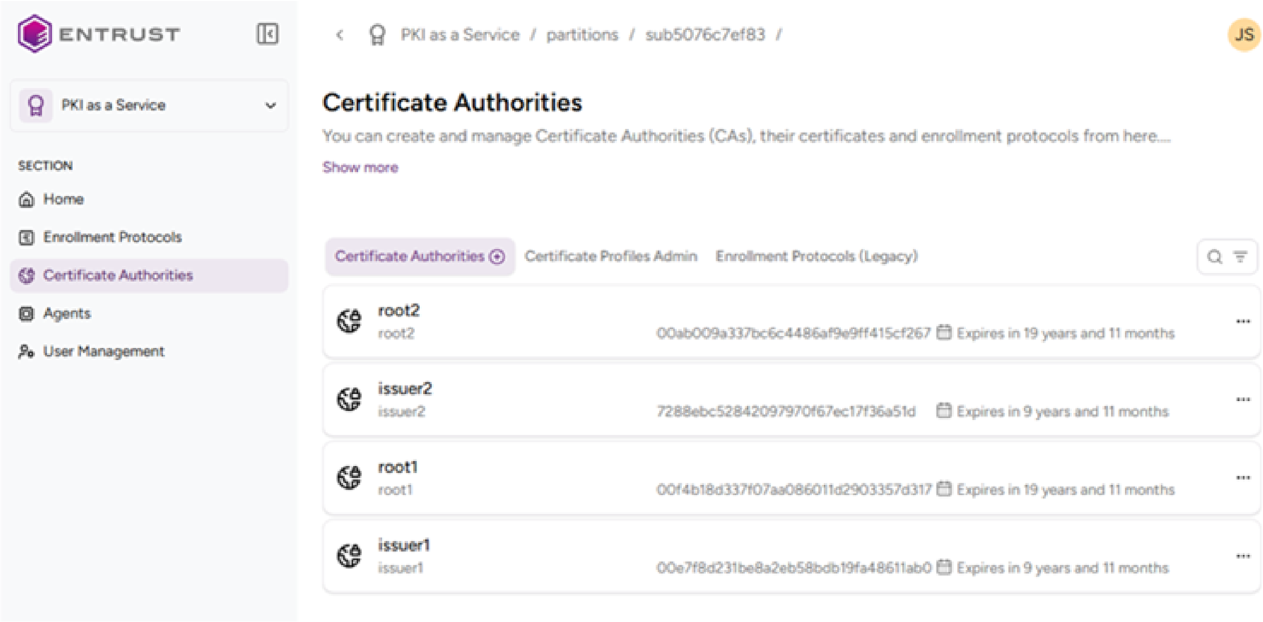
As explained in the previous sections, the Certificate Signing Certificate of a certificate authority can be:

- A self-signed certificate generated by Entrust PKIaaS when Creating a root CA.
- A certificate issued by a root CA when Creating an intermediate subordinate CA or a Creating an issuing subordinate CA.
- A certificate manually imported from file when Importing an external root CA.

See below for downloading this certificate.

To download the certificate signing certificate of a CA:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
   - Owners
   - CA Administrators
   - Certificate Administrators
2. Click **Certificate Authorities** in the sidebar.
3. In the **Certificate Authorities** tab, click the name of the certificate authority.


ENTRUST
PKI as a Service
SECTION
Home
Enrollment Protocols
Certificate Authorities
Agents
User Management
PKI as a Service / partitions / sub5076c7ef83 /
JS
Certificate Authorities ⊙
Certificate Profiles Admin
Enrollment Protocols (Legacy)

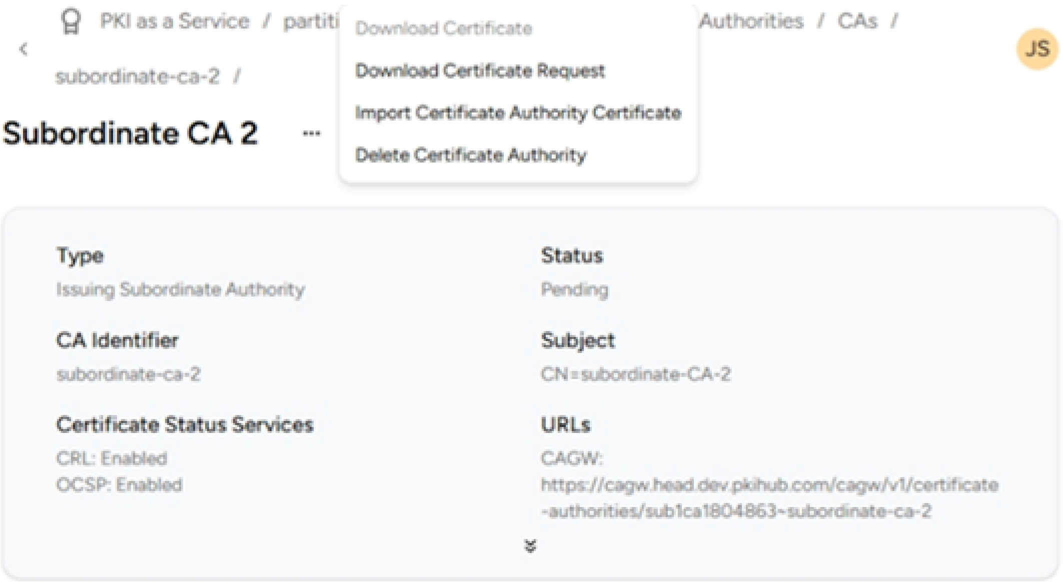
Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

Show more

root2 root2	00ab009a337bc6c4486af9e9ff415cf267	Expires in 19 years and 11 months	...
issuer2 issuer2	7288ebc52842097970f67ec17f36a51d	Expires in 9 years and 11 months	...
root1 root1	00f4b18d337f07aa086011d2903357d317	Expires in 19 years and 11 months	...
issuer1 issuer1	00e7f8d231be8a2eb58bdb19fa48611ab0	Expires in 9 years and 11 months	...

4. On the CA details page, click the three dots to the right of the authority name.



PKI as a Service / partiti
Authorities / CAs /
subordinate-ca-2 /
JS
Download Certificate
Download Certificate Request
Import Certificate Authority Certificate
Delete Certificate Authority

Subordinate CA 2

Type
Issuing Subordinate Authority

Status
Pending

CA Identifier
subordinate-ca-2

Subject
CN=subordinate-CA-2

Certificate Status Services
CRL: Enabled
OCSP: Enabled

URLs
CAGW:
https://cagw.head.dev.pkihub.com/cagw/v1/certificate-authorities/sub1ca1804863~subordinate-ca-2

5. Select **Download Certificate**.

Deleting a CA

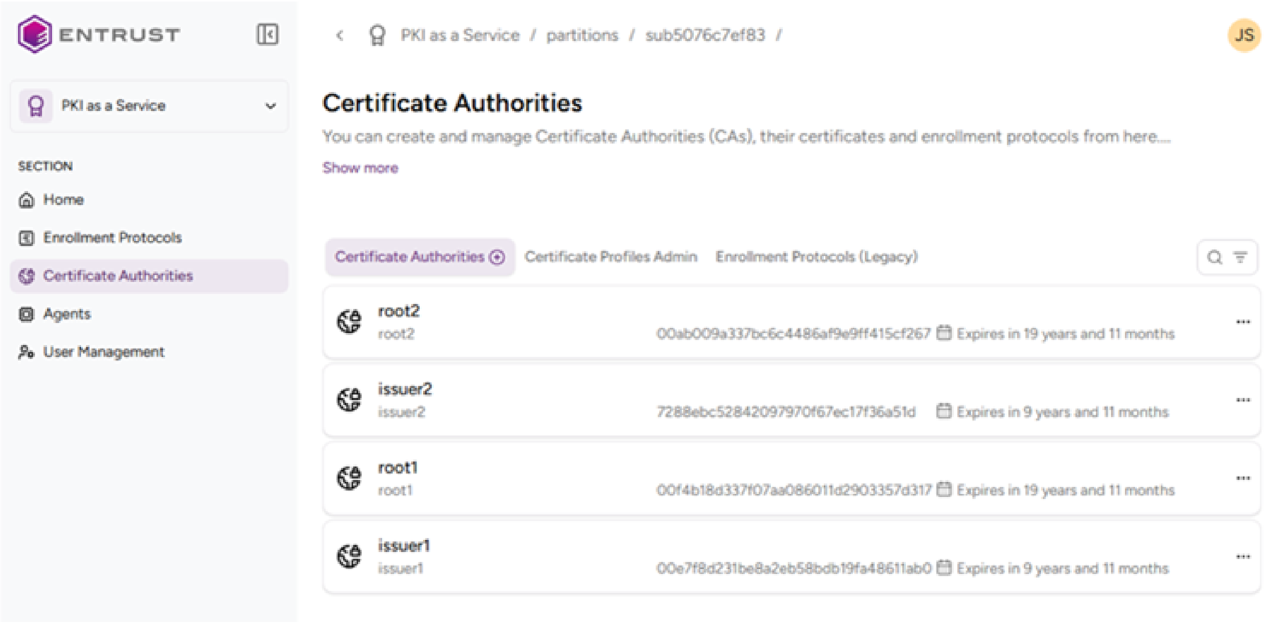
When deleting a certificate authority:

- All certificates issued for end-entities or other certificate authorities become unusable. Specifically, when deleting a root certificate authority, all its subordinate certificate authorities and all certificates issued by these subordinate certificate authorities become unusable.
- You must wait 24 hours before creating a CA with the same identifier. During these 24 hours, your number of active CAs will still include this CA.

See below for deleting a certificate authority.

To delete a certificate authority:

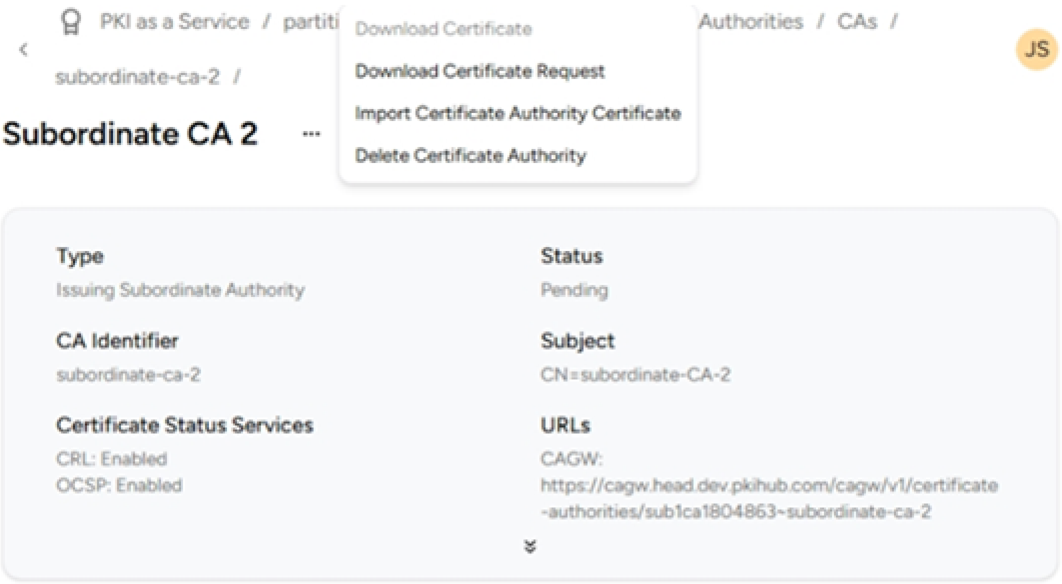
1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
   - Owners
   - CA Administrators
   - Certificate Administrators
2. Click **Certificate Authorities** in the sidebar.
3. In the **Certificate Authorities** tab, click the name of the certificate authority.



You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

root2 root2	00ab009a337bc6c4486af9e9ff415cf267	Expires in 19 years and 11 months
issuer2 issuer2	7288ebc52842097970f67ec17f36a51d	Expires in 9 years and 11 months
root1 root1	00f4b18d337f07aa086011d2903357d317	Expires in 19 years and 11 months
issuer1 issuer1	00e7f8d231be8a2eb58bdb19fa48611ab0	Expires in 9 years and 11 months

4. On the CA details page, click the three dots to the right of the authority name.


PKI as a Service / partiti
Authorities / CAs /
subordinate-ca-2 /
JS
Subordinate CA 2
Download Certificate
Download Certificate Request
Import Certificate Authority Certificate
Delete Certificate Authority

Type
Issuing Subordinate Authority

Status
Pending

CA Identifier
subordinate-ca-2

Subject
CN=subordinate-CA-2

Certificate Status Services
CRL: Enabled
OCSP: Enabled

URLs
CAGW:
https://cagw.head.dev.pkihub.com/cagw/v1/certificate-authorities/sub1ca1804863~subordinate-ca-2

5. Select **Delete Certificate Authority**.

6. Click **Delete** in the confirmation dialog.

Managing certificates

Issue and manage certificates with the certificate authorities of your PKIaaS subscription.

- Browsing certificates
- Issuing a certificate from CSR
- Issuing a certificate in a PKCS #12
- Changing the certificate status
- Downloading certificates

Browsing certificates

PKIaaS keeps track of all the issued certificates. That is:

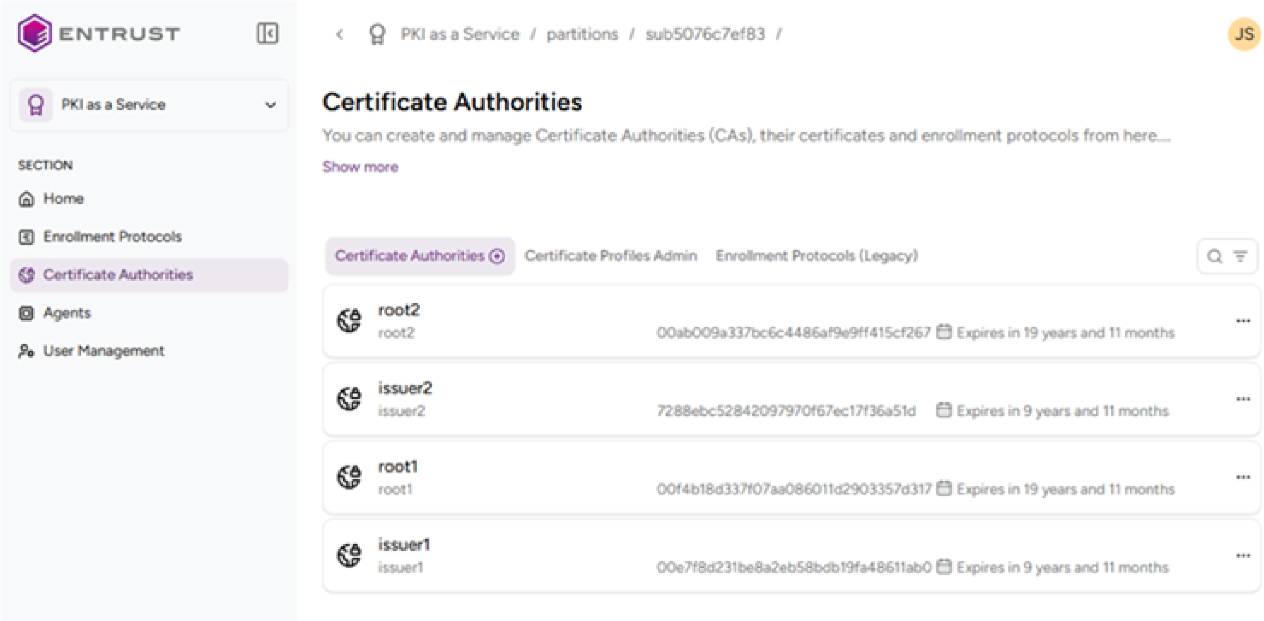
- The certificates manually issued as explained in:
  - Issuing a certificate from CSR
  - Issuing a certificate in a PKCS #12
- The certificates automatically enrolled as explained in:
  - Automating ACME enrollment
  - Automating MDM Intune enrollment
  - Automating MDM Jamf enrollment
  - Automating MDM Workspace ONE enrollment
  - Automating MDM Ivanti enrollment
  - Automating MDM IBM MaaS360 enrollment

See below to browse and inspect the details of all these certificates.

To browse certificates:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the roles described under Role permissions.

2. Click **Certificate Authorities** in the sidebar.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

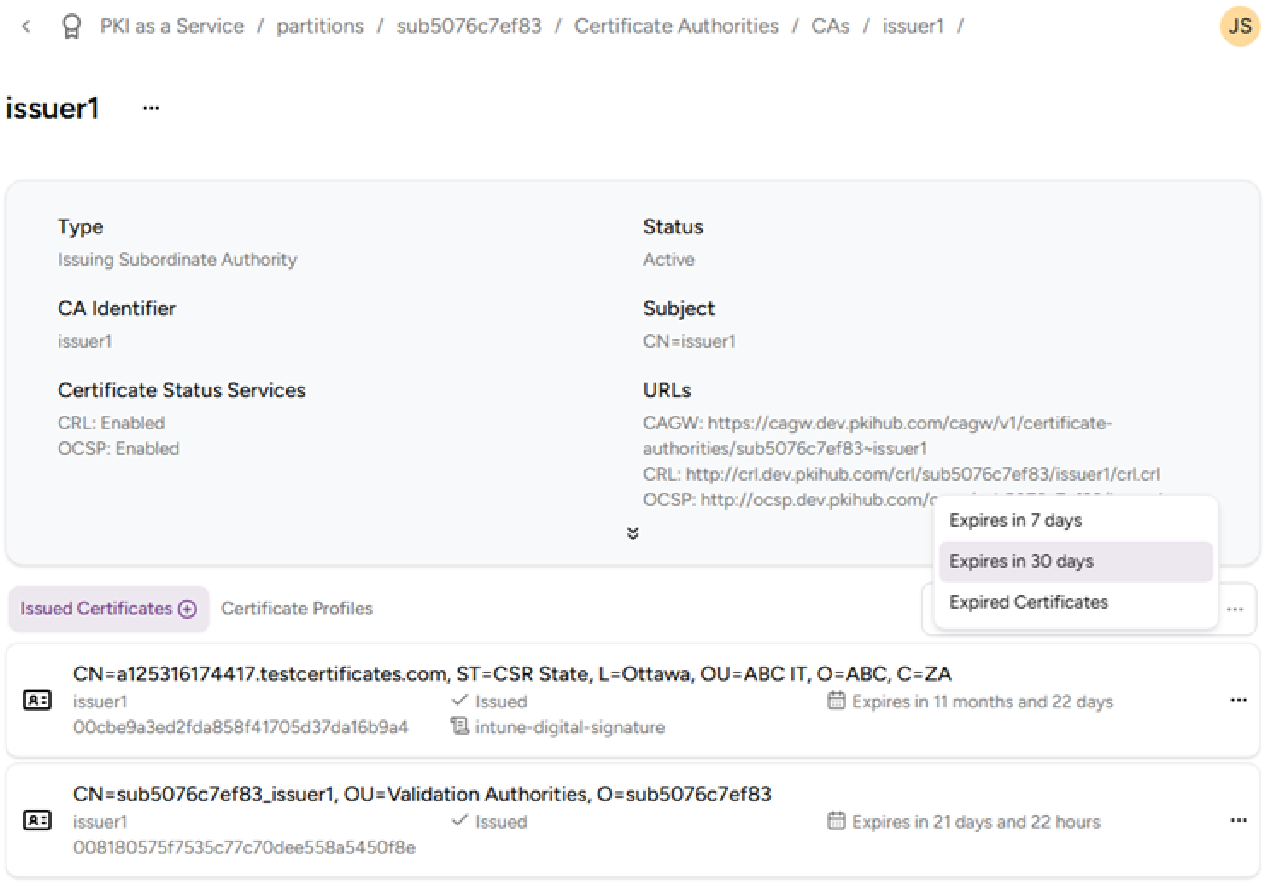
root2
root2 00ab009a337bc6c4486af9e9ff415cf267 Expires in 19 years and 11 months

issuer2
issuer2 7288ebc52842097970f67ec17f36a51d Expires in 9 years and 11 months

root1
root1 00f4b18d337f07aa086011d2903357d317 Expires in 19 years and 11 months

issuer1
issuer1 00e7f8d231be8a2eb58bdb19fa48611ab0 Expires in 9 years and 11 months

3. In the **Certificate Authorities** tab, click the name of a certificate authority to display the list of issued certificates.



issuer1

Type
Issuing Subordinate Authority

Status
Active

CA Identifier
issuer1

Subject
CN=issuer1

Certificate Status Services
CRL: Enabled
OCSP: Enabled

URLs
CAGW: https://cagw.dev.pkihub.com/cagw/v1/certificate-authorities/sub5076c7ef83~issuer1
CRL: http://crl.dev.pkihub.com/crl/sub5076c7ef83/issuer1/crl.crl
OCSP: http://ocsp.dev.pkihub.com/c

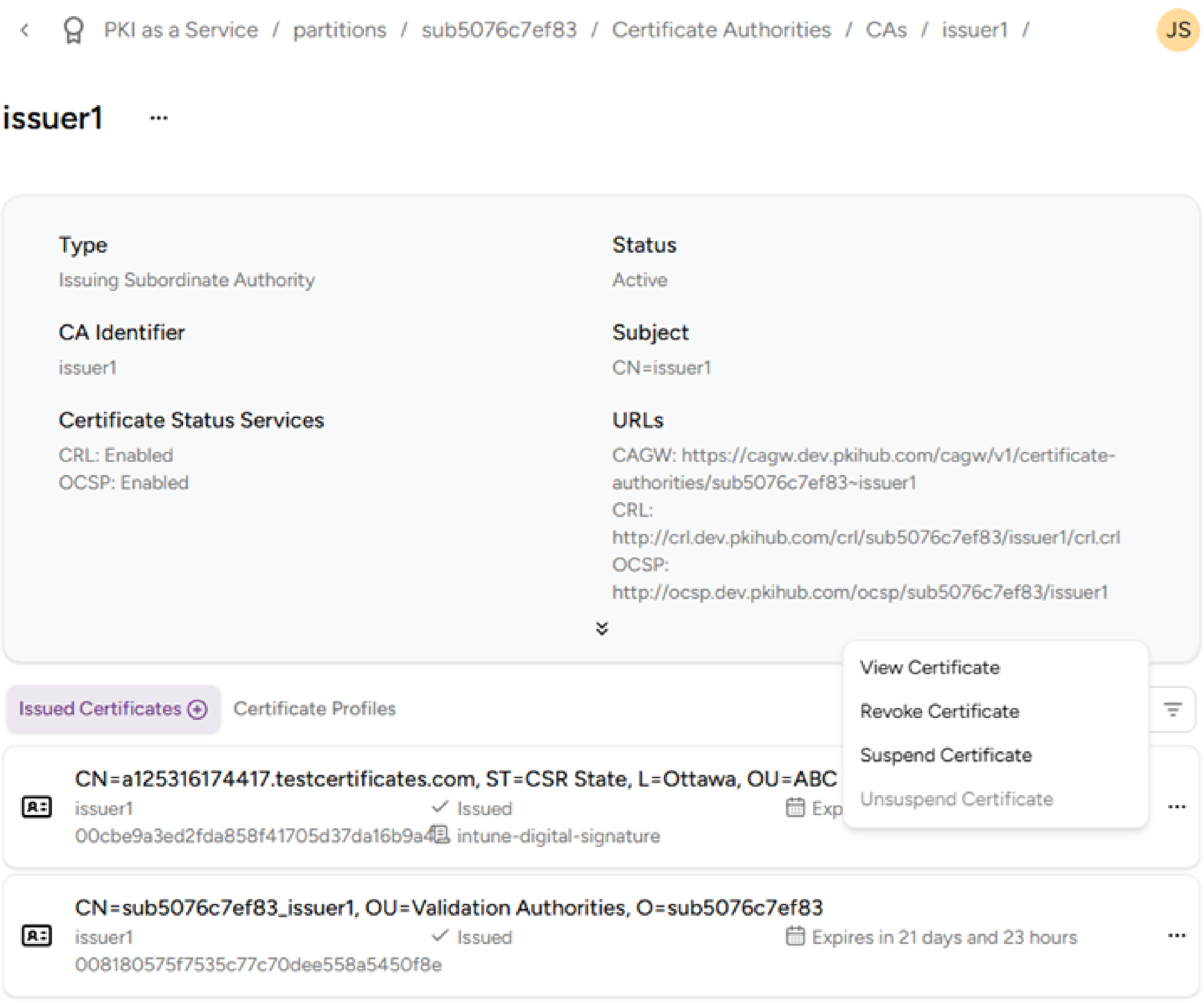
CN=a125316174417.testcertificates.com, ST=CSR State, L=Ottawa, OU=ABC IT, O=ABC, C=ZA
issuer1 ✓ Issued Expires in 11 months and 22 days
00cbe9a3ed2fda858f41705d37da16b9a4 intune-digital-signature

CN=sub5076c7ef83_issuer1, OU=Validation Authorities, O=sub5076c7ef83
issuer1 ✓ Issued Expires in 21 days and 22 hours
008180575f7535c77c70dee558a5450f8e

4. In the search box, enter a search key or click the three dots **"..."** and select a predefined filter.

- Expires in 7 days
- Expires in 30 days
- Expired Certificates

5. In the certificate grid, click the three dots **"..."** to the right of a certificate and select **View Certificate**.



PKI as a Service / partitions / sub5076c7ef83 / Certificate Authorities / CAs / issuer1 /

issuer1 ···

Type
Issuing Subordinate Authority

Status
Active

CA Identifier
issuer1

Subject
CN=issuer1

Certificate Status Services
CRL: Enabled
OCSP: Enabled

URLs
CAGW: https://cagw.dev.pkihub.com/cagw/v1/certificate-authorities/sub5076c7ef83~issuer1
CRL:
http://crl.dev.pkihub.com/crl/sub5076c7ef83/issuer1/crl.crl
OCSP:
http://ocsp.dev.pkihub.com/ocsp/sub5076c7ef83/issuer1

CN=a125316174417.testcertificates.com, ST=CSR State, L=Ottawa, OU=ABC
issuer1 ✓ Issued Exp
00cbe9a3ed2fda858f41705d37da16b9a4 intune-digital-signature

CN=sub5076c7ef83_issuer1, OU=Validation Authorities, O=sub5076c7ef83
issuer1 ✓ Issued Expires in 21 days and 23 hours
008180575f7535c77c70dee558a5450f8e

6. Check the following certificate details.

- Status
- Profile ID
- Serial Number
- Issuer
- Valid From
- Expiry Date
- Public Key Type
- Signature Algorithm
- Subject Alternative Names
- Basic Constraints
- Key Usages
- Extended Key Usages
- Authority Info Access OCSP
- Authority Info Access CA Issuers
- Authority Key Identifier
- Subject Key Identifier
- CRL Distribution Points
- Certificate Policies

ℹ See RFC 5280 for more details on the standard certificate extensions.

Status

The validity status of the certificate.

Status	Description
Issued	The certificate is valid
Revoked	The certificate is no longer valid
Suspended	The certificate is no longer valid, but its validity can be restored

See Changing the certificate status for how to change the validity status of a certificate.

Profile ID

The certificate profile selected when issuing the certificate.

Serial Number

The serial number (SN) of the issued certificate.

Issuer

The subject distinctive name of the CA certificate used to issue the certificate.

Valid From

The time and date when the certificate was issued.

Expiry Date

The expiry date selected when issuing the certificate.

Public Key Type

The type and size of the certificate public key.

Signature Algorithm

The hash and encryption algorithms used to sign the certificate.

Subject Alternative Names

The Subject Alternative Names (SAN) selected when issuing the certificate.

Basic Constraints

The type of holder to whom the certificate has been issued.

Value	Holder
CA	A certificate authority
EndEntity	An end-entity, like a device or a corporate user

Key Usages

The purpose of the key contained in the certificate -- for example:

- encipherment
- signature
- certificate signing

Extended Key Usages

One or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the **Key Usage** extension.

Authority Info Access OCSP

The URL of the OCSP service for checking the certificate validity status.

ℹ This value is set to `Undefined` when this service is not enabled for the CA.

Authority Info Access CA Issuers

Information for accessing the information service of the CA that issued the certificate.

ℹ This value is set to `Undefined` when this service is not enabled for the CA.

Authority Key Identifier

The identifier of the public key corresponding to the private key used to sign the certificate.

Subject Key Identifier

The identifier of the certificate public key.

CRL Distribution Points

The URLs for downloading the CRLs (Certificate Revocation Lists) generated by the CA that issued the certificate.

ℹ This value is set to `Undefined` when the CRL service is not enabled for the CA.

Certificate Policies

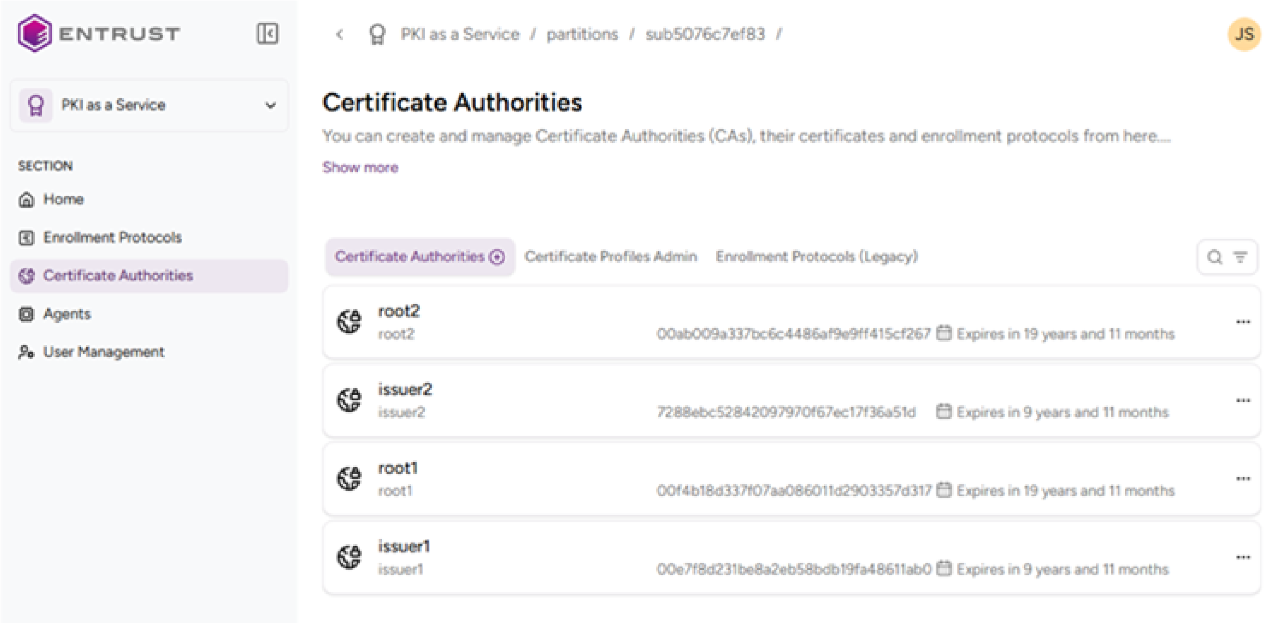
A sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers.

Issuing a certificate from CSR

See below for the certificate authority to process a PKCS #10 Certificate Signing Request (CSR) for a locally generated key pair.

To issue a certificate for server-generated keys:

1. Generate a key pair and a CSR on your local machine using your preferred tools.
2. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
   - Owners
   - Certificate Administrators
3. Click **Certificate Authorities** in the sidebar.

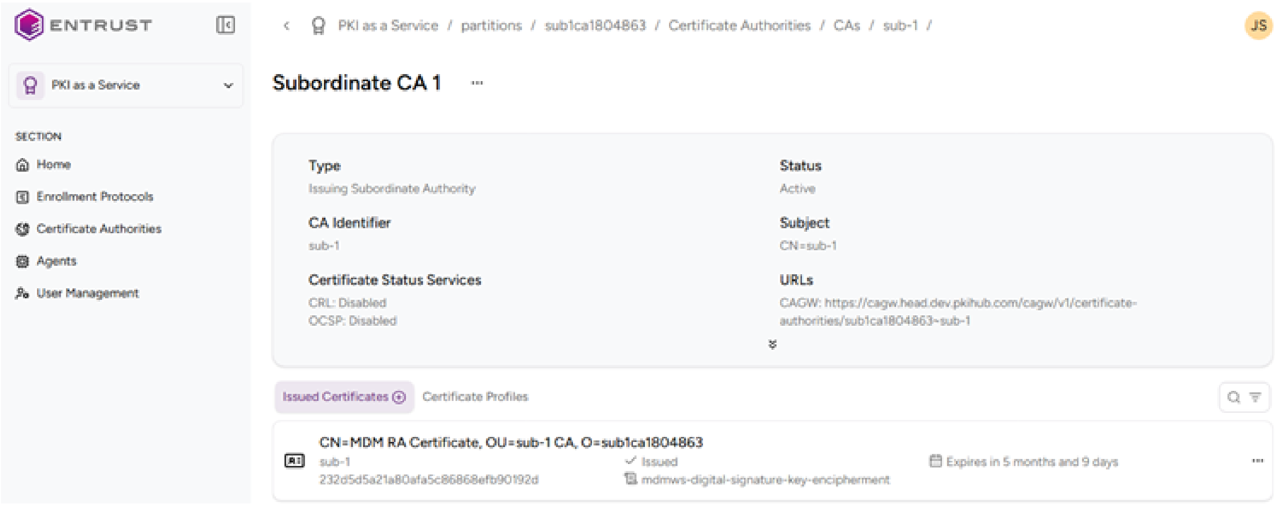


Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

root2 root2	00ab009a337bc6c4486af9e9ff415cf267	Expires in 19 years and 11 months
issuer2 issuer2	7288ebc52842097970f67ec17f36a51d	Expires in 9 years and 11 months
root1 root1	00f4b18d337f07aa086011d2903357d317	Expires in 19 years and 11 months
issuer1 issuer1	00e7f8d231be8a2eb58bdb19fa48611ab0	Expires in 9 years and 11 months

4. In the **Certificate Authorities** tab, click the name of the certificate authority that will issue the certificates.



Subordinate CA 1

Type
Issuing Subordinate Authority

Status
Active

CA Identifier
sub-1

Subject
CN=sub-1

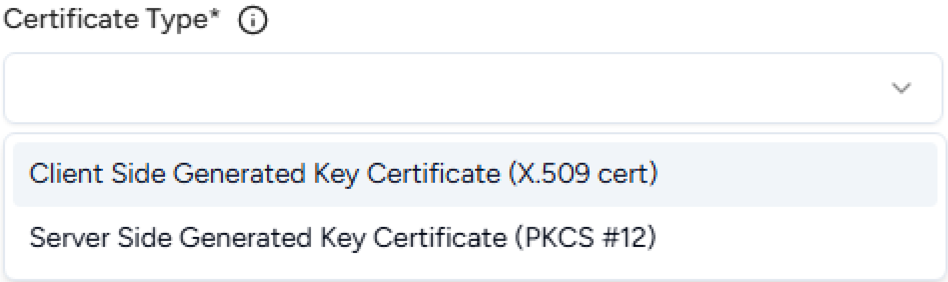
Certificate Status Services
CRL: Disabled
OCSP: Disabled

URLs
CAGW: https://cagw.head.dev.pkihub.com/cagw/v1/certificate-authorities/sub1ca1804863-sub-1

CN=MDM RA Certificate, OU=sub-1 CA, O=sub1ca1804863
sub-1
232d5d5a21a80afa5c86868efb90192d
✓ Issued
mdmws-digital-signature-key-encipherment
Expires in 5 months and 9 days

5. Click the plus **+** icon to the right of the **Issued Certificates** tab.

6. Select **Client-Side Generated Key Certificate (X.509 cert)** in the **Certificate type** list.


Certificate Type*
Client Side Generated Key Certificate (X.509 cert)
Server Side Generated Key Certificate (PKCS #12)

7. Complete the following values.

   - Certificate profile
   - Certificate Signing Request
   - Use Subject from CSR
   - Subject
   - Subject Alternative Names

Certificate profile

Select one of the Subscriber certificate profiles for the certificate authority to issue this certificate.

---

i The list only includes the certificate profiles selected when Creating an issuing subordinate CA.

Certificate Signing Request

Paste the encoded text of a Certificate Signing Request (CSR) you have locally generated for a key pair.

Use Subject from CSR

Check this box if you want the issued certificate to have the same Subject's Distinguished Name (DN) as the CSR pasted in the **Certificate Signing Request** field.

ℹ When checking this box, the **Subject** field is read-only and displays the DN set in the CSR.

Subject

Write the Distinguished Name (DN) of the certificate Subject in RFC 5280 syntax. For example, if the certificate subject is a corporate employee:

```
CN=John Doe, OU=Sales, O=Example Corp, L=San Francisco, ST=California, C=US
```

If the certificate subject is a corporate domain:

```
CN=server1.example.com, CN=server2.example.com, OU=IT, O=Example Corp, L=Chicago,
ST=Illinois, C=US
```

Subject Alternative Names

Add optional Subject Alternative Names (SANs) for the certificate subject. Typically, SANs extend the domain names or IP addresses set in the Subject field of a TLS certificate. For example:

San Type	SAN Value
DNS Name	`example.com`
DNS Name	`www.example.com`
DNS Name	`example.net`
DNS Name	`mail.example.com`
DNS Name	`support.example.com`
DNS Name	`example2.com`
IP Address	`93.184.216.34`
IP Address	`2606:2800:220:1:248:1893:25c8:1946`

Issuing a certificate in a PKCS #12

See below for the certificate authority to generate a PKCS #12 file containing:

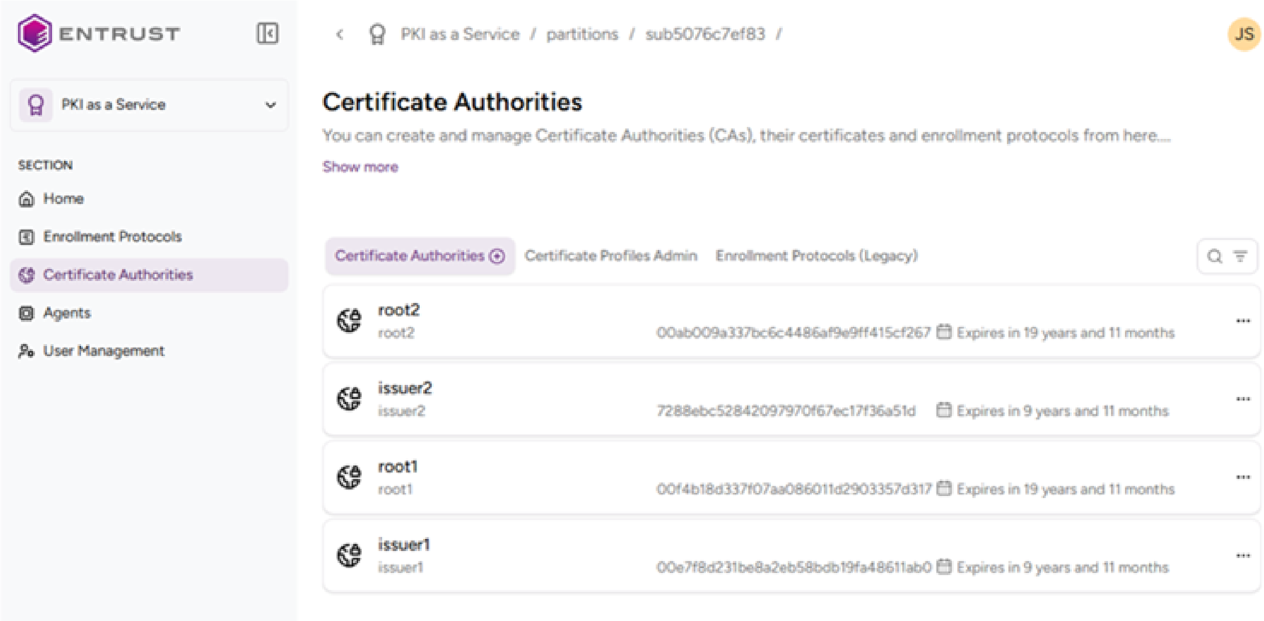
- A key pair generated by Entrust PKIaaS.
- The issued certificate.
- The CA certificate chain of the issued certificate.

To issue a PKCS #12:

1. Generate a key pair and a CSR on your local machine using your preferred tools.

2. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
    - Owners
    - Certificate Administrators

3. Click **Certificate Authorities** in the sidebar.


ENTRUST
PKI as a Service
SECTION
Home
Enrollment Protocols
Certificate Authorities
Agents
User Management
PKI as a Service / partitions / sub5076c7ef83 /
JS
Certificate Authorities ⊕
Certificate Profiles Admin
Enrollment Protocols (Legacy)

Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

Show more

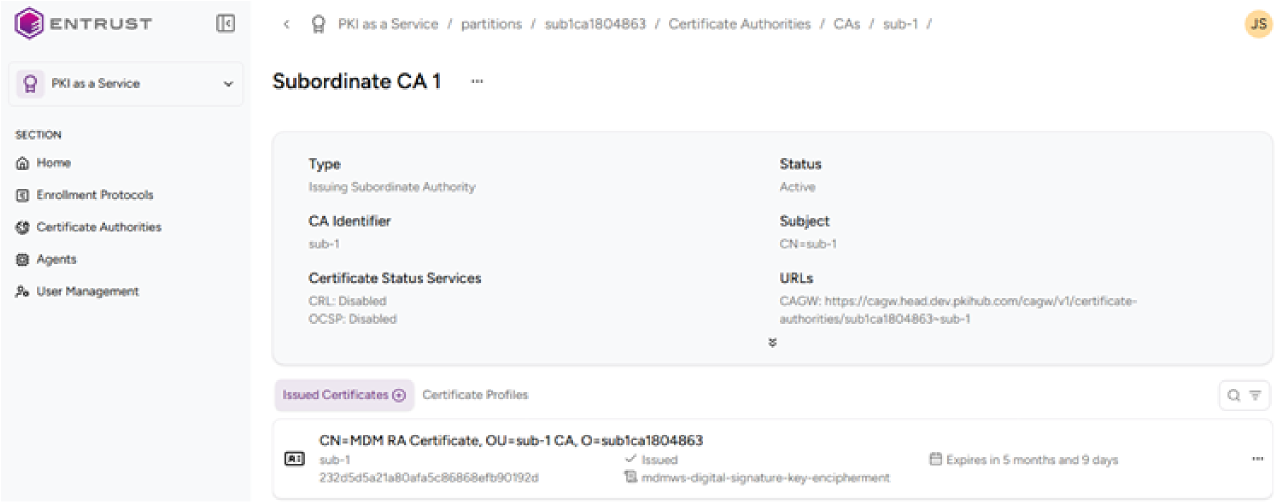
root2
root2 00ab009a337bc6c4486af9e9ff415cf267 Expires in 19 years and 11 months

issuer2
issuer2 7288ebc52842097970f67ec17f36a51d Expires in 9 years and 11 months

root1
root1 00f4b18d337f07aa086011d2903357d317 Expires in 19 years and 11 months

issuer1
issuer1 00e7f8d231be8a2eb58bdb19fa48611ab0 Expires in 9 years and 11 months

4. In the **Certificate Authorities** tab, click the name of the certificate authority that will issue the certificates.



Subordinate CA 1

Type: Issuing Subordinate Authority

Status: Active

CA Identifier: sub-1

Subject: CN=sub-1

Certificate Status Services: CRL: Disabled, OCSP: Disabled

URLs: CAGW: https://cagw.head.dev.pkihub.com/cagw/v1/certificate-authorities/sub1ca1804863~sub-1

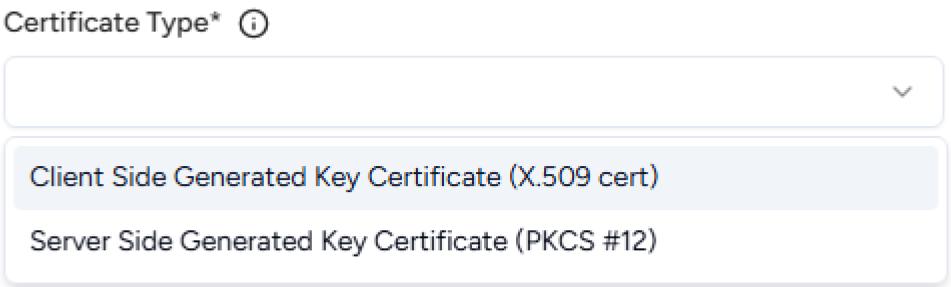
CN=MDM RA Certificate, OU=sub-1 CA, O=sub1ca1804863
sub-1
232d5d5a21a80afa5c86868efb90192d
✓ Issued
mdmws-digital-signature-key-encipherment
Expires in 5 months and 9 days

⚠ Root certificate authorities are not granted profiles to issue PKCS #12 files.

---

5. Click the plus **+** icon to the right of the **Issued Certificates** tab.

6. Select **Server-Side Generated Key Certificate (PKCS #12)** in the **Certificate type** list.



Certificate Type*

Client Side Generated Key Certificate (X.509 cert)

Server Side Generated Key Certificate (PKCS #12)

7. Complete the following values.
   - Certificate profile
   - PKCS #12 Password
   - Subject
   - Subject Alternative Names
8. Click **Issue**.
9. Check the certificate details and click **Download your PKCS #12** to download the issued PKCS #12 file.

> ⚠ Entrust PKIaaS does not store the generated key pair in any way. Therefore, you won't be able to download the PKCS #12 file after leaving this page.

Certificate profile

Select one of the Subscriber certificate profiles for the certificate authority to issue this certificate.

> ℹ The list only includes the certificate profiles selected when Creating an issuing subordinate CA.

PKCS #12 Password

Type and confirm a password to protect the contents of the PKCS #12 file.

Subject

Write the Distinguished Name (DN) of the certificate Subject in RFC 5280 syntax.

Subject example for a corporate employee

```
CN=John Doe, OU=Sales, O=Example Corp, L=San Francisco, ST=California, C=US
```

Subject example for a corporate domain

```
CN=server1.example.com, CN=server2.example.com, OU=IT, O=Example Corp, L=Chicago,
ST=Illinois, C=US
```

Subject Alternative Names

Add optional Subject Alternative Names (SANs) for the certificate subject. Typically, SANs extend the domain names or IP addresses set in the Subject field of a TLS certificate. For example:

San type	SAN example value
DNS Name	`example.com`
DNS Name	`www.example.com`
DNS Name	`example.net`
DNS Name	`mail.example.com`
DNS Name	`support.example.com`
DNS Name	`example2.com`
IP Address	`93.184.216.34`
IP Address	`2606:2800:220:1:248:1893:25c8:1946`

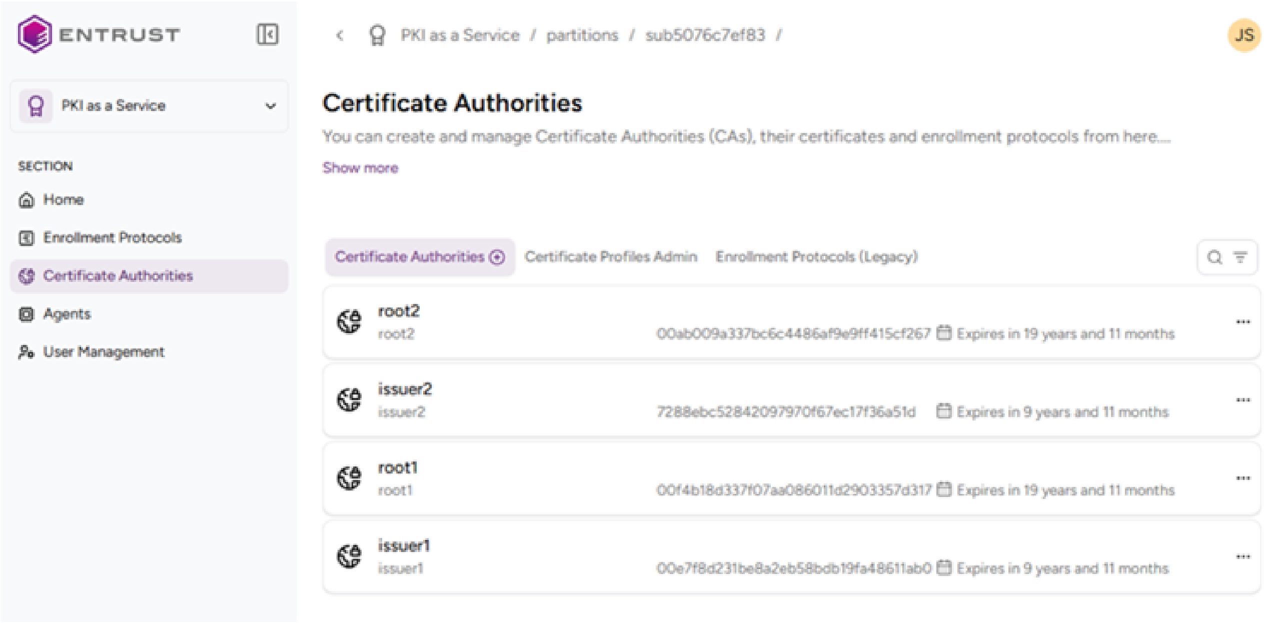
Changing the certificate status

See below to change the validity status of a certificate.

ℹ The CRL and OCSP services of the issuing CA report the validity status of a certificate. See Browsing certificates for how to get the URL of these services.

To change the validity status of a certificate:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
   - Owners
   - Certificate Administrators
2. Click **Certificate Authorities** in the sidebar.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

Show more

root2
root2 00ab009a337bc6c4486af9e9ff415cf267 Expires in 19 years and 11 months

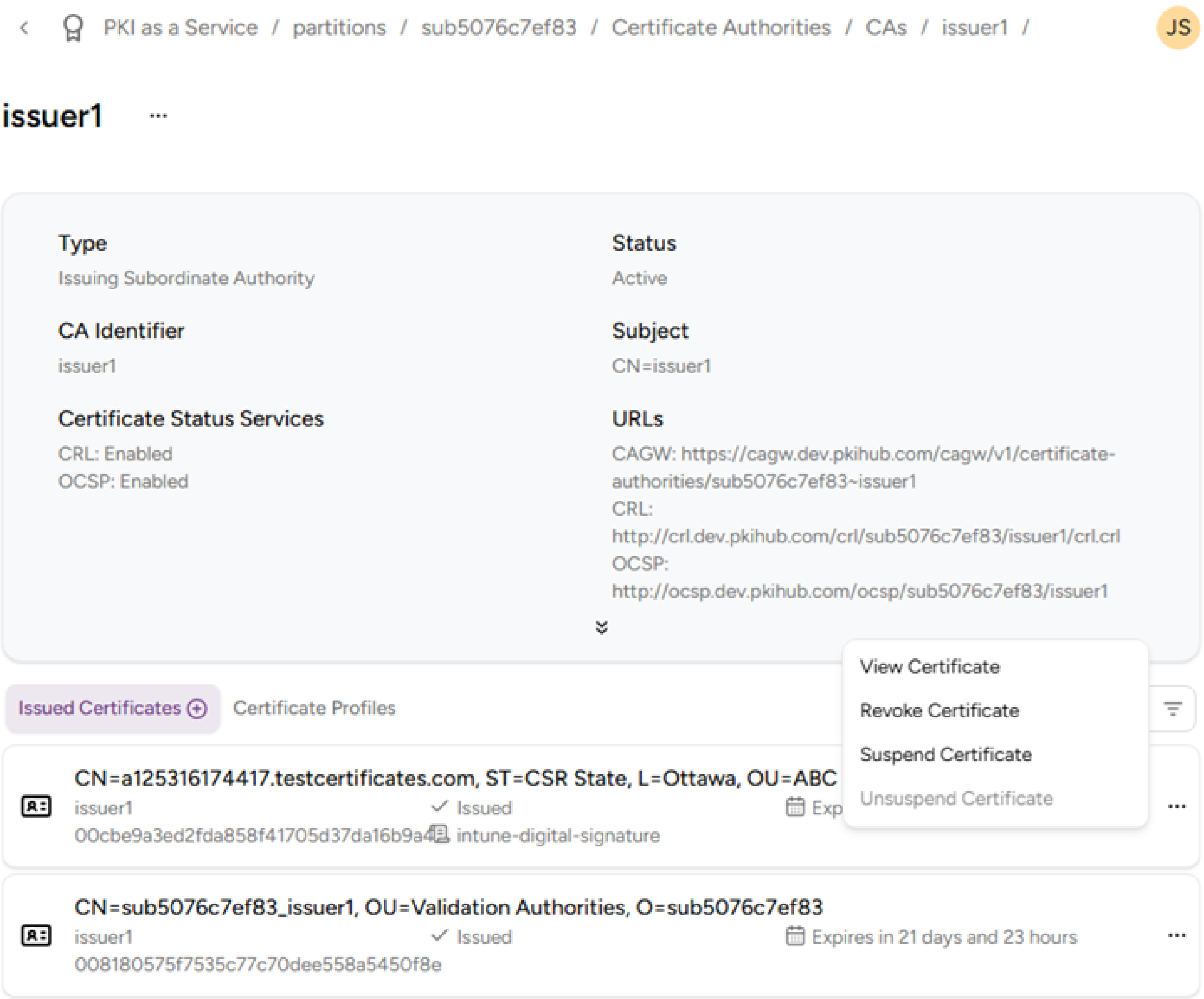
issuer2
issuer2 7288ebc52842097970f67ec17f36a51d Expires in 9 years and 11 months

root1
root1 00f4b18d337f07aa086011d2903357d317 Expires in 19 years and 11 months

issuer1
issuer1 00e7f8d231be8a2eb58bdb19fa48611ab0 Expires in 9 years and 11 months

3. In the **Certificate Authorities** tab, click the name of the certificate authority that issued the certificate.

4. Click the three dots to the right of the certificate.



PKI as a Service / partitions / sub5076c7ef83 / Certificate Authorities / CAs / issuer1 /
JS

issuer1 ···

Type
Issuing Subordinate Authority

Status
Active

CA Identifier
issuer1

Subject
CN=issuer1

Certificate Status Services
CRL: Enabled
OCSP: Enabled

URLs
CAGW: https://cagw.dev.pkihub.com/cagw/v1/certificate-authorities/sub5076c7ef83~issuer1
CRL:
http://crl.dev.pkihub.com/crl/sub5076c7ef83/issuer1/crl.crl
OCSP:
http://ocsp.dev.pkihub.com/ocsp/sub5076c7ef83/issuer1

CN=a125316174417.testcertificates.com, ST=CSR State, L=Ottawa, OU=ABC
issuer1 ✓ Issued Exp
00cbe9a3ed2fda858f41705d37da16b9a4 intune-digital-signature

CN=sub5076c7ef83_issuer1, OU=Validation Authorities, O=sub5076c7ef83
issuer1 ✓ Issued Expires in 21 days and 23 hours
008180575f7535c77c70dee558a5450f8e

5. Select one of the following options.

- Revoke Certificate
- Suspend Certificate

- Unsuspend Certificate

ℹ See Browsing certificates for a reference of the certificate details.

Revoke Certificate

Select this option to invalidate the digital certificate before its expiration date. See the table below for the supported **Revocation Reason** values.

Revocation reason	Description
Unspecified	Unknown revocation reason.
Key Compromise	The private key associated with the certificate has been compromised, and therefore, the certificate should be revoked to prevent unauthorized use.
CA compromise	The certificate authority is compromised, and revoking all the issued certificates mitigates risks.
Affiliation Changed	The certificate holder is no longer affiliated with the organization that requested the certificate.
Superseded	A newer certificate has replaced the certificate.
Cessation of Operation	The entity or service associated with the certificate is no longer operational.
Privilege Withdrawn	The privileges or rights granted by the certificate have been withdrawn.
AA Compromise	The entity responsible for issuing or managing attributes associated with the certificate has been compromised.

Suspend Certificate

Select this option to invalidate the digital certificate for a specified period.

ℹ Unlike certificate revocation, which permanently invalidates a certificate, suspension is typically used when there is a need to temporarily disable the certificate due to certain conditions or suspicions, but the certificate may be reinstated later if those conditions are resolved.

Unsuspend Certificate

Select this option to reverse the suspension of a certificate, making it valid again for use.

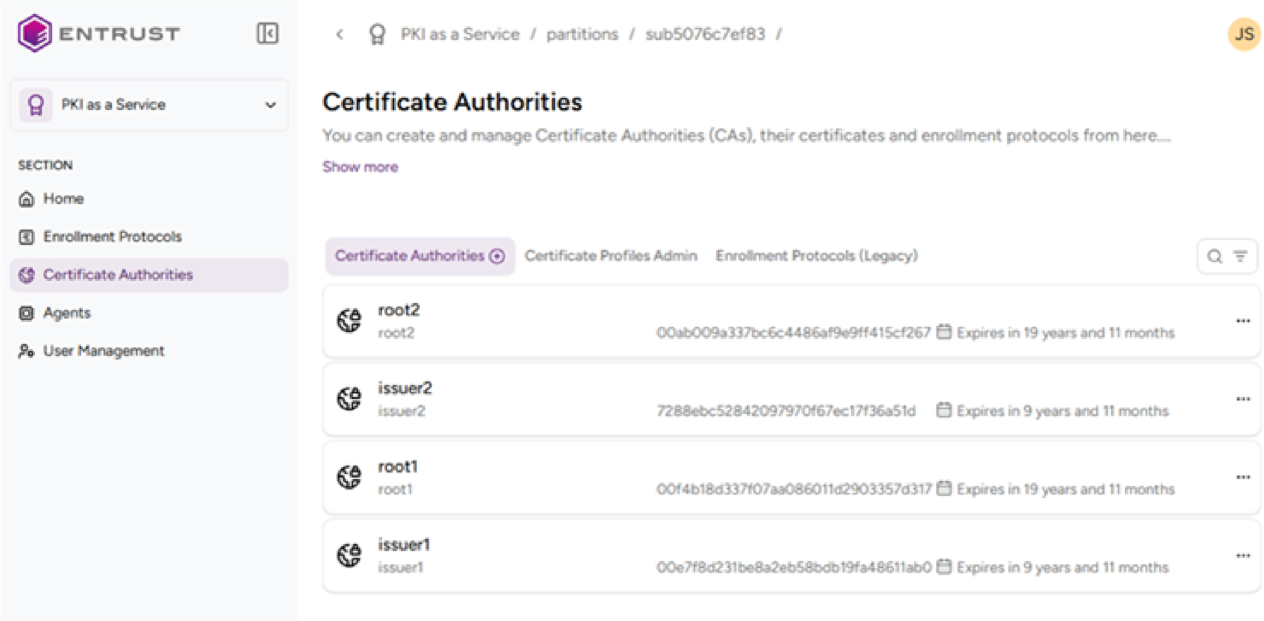
Downloading certificates

See below to download issued certificates.

To download a certificate:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the roles described under Managing roles.

2. Click **Certificate Authorities** in the sidebar.


ENTRUST
PKI as a Service
SECTION
Home
Enrollment Protocols
Certificate Authorities
Agents
User Management
PKI as a Service / partitions / sub5076c7ef83 /
JS
Certificate Authorities ⊕
Certificate Profiles Admin
Enrollment Protocols (Legacy)
...

Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

Show more

root2
root2 00ab009a337bc6c4486af9e9ff415cf267 Expires in 19 years and 11 months

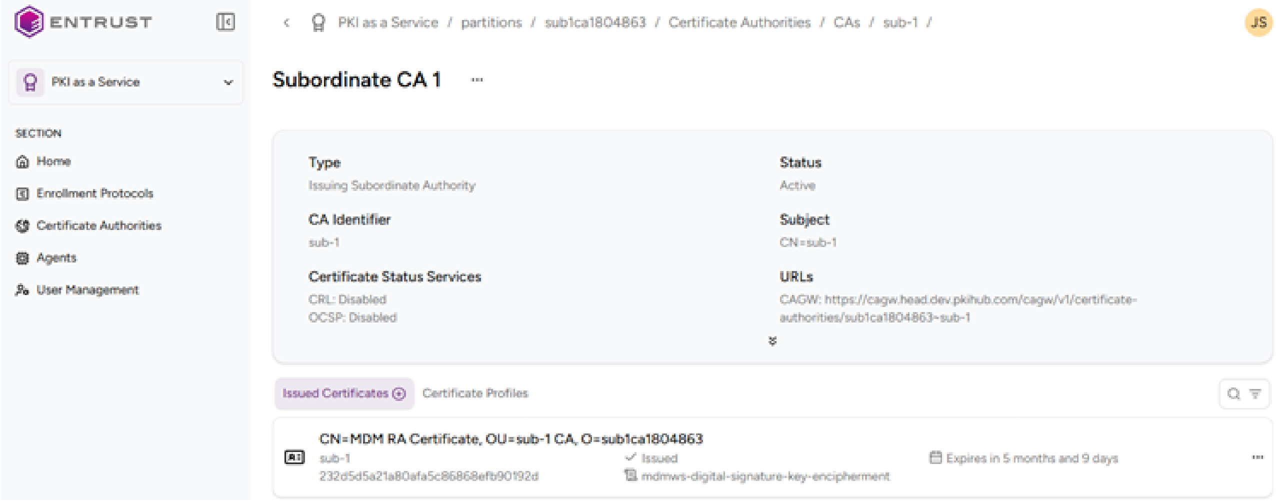
issuer2
issuer2 7288ebc52842097970f67ec17f36a51d Expires in 9 years and 11 months

root1
root1 00f4b18d337f07aa086011d2903357d317 Expires in 19 years and 11 months

issuer1
issuer1 00e7f8d231be8a2eb58bdb19fa48611ab0 Expires in 9 years and 11 months

3. In the **Certificate Authorities** tab, click the name of the certificate authority that issued the certificate.

4. In the **Issued Certificates** tab, click the certificate subject name.



Subordinate CA 1

Type
Issuing Subordinate Authority

Status
Active

CA Identifier
sub-1

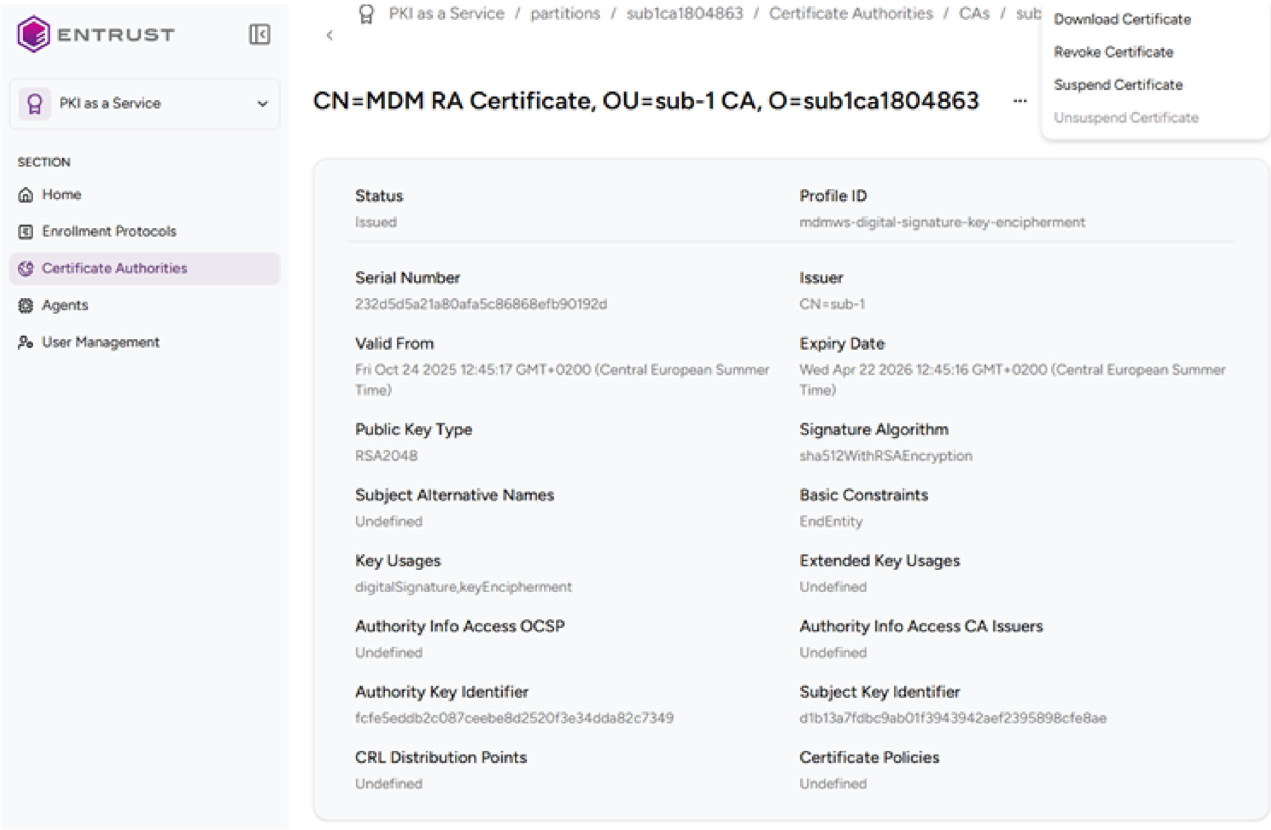
Subject
CN=sub-1

Certificate Status Services
CRL: Disabled
OCSP: Disabled

URLs
CAGW: https://cagw.head.dev.pkihub.com/cagw/v1/certificate-authorities/sub1ca1804863-sub-1

CN=MDM RA Certificate, OU=sub-1 CA, O=sub1ca1804863
sub-1
232d5d5a21a80afa5c86868efb90192d
✓ Issued
mdmws-digital-signature-key-encipherment
Expires in 5 months and 9 days

5. In the certificate details page, click the three dots to the right of the certificate subject name and select **Download Certificate**.



CN=MDM RA Certificate, OU=sub-1 CA, O=sub1ca1804863

Status
Issued

Profile ID
mdmws-digital-signature-key-encipherment

Serial Number
232d5d5a21a80afa5c86868efb90192d

Issuer
CN=sub-1

Valid From
Fri Oct 24 2025 12:45:17 GMT+0200 (Central European Summer Time)

Expiry Date
Wed Apr 22 2026 12:45:16 GMT+0200 (Central European Summer Time)

Public Key Type
RSA2048

Signature Algorithm
sha512WithRSAEncryption

Subject Alternative Names
Undefined

Basic Constraints
EndEntity

Key Usages
digitalSignature,keyEncipherment

Extended Key Usages
Undefined

Authority Info Access OCSP
Undefined

Authority Info Access CA Issuers
Undefined

Authority Key Identifier
fcfe5eddb2c087ceebe8d2520f3e34dda82c7349

Subject Key Identifier
d1b13a7fdbc9ab01f3943942aef2395898cfe8ae

CRL Distribution Points
Undefined

Certificate Policies
Undefined

Automating ACME enrollment

Configure PKIaaS to process ACME (Automated Certificate Management Environment) enrollment requests with PKIaaS Certification Authorities.

- ACME requirements
- Configuring ACME in PKIaaS
- ACME enrollment with Certbot

ACME requirements

You must meet the following requirements to automate ACME enrollment with a PKIaaS gateway.

- PKIaaS account requirements
- Certificate authority requirements
- Operating system requirements
- TLS Cipher requirements

PKIaaS account requirements

You need an Entrust PKIaaS account with privileges to create an issuing certificate authority.

Certificate authority requirements

Make sure you have a subordinate CA with a profile of the privatessl group. You can either:

- Create a new CA with this group, as explained in Creating an issuing subordinate CA.
- Add this group to an existing CA, as explained in Selecting CA profiles.

Operating system requirements

Enrollment integration for this release is tested and validated on the following operating system versions.

OS	Version
iPad	16.6
iPhone	16.6
macOS	Ventura 13.5.1
Windows	10 and 11
Android	13
ChromeOS	Not supported

TLS Cipher requirements

Enrollment URLs support the following TLS Ciphers.

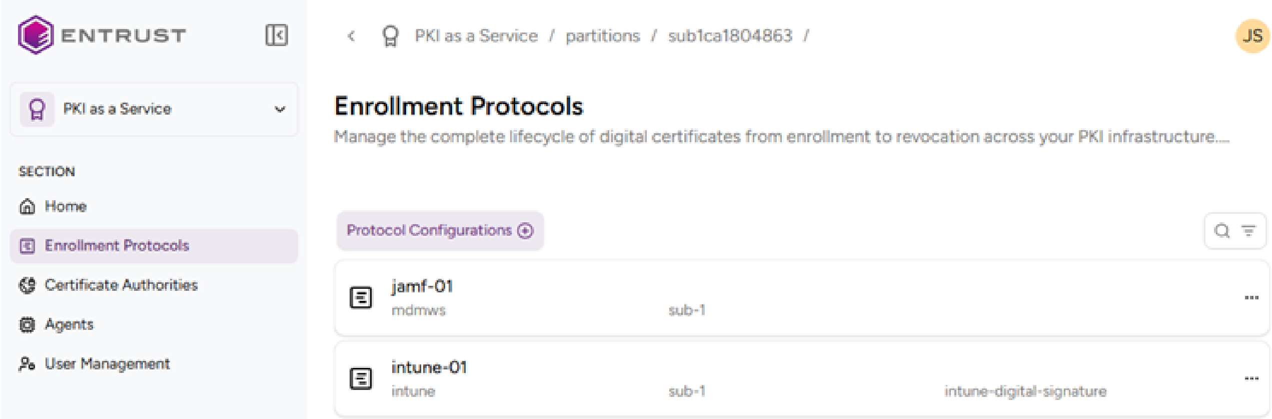
- `ECDHE-RSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES256-GCM-SHA384`

Configuring ACME in PKIaaS

Create a PKIaaS protocol configuration for ACME enrollment.

To create an ACME configuration in PKIaaS:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the following roles:
   - Owners
   - Protocol Operators
2. Click **Enrollment Protocols** in the sidebar.



Enrollment Protocols

Manage the complete lifecycle of digital certificates from enrollment to revocation across your PKI infrastructure....

jamf-01 | mdmws | sub-1

intune-01 | intune | sub-1 | intune-digital-signature

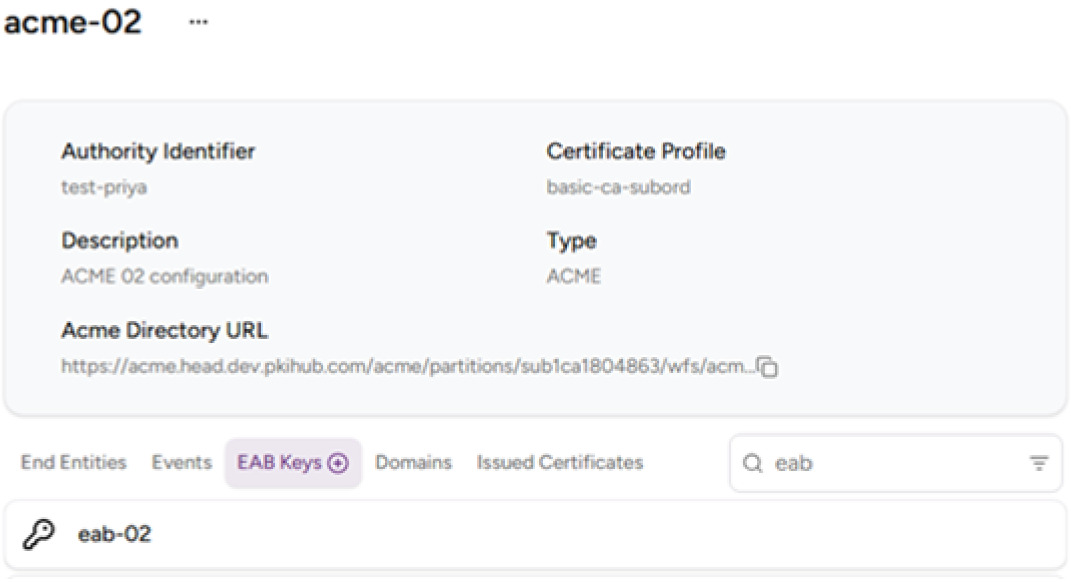
3. Click the plus **+** icon to the right of the **Protocol Configurations** tab.
4. Select **ACME** in the **Type** list.

5. Configure the following values in the **Create Protocol Config** dialog.

Field	Value
Protocol Configuration Identifier	Enter a unique identifier for the new configuration in your PKI. This identifier must be 2-18 characters long and can only include lowercase letters, numbers, hyphens (â□□-â□□), and underscores (â□□_â□□).
Description	Enter an optional description of the protocol purpose.
Authority Identifier	Select an issuing subordinate authority with profiles of the privatessl group.
Certificate Profile	Select a privatessl profile of the selected CA to enroll the certificates.

6. Click **Create**.

7. In the confirmation dialog, copy the URL under the **ACME Directory URL** section.



acme-02 ···

Authority Identifier
test-priya

Certificate Profile
basic-ca-subord

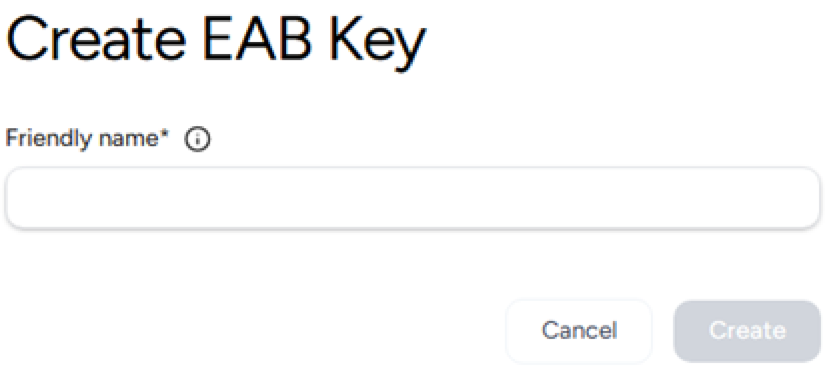
Description
ACME 02 configuration

Type
ACME

Acme Directory URL
https://acme.head.dev.pkihub.com/acme/partitions/sub1ca1804863/wfs/acm...

8. Click the plus **+** icon to the right of the **EAB Keys** tab.

9. In the **Create EAB Key Credentials** dialog, enter a username that is 2-18 characters long and only includes lowercase letters, numbers, hyphens (â□□-â□□), and underscores (â□□_â□□).

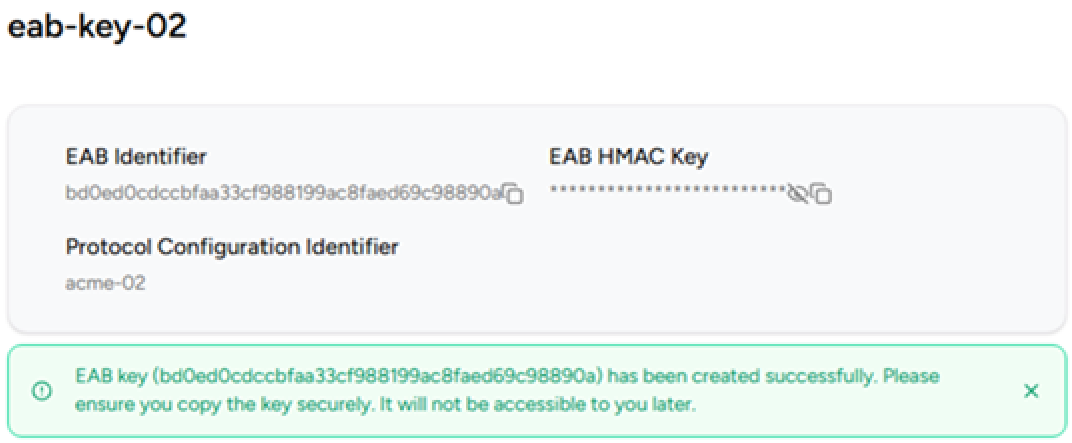


Create EAB Key

Friendly name*

10. Click **Create**.

11. Copy the **EAB Identifier** and **EAB HMAC Key** values displayed in the confirmation dialog.



eab-key-02

EAB Identifier
bd0ed0cdccbfaa33cf988199ac8faed69c98890a

EAB HMAC Key
****

Protocol Configuration Identifier
acme-02

EAB key (bd0ed0cdccbfaa33cf988199ac8faed69c98890a) has been created successfully. Please ensure you copy the key securely. It will not be accessible to you later.

⚠ As stated in the confirmation dialog before leaving this page, Entrust PKIaaS will not display the credential password again.

ACME enrollment with Certbot

See below for an example of ACME enrollment with Entrust PKIaaS and Certbot.

- Installing Certbot
- Setting REQUESTS_CA_BUNDLE
- Running Certbot

Installing Certbot

See below for installing Cerbot.

- Installing Certbot on Linux
- Installing Certbot on Windows

Installing Certbot on Linux

To install Certbot in a Linux distribution, you have the following options.

Distribution	Command
Most modern Linux distributions	`sudo snap install --classic certbot`
Debian-based systems like Ubuntu	`sudo apt update && sudo apt install certbot`

Installing Certbot on Windows

To install Certbot on a Windows platform, we recommend to:

1. Install Python3.

2. Run the `python -m pip install certbot` command.

Setting REQUESTS_CA_BUNDLE

For Certbot to trust your root CA certificates set the `REQUESTS_CA_BUNDLE` environment variable to the file path that contains the certificate.

Platform	Command	Example
Linux	`sudo REQUESTS_CA_BUNDLE=<root-CA-cert-file>`	`sudo REQUESTS_CA_BUNDLE=/tmp/root_ca.crt`
Windows	`set REQUESTS_CA_BUNDLE=<root-CA-cert-file>`	`set REQUESTS_CA_BUNDLE= "C:\root_ca.crt"`

Running Certbot

Run the following Certbot command to enroll a certificate using PKIaaS and the ACME protocol.

```
certbot certonly -d <domain> --server <acme-url> --standalone --no-eff-email --
agree-tos -m <email> --eab-kid <eab-kid>Â --eab-hmac-key <eab-hmac-key>
```

See below for a description of each parameter.

- `-d <domain>`
- `--server <acme-url>`
- `--standalone`
- `--agree-tos`
- `-m <email>`
- `--no-eff-email`
- `--eab-kid <eab-kid>`
- `--eab-hmac-key <eab-hmac-key>`

`-d <domain>`

Include the `<domain>` domain in the certificate. This option allows repetition, for example:

```
-d example.com -d www.example.com
```

`--server <acme-url>`

Use the `<acme-url>` enrollment URL, where `<acme-url>` is the **ACME Directory URL** described in Configuring ACME in PKIaaS.

`--standalone`

Make Certbot start its own lightweight web server to respond to ACME challenges from the certificate authority and verify that you control the specified domain.

⚠ If another application, such as a Web server, is running and using ports 80 or 443, disable the application.

`--agree-tos`

Automatically agree to the terms of service of the ACMEv2 server.

`-m <email>`

Use the `<email>` email address to register the ACME account with Entrust PKiaaS.

ℹ Entrust PKiaaS will not send email messages to this email address.

`--no-eff-email`

Do not share the `<email>` email address with the Electronic Frontier Foundation.

`--eab-kid <eab-kid>`

Use the `<eab-kid>` Key Identifier provided by Entrust PKIaaS for External Account Binding (EAB).

`--eab-hmac-key <eab-hmac-key>`

Use the `<eab-hmac-key>` HMAC Key provided by Entrust PKIaaS for External Account Binding (EAB).

Automating MDM Intune enrollment

Configure PKIaaS to operate as an SCEP Server and process MDM (Mobile Device Management) Intune enrollment requests with PKIaaS-hosted Certification Authorities.

- Intune requirements
- Creating an Intune application in Azure
- Configuring Intune in PKIaaS
- Downloading the Intune certification chain
- Configuring Intune profiles in Azure
- Enrolling user devices with the Intune Company Portal
- Renewing enrolled certificates
- Revoking and removing certificates

See the Microsoft documentation for details on the third-party SCEP integration with Intune.

https://learn.microsoft.com/en-us/mem/intune/protect/certificate-authority-add-scep-overview

Intune requirements

You must meet the following requirements to automate MDM Intune enrollment with a PKIaaS gateway.

- PKIaaS account requirements
- Certificate authority requirements
- Microsoft Azure requirements
- Operating system requirements
- Encryption algorithm requirements
- TLS Cipher requirements

PKIaaS account requirements

You need an Entrust PKIaaS account with privileges to create an issuing certificate authority.

Certificate authority requirements

Make sure you have a subordinate CA with a profile of the intune group. You can either:

- Create a new CA with this group, as explained in Creating an issuing subordinate CA.
- Add this group to an existing CA, as explained in Selecting CA profiles.

Microsoft Azure requirements

You need a Microsoft Azure account with privileges to create and configure an Intune application.

Operating system requirements

This release of the Intune automated enrollment is tested with devices running the following operating systems.

OS	Tested versions
macOS	Ventura 13.2.1
iPhone/iPad	16.3.1
AndroidOS	13
Microsoft Windows	10 and 11
ChromeOS	--

For more details on the supported operating systems, please check the Microsoft documentation:

https://learn.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers

Encryption algorithm requirements

The Intune automated enrollment with a PKIaaS gateway supports the following encryption algorithms.

- `aes128-CBC-PAD`
- `aes128-GCM`
- `aes256-CBC-PAD`

- `aes256-GCM`
- `desCBC`
- `des-ede3-cbc`
- `id-RSAES-OAEP`
- `rsaEncryption`

TLS Cipher requirements

Enrollment URLs support the following TLS Ciphers.

- `ECDHE-RSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES256-GCM-SHA384`

Creating an Intune application in Azure

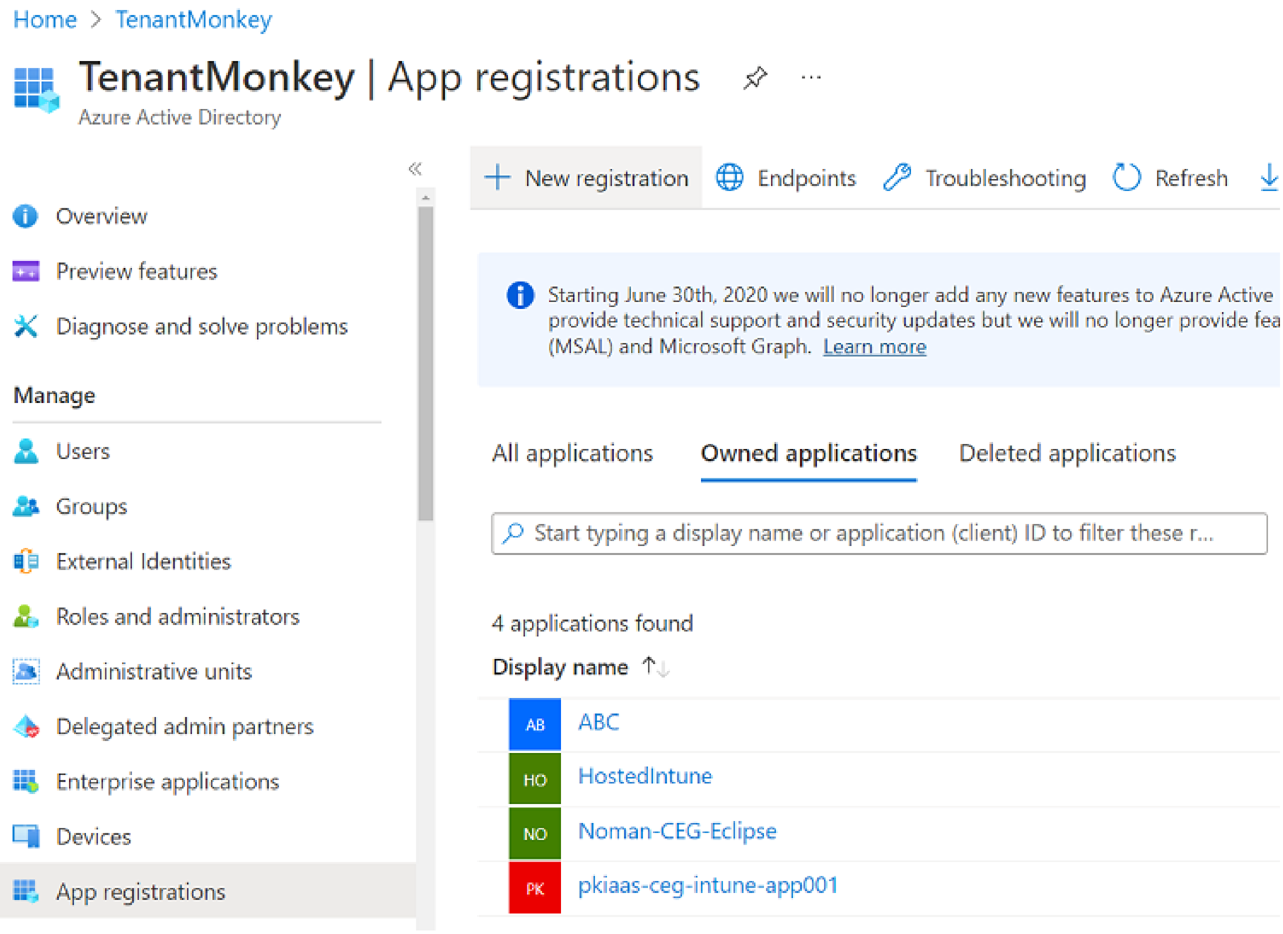
Create an application in the Microsoft Azure portal to run the Intune service.

---

i At the end of this process, you should have the **Application (client) ID**, **Directory (tenant) ID**, and **Client secret** values required when Configuring Intune in PKIaaS.

To create an Intune application in Azure:

1. Log in to https://portal.azure.com as a user with administrative permissions.
2. Go to **Home > App** registrations.

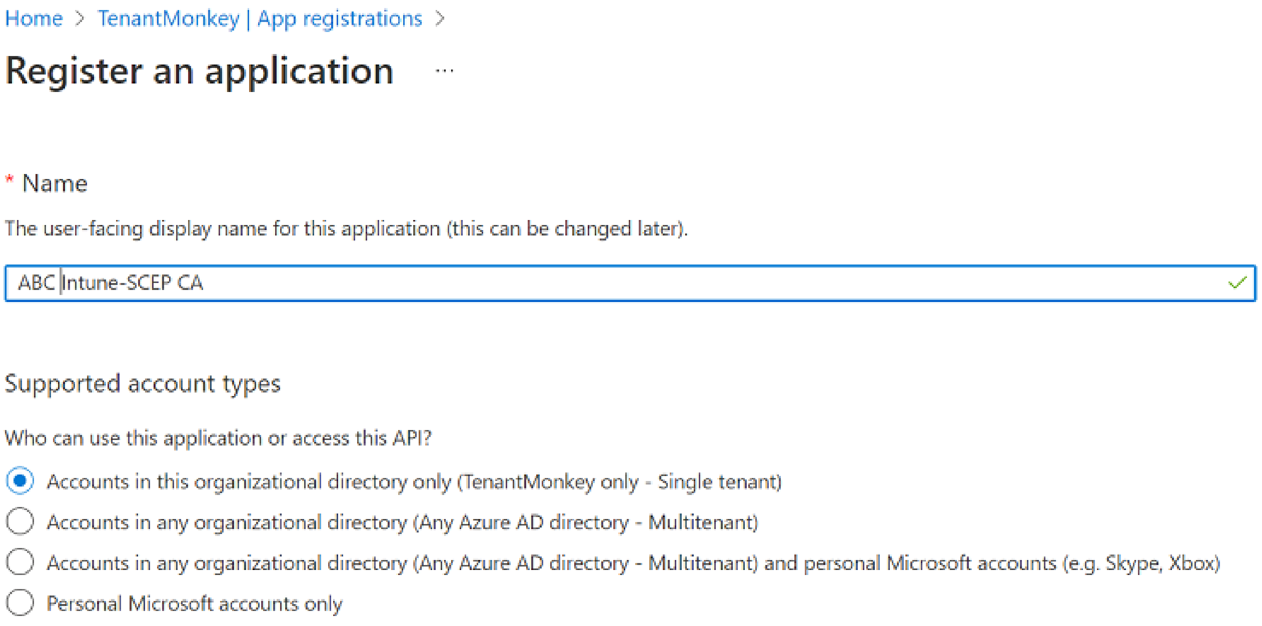


Starting June 30th, 2020 we will no longer add any new features to Azure Active provide technical support and security updates but we will no longer provide fea (MSAL) and Microsoft Graph. Learn more

4 applications found

Display name
AB ABC
HO HostedIntune
NO Noman-CEG-Eclipse
PK pkiaas-ceg-intune-app001

3. Click **New registration** to display the **Register an application** page.



Home > TenantMonkey | App registrations >

Register an application ···

* Name

The user-facing display name for this application (this can be changed later).

ABC Intune-SCEP CA ✓

Supported account types

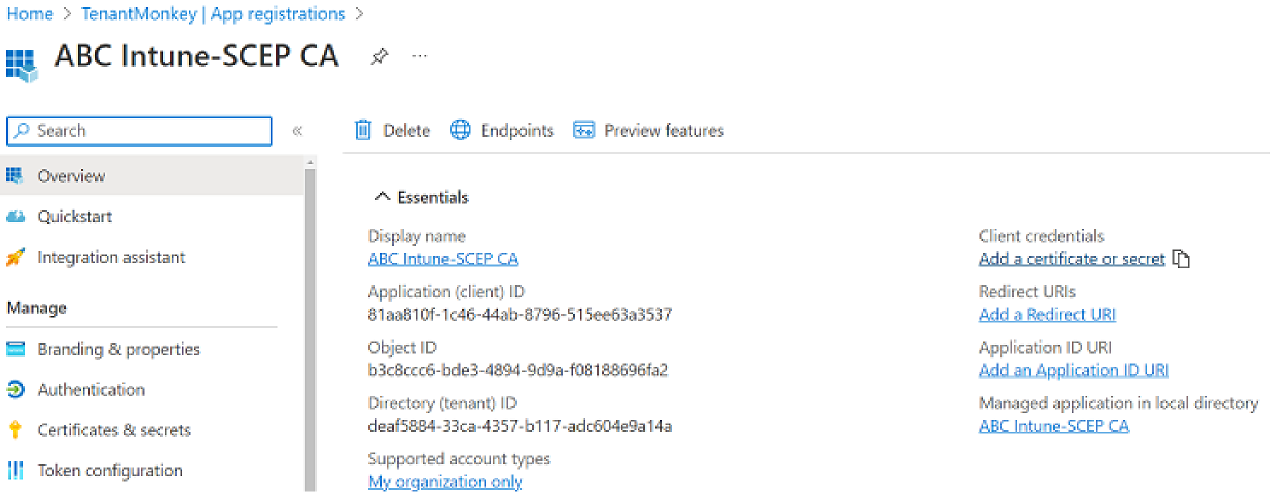
Who can use this application or access this API?

● Accounts in this organizational directory only (TenantMonkey only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

4. In the **Name** field, type the name of the new Intune application.

5. In the **Supported account types** list, ensure **Accounts in this organizational directory only (TenantMonkey only - Single tenant)** is selected.

6. Click **Register** to display the details of the new application.



Home > TenantMonkey | App registrations >

ABC Intune-SCEP CA

Essentials

Display name
ABC Intune-SCEP CA

Application (client) ID
81aa810f-1c46-44ab-8796-515ee63a3537

Object ID
b3c8ccc6-bde3-4894-9d9a-f08188696fa2

Directory (tenant) ID
deaf5884-33ca-4357-b117-adc604e9a14a

Supported account types
My organization only

Client credentials
Add a certificate or secret

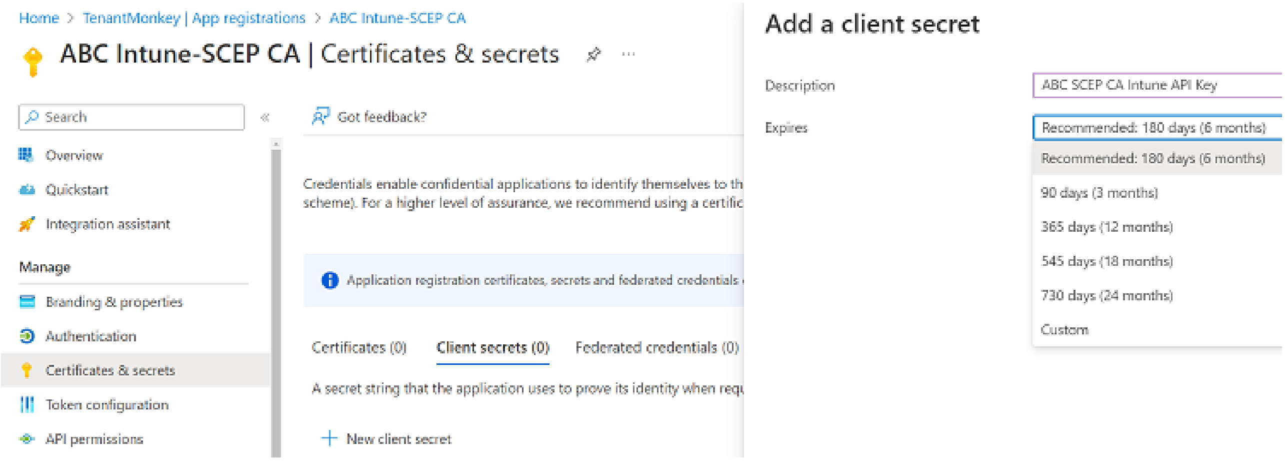
Redirect URIs
Add a Redirect URI

Application ID URI
Add an Application ID URI

Managed application in local directory
ABC Intune-SCEP CA

7. Copy the **Application (client) ID** and **Directory (tenant) ID** values in a text file. You will use these values when Configuring Intune in PKIaaS.

8. Click **Add a certificate or secret** to display the **Certificates & secrets** page.



Credentials enable confidential applications to identify themselves to th scheme). For a higher level of assurance, we recommend using a certific

Application registration certificates, secrets and federated credentials

A secret string that the application uses to prove its identity when requ

Description: ABC SCEP CA Intune API Key

Expires: Recommended: 180 days (6 months)

9. Click **New client secret** to display the **Add a client secret** dialog.

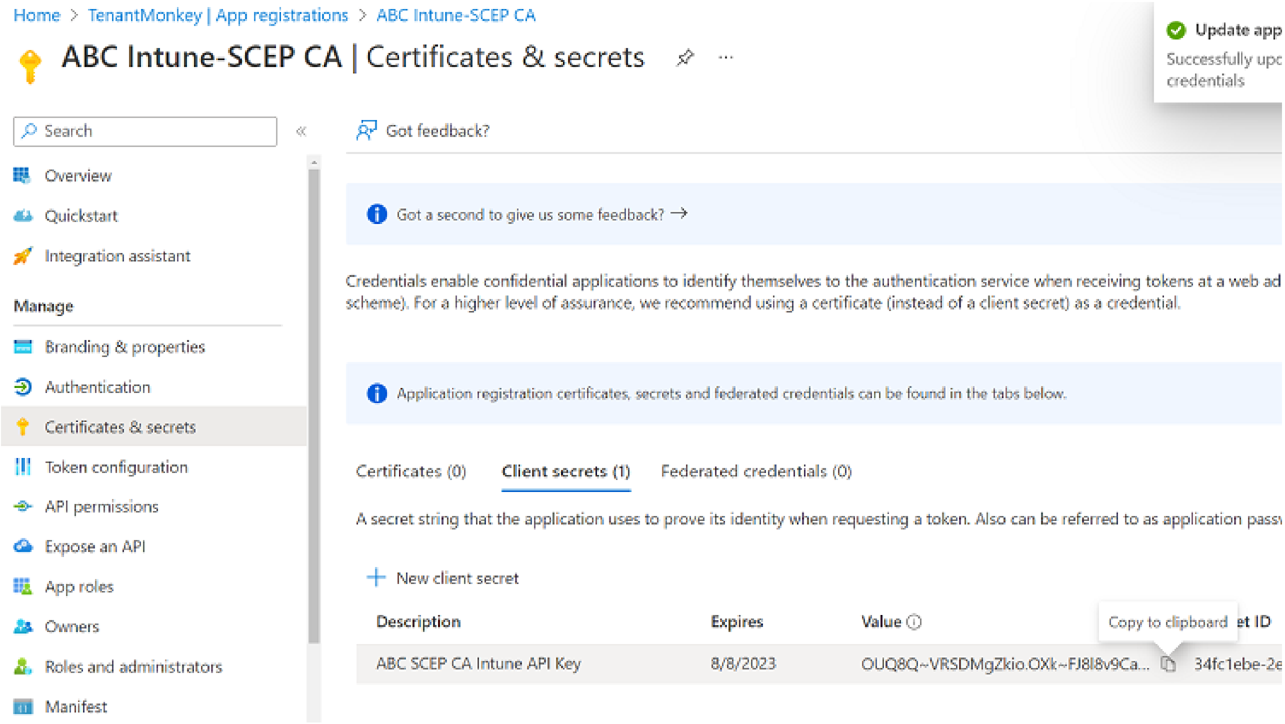
10. In the **Description** field, write a description of the new secret.

11. In the **Expires** drop-down list, select the expiration date of the new secret.

12. Click **Add** to add the new secret and close the **Add a client secret** dialog.

13. On the **Certificates & secrets** page, copy the **Value** of the new secret in a text file. You will use this value when Configuring Intune in PKIaaS.

⚠ The secret value will no longer be available after leaving this page.



Update app
Successfully upc credentials

Got a second to give us some feedback? →

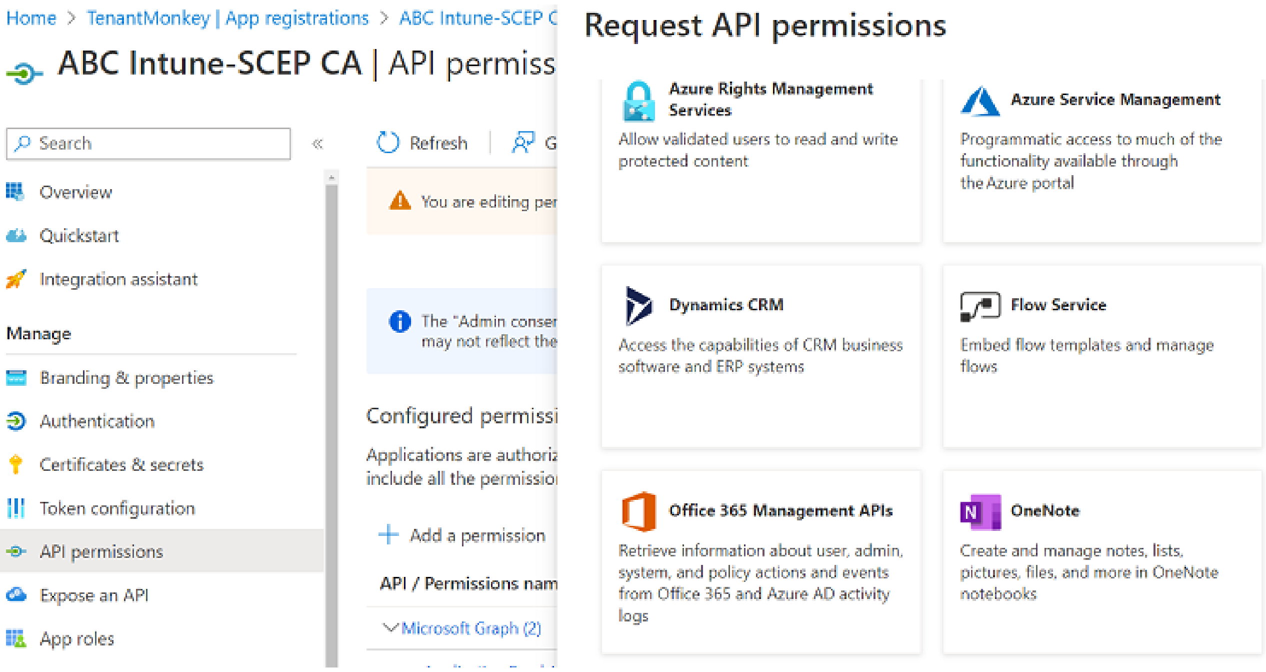
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web ad scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application passv

Description	Expires	Value	et ID
ABC SCEP CA Intune API Key	8/8/2023	OUQ8Q~VRSDMgZkio.OXk~FJ8l8v9Ca...	34fc1ebe-2e

14. In the navigation sidebar, click **API permissions** to display the **API permissions** page.



Request API permissions

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

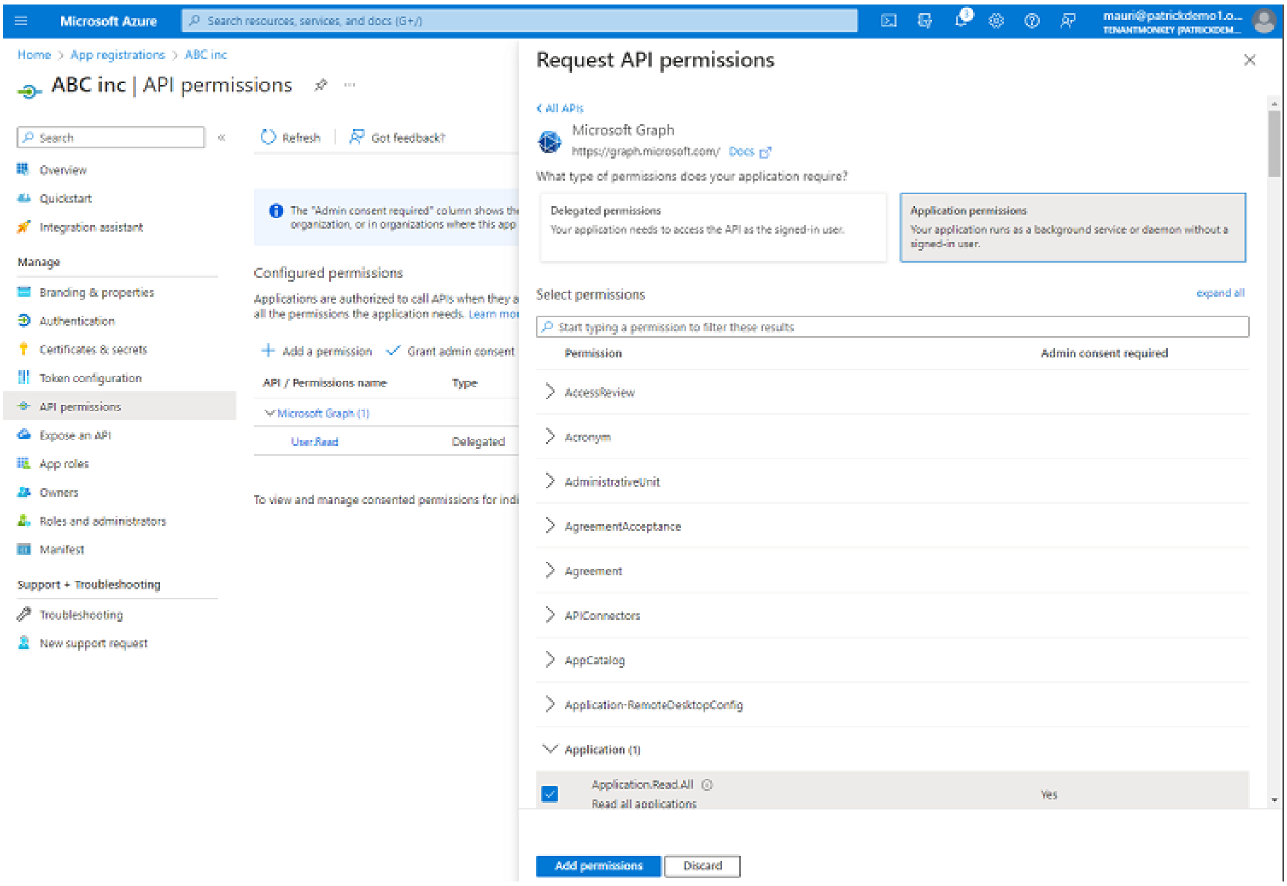
Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Flow Service
Embed flow templates and manage flows

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

OneNote
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

15. Click **Add a permission** to display the **Request API permissions** sidebar.



The "Admin consent required" column shows the organization, or in organizations where this app

Configured permissions

Applications are authorized to call APIs when they a all the permissions the application needs. Learn mor

API / Permissions name	Type
Microsoft Graph (1)	
User.Read	Delegated

To view and manage consented permissions for indi

Request API permissions

Microsoft Graph
https://graph.microsoft.com/

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Start typing a permission to filter these results

Permission	Admin consent required
AccessReview	
Acronym	
AdministrativeUnit	
AgreementAcceptance	
Agreement	
APIConnectors	
AppCatalog	
Application-RemoteDesktopConfig	
Application (1)	
☑ Application.Read.All Read all applications	Yes

16. In the **Request API permissions** sidebar:

    1. Click **Microsoft Graph**.
    2. Click **Application permissions**.
    3. Under **Select permissions**, expand the **Application** list and select the **Application.ReadAll** permissions.
    4. Click **Add permissions**.

17. Click **Add a permission** to display the **Request API permissions** sidebar again.

   1. In the **Request API permissions** sidebar:
   2. Click **Intune**.
   3. Click **Application permissions**.
   4. Under **Select permissions**, select the **scep_challenge_provider** permission.
   5. Click **Add permissions**.

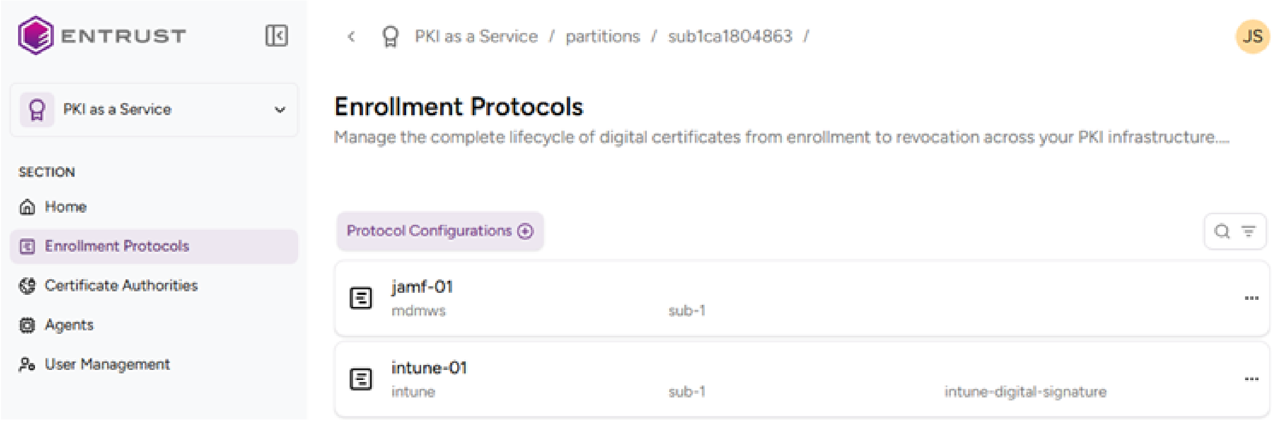
18. On the **API permissions** page, click **Add admin consent for the TenantMonkey** for granting these permissions to the new Intune application.

Configuring Intune in PKIaaS

Create a PKIaaS protocol configuration for MDM Intune enrollment.

To create a MDM Intune configuration in PKIaaS:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the following roles:
   - Owners
   - Protocol Operators
2. Click **Enrollment Protocols** in the sidebar.



Enrollment Protocols

Manage the complete lifecycle of digital certificates from enrollment to revocation across your PKI infrastructure....

jamf-01 mdmws	sub-1	
intune-01 intune	sub-1	intune-digital-signature

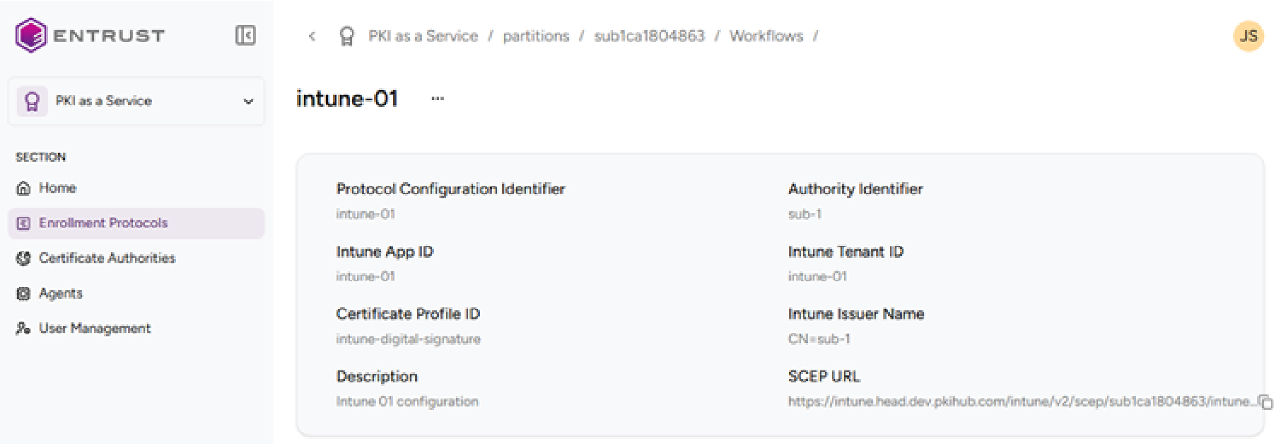
3. Click the plus **+** icon to the right of the **Protocol Configurations** tab.
4. Select **MDM Intune** in the **Type** list.
5. Configure the following values.

Field	Value
Protocol Configuration Identifier	Enter a unique identifier for the new configuration in your PKI. This identifier must be 2-18 characters long and can only include lowercase letters, numbers, hyphens (â□□-â□□), and underscores (â□□_â□□).
Intune Tenant ID	Paste the **Directory (tenant) ID** value previously obtained when Creating an Intune application in Azure.
Intune App ID	Paste the **Application (client) ID** value previously obtained when Creating an Intune application in Azure.

Field	Value
Intune App key	Paste the secret value previously obtained when Creating an Intune application in Azure.
Description	Enter an optional description of the protocol purpose.
Authority Identifier	Select an issuing subordinate CA with profiles of the intune group.
Certificate Profile	Select an intune profile of the CA for issuing the enrolled certificates.

6. Click **Create**.

7. In the confirmation dialog, copy the URL of the **SCEP URL** field.



intune-01

Protocol Configuration Identifier: intune-01

Authority Identifier: sub-1

Intune App ID: intune-01

Intune Tenant ID: intune-01

Certificate Profile ID: intune-digital-signature

Intune Issuer Name: CN=sub-1

Description: Intune 01 configuration

SCEP URL: https://intune.head.dev.pkihub.com/intune/v2/scep/sub1ca1804863/intune...

Downloading the Intune certification chain

Follow the steps described in Downloading a CA certificate to download the certificates for:

- The subordinate CA described in Configuring Intune in PKIaaS.
- The root CA of this subordinate CA.

You will need these certificates when Configuring Intune profiles in Azure.

Configuring Intune profiles in Azure

In the Microsoft Azure portal, create and configure the required profiles to automate Intune enrollment with a PKIaaS gateway.

- Creating Intune profiles for Windows in Azure
- Creating Intune profiles for Android in Azure
- Creating Intune profiles for macOS in Azure
- Creating Intune profiles for iOS and iPadOS in Azure

See the following Microsoft guides for more details on Azure profile management.

- https://learn.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root
- https://learn.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep

- https://learn.microsoft.com/en-us/troubleshoot/mem/intune/certificates/troubleshoot-scep-certificate-profiles

Creating Intune profiles for Windows in Azure

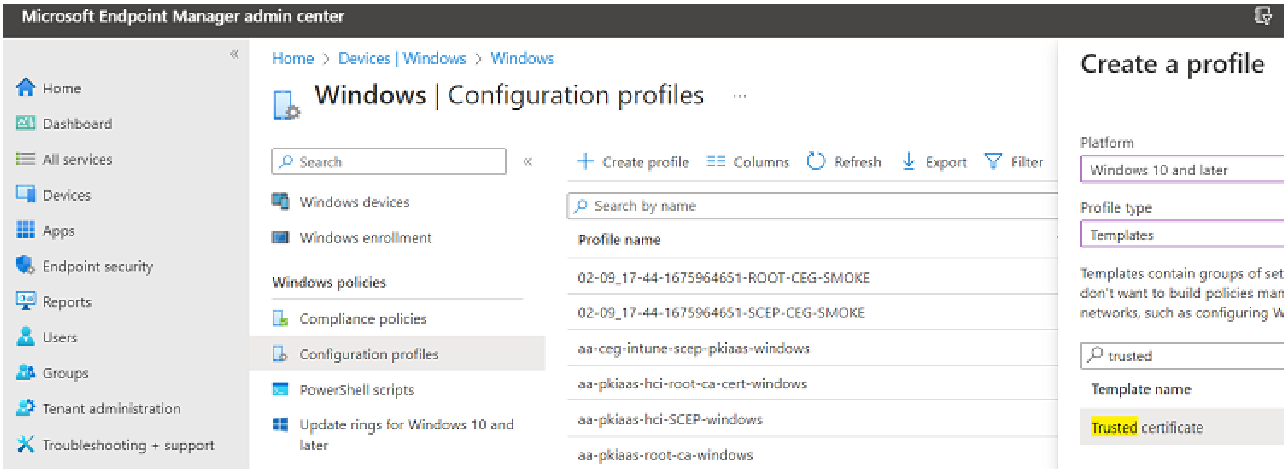
Create the following profiles to enroll Microsoft Windows devices with Intune.

- A root CA profile
- An issuing CA profile
- An SCEP profile

To create a Windows profile for Intune:

1. Log in to https://endpoint.microsoft.com as a user with administrative privileges.

2. Go to **Devices** > **Windows** > **Configuration profiles**.



Profile name
02-09_17-44-1675964651-ROOT-CEG-SMOKE
02-09_17-44-1675964651-SCEP-CEG-SMOKE
aa-ceg-intune-scep-pkiaas-windows
aa-pkiaas-hci-root-ca-cert-windows
aa-pkiaas-hci-SCEP-windows
aa-pkiaas-root-ca-windows

Platform: Windows 10 and later
Profile type: Templates

Templates contain groups of set don't want to build policies man networks, such as configuring W

trusted
Template name
Trusted certificate

3. Click **Create profile**.

4. Configure the values described in the following sections.
   - Create a profile
   - Basics
   - Configuration settings
   - Assignments
   - Applicability Rules
   - Review and create

Create a profile

In the **Create a profile** dialog, select the following values for each Windows profile.

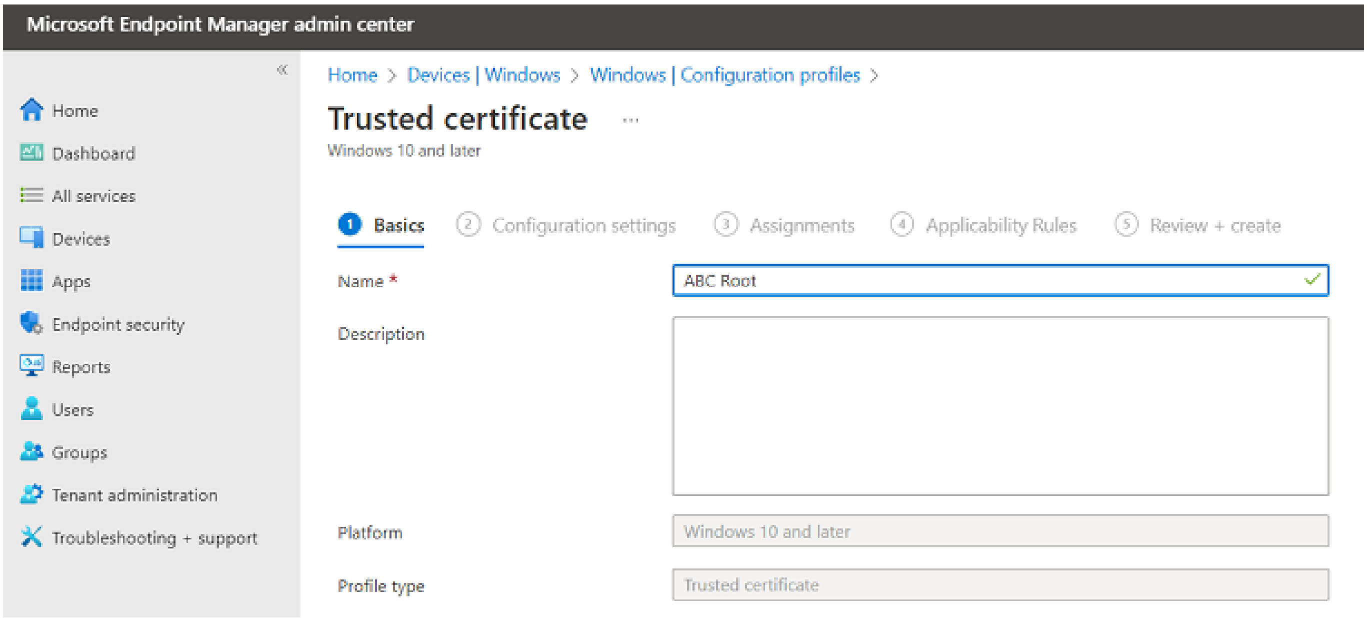
Setting	root CA profile	issuing CA profile	SCEP profile
â□□Platform	Windows 10 and laterâ□□	Windows 10 and laterâ□□	Windows 10 and laterâ□□
Profile type	Templates	Templates	Templates
Template name	Trusted certificate	Trusted certificate	SCEP certificate

Basics

In the **Name** field of the **Basics** page, type the name of the profile â□□ for example:

- ABC Root
- ABC Issuing
- ABC Digital Signature SCEP Cert

Optionally, add a description of the profile purpose.



Trusted certificate ...

Windows 10 and later

Name * ABC Root

Description

Platform Windows 10 and later

Profile type Trusted certificate

Configuration settings

When creating a root or issuing CA profile for Windows, configure the following settings on the **Configuration settings** page.

Setting	Root CA profile	Issuing CA profile
â□□Certificate file	The root certificate authority certificate	The issuing certificate authority certificate
Destination store	Computer certificate store - Root	Computer certificate store - Intermediate

⚠ See Downloading a CA certificate to download CA certificates.

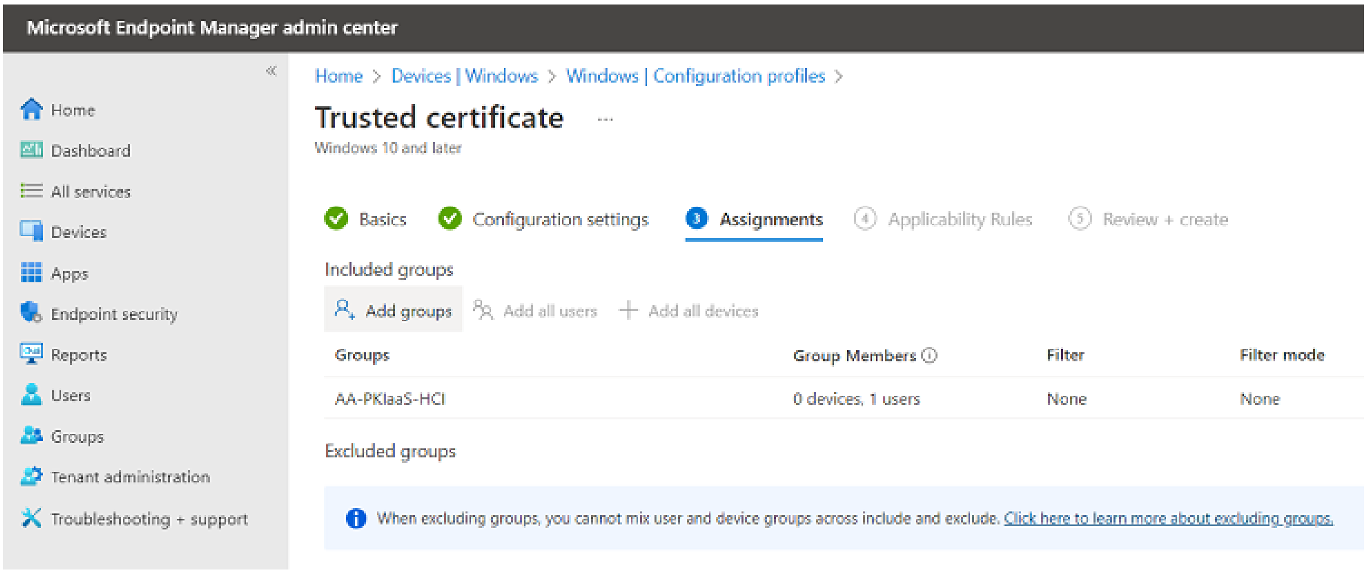
When creating an SCEP profile for Windows, configure the following settings on the Configuration settings page.

Setting	Value
Certificate type	Select **User**.
Subject name format	The syntax of the certificate subject names. This field supports the variables described in https://learn.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep

Setting	Value
Subject alternative name	The value of each attribute in the certificate subject alternative name. Optional.
Certificate validity period	The validity period of the certificates.
Key storage provider (KSP)	Select **Enroll to Software KSP** for Windows 10 Intune enrollments; select any of the listed values for Windows 11.
Key usage	The key usage of the enrolled certificates.
Key size (bits)	Select **2048** (Entrust PKIaaS does not support key sizes below 2048).
Hash algorithm	Select **SHA-2**.
Root certificate	Select the root CA profile.
Extended key usage	Select **Client Authentication**.
SCEP Server URLs	Paste one of the URLs obtained when Configuring Intune in PKIaaS.

Assignments

On the Assignments page, select the user group of the Intune-enrolled devices.



Included groups

Groups	Group Members	Filter	Filter mode
AA-PKIaaS-HCI	0 devices, 1 users	None	None

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

Applicability Rules

On the **Applicability Rules** page, select optional filters for the selected group - for example, the operating system of the devices.

Review and create

On the **Review + create** page, check the settings of the new profile and click **Create** to confirm the profile creation.

Creating Intune profiles for Android in Azure

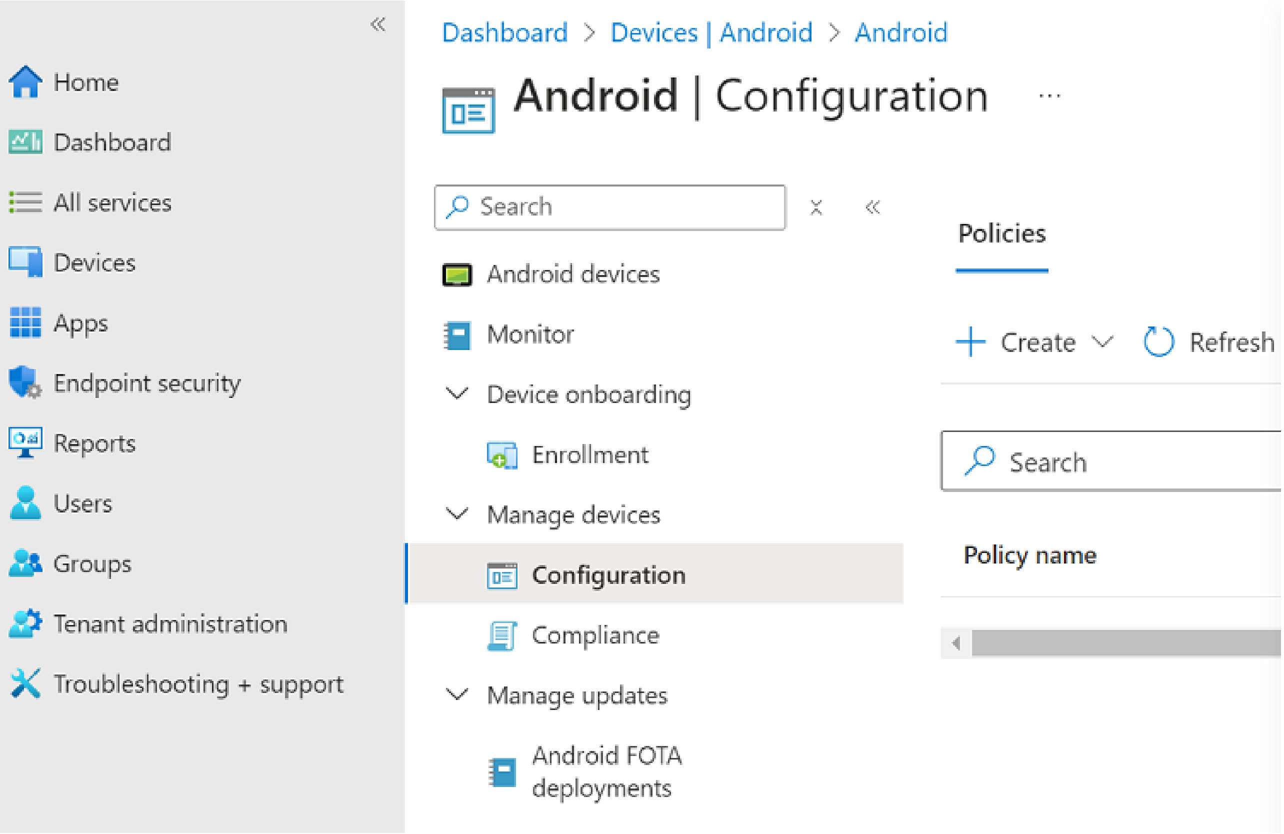
Create the following profiles to enroll Microsoft Windows devices with Intune.

- A root CA profile
- An issuing CA profile
- An SCEP profile

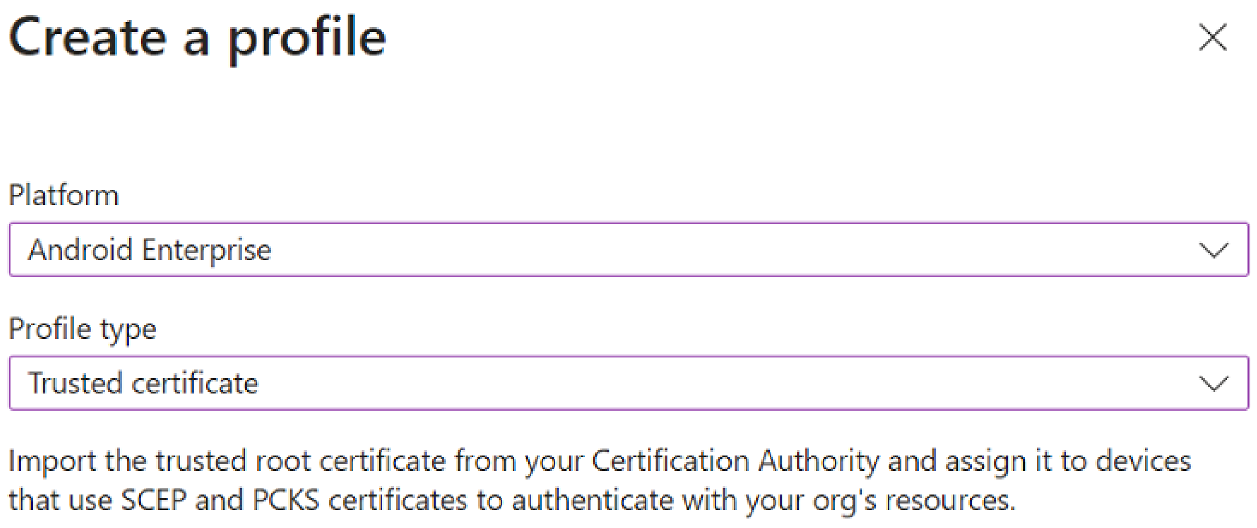
To create an Android profile for Intune:

1. Log in to https://endpoint.microsoft.com as a user with administrative privileges.

2. Go to **Devices** > **Android**.



3. Select **Manage devices** > **Configuration** and click **Create**.



Create a profile

Platform

Android Enterprise

Profile type

Trusted certificate

Import the trusted root certificate from your Certification Authority and assign it to devices that use SCEP and PCKS certificates to authenticate with your org's resources.

4. In the **Create a profile** dialog, configure the settings described in the following sections.
   - Create a profile
   - Basics
   - Configuration settings
   - Assignments
   - Review and create

Create a profile

In the **Create a profile** dialog, select the following fields for each Android profile.

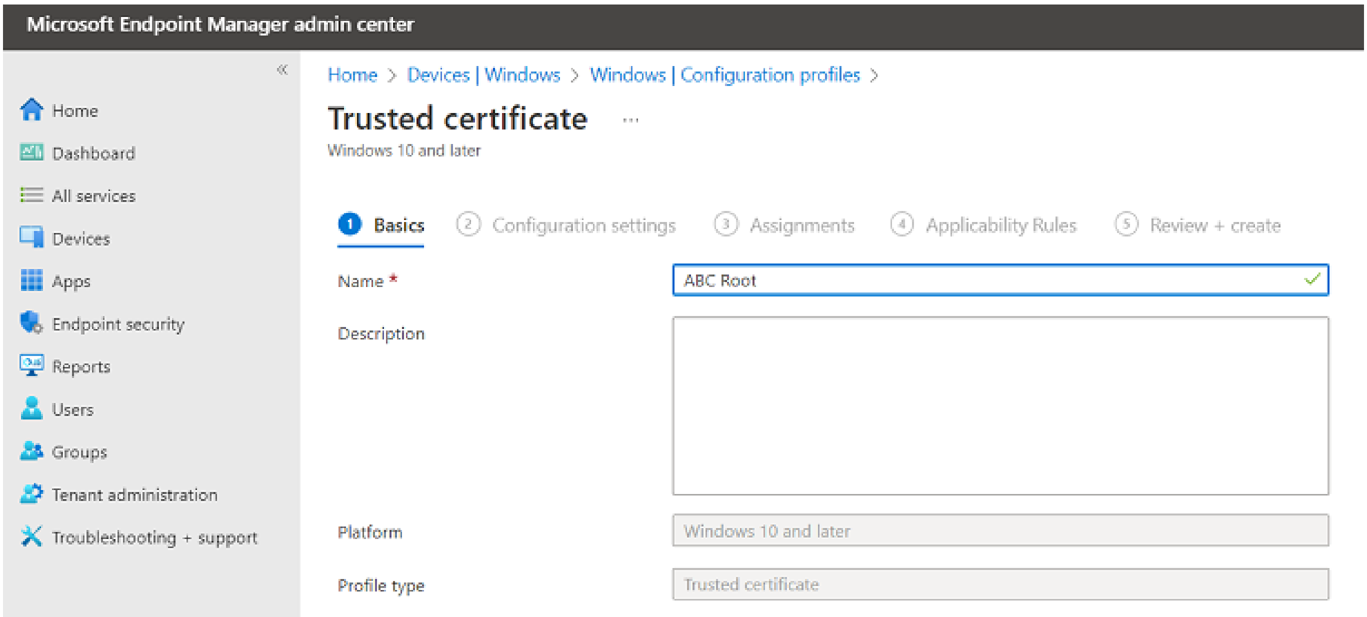
Setting	Root CA profile	Issuing CA profile	SCEP profile
â□□Platform	Android Enterprise	Android Enterprise	Android Enterprise
Profile type	Trusted certificate	Trusted certificate	SCEP certificate

Basics

In the **Name** field of the **Basics** page, type the name of the profile â□□ for example:

- ABC Root
- ABC Issuing
- ABC Digital Signature SCEP Cert

Optionally, add a description of the profile purpose.



Trusted certificate

Windows 10 and later

Name * ABC Root

Description

Platform Windows 10 and later

Profile type Trusted certificate

Configuration settings

When creating root or issuing CA profiles, configure the following settings on the Configuration settings page.

Settings	Root CA profile	Issuing CA profile
â□□Certificate file	The root certificate authority certificate	The issuing certificate authority certificate

ℹ See Downloading a CA certificate to download CA certificates.

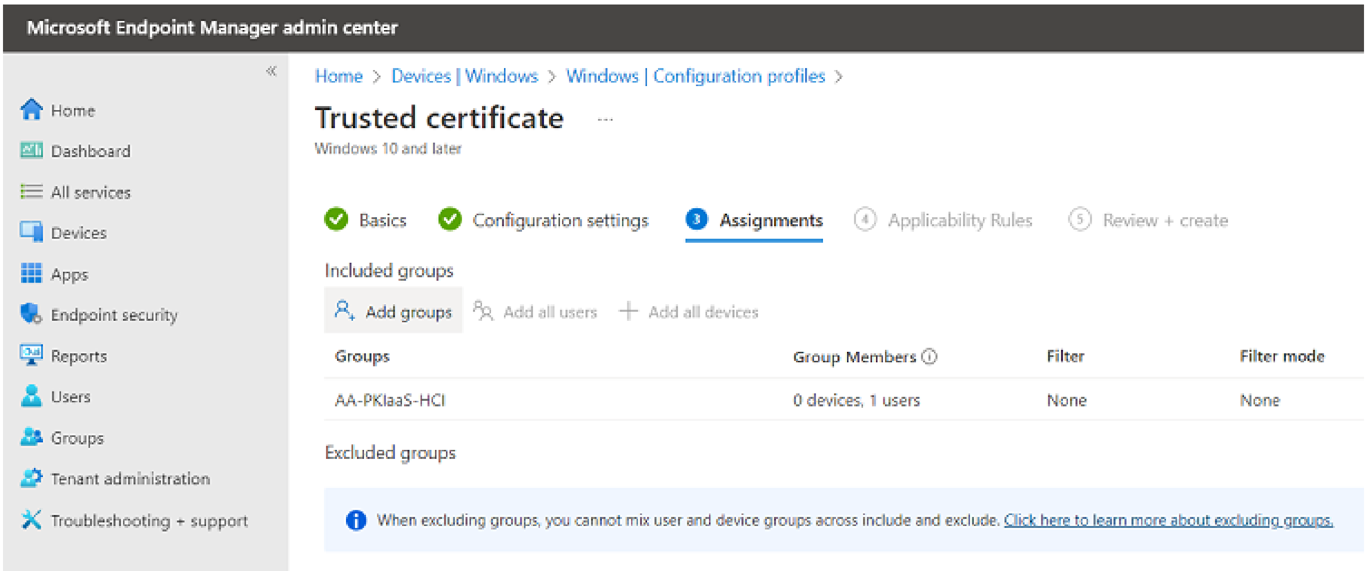
When creating an SCEP profile for Android, configure the following settings on the **Configuration settings** page.

Setting	Value
Certificate type	Select User.
Subject name format	The syntax of the certificate subject names. This field supports the variables described in https://learn.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep
Subject alternative name	The value of each attribute in the certificate subject alternative name. Optional.
Certificate validity period	The validity period of the certificates.
Key usage	The key usage of the enrolled certificates.
Key size (bits)	Select 2048 or 4096 (Entrust PKIaaS does not support key sizes below 2048).

Setting	Value
Hash algorithm	Select SHA-2.
Root certificate	Select the root CA profile
Extended key usage	Select Client Authentication.
SCEP Server URLs	Paste one of the URLs obtained when Configuring Intune in PKIaaS.

Assignments

On the **Assignments** page, select the user group of the Intune-enrolled devices.



Included groups

Groups	Group Members	Filter	Filter mode
AA-PKIaaS-HCI	0 devices, 1 users	None	None

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

Review and create

On the **Review + create** page, check the settings of the new profile and click **Create** to confirm the profile creation.

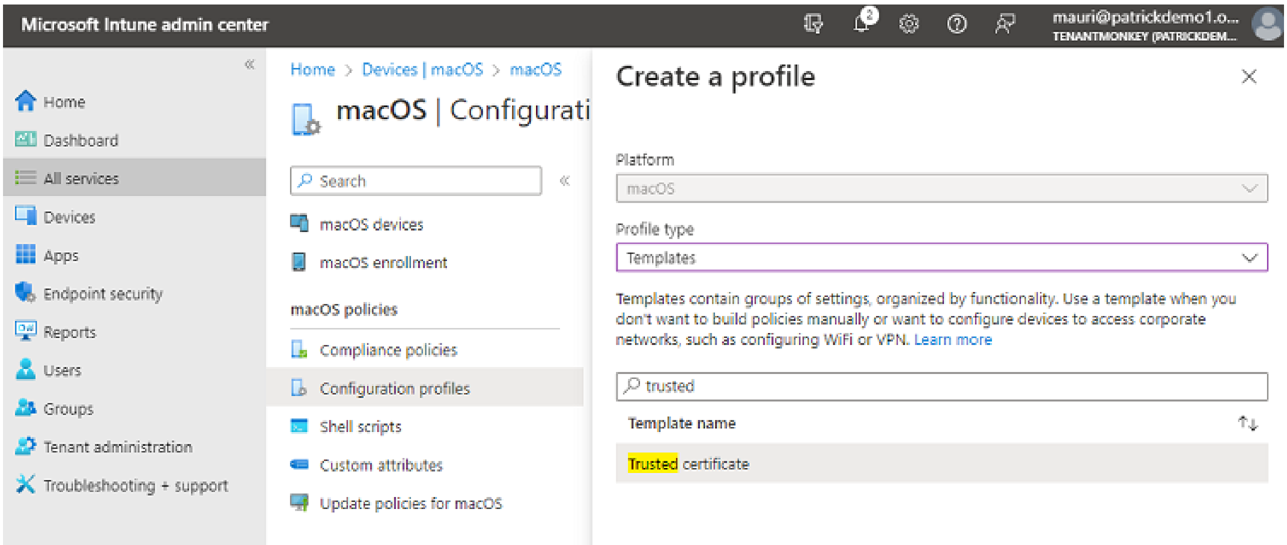
Creating Intune profiles for macOS in Azure

Create the following profiles to enroll macOS devices with Intune.

- A root CA profile
- An issuing CA profile
- An SCEP profile

To create a macOS profile for Intune:

1. Log in to https://endpoint.microsoft.com as a user with administrative privileges.
2. Go to **Devices > macOS > Configuration profiles**.



Create a profile

Platform: macOS

Profile type: Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

trusted

Template name
Trusted certificate

3. Click **Create profile**.

4. Configure the settings described in the following sections.

    - Create a profile
    - Configuration settings
    - Assignments
    - Review and create

Create a profile

On the **Create a profile** dialog, select the following fields for the SCEP profile.

Setting	Root CA profile	Issuing CA profile	SCEP profile
â□□Platform	macOS Enterprise	macOS Enterprise	macOS Enterprise
Profile type	Templates	Templates	Templates
Template name	Trusted certificate	Trusted certificate	SCEP certificate

Configuration settings

When creating root or issuing CA profiles, configure the following settings on the **Configuration settings** page.

Setting	Root CA profile	Issuing CA profile
â□□Certificate file	The root certificate authority certificate	The issuing certificate authority certificate

ℹ See Downloading a CA certificate to download CA certificates.

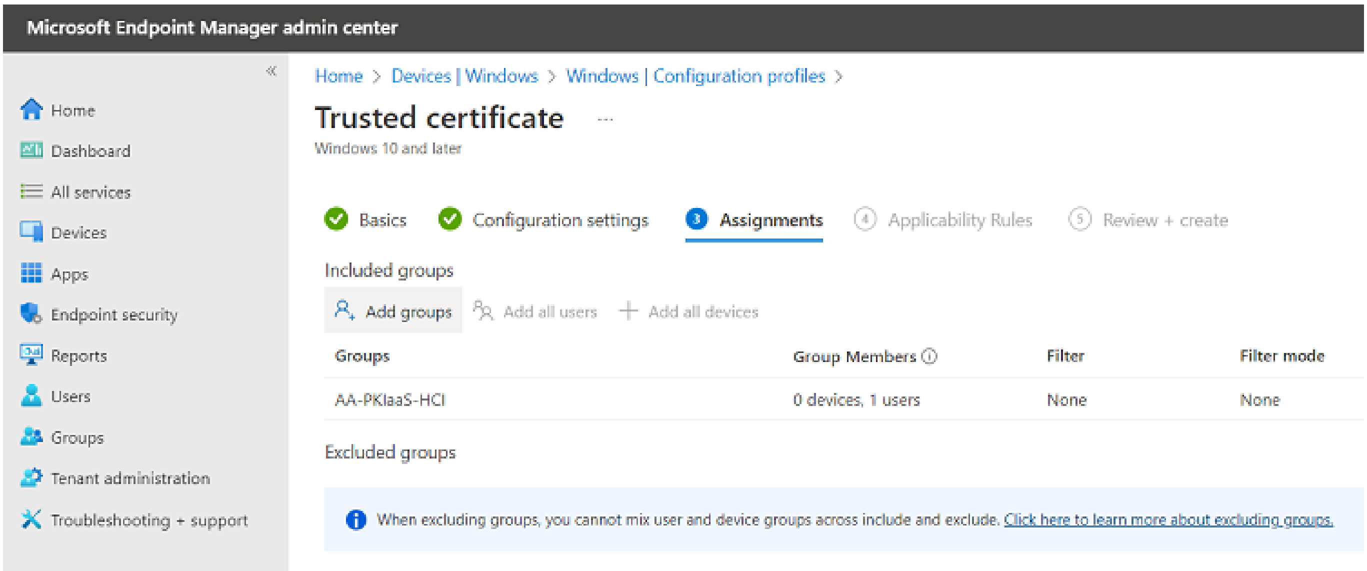
When creating an SCEP profile, configure the following settings on the **Configuration settings** page.

Setting	Value

Setting	Value
Certificate type	Select **User**
Subject name format	The syntax of the certificate subject names. This field supports the variables described in https://learn.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep
Subject alternative name	The value of each attribute in the certificate subject alternative name. Optional.
Certificate validity period	The validity period of the certificates.
Key usage	The key usage of the enrolled certificates.
Key size (bits)	Select **2048** or **4096** (Entrust PKIaaS does not support key sizes below 2048).
Hash algorithm	Select **SHA-2**.
Root certificate	Select the root CA profile.
Extended key usage	Select **Client Authentication**.
SCEP Server URLs	Paste one of the URLs obtained when Configuring Intune in PKIaaS.

Assignments

On the **Assignments** page, select the user group of the Intune-enrolled devices.



Groups	Group Members ⓘ	Filter	Filter mode
AA-PKIaaS-HCI	0 devices, 1 users	None	None

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

Review and create

On the **Review + create** page, check the settings of the new profile and click **Create** to confirm the profile creation.

Creating Intune profiles for iOS and iPadOS in Azure

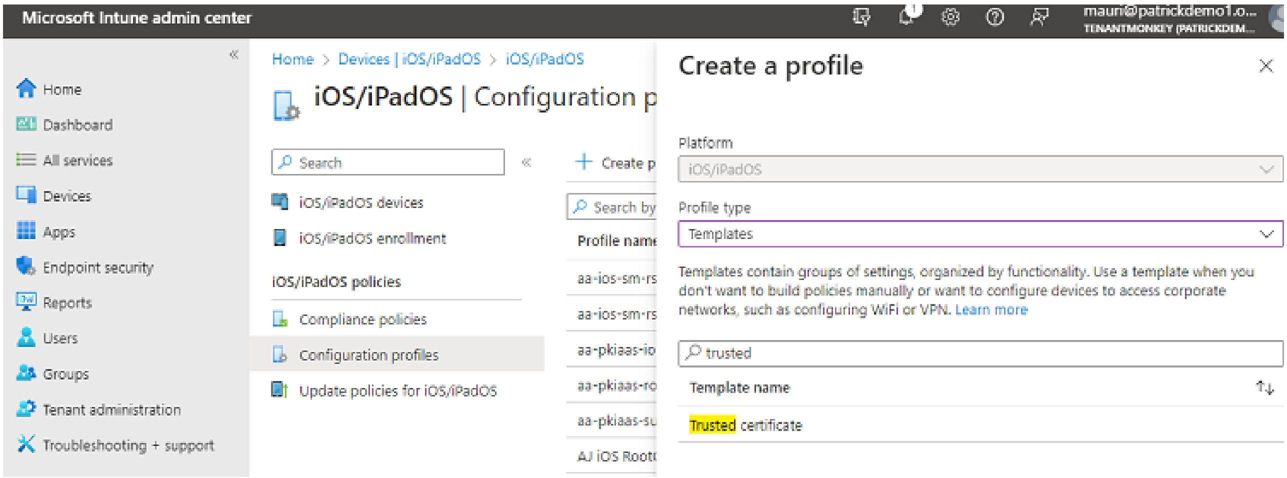
Create the following profiles to enroll iOS and iPadOS devices with Intune.

- A root CA profile
- An issuing CA profile
- An SCEP profile

To create an iOS or iPadOS profile for Intune:

1. Log in to https://endpoint.microsoft.com as a user with administrative privileges.

2. Go to **Devices > iOS/iPadOS > Configuration profiles**.



Platform: iOS/iPadOS

Profile type: Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

trusted

Template name
Trusted certificate

3. Click **Create profile**.

4. Configure the settings described in the following sections.

   - Create a profile
   - Configuration settings
   - Assignments
   - Review and create

Create a profile

On the **Create a profile** dialog, select the following fields for the SCEP profile.

Setting	Root CA profile	Issuing CA profile	SCEP profile
â□□Platform	iOS/iPadOS	iOS/iPadOS	iOS/iPadOS
Profile type	Templates	Templates	Templates
Template name	Trusted certificate	Trusted certificate	SCEP certificate

Configuration settings

When creating root or issuing CA profiles, configure the following settings on the **Configuration settings** page.

Setting	Root CA profile	Issuing CA profile
â□□Certificate file	The root certificate authority certificate	The issuing certificate authority certificate

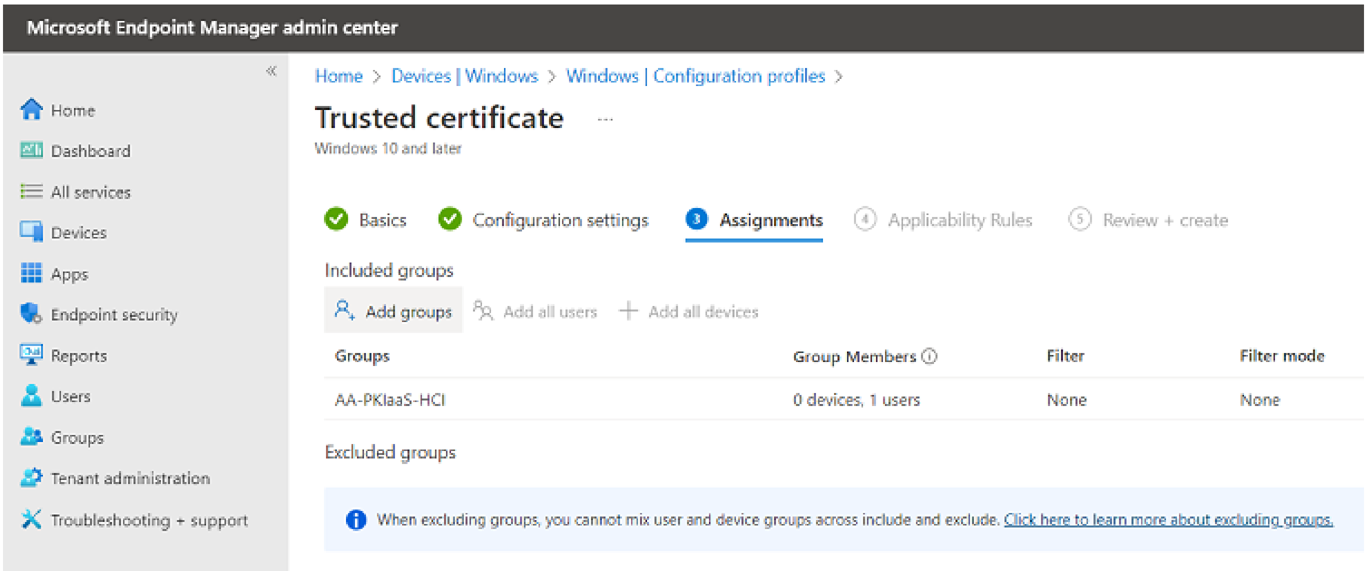
ℹ See Downloading a CA certificate to download CA certificates.

When creating an SCEP profile, configure the following settings on the **Configuration settings** page.

Setting	Value
Certificate type	Select **User**
Subject name format	The syntax of the certificate subject names. This field supports the variables described in https://learn.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep
Subject alternative name	The value of each attribute in the certificate subject alternative name. Optional.
Certificate validity period	The validity period of the certificates.
Key usage	The key usage of the enrolled certificates.
Key size (bits)	Select **2048** or **4096** (Entrust PKIaaS does not support key sizes below 2048).
Hash algorithm	Select **SHA-2**.
Root certificate	Select the root CA profile.
Extended key usage	Select **Client Authentication**.
SCEP Server URLs	Paste one of the URLs obtained when Configuring Intune in PKIaaS.

Assignments

On the **Assignments** page, select the user group of the Intune-enrolled devices.



Trusted certificate ...

Windows 10 and later

Included groups

Groups	Group Members ⓘ	Filter	Filter mode
AA-PKIaaS-HCI	0 devices, 1 users	None	None

Excluded groups

ⓘ When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

Review and create

On the **Review + create** page, check the settings of the new profile and click **Create** to confirm the profile creation.

Enrolling user devices with the Intune Company Portal

When completing the Intune integration steps, download and install the Intune Company Portal to enroll your device.

- Enrolling Windows devices with the Intune Company Portal
- Enrolling Android devices with the Intune Company Portal
- Enrolling macOS devices with the Intune Company Portal
- Enrolling iOS devices with the Intune Company Portal

For more details, check the Microsoft Intune documentation at https://learn.microsoft.com/en-us/intune/intune-service/user-help

Enrolling Windows devices with the Intune Company Portal

Install the Intune Company Portal application to enroll your Windows device with Intune.

To enroll a Windows device with Intune:

1. Download the Intune Company Portal app from the Microsoft Store at https://apps.microsoft.com/store/detail/company-portal/9WZDNCRFJ3PZ
2. Log in to the application with your Microsoft user credentials.
3. Follow the application instructions to enroll your device with Intune.
4. In the **Windows Settings** panel of your device, go to **User accounts** > **Sync your settings**.
5. Enable the device synchronization.

Enrolling Android devices with the Intune Company Portal

Install the Intune Company Portal application to enroll your Android device with Intune.

To enroll an Android device with Intune:

1. Download the Intune Company Portal app from the Google Play Store at https://play.google.com/store/apps/details?id=com.microsoft.windowsintune.companyportal
2. Log in to the application with your Microsoft user credentials.
3. Follow the application instructions to enroll your device with Intune.
4. Wait while the installation process adds the application to:
   - The **Personal** workspace.
   - The **Work** workspace.

Enrolling iOS devices with the Intune Company Portal

Install the Intune Company Portal mobile application to enroll your iOS device with Intune.

To enroll an iOS device with Intune:

1. Download the Intune Company Portal application from the App Store at https://apps.apple.com/us/app/intune-company-portal/id719171358
2. Log in to the application with your Microsoft user credentials.
3. Follow the application instructions to enroll your device and install the Certificate Management Profile.

Enrolling macOS devices with the Intune Company Portal

Enroll your macOS device with the Intune Company Portal application as explained in https://learn.microsoft.com/en-us/mem/intune/user-help/enroll-your-device-in-intune-macos-cp

Renewing enrolled certificates

When close to expiring, the Microsoft Intune protocol automatically renews certificates on Windows and Android devices. However, as reported in https://learn.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep, the iOS, iPadOS, and macOS devices have the following issue.

> Renewal behavior on iOS/iPadOS and macOS: Certificates can only be renewed during the renewal threshold phase. In addition, the device has to be unlocked while synching with Intune. If the renewal was not successful, the expired certificate will remain on the device and Intune does not trigger a renewal anymore. Also, Intune does not offer an option to redeploy expired certificates. Affected devices need to be excluded from the SCEP profile temporarily to remove the expired certificate and request a new one.

Therefore, if iOS, iPad, or macOS device certificates could not auto-renew during the renewal window, you must:

1. Deselect the device on the Intune Company Portal application.
2. Reenroll the device on the Intune Company Portal.

Revoking and removing certificates

Please refer to the Microsoft Intune documentation for the scenarios in which to remove or revoke certificates.

https://learn.microsoft.com/en-us/mem/intune/protect/remove-certificates

⚠ PKIaaS Intune Integration supports SCEP certificates only. PKCS #10 and other PKCS certificates are not supported.

With a periodicity of 24 hours, PKIaaS invokes the Microsoft Intune API to:

1. Fetch the list of certificates that need to be revoked.
2. Revoke all certificates in the list.
3. Update the status of each processed certificate.

Automating MDM Jamf enrollment

Configure PKIaaS to process MDM (Mobile Device Management) Jamf enrollment requests with PKIaaS Certification Authorities.

- Jamf requirements
- Configuring Jamf in PKIaaS
- Configuring MDM automation in Jamf

Jamf requirements

You must meet the following requirements to automate MDM Jamf enrollment with a PKIaaS gateway.

- PKIaaS account requirements
- Certificate authority requirements
- Operating system requirements
- TLS Cipher requirements

PKIaaS account requirements

You need an Entrust PKIaaS account with privileges to create an issuing certificate authority.

Certificate authority requirements

Make sure you have a subordinate CA with a profile of the mdmws group. You can either:

- Create a new CA with this group, as explained in Creating an issuing subordinate CA.
- Add this group to an existing CA, as explained in Selecting CA profiles.

Operating system requirements

Enrollment integration for this release is tested and validated on the following operating system versions.

OS	Version
iPad	16.6
iPhone	16.6
macOS	Ventura 13.5.1
Windows	Not supported

OS	Version
Android	Not supported
ChromeOS	Not supported

Other devices and operating systems listed in the MDM vendor support documents should work, but have not been tested.

TLS Cipher requirements

Enrollment URLs support the following TLS Ciphers.

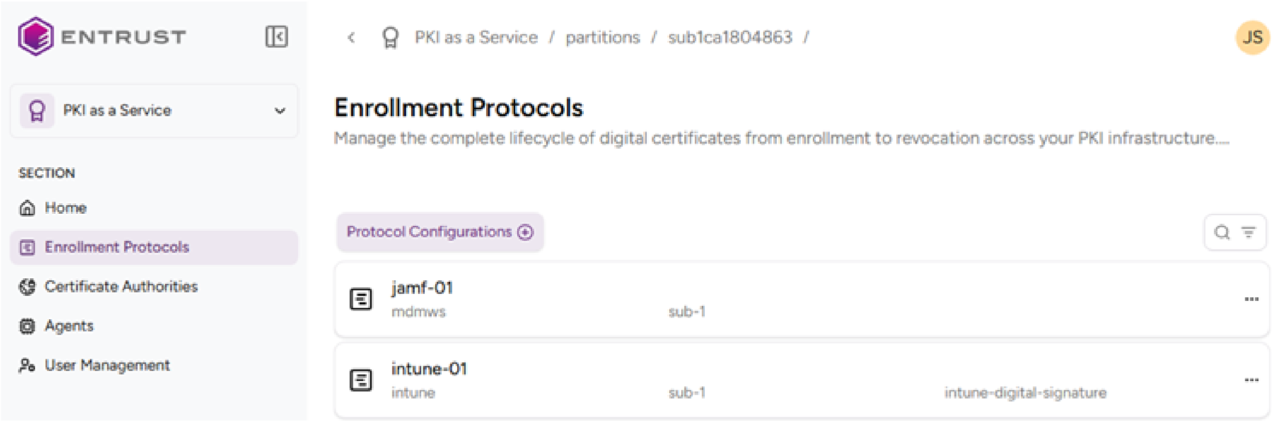
- `ECDHE-RSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES256-GCM-SHA384`

Configuring Jamf in PKIaaS

Configure a PKIaaS workflow to process MDM (Mobile Device Management) Jamf enrollment requests with PKIaaS Certification Authorities.

To configure an MDM Jamf workflow in PKIaaS:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the following roles:
   - Owners
   - Protocol Operators
2. Click **Enrollment Protocols** in the sidebar.



Enrollment Protocols

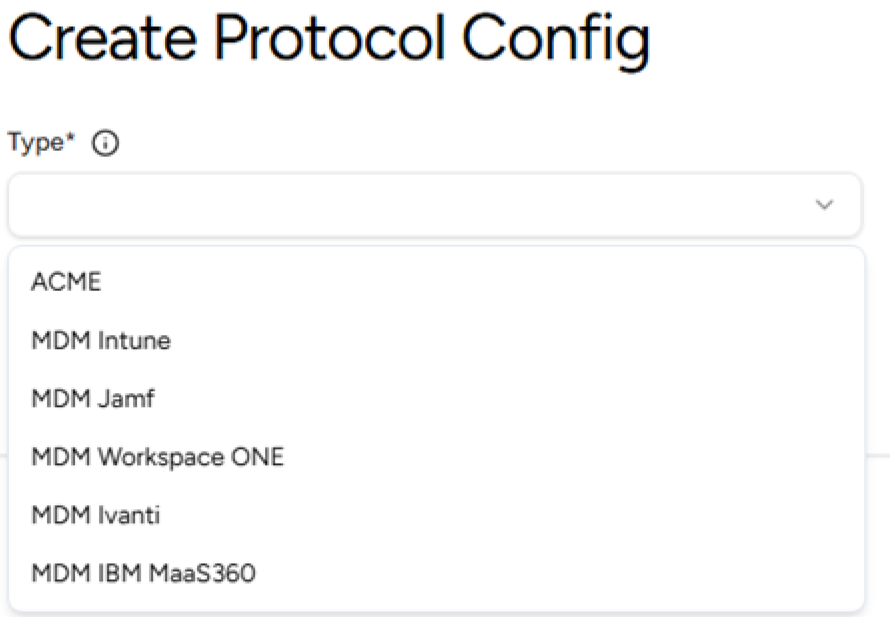
Manage the complete lifecycle of digital certificates from enrollment to revocation across your PKI infrastructure....

jamf-01 mdmws	sub-1	
intune-01 intune	sub-1	intune-digital-signature

3. Click the plus **+** icon to the right of the **Protocol Configurations** tab.
4. Configure the following values in the **Create Protocol Config** dialog.

Field	Value
Type	Select **MDM Jamf**

Field	Value
Protocol Configuration Identifier	Enter a unique identifier for the new configuration in your PKI. This identifier must be 2-18 characters long and can only include lowercase letters, numbers, hyphens (â□□-â□□), and underscores (â□□_â□□).
Description	Enter an optional description of the protocol purpose.
CA Identifier	Select an issuing subordinate authority with profiles of the mdmws group.

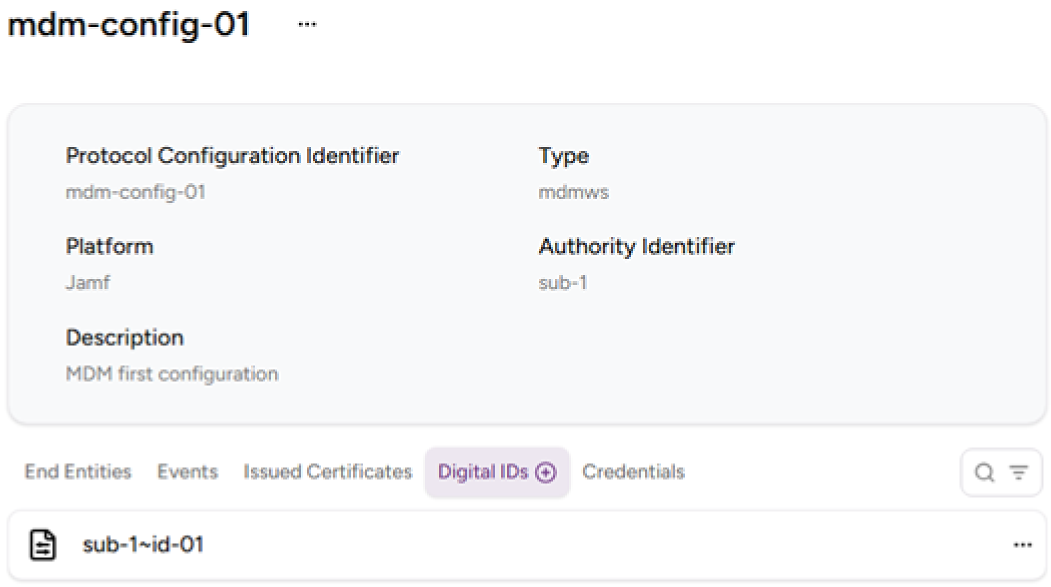


Create Protocol Config

Type*

5. Click **Create**.

6. In the confirmation window, select the **Digital IDs** tab.



mdm-config-01

Protocol Configuration Identifier: mdm-config-01

Type: mdmws

Platform: Jamf

Authority Identifier: sub-1

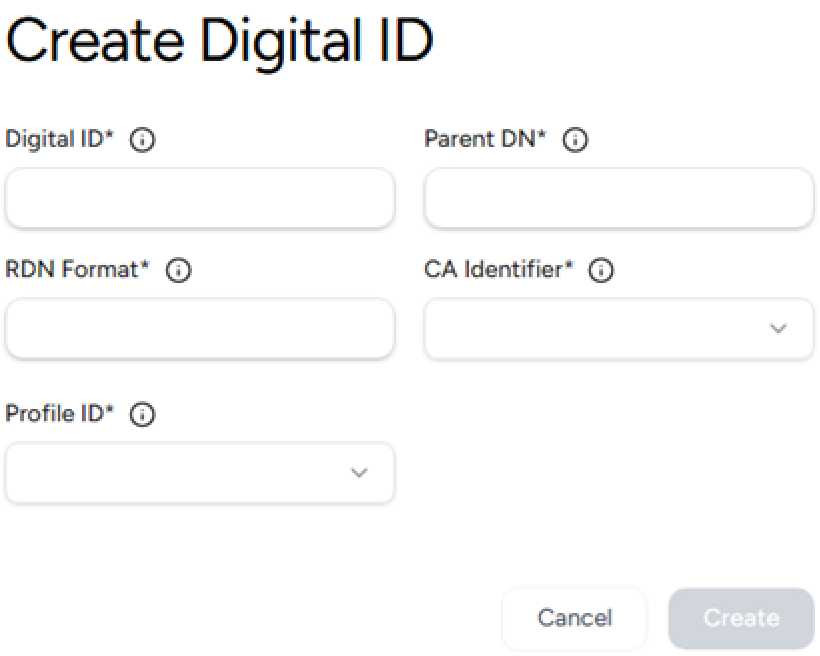
Description: MDM first configuration

sub-1~id-01

7. Click the plus **+** icon to the right of **Digital IDs**.

8. Configure the following values in the **Digital identifier** dialog.

Field	Value
Digital ID	Enter a unique name of the new digital identifier.
Parent DN	Enter the parent Distinguished Name (DN) for building the RDN of a certificate. This value is appended to the end of the Subject DN after the **RDN Format** variables have been processed.
RDN Format	Enter the Relative Distinguished Name (RDN) format to build certificate Subject Names. See Jamf RDN Format for considerations on this value.
CA Identifier	Select an issuing subordinate authority with profiles of the mdmws group.
Profile ID	Select the mdmws profile to process the enrollment requests.



Create Digital ID

Digital ID*

Parent DN*

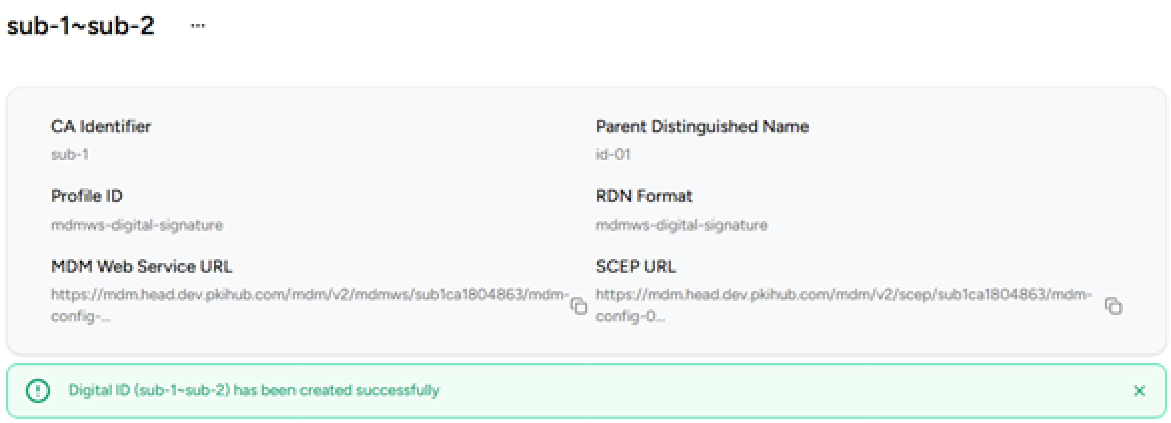
RDN Format*

CA Identifier*

Profile ID*

9. Click **Create**.

10. Copy the URLs under the **MDM Web Service URL** and **SCEP URL** fields of the confirmation dialog.



sub-1~sub-2

CA Identifier
sub-1

Parent Distinguished Name
id-01

Profile ID
mdmws-digital-signature

RDN Format
mdmws-digital-signature

MDM Web Service URL
https://mdm.head.dev.pkihub.com/mdm/v2/mdmws/sub1ca1804863/mdm-config-...

SCEP URL
https://mdm.head.dev.pkihub.com/mdm/v2/scep/sub1ca1804863/mdm-config-0...

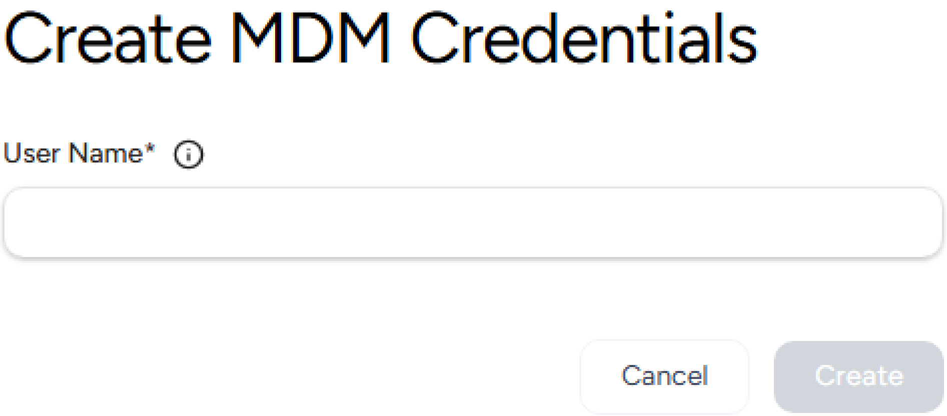
Digital ID (sub-1~sub-2) has been created successfully

11. In the navigation tree, select the name of the new protocol configuration.

12. Select the **Credentials** tab.

13. Click **CREATE**.

14. In the **Create MDM Credentials** dialog, enter a username that is 2-18 characters long and only includes lowercase letters, numbers, hyphens (â□□-â□□), and underscores (â□□_â□□).

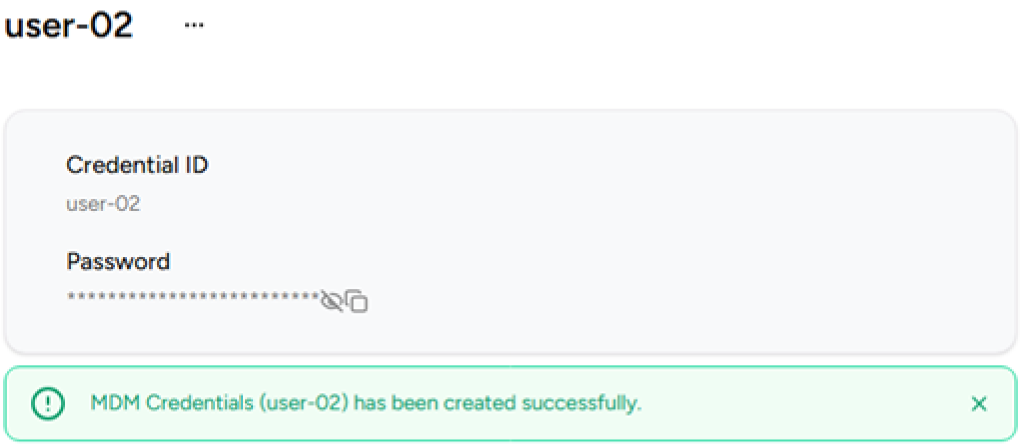


Create MDM Credentials

User Name*

15. Click **Create**.

16. Copy the **Password** value displayed in the confirmation dialog.



user-02 ···

Credential ID

user-02

Password

****

MDM Credentials (user-02) has been created successfully.

⚠ As stated in the confirmation dialog before leaving this page, Entrust PKIaaS will not display the credential password again.

Jamf RDN Format

As explained in Configuring Jamf in PKIaaS, adding a digital identifier requires a Relative Distinguished Name (RDN) format to build certificate Subject Names. See below for considerations on this value.

- Custom variable names
- Automated renewal
- Request values

Custom variable names

Subject Names support custom variable names using the `<variable>` syntax â□□ for example:

```
CN=<var1> <var2> <var3> SampleStaticText
```

See RDN Variables for how to set the value of each variable in the Jamf portal.

⚠ Entrust PKIaaS will only process enrollment requests containing values for all variables.

Automated renewal

Add the `idprofile` variable to support automated certificate renewal â□□ for example:

```
CN=<var1> <profileid>
```

See RDN Variables for how to set the value of this variable in the Jamf portal.

Request values

Jamf enrollment requests will always contain values for the following RDN variables.

- The `igusername` name of the device user.
- The `iggroup` group of enrolled devices.
- The `devicetype` type of enrolled device.

For example:

```
CN=<igusername> <iggroup> <devicetype>
```

ℹ You don't need to inform these variables in the Jamf portal.

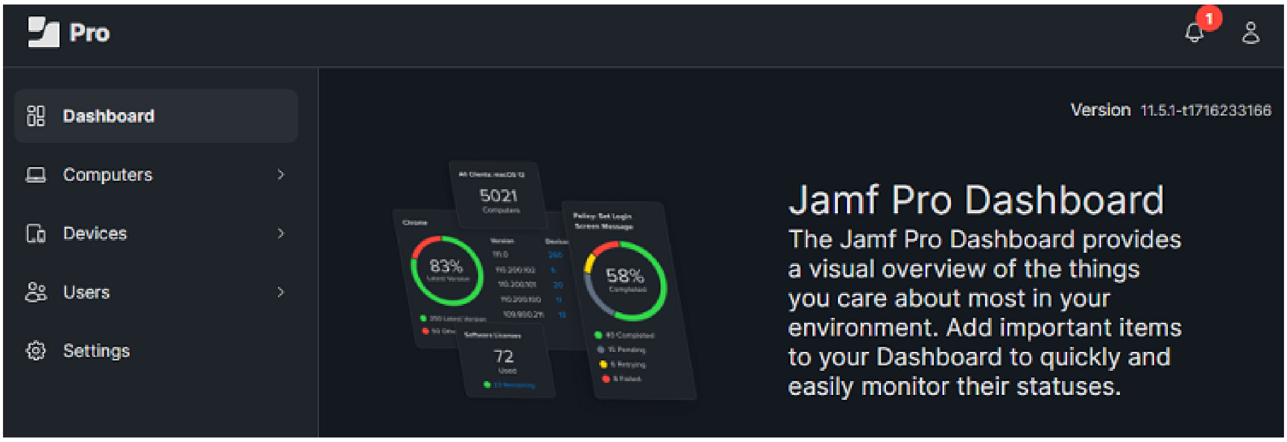
Configuring MDM automation in Jamf

If using Jamf as an MDM provider, configure and install a profile as described below.

ℹ Jamf is a cloud service for managing Apple devices like Mac, iPad, or iPhone. When enrolling these devices, the SCEP Payload must include the settings described in https://support.apple.com/guide/deployment/scep-payload-settings-dep495a6d79/web

To configure and install an MDM profile in Jamf:

1. Log in to the Jamf administration portal.

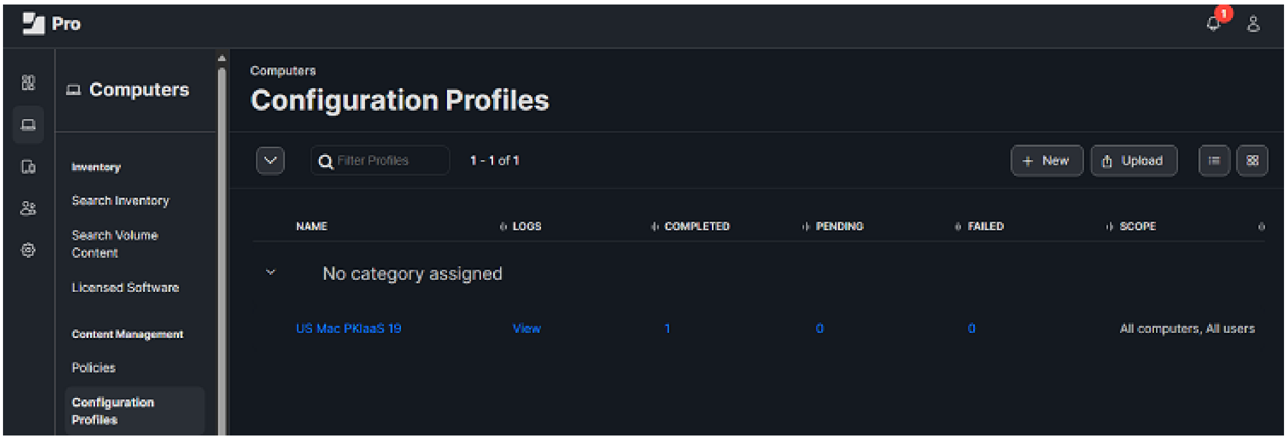


Jamf Pro Dashboard

The Jamf Pro Dashboard provides a visual overview of the things you care about most in your environment. Add important items to your Dashboard to quickly and easily monitor their statuses.

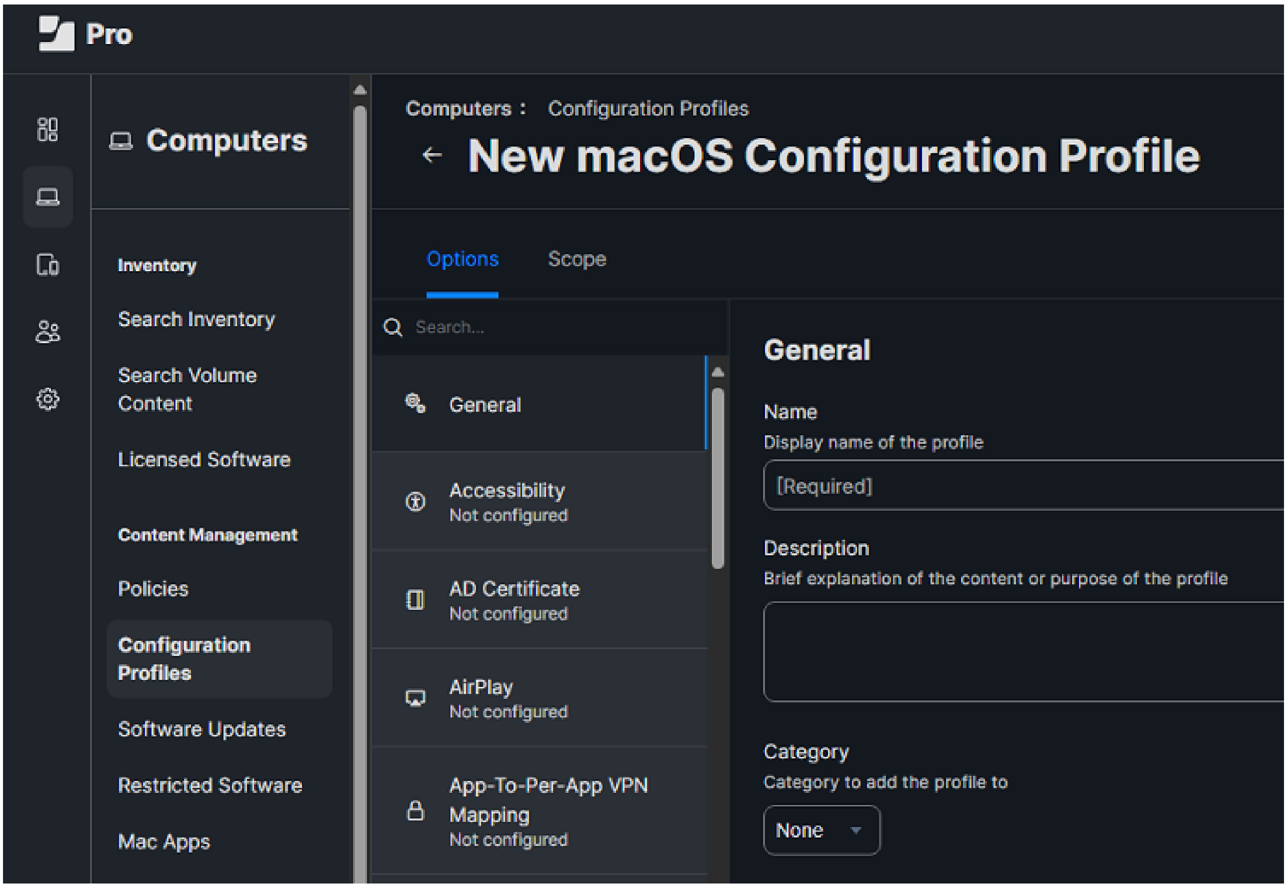
2. Select:
   - **Computers** to create a profile for enrolling Apple computers like MacBooks.
   - **Devices** to create a profile for enrolling iPhones, iPads, etc.

3. Select **Configuration profiles** in the sidebar and click **New**.



NAME	LOGS	COMPLETED	PENDING	FAILED	SCOPE
No category assigned					
US Mac PKIaaS 19	View	1	0	0	All computers, All users

4. Configure the Options and Scope settings in the **New macOS Configuration Profile** form.



Pro

Computers

Inventory

Search Inventory

Search Volume Content

Licensed Software

Content Management

Policies

Configuration Profiles

Software Updates

Restricted Software

Mac Apps

Computers : Configuration Profiles

New macOS Configuration Profile

Options | Scope

Search...

General

Accessibility
Not configured

AD Certificate
Not configured

AirPlay
Not configured

App-To-Per-App VPN Mapping
Not configured

General

Name
Display name of the profile
[Required]

Description
Brief explanation of the content or purpose of the profile

Category
Category to add the profile to
None

5. Click **Save**.

6. To enroll devices, users must log in to Jamf and follow the prompts for enrollment.

   - Depending on how Jamf was configured, users may or may not be prompted to download and install CA Certificates.
   - Users will be prompted to download and install a profile.
   - Wait while the device is enrolled. Certificates will automatically be issued during enrollment.

Options

Configure the following settings in the **Options** tab of the **New macOS Configuration Profile**.

- General
- Certificate
- SCEP

General

Click **General** on the **Options** tab and configure the following settings.

Settings	Value	Mandatory
Name	Write a profile name to display on the device	✓
Description	Write a description of the profile purpose	✗
Category	Select a profile category	✗

Settings	Value	Mandatory
Level	Select **Device Level**	✓
Distribution Method	Select **Install Automatically**	✓

Certificate

Click **Certificate** on the **Options** tab and configure the following settings.

Settings	Value	Mandatory
Certificate Name	Write a name for the certificate	✓
Select certificate option	Click **Upload**	✓
Certificate	Upload the certificate of the CA that was selected when adding a Digital ID in section Configuring Jamf in PKIaaS (see Downloading a CA certificate for how to download a CA certificate).	✓

SCEP

Click **SCEP** on the **Options** tab and configure the following settings.

- URL
- Name
- Redistribute Profile
- Subject
- Subject Alternative Name Type
- Retries
- Retry delay
- Challenge type
- Entrust Web Service URL
- Administrator Username
- Administrator Password
- Verify Password
- Digital ID Configuration Name
- Group Name
- RDN Variables
- Key Size
- Use as digital signature
- Use for key encipherment
- Fingerprint

URL

Paste the **SCEP URL** value obtained when Configuring Jamf in PKIaaS.

Mandatory: Yes.

Name

Enter the name of the SCEP service to display on the device.

Mandatory: Yes.

Redistribute Profile

Select **Never**.

Mandatory: Yes.

Subject

Enter the Subject Distinguished Name to include in the Certificate Signing Requests (CSRs). The enrollment process will ignore this dummy value and use the digital identifier.

â□¹ See Configuring Jamf in PKIaaS for how to add a CA digital identifier.

Mandatory: Yes.

Subject Alternative Name Type

Select the type of Subject Alternative Name.

Mandatory: No.

Retries

Select the maximum number of retries after a `PENDING` response.

Mandatory: No.

Retry delay

Select the period between retries.

Mandatory: No.

Challenge type

Select **Dynamic Entrust**.

Mandatory: Yes.

Entrust Web Service URL

Paste the **Web Service URL** value obtained when Configuring Jamf in PKIaaS.

Mandatory: Yes.

Administrator Username

Paste the **Credential Identifier** value set when Configuring Jamf in PKIaaS.

Mandatory: Yes.

Administrator Password

Paste the **Password** value that obtained after generating a credential in section Configuring Jamf in PKIaaS.

Mandatory: Yes.

Verify Password

Paste the credential **Password** value obtained when Configuring Jamf in PKIaaS.

Mandatory: Yes.

Digital ID Configuration Name

Paste the **User Name** value that was used for adding a credential in section Configuring Jamf in PKIaaS.

Mandatory: Yes.

Group Name

Enter a name for the group.

Mandatory: When the **RDN Format** of the digital identifier includes the `<iggroup>` variable. In this case, Jamf will automatically map this **Group Name** to the `<iggroup>` variable.

---

i See Configuring Jamf in PKIaaS for how to add digital identifiers.

RDN Variables

Enter a value for each variable added to the **RDN Format** field when Configuring Jamf in PKIaaS.

- Configuring the profileid variable for automated renewal
- Using Jamf payload variables
- Omitting Jamf preloaded variables

Mandatory: Yes.

Configuring the profileid variable for automated renewal

To support automated certificate renewal, add the following variable.

Variable name	Variable value
`profileid`	`â□□$PROFILE_IDENTIFIER`

Where profiled is the **RDN Format** value set when Configuring Jamf in PKIaaS.

Using Jamf payload variables

RDN values support the following Jamf payload variables.

Variables	Jamf documentation
â□□Payload Variables for Computer Configuration Profiles	https://learn.jamf.com/bundle/jamf-pro-documentation-current/page/Computer_Configuration_Profiles.html#ariaid-title2
Payload Variables for Device Configuration Profiles	https://learn.jamf.com/bundle/jamf-pro-documentation-current/page/Mobile_Device_Configuration_Profiles.html#ariaid-title3

Omitting Jamf preloaded variables

Do not set the following variables, as Jamf requests always provide values for them.

Variable	Value
igusername	The name of the device user.
iggroup	The group of enrolled devices.
devicetype	The type of enrolled device.

Key Size

Select one of the following values.

- 2048
- 4096

⚠ Entrust PKIaaS does not support key sizes below 2048.

Mandatory: Yes.

Use as digital signature

Check to use the enrolled certificates for signing data.

Mandatory: No.

Use for key encipherment

Check to use the enrolled certificates for ciphering keys.

Mandatory: No.

Fingerprint

Paste the SHA-256 fingerprint (in hexadecimal format) of the whole root CA certificate in DER binary encoding (not in PEM). You can obtain this value from the certificate properties or run the following commands.

OS	Command
Windows	`certutil -hashfile rootca.der SHA256`
macOS	`openssl x509 -fingerprint -sha256 -noout -in rootca.crt | sed "s/[:]//g"`

Mandatory: Yes. It is recommended to always configure this field when possible.

Scope

Configure the following settings on the Scope tab of the New macOS Configuration Profile.

Setting	Value	Mandatory
â□□Target Mobile Devices	Mobile devices to assign the profile to	✓
Target Users	Users to distribute the profile to	✓

Automating MDM Workspace ONE enrollment

Configure a PKIaaS workflow to process MDM (Mobile Device Management) Workspace ONE enrollment requests with PKIaaS Certification Authorities.

- Workspace ONE requirements
- Configuring Workspace ONE in PKIaaS
- Configuring MDM automation in Workspace ONE

Workspace ONE requirements

You must meet the following requirements to automate MDM Workspace ONE enrollment with a PKIaaS gateway.

- PKIaaS account requirements
- Certificate authority requirements
- Operating system requirements
- TLS Cipher requirements

PKIaaS account requirements

You need an Entrust PKIaaS account with privileges to create an issuing certificate authority.

Certificate authority requirements

Make sure you have a subordinate CA with a profile of the mdmws group. You can either:

- Create a new CA with this group, as explained in Creating an issuing subordinate CA.
- Add this group to an existing CA, as explained in Selecting CA profiles.

Operating system requirements

Enrollment integration for this release is tested and validated on the following operating system versions.

OS	Version
iPad	16.6
iPhone	16.6
macOS	Ventura 13.5.1
Windows	10 and 11
Android	13
ChromeOS	Not supported

Other devices and operating systems listed in the MDM vendor support documents should work, but have not been tested.

TLS Cipher requirements

Enrollment URLs support the following TLS Ciphers.

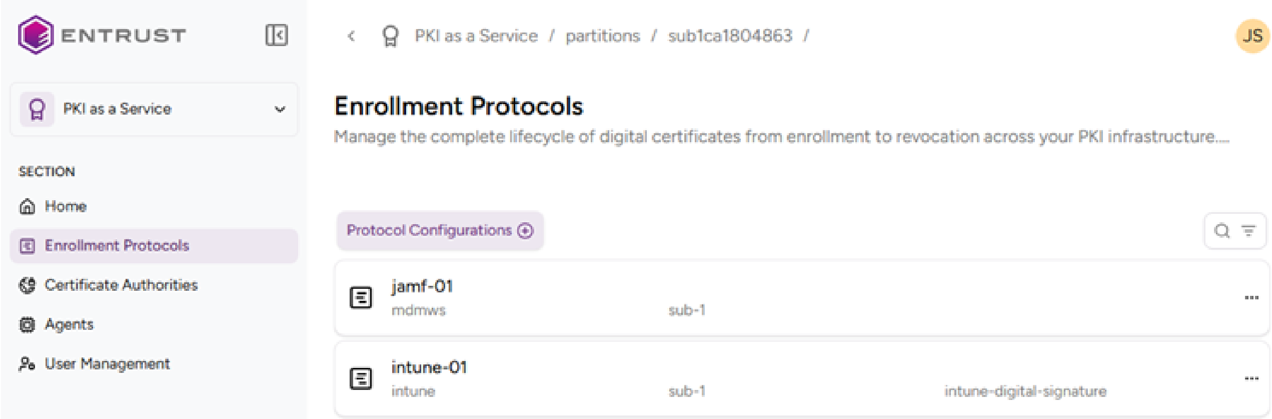
- `ECDHE-RSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES256-GCM-SHA384`

Configuring Workspace ONE in PKIaaS

Configure a PKIaaS workflow to process MDM (Mobile Device Management) Workspace ONE enrollment requests with PKIaaS Certification Authorities.

To configure an MDM Workspace ONE workflow in PKIaaS:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the following roles:
   - Owners
   - Protocol Operators
2. Click **Enrollment Protocols** in the sidebar.



Enrollment Protocols

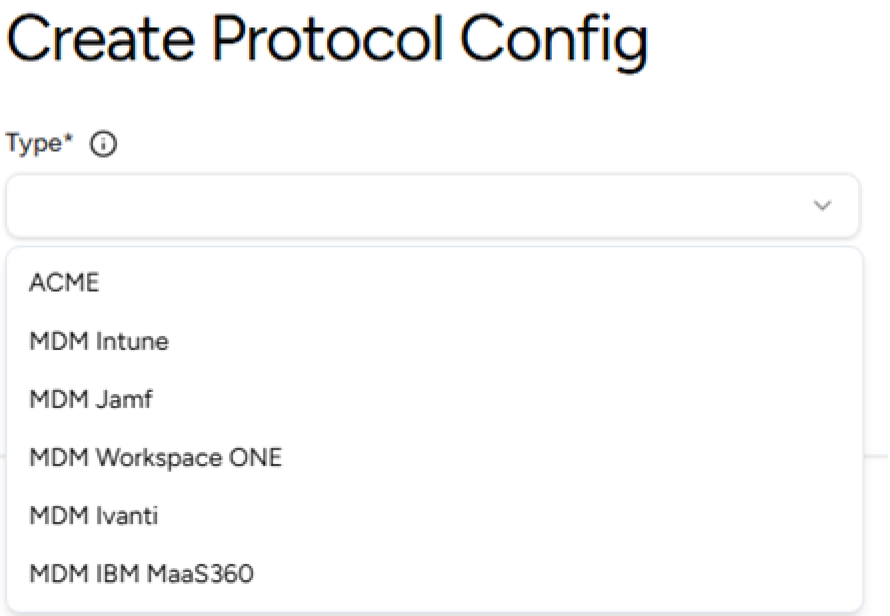
Manage the complete lifecycle of digital certificates from enrollment to revocation across your PKI infrastructure....

jamf-01 mdmws	sub-1	
intune-01 intune	sub-1	intune-digital-signature

3. Click **Create**.

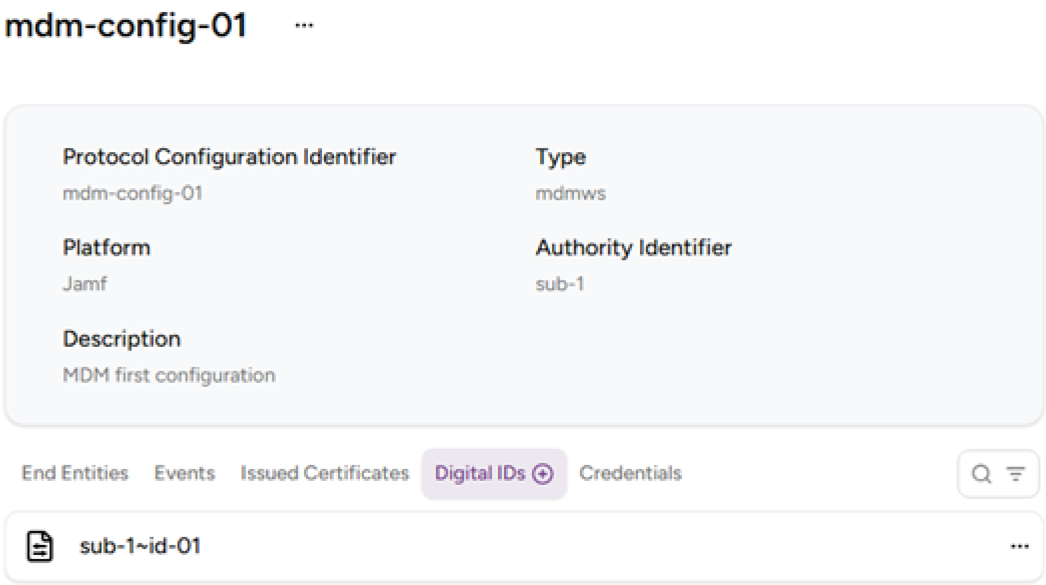
4. Configure the settings described in **Create Protocol Config** dialog.

Field	Value
Type	Select **MDM Workspace ONE**
Protocol Configuration Identifier	Enter a unique identifier for the new configuration in your PKI. This identifier: Must be 2-18 characters long, can only include lowercase letters, numbers, hyphens ('-'), and underscores ('_').
Description	Enter an optional description of the protocol purpose.
CA Identifier	Select an issuing subordinate authority with profiles of the mdmws group.



5. Click **Create**.

6. In the confirmation window, select the **Digital IDs** tab.


mdm-config-01

Protocol Configuration Identifier
mdm-config-01

Type
mdmws

Platform
Jamf

Authority Identifier
sub-1

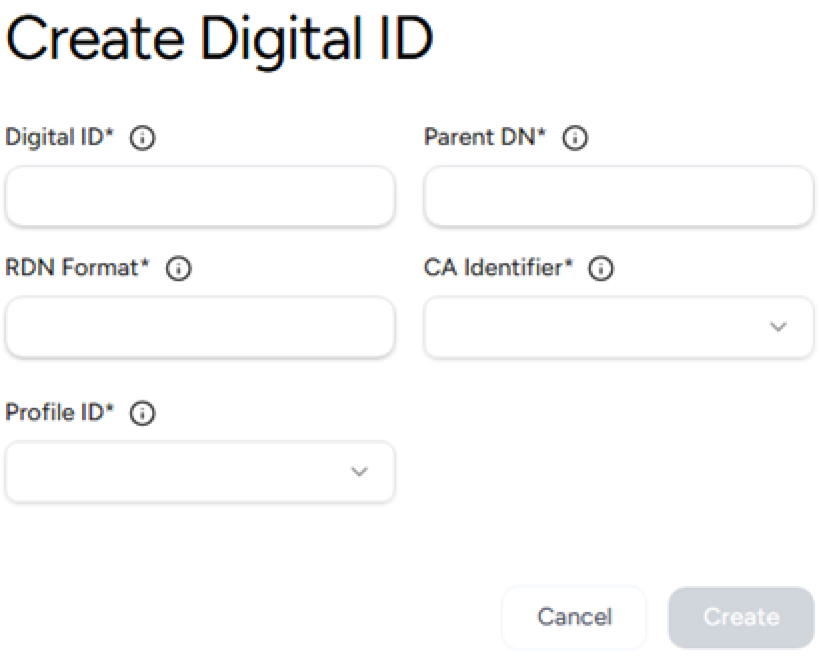
Description
MDM first configuration

sub-1~id-01

7. Click **CREATE**.

8. Configure the following settings in the **Digital identifier** dialog.

Field	Value
Digital ID	Enter a unique name of the new digital identifier.
Parent DN	Enter the parent Distinguished Name (DN) for building the RDN of a certificate. This value is appended to the end of the Subject DN after the **RDN Format** variables have been processed.
RDN Format	Enter the Relative Distinguished Name (RDN) format to build certificate Subject Names.
CA Identifier	Select an issuing subordinate authority with profiles of the mdmws group.
Profile ID	Select the mdmws profile to process the enrollment requests.



Create Digital ID

Digital ID*

Parent DN*

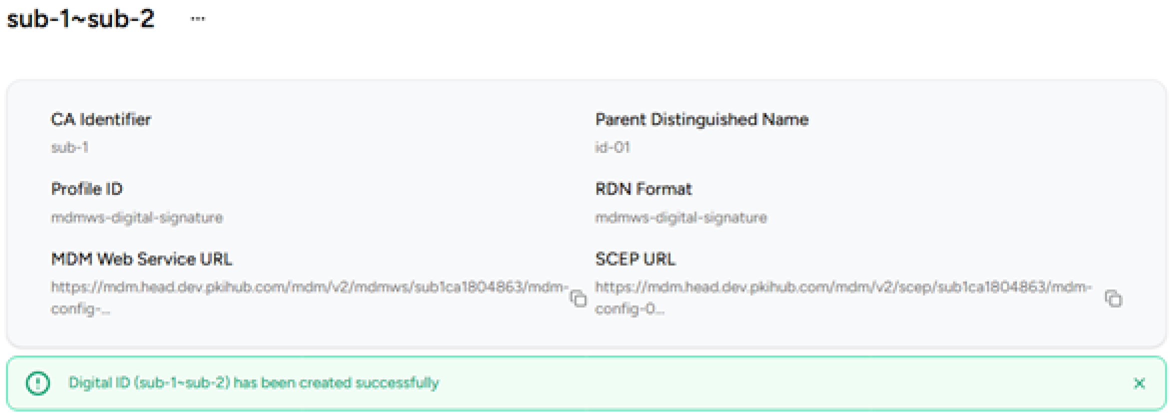
RDN Format*

CA Identifier*

Profile ID*

9. Click **Create**.

10. Copy the URLs under the **Web Service URL** and **SCEP URL** fields of the confirmation dialog.



sub-1~sub-2 ···

CA Identifier
sub-1

Parent Distinguished Name
id-01

Profile ID
mdmws-digital-signature

RDN Format
mdmws-digital-signature

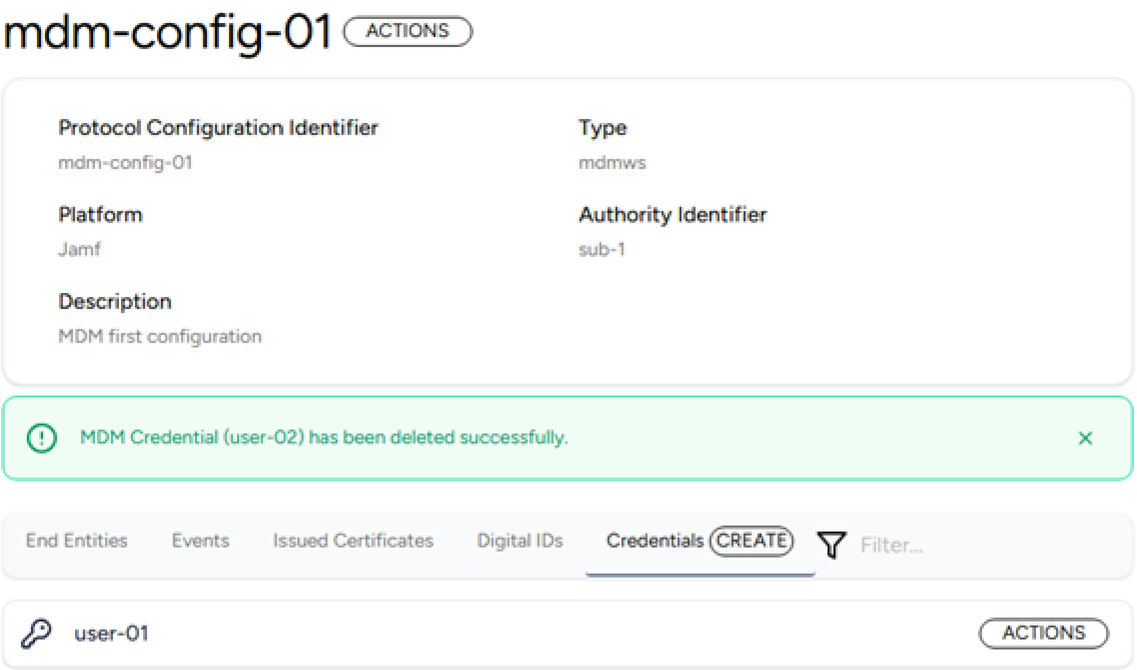
MDM Web Service URL
https://mdm.head.dev.pkihub.com/mdm/v2/mdmws/sub1ca1804863/mdm-config-...

SCEP URL
https://mdm.head.dev.pkihub.com/mdm/v2/scep/sub1ca1804863/mdm-config-0...

Digital ID (sub-1~sub-2) has been created successfully

11. In the navigation tree, select the name of the new protocol configuration.

12. Select the **Credentials** tab.



mdm-config-01 ACTIONS

Protocol Configuration Identifier
mdm-config-01

Type
mdmws

Platform
Jamf

Authority Identifier
sub-1

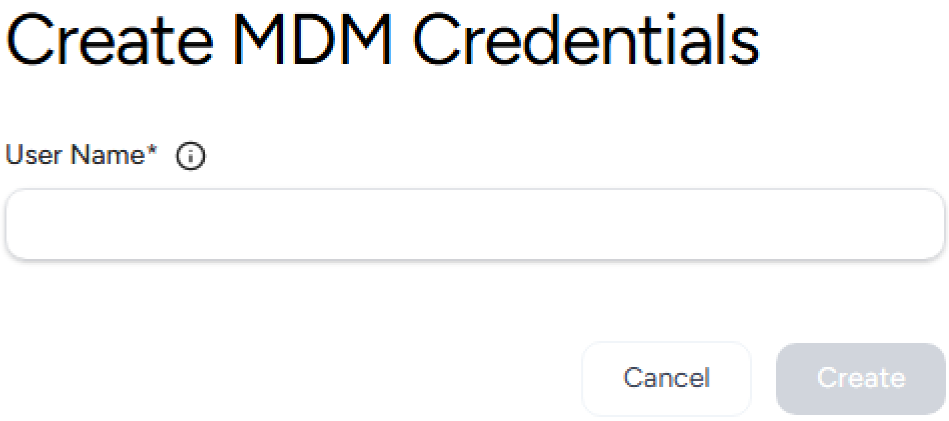
Description
MDM first configuration

MDM Credential (user-02) has been deleted successfully.

user-01 ACTIONS

13. Click **CREATE**.

14. In the **Create MDM Credentials** dialog, enter a username that is 2-18 characters long and only includes lowercase letters, numbers, hyphens (â□□-â□□), and underscores (â□□_â□□).

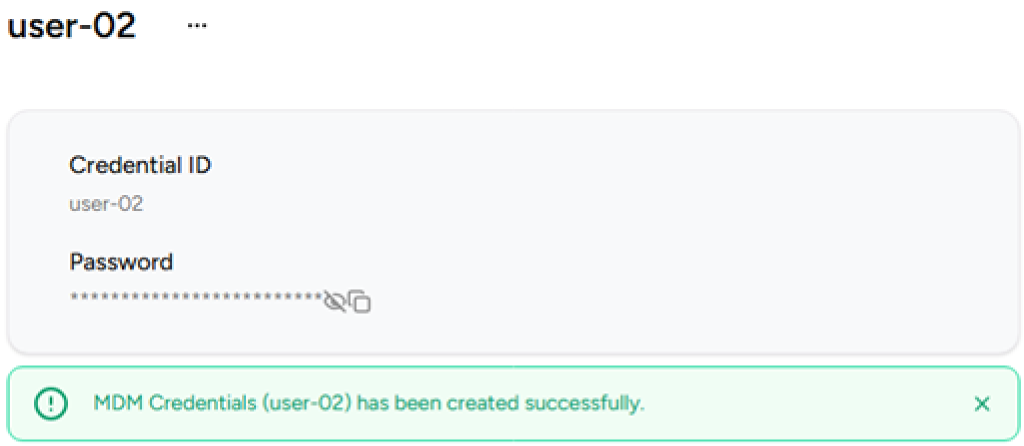


Create MDM Credentials

User Name*

15. Click **Create**.

16. Copy the **Password** value displayed in the confirmation dialog.



user-02 ···

Credential ID

user-02

Password

****

MDM Credentials (user-02) has been created successfully.

⚠ As stated in the confirmation dialog before leaving this page, Entrust PKIaaS will not display the credential password again.

Configuring MDM automation in Workspace ONE

Configure PKIaaS to process MDM (Mobile Device Management) Workspace ONE enrollment requests with PKIaaS Certification Authorities.

- Supported protocols for MDM automation in VMware Workspace ONE
- Adding a CA and a Request Template for MDM automation in VMware Workspace ONE
- Adding a profile for trusted certificates in VMware Workspace ONE
- Adding a PKI profile for MDM automation in VMware Workspace ONE
- Adding an SCEP profile for MDM automation in VMware Workspace ONE
- Testing MDM automation in VMware Workspace ONE

Supported protocols for MDM automation in VMware Workspace ONE

When using VMware Workspace ONE as an MDM provider, the enrollment automation supports the following protocols.

- The PKI protocol for Entrust MDMWS PKCS #12 enrollment.
- The Simple Certificate Enrollment Protocol (SCEP).

See below the profiles of the mdmws group supported by each protocol.

Profile	**PKI**	**SCEP**
mdmws-digital-signature	✗	✓
mdmws-digital-signature-key-encipherment	✗	✓
mdmws-digital-signature-key-encipherment-clientauth	✗	✓
mdmws-key-encipherment	✗	✓

Profile	PKI	SCEP
mdmws-non-repudiation	✗	✓
mdmws-p12-digital-signature	✓	✓
mdmws-p12-digital-signature-key-encipherment	✓	✓
mdmws-p12-digital-signature-key-encipherment-clientauth	✓	✓
mdmws-p12-key-encipherment	✓	✓
mdmws-p12-non-repudiation	✓	✓

See below for additional protocol differences.

- Private key
- Certificate information
- CSR challenge passwords
- Enrollment request
- Support status

Private key

Key generation has the following protocol-related differences.

- With PKI:
    1. The Entrust CA generates the private key and delivers it to Workspace One as a PKCS #12.
    2. Workspace One delivers the resulting private key and certificate to the managed device.
- With SCEP, the managed device generates the private key along with the CSR.

Certificate information

Certificate information has the following protocol-related differences.

- With PKI, Entrust CA provides certificate information using the MDMWS API.
- With SCEP, the certificate information is in the CSR.

CSR challenge passwords

CSR challenge passwords have the following protocol-related differences.

- The PKI protocol does not use CSR challenge passwords.
- With SCEP:
    1. Workspace One requests challenge passwords from the MDMWS API of the Entrust CA.
    2. Workspace One provides the challenge password to the managed devices.
    3. The devices embed the challenge password into the CSR for SCEP enrollment.

Enrollment request

Enrollment requests have the following protocol-related differences.

- With the PKI protocol, Workspace One submits the enrollment requests.
- With the SCEP protocol:
  - The managed devices submit the enrollment requests to the SCEP endpoint of the Entrust CA.
  - Optionally, you can use Workspace One as an SCEP Proxy to perform SCEP against Workspace One instead of the Entrust CA.

Support status

The PKI protocol is fully supported. However, support for the SCEP protocol is temporarily broken because Workspace One:

- Sends an incorrect SCEP URL to the managed devices
- Ignores the **RDN Format** custom variables selected when Configuring Workspace ONE in PKIaaS.

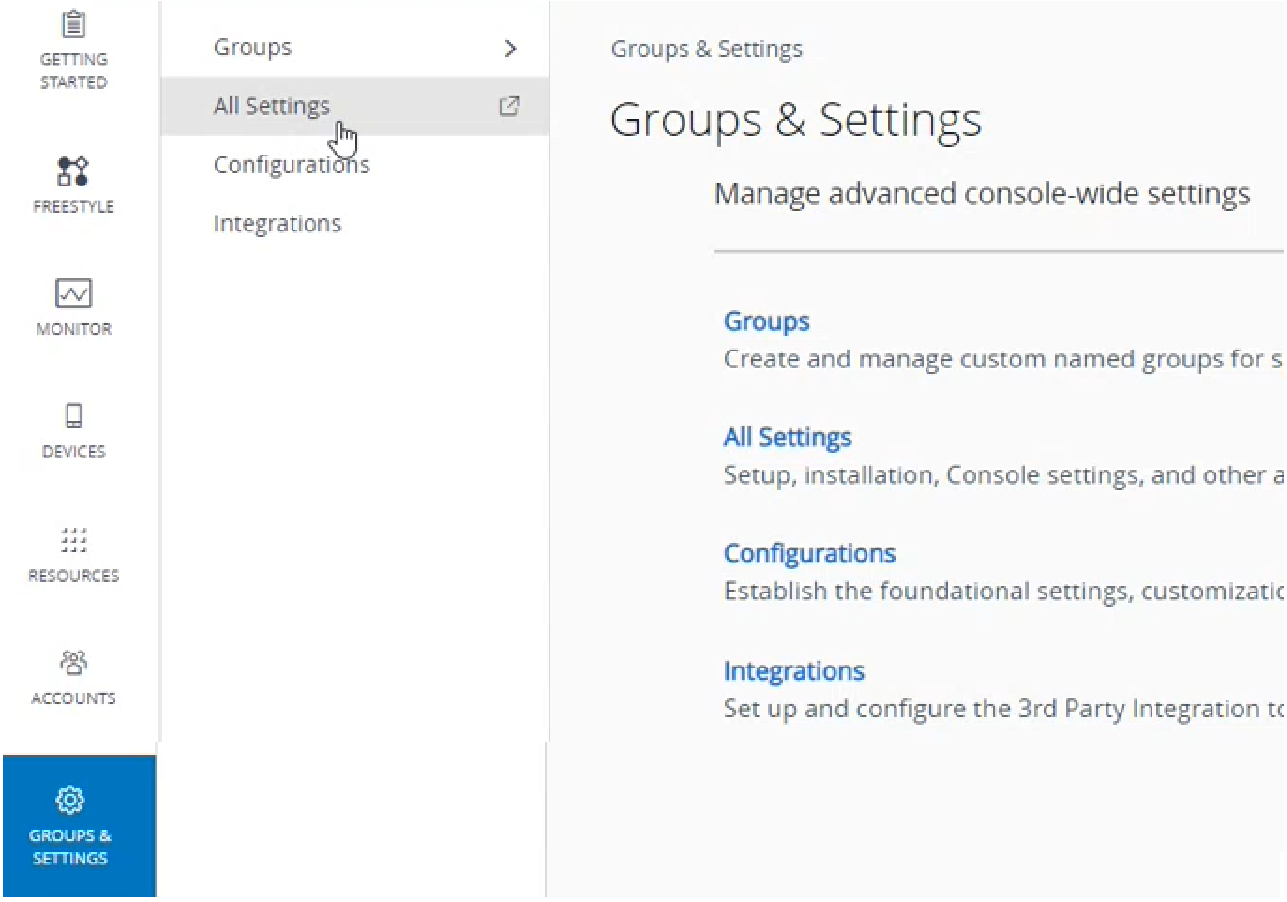
ℹ Entrust is working with Workspace One to fix these issues.

Adding a CA and a Request Template for MDM automation in VMware Workspace ONE

Add a certificate authority and a request template for MDM automation in VMware Workspace ONE.

To add a Certificate Authority and a request template:

1. Log in to your Workspace ONE UEM (Unified Endpoint Management).



Groups & Settings

Manage advanced console-wide settings

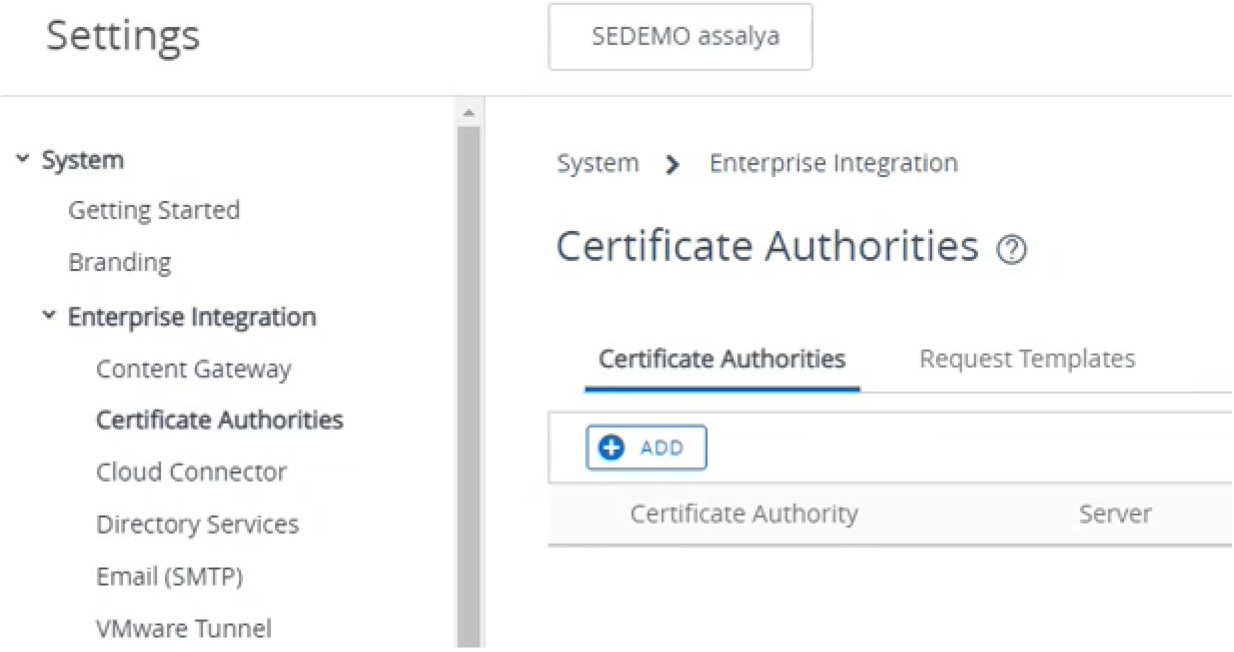
Groups
Create and manage custom named groups for s

All Settings
Setup, installation, Console settings, and other a

Configurations
Establish the foundational settings, customizatic

Integrations
Set up and configure the 3rd Party Integration tc

2. In the sidebar menu, go to **Groups & Settings** > **All Settings**.



3. In the **All Settings** pop-up, go to **System > Enterprise integration > Certificate Authorities**.

4. Configure the following settings.

   - Certificate Authorities
   - Requests Templates

Certificate Authorities

In the Certificate Authorities tab:

1. Click **ADD**.

2. Configure the following CA settings.

   - Name
   - Description
   - Authority Type
   - Protocol
   - Server URL
   - Username
   - Password
   - SCEP Endpoint URL

3. Click TEST CONNECTION to check the connection with the Entrust CA.

4. Click SAVE to save the new CA settings.

Name

Enter a name for the CA in the VMware environment.

Description

Enter an optional description for the CA in the VMware environment.

Authority Type

Select **Entrust**.

Protocol

Select the **SCEP** or **PKI** protocols described in Supported protocols for MDM automation in VMware Workspace ONE.

Server URL

Paste the **Web Service URL** value generated when Configuring Jamf in PKIaaS. Specifically, use the following URL formats to support certificate revocation.

Region	Supported URL format
US	`https://mdm.PKIaaS.entrust.com/mdm/mdmws/{accountId}/AdminServiceV9`
EU	`https://mdm.eu.PKIaaS.entrust.com/mdm/mdmws/{accountId}/AdminServiceV9`

Username

Paste the **Digital ID** value described in Configuring Jamf in PKIaaS.

Password

Paste the credential **Password** value obtained when Configuring Jamf in PKIaaS.

SCEP Endpoint URL

When Protocol is SCEP, paste the **SCEP URL** value obtained when Configuring Jamf in PKIaaS.

Requests Templates

In the **Request Templates** tab:

1. Click **ADD**.
2. Configure a new template for the CA.
3. Click SAVE to save the new template settings.

Name

Enter a name for the template in the VMware environment.

Description

Enter an optional description for the template in the VMware environment.

Certificate Authority

Select the name of the CA previously created in the **Certificate Authorities** tab.

Managed CA

Select the same CA name that was used for Configuring Workspace ONE in PKIaaS.

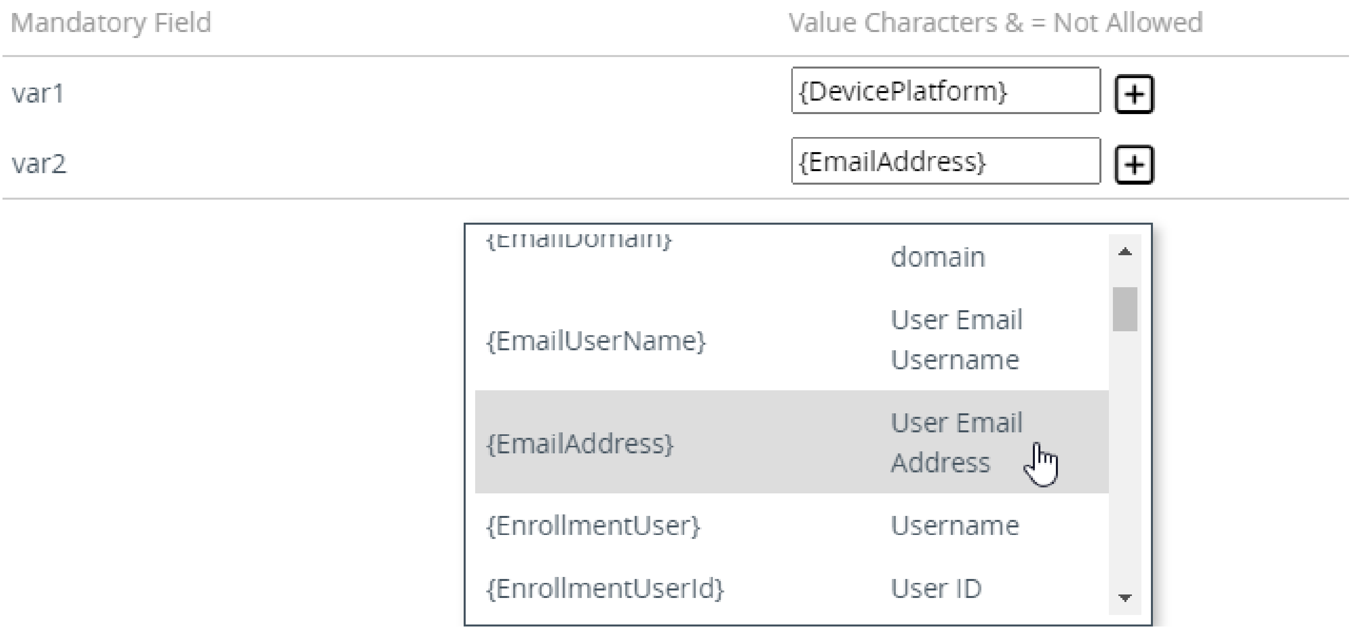
Profile name

Select the same **Profile ID** value that was selected for Configuring Workspace ONE in PKIaaS.

`<field>`

Configure the same **RDN Format** variables selected for Configuring Workspace ONE in PKIaaS. You can either:

- Provide static text
- Click ✚ and select a Workspace One variable



Mandatory Field	Value Characters & = Not Allowed
var1	{DevicePlatform}
var2	{EmailAddress}

{EmailDomain}	domain
{EmailUserName}	User Email Username
{EmailAddress}	User Email Address
{EnrollmentUser}	Username
{EnrollmentUserId}	User ID

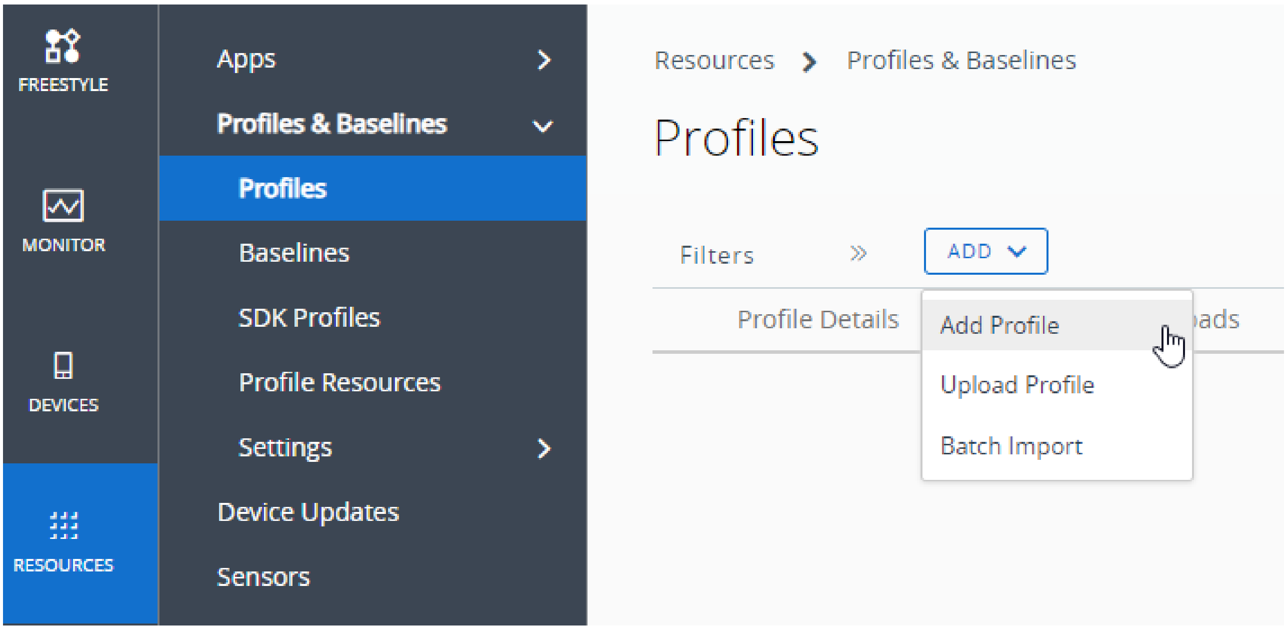
Adding a profile for trusted certificates in VMware Workspace ONE

Profiles with the **User Profile** context do not support uploading certificates to the **Trusted Root** certificate store. Therefore, you must create a profile with the **Device Profile** context and the following settings.

⚠ When creating a Workspace One profile with the **User Profile** context, assign them to the same **Smart Group**. This way, the devices managed by the user profile will trust the CA certificate chain of the device profile.

To add a device profile in Workspace One:

1. In Workspace One, navigate to **Resources** > **Profiles & Baselines** > **Profiles**.



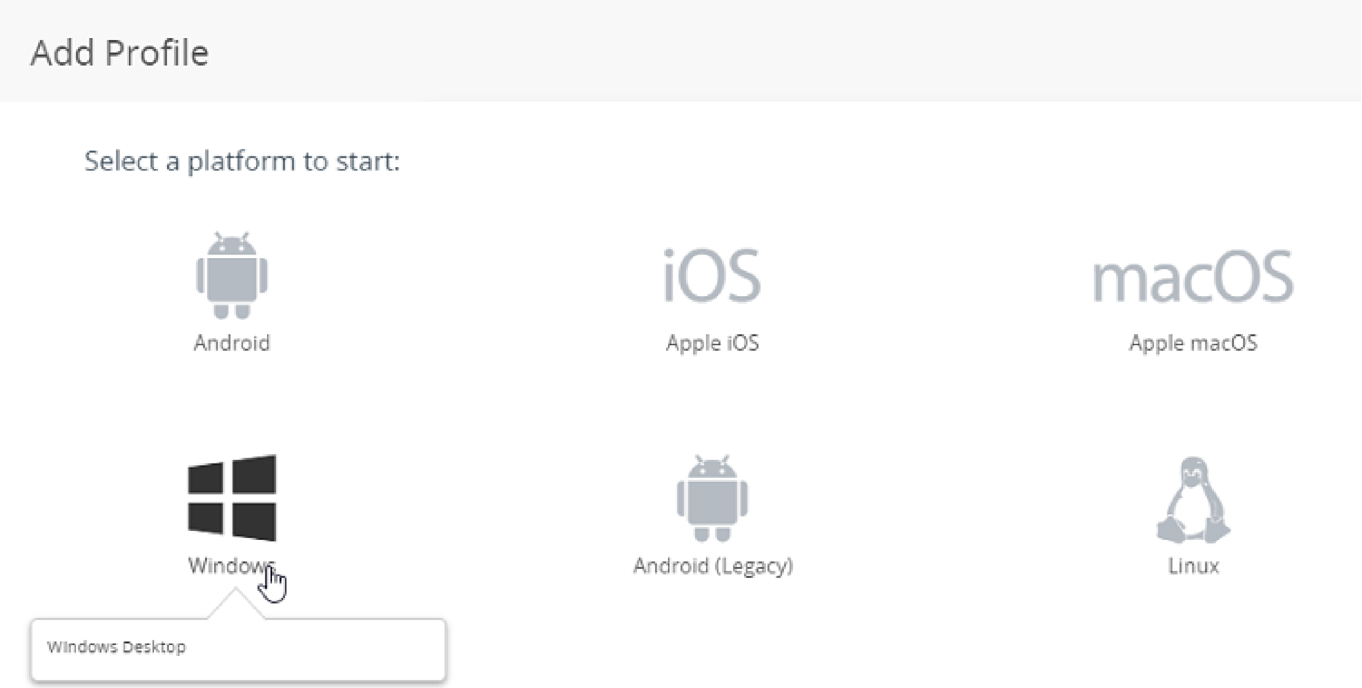
2. In the content pane, click **Add > Add Profile**.

3. Follow the wizard pages described below.

   - Add Profile
   - Select Device Type
   - Select Context
   - General
   - Credentials

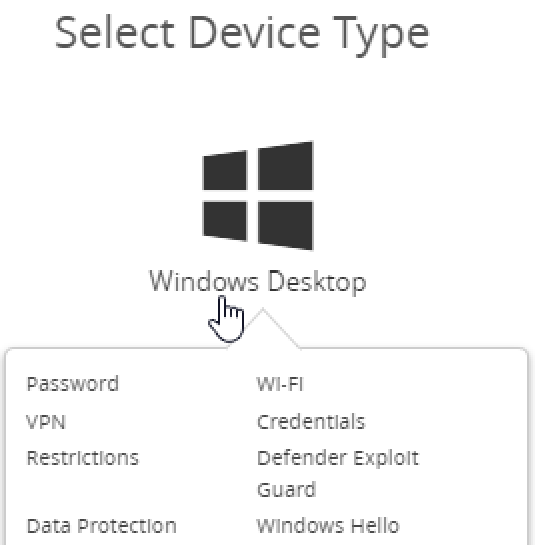
Add Profile

Click on the name of the platform running the enrollment device.



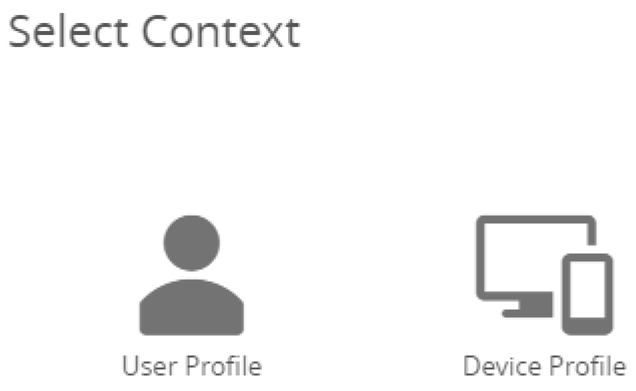
Select Device Type

Click on the type of enrolled device.



Select Context

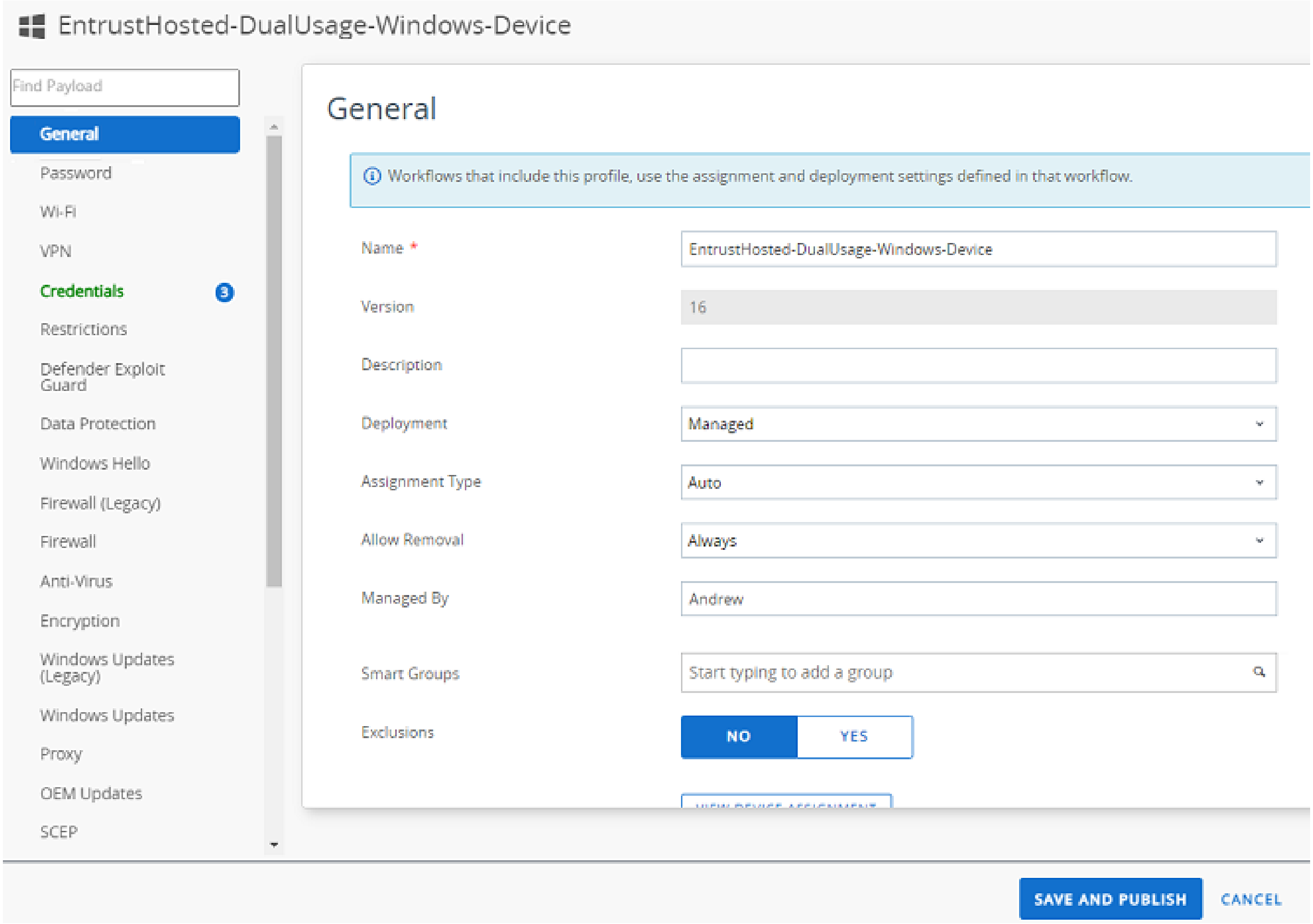
Click on **Device Profile** to enroll devices.



General

Click **General** in the sidebar menu to configure the following settings in the content pane.

Field	Value
â□□Name	Enter a name for the profile.
Smart Group	Select the smart group containing the managed users or devices.



EntrustHosted-DualUsage-Windows-Device

General

Workflows that include this profile, use the assignment and deployment settings defined in that workflow.

Name * EntrustHosted-DualUsage-Windows-Device

Version 16

Description

Deployment Managed

Assignment Type Auto

Allow Removal Always

Managed By Andrew

Smart Groups Start typing to add a group

Exclusions NO YES

Credentials

Click **Credentials** in the sidebar menu to configure the user credentials.

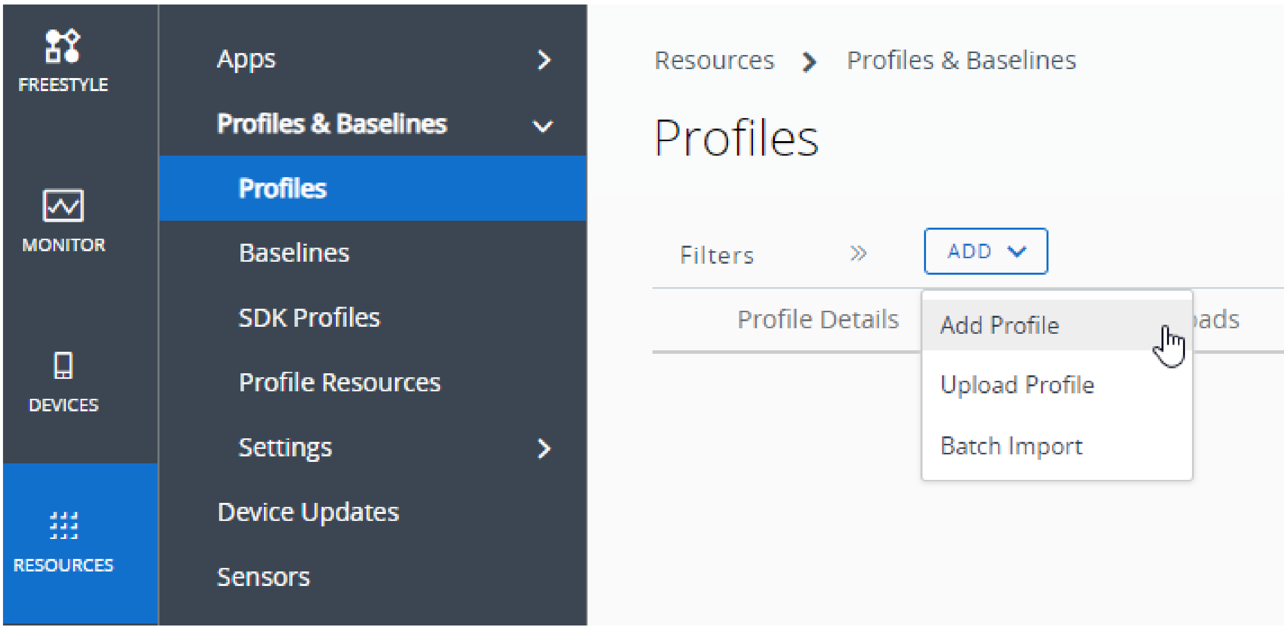
Field	Value
Credential Source	Select **Defined Certificate Authority**.
Certificate	Upload separately the certificates of the root and issuing CAs.
Certificate Store	Select **Trusted Root**.

Adding a PKI profile for MDM automation in VMware Workspace ONE

See below for creating an MDM automation profile to issue certificates with the PKI protocol.

To add a PKI profile in Workspace One:

1. In Workspace One, navigate to **Resources > Profiles & Baselines > Profiles**.



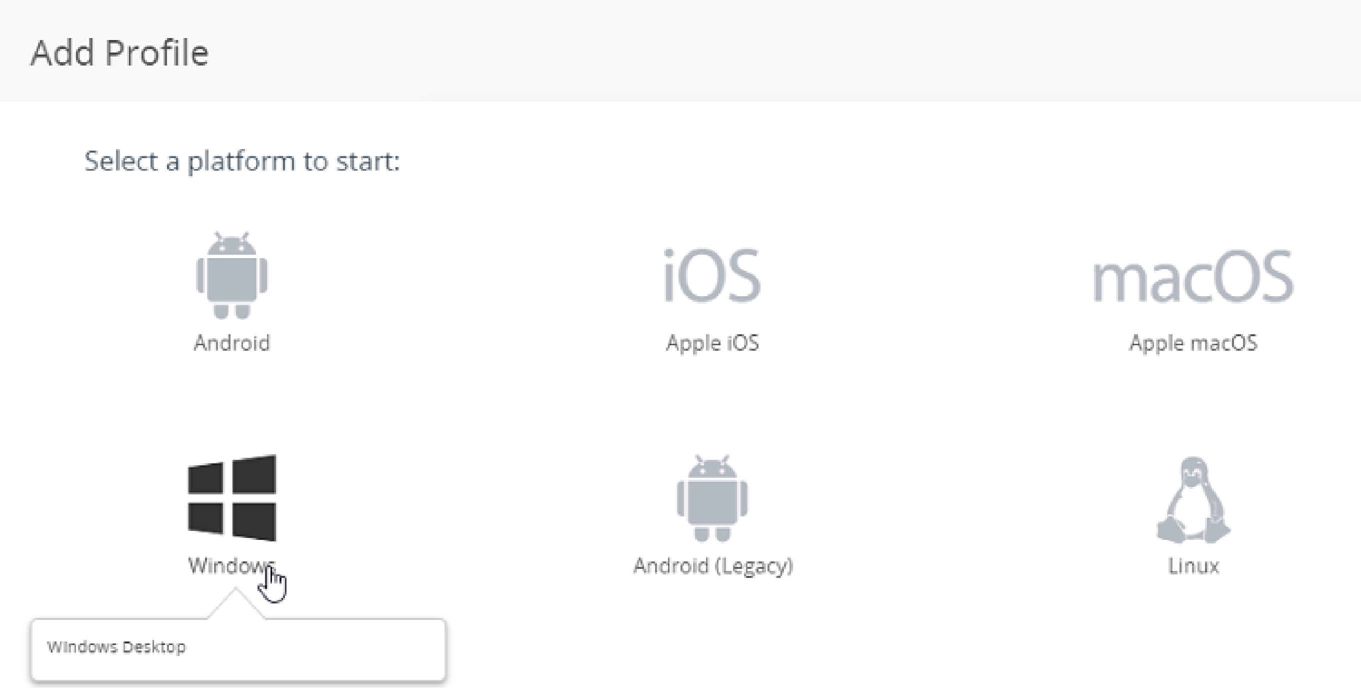
2. In the content pane, click **Add > Add Profile**.

3. Follow the wizard pages described below.

    - Add Profile
    - Select Device Type
    - Select Context
    - General
    - Credentials

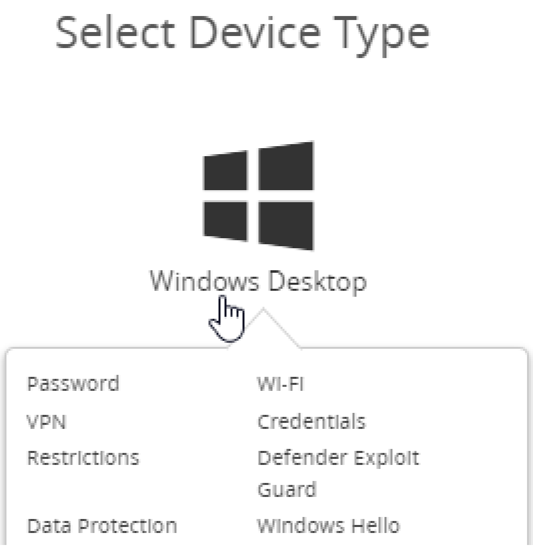
Add Profile

Click on the name of the platform running the enrollment device.



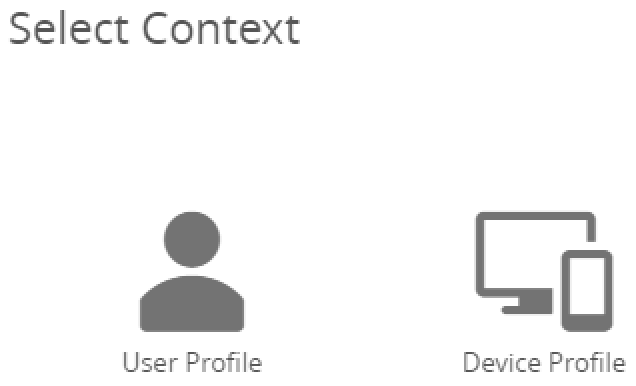
Select Device Type

Click on the type of enrolled device.



Select Context

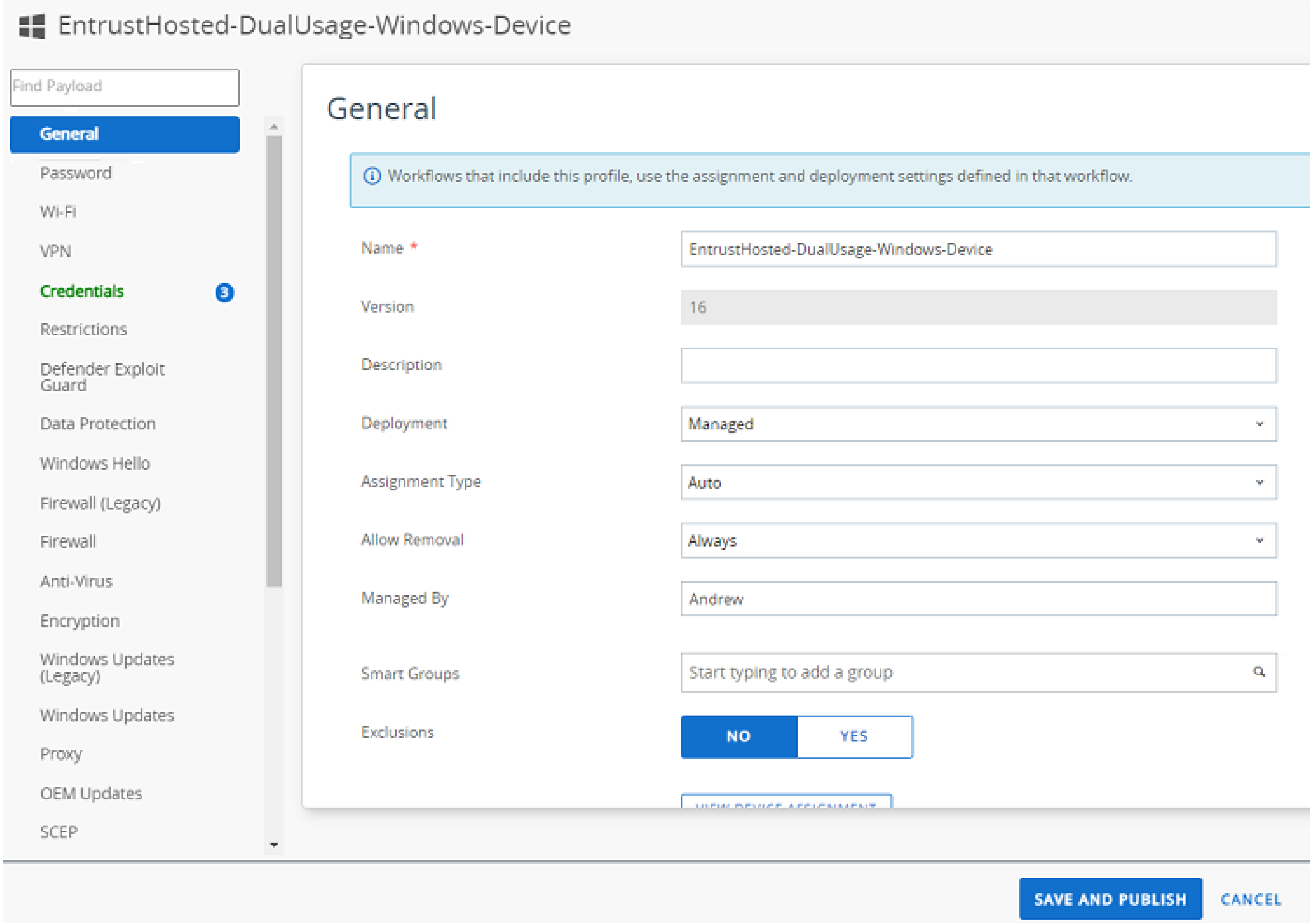
Click on **User Profile** to enroll users or **Device Profile** to enroll devices.



General

Click **General** in the sidebar menu to configure the following settings in the content pane.

Field	Value
â□□Name	Enter a name for the profile.
Smart Group	Select the smart group containing the managed users or devices.



General

ⓘ Workflows that include this profile, use the assignment and deployment settings defined in that workflow.

Name *	EntrustHosted-DualUsage-Windows-Device
Version	16
Description	
Deployment	Managed
Assignment Type	Auto
Allow Removal	Always
Managed By	Andrew
Smart Groups	Start typing to add a group
Exclusions	NO YES

Credentials

Click **Credentials** in the sidebar menu to configure the user credentials.

Field	Value
Credential Source	Select **Defined Certificate Authority**.
Certificate	Upload separately the certificates of the root and issuing CAs.
Certificate Store	Select **Personal** or **Intermediate** for profiles with the **User Profile** context. Select **Trusted Root** for profiles with the **User Device** context.

Click ✚ to create a new credential with the following settings.

Field	Value
Credential Source	Select **Defined Certificate Authority**.
Certificate Authority	Select the CA configured in Adding a CA and a Request Template for MDM automation in VMware Workspace ONE.
Certificate Template	Select the request template configured in Adding a CA and a Request Template for MDM automation in VMware Workspace ONE.

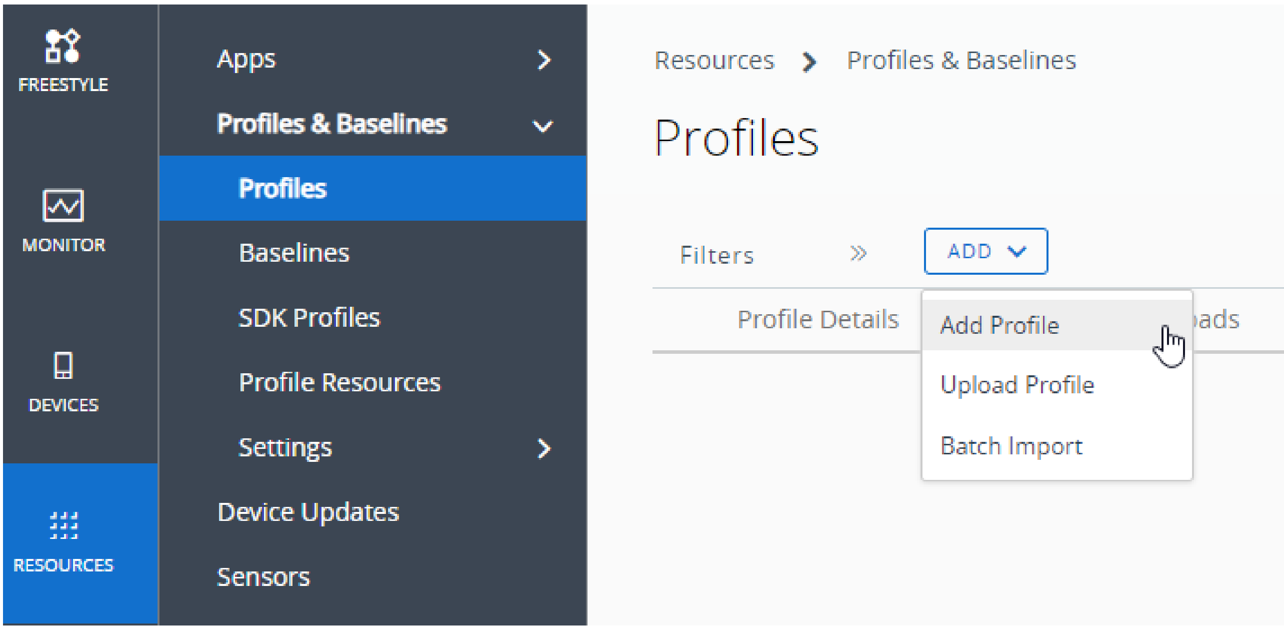
Field	Value
Key Location	Specify the location for the issued certificate: **Software** or **Hardware**.
Certificate Store	Enter the name of the certificate store.

Adding an SCEP profile for MDM automation in VMware Workspace ONE

See below for creating an MDM automation profile to issue certificates with the SCEP protocol.

To add an SCEP profile in Workspace One:

1. In Workspace One, navigate to **Resources > Profiles & Baselines > Profiles**.



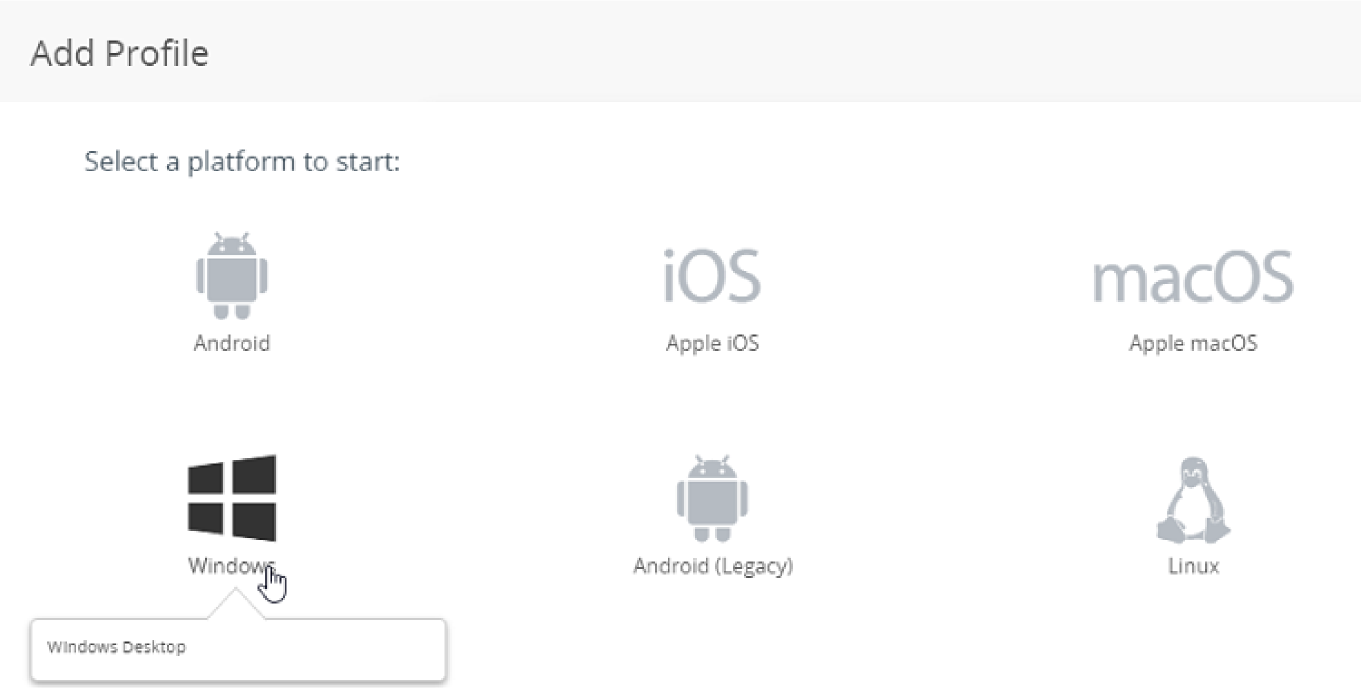
2. In the content pane, click **Add > Add Profile**.

3. Follow the wizard pages described below.

   - Add Profile
   - Select Device Type
   - Select Context
   - General
   - Credentials
   - SCEP

Add Profile

Click on the name of the platform running the enrollment device.

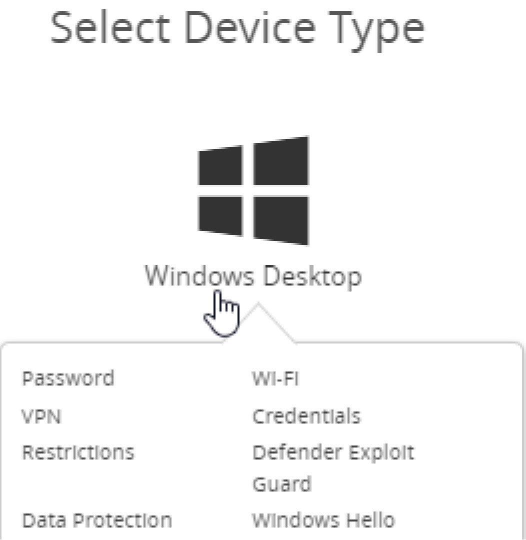


Add Profile

Select a platform to start:

Select Device Type

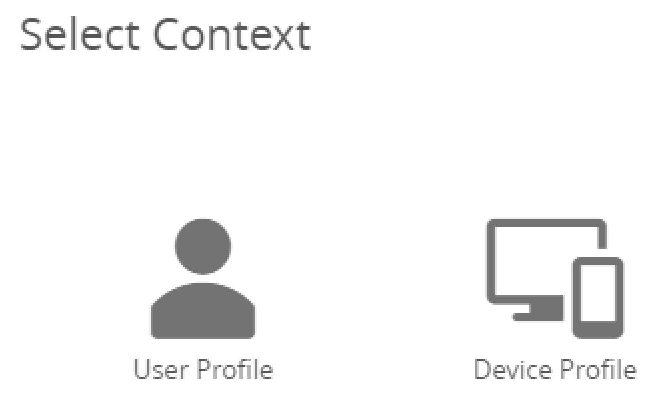
Click on the type of enrolled device.



Select Device Type

Select Context

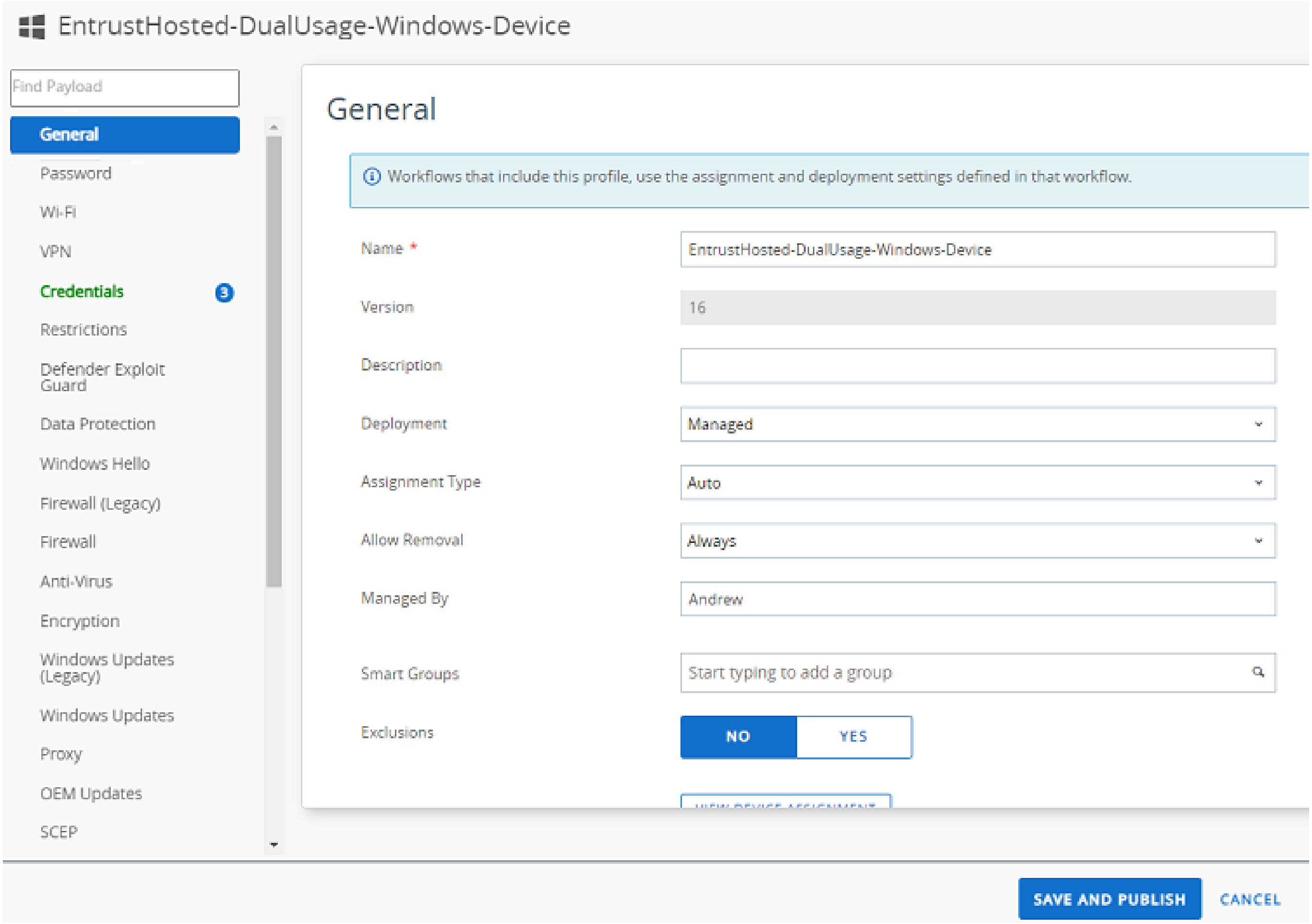
Click on **User Profile** to enroll users or **Device Profile** to enroll devices.



General

Click **General** in the sidebar menu to configure the following settings in the content pane.

Field	Value
â□□Name	Enter a name for the profile.
Smart Group	Select the smart group containing the managed users or devices.



General

ⓘ Workflows that include this profile, use the assignment and deployment settings defined in that workflow.

Name *	EntrustHosted-DualUsage-Windows-Device
Version	16
Description	
Deployment	Managed
Assignment Type	Auto
Allow Removal	Always
Managed By	Andrew
Smart Groups	Start typing to add a group
Exclusions	[✓ NO] YES

Credentials

Click **Credentials** in the sidebar menu to configure the user credentials.

Field	Value
Credential Source	Select **Defined Certificate Authority**.
Certificate	Upload separately the certificates of the root and issuing CAs.
Certificate Store	Select **Personal** or **Intermediate** for profiles with the **User Profile** context. Select **Trusted Root** for profiles with the **User Device** context.

SCEP

Click **SCEP** in the sidebar menu to configure the following settings in the content pane.

Field	Value
Credential Source	Select **Defined Certificate Authority**.
Certificate Authority	Select the CA configured in Adding a CA and a Request Template for MDM automation in VMware Workspace ONE.
Certificate Template	Select the request template configured in Adding a CA and a Request Template for MDM automation in VMware Workspace ONE.
Key Location	Specify the location for the issued certificate: **Software** or **Hardware**.

Testing MDM automation in VMware Workspace ONE

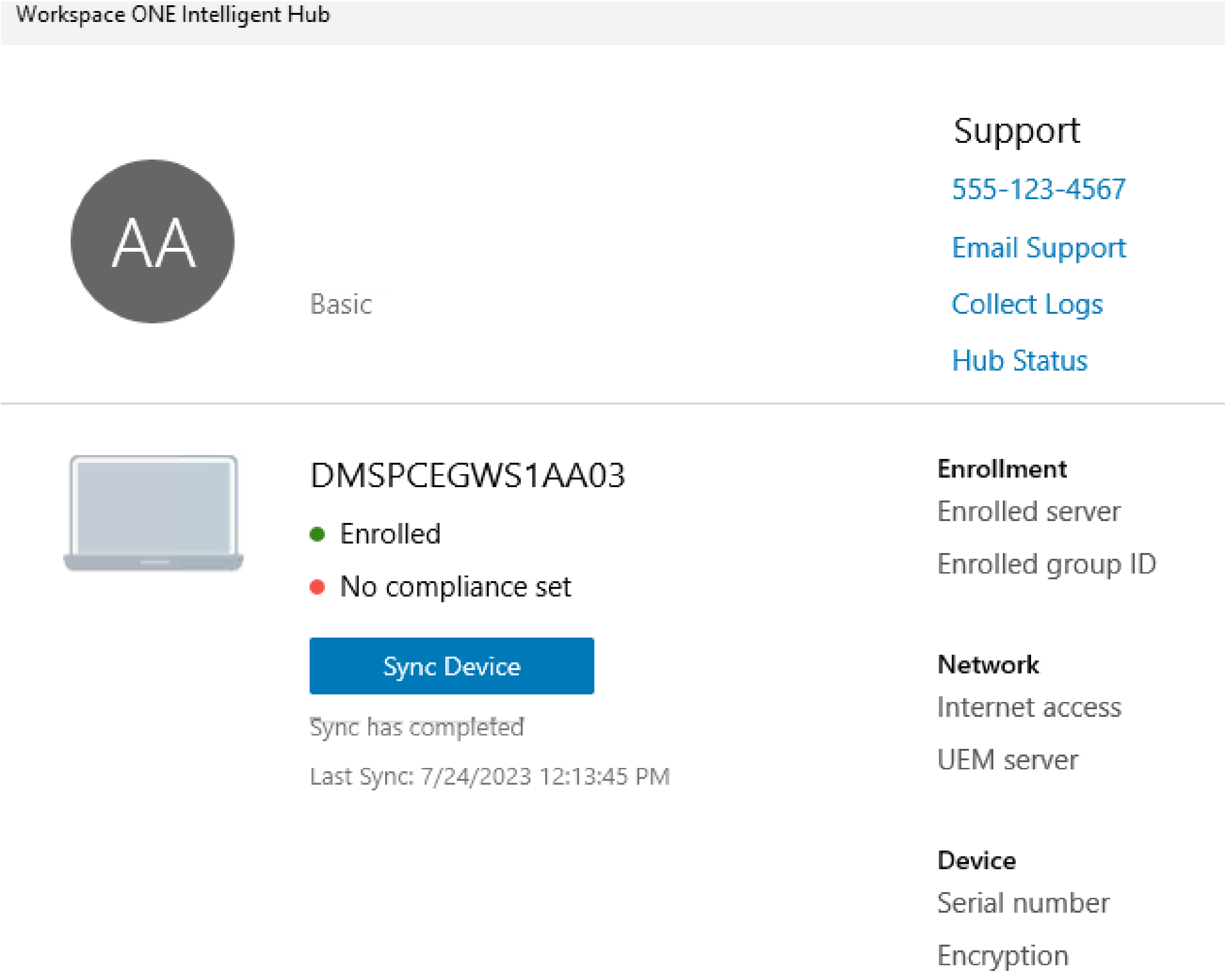
Test the MDM automation in VMware Workspace ONE after completing the configuration steps.

To test MDM automation in VMware Workspace ONE:

1. Open a browser at https://getwsone.com
2. Download the VMware Workspace ONE Intelligent Hub application.
3. Install the application on the device you want to enroll.
4. Log in to the VMware Workspace ONE Intelligent Hub.

   > ⚠ The user must belong to the Smart Group selected when adding the profile.

5. Click **Sync Device**.



Workspace ONE Intelligent Hub

AA

Basic

Support

555-123-4567

Email Support

Collect Logs

Hub Status

DMSPCEGWS1AA03

● Enrolled

● No compliance set

Sync Device

Sync has completed

Last Sync: 7/24/2023 12:13:45 PM

Enrollment

Enrolled server

Enrolled group ID

Network

Internet access

UEM server

Device

Serial number

Encryption

Automating MDM Ivanti enrollment

Configure PKIaaS to process MDM (Mobile Device Management) Ivanti enrollment requests with PKIaaS Certification Authorities.

- Ivanti requirements
- Configuring Ivanti in PKIaaS
- Configuring MDM automation in Ivanti Neurons MDM

Ivanti requirements

You must meet the following requirements to automate MDM Ivanti enrollment with a PKIaaS gateway.

- PKIaaS account requirements
- Operating system requirements
- TLS Cipher requirements

PKIaaS account requirements

You need an Entrust PKIaaS account with privileges to create an issuing certificate authority.

Operating system requirements

Enrollment integration for this release is tested and validated on the following operating system versions.

OS	Version
iPad	17.5.1
iPhone	17.5.1
macOS	Ventura 13.5.1
Windows	10
Android	14
ChromeOS	Not supported

Other devices and operating systems listed in the MDM vendor support documents should work, but have not been tested.

TLS Cipher requirements

Enrollment URLs support the following TLS Ciphers.

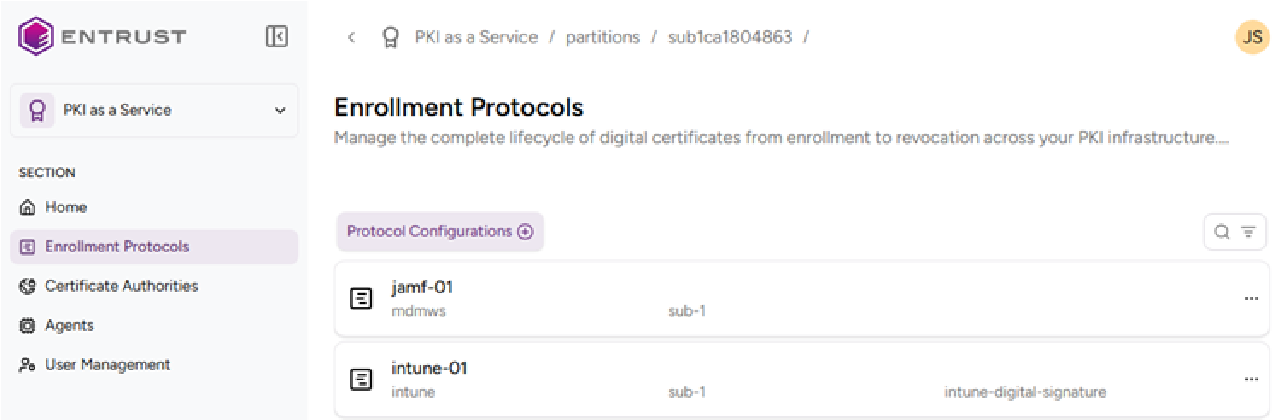
- `ECDHE-RSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES256-GCM-SHA384`

Configuring Ivanti in PKIaaS

Configure a PKIaaS workflow to process MDM (Mobile Device Management) Ivanti enrollment requests with PKIaaS Certification Authorities.

To configure an MDM Ivanti workflow in PKIaaS:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the following roles:
   - Owners
   - Protocol Operators
2. Click **Enrollment Protocols** in the sidebar.



Enrollment Protocols

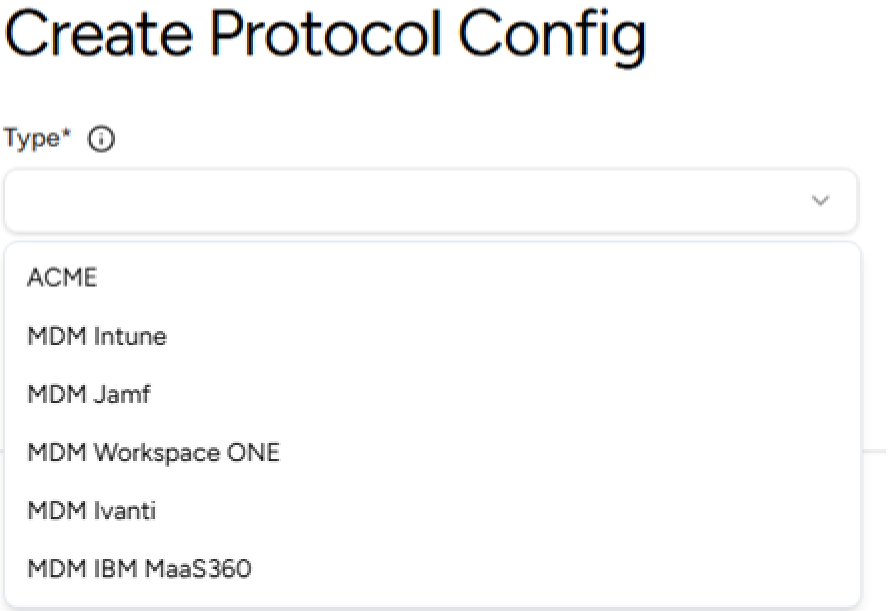
Manage the complete lifecycle of digital certificates from enrollment to revocation across your PKI infrastructure....

jamf-01 mdmws	sub-1	
intune-01 intune	sub-1	intune-digital-signature

3. Click **Create**.

4. Configure the following values in the **Create Protocol Config** dialog.

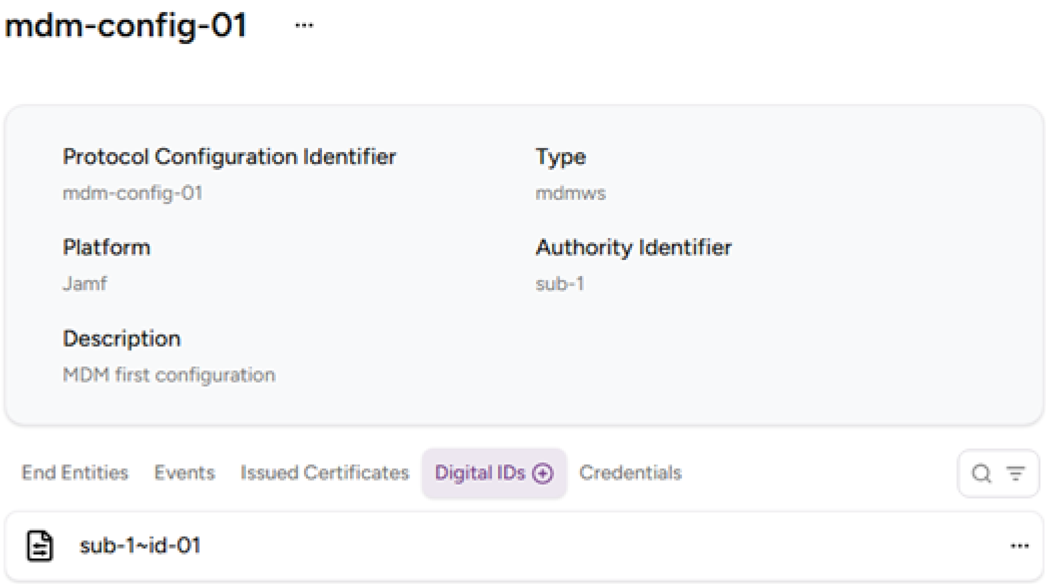
Field	Value
Type	Select **MDM Ivanti**
Protocol Configuration Identifier	Enter a unique identifier for the new configuration in your PKI. This identifier: Must be 2-18 characters long, can only include lowercase letters, numbers, hyphens ('-'), and underscores ('_').
Description	Enter an optional description of the protocol purpose.
CA Identifier	Select an issuing subordinate authority with profiles of the mdmws group.


Create Protocol Config

Type*

5. Click **Create**.

6. In the confirmation window, select the **Digital IDs** tab.


mdm-config-01

Protocol Configuration Identifier
mdm-config-01

Type
mdmws

Platform
Jamf

Authority Identifier
sub-1

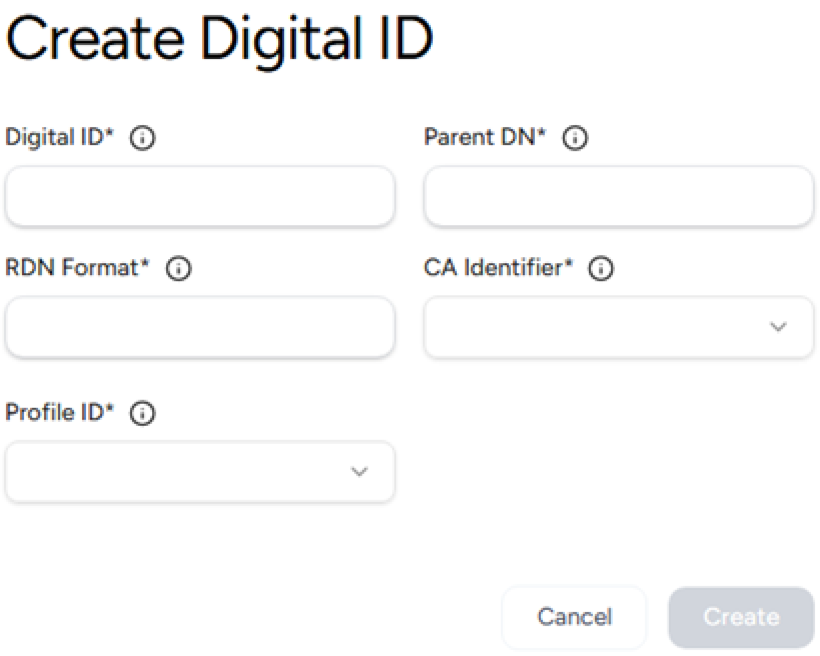
Description
MDM first configuration

sub-1~id-01

7. Click **CREATE**.

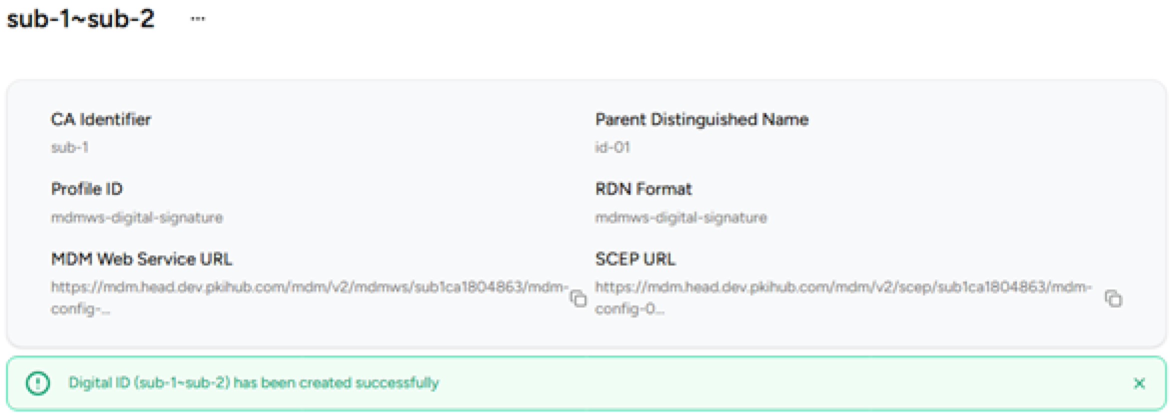
8. Configure the following values in the **Digital identifier** dialog.

Field	Value
Digital ID	Enter a unique name of the new digital identifier.
Parent DN	Enter the parent Distinguished Name (DN) for building the RDN of a certificate. This value is appended to the end of the Subject DN after the **RDN Format** variables have been processed.
RDN Format	Enter the Relative Distinguished Name (RDN) format to build certificate Subject Names.
CA Identifier	Select an issuing subordinate authority with profiles of the mdmws group.
Profile ID	Select the mdmws profile to process the enrollment requests.



9. Click **Create**.

10. Copy the URLs under the **Web Service URL** and **SCEP URL** fields of the confirmation dialog.



sub-1~sub-2

CA Identifier
sub-1

Parent Distinguished Name
id-01

Profile ID
mdmws-digital-signature

RDN Format
mdmws-digital-signature

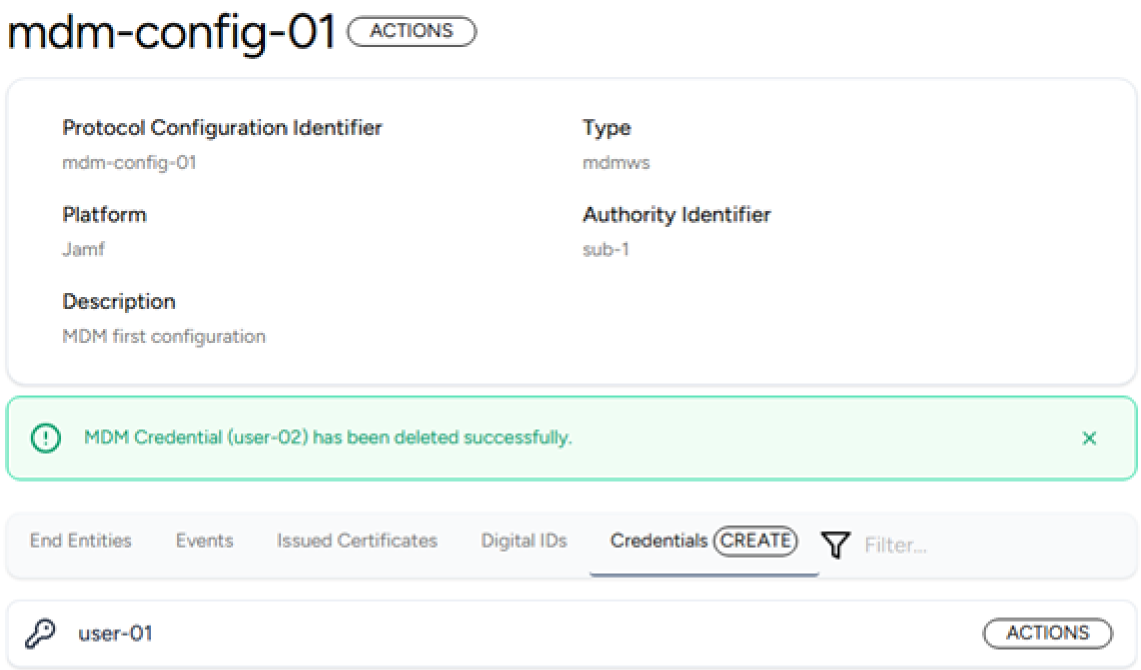
MDM Web Service URL
https://mdm.head.dev.pkihub.com/mdm/v2/mdmws/sub1ca1804863/mdm-config-...

SCEP URL
https://mdm.head.dev.pkihub.com/mdm/v2/scep/sub1ca1804863/mdm-config-0...

Digital ID (sub-1~sub-2) has been created successfully

11. In the navigation tree, select the name of the new protocol configuration.

12. Select the **Credentials** tab.



mdm-config-01

Protocol Configuration Identifier
mdm-config-01

Type
mdmws

Platform
Jamf

Authority Identifier
sub-1

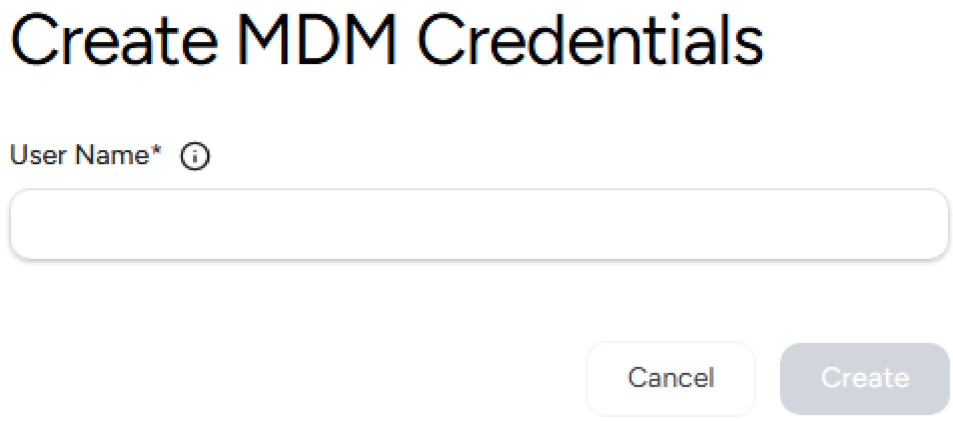
Description
MDM first configuration

MDM Credential (user-02) has been deleted successfully.

user-01

13. Click **CREATE**.

14. In the **Create MDM Credentials** dialog, enter a username that is 2-18 characters long and only includes lowercase letters, numbers, hyphens (â□□-â□□), and underscores (â□□_â□□).

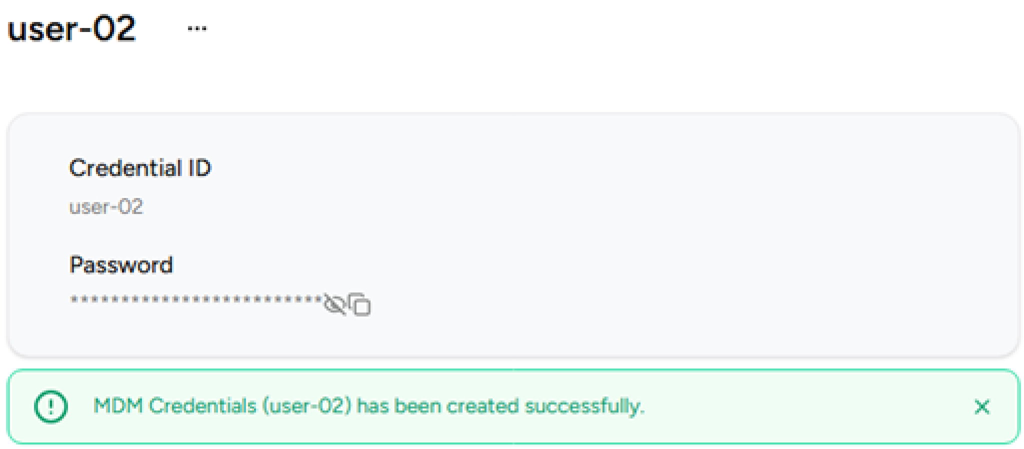


Create MDM Credentials

User Name*

15. Click **Create**.

16. Copy the **Password** value displayed in the confirmation dialog.



user-02 ···

Credential ID
user-02

Password
****

MDM Credentials (user-02) has been created successfully.

⚠ As stated in the confirmation dialog before leaving this page, Entrust PKIaaS will not display the credential password again.

Configuring MDM automation in Ivanti Neurons MDM

See below for configuring Ivanti Neurons as an MDM provider.

- Supported protocols for MDM automation with Ivanti Neurons
- Adding a PKIaaS issuing CA to Ivanti Neurons MDM
- Adding the PKIaaS issuing and root CA certificates in Ivanti Neurons MDM
- Adding an identity certificate in Ivanti Neurons MDM

Supported protocols for MDM automation with Ivanti Neurons

When using Ivanti Neurons for MDM as a provider, the enrollment automation:

- Supports the PKI protocol for Entrust MDMWS PKCS #12 enrollment.
- Does not yet support the Simple Certificate Enrollment Protocol (SCEP). MobileIron Cloud is addressing the limitations in its SCEP implementation to ensure full support for all profiles.

See below the profiles of the mdmws group supported by each protocol.

Profile	PKI	SCEP
`mdmws-digital-signature`	â□□	â□□
`mdmws-digital-signature-key-encipherment`	â□□	â□□
`mdmws-digital-signature-key-encipherment-clientauth`	â□□	â□□
`mdmws-key-encipherment`	â□□	â□□
`mdmws-non-repudiation`	â□□	â□□
`mdmws-p12-digital-signature`	✓	â□□

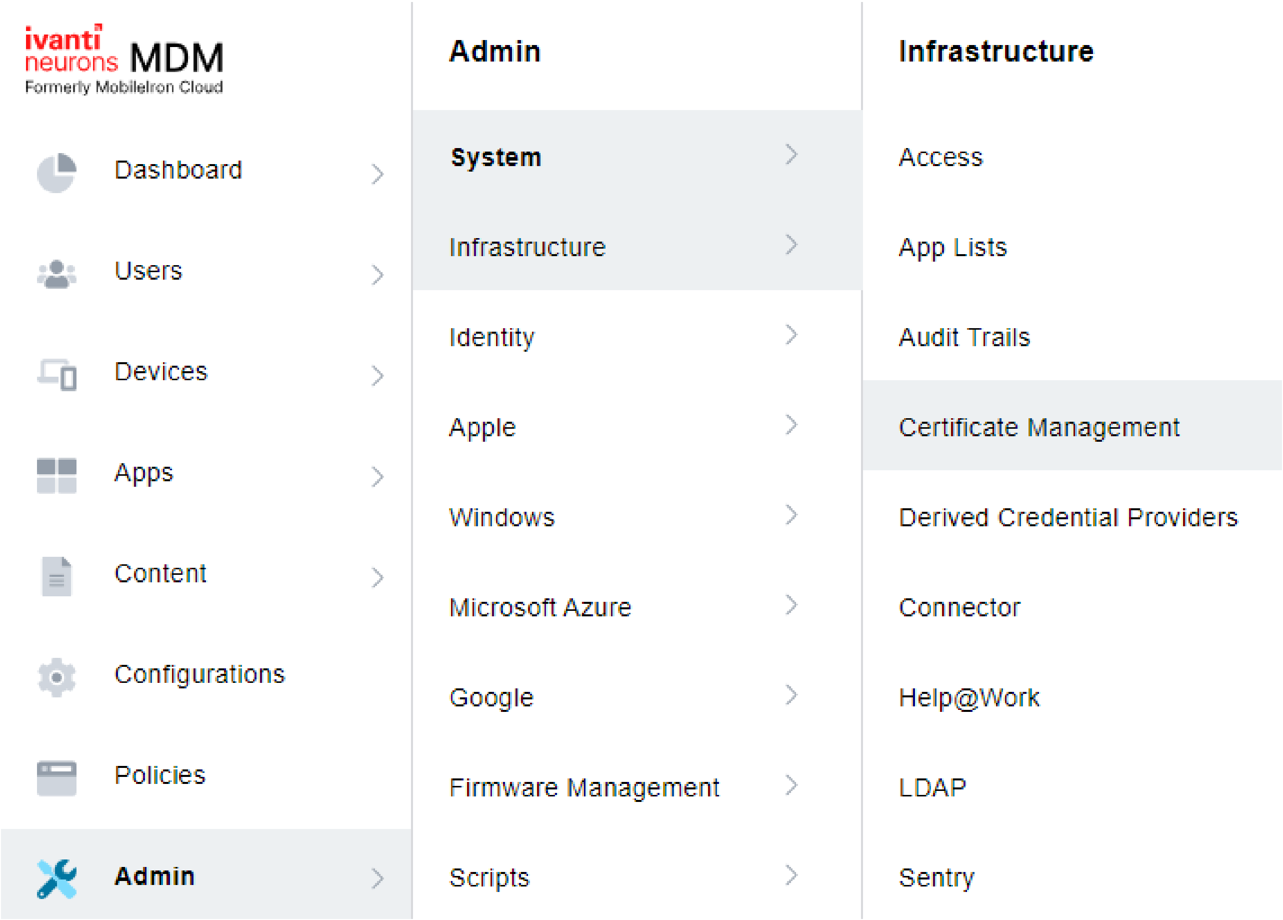
Profile	PKI	SCEP
`mdmws-p12-digital-signature-key-encipherment`	✓	â□□
`mdmws-p12-digital-signature-key-encipherment-clientauth`	✓	â□□
`mdmws-p12-key-encipherment`	✓	â□□
`mdmws-p12-non-repudiation`	✓	â□□

Adding a PKIaaS issuing CA to Ivanti Neurons MDM

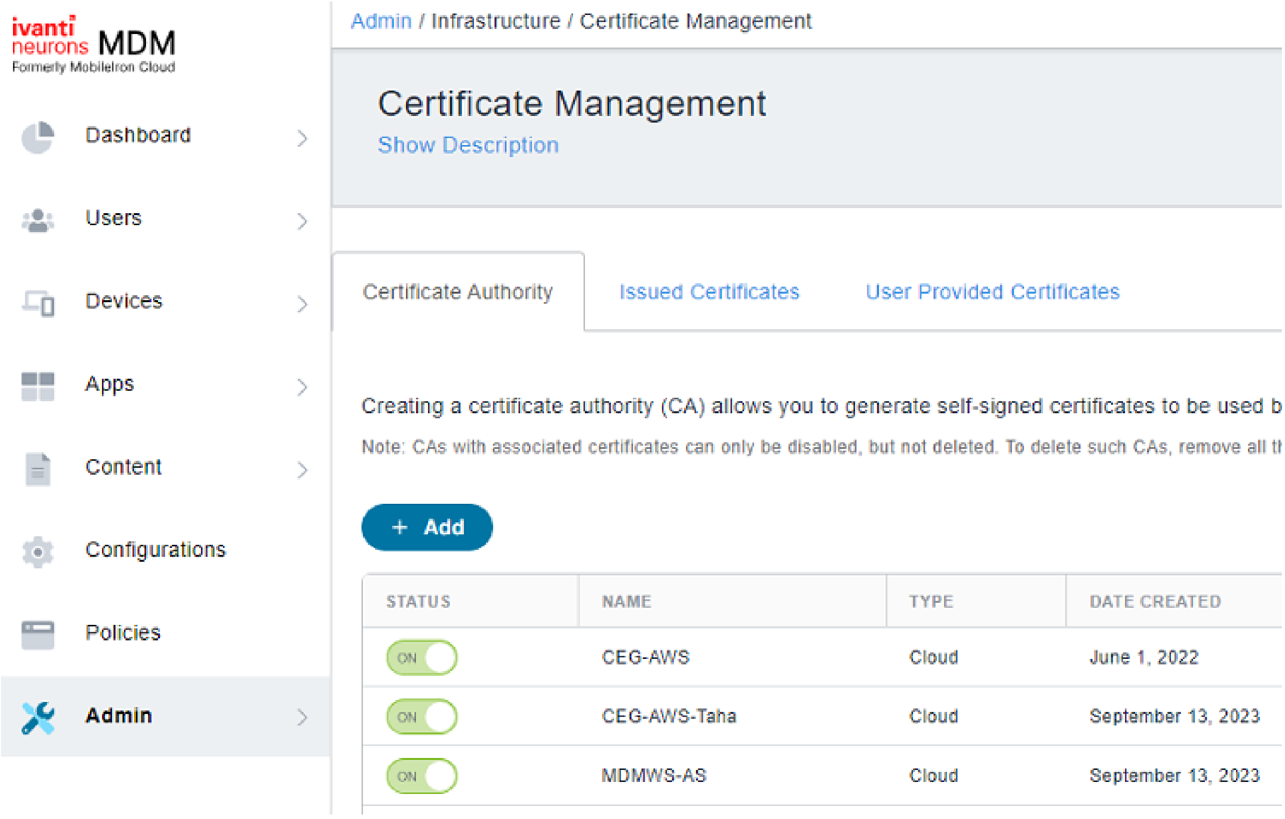
Add and configure a PKIaaS issuing certificate authority in Ivanti Neurons to automate MDM enrollment.

To add a PKIaaS issuing certificate authority in Ivanti Neurons:

1. Log in to the Ivanti Neurons portal.
2. Go to **Admin > Infrastructure> Certificate Management**.



3. Click the **Add** button of the **Certificate Authority** tab.



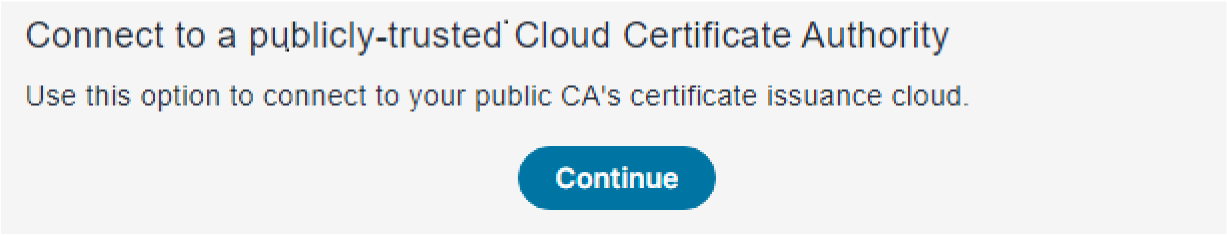
Certificate Management

Creating a certificate authority (CA) allows you to generate self-signed certificates to be used b

Note: CAs with associated certificates can only be disabled, but not deleted. To delete such CAs, remove all tl

STATUS	NAME	TYPE	DATE CREATED
ON	CEG-AWS	Cloud	June 1, 2022
ON	CEG-AWS-Taha	Cloud	September 13, 2023
ON	MDMWS-AS	Cloud	September 13, 2023

4. Click **Continue**.

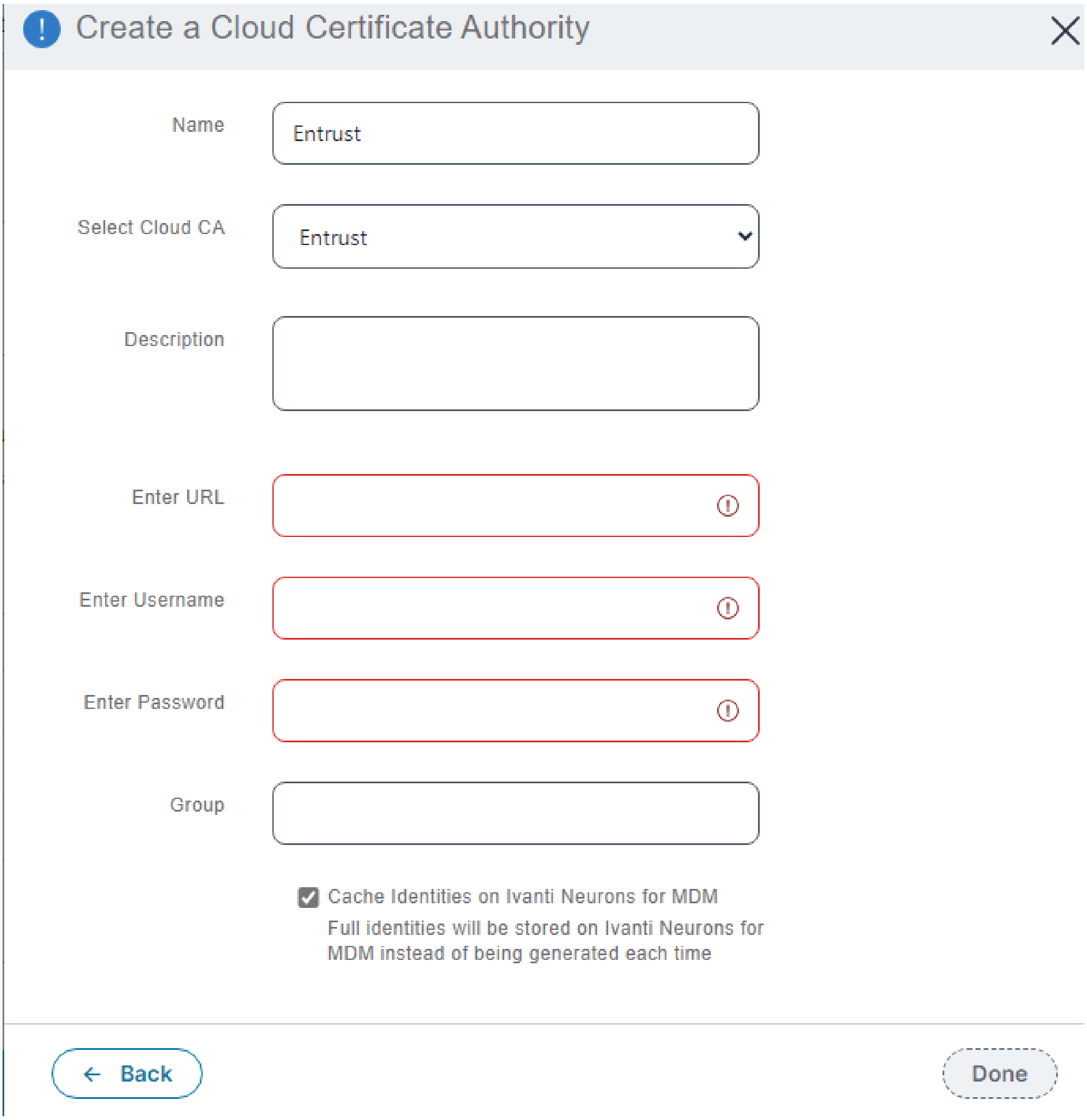


Connect to a publicly-trusted Cloud Certificate Authority

Use this option to connect to your public CA's certificate issuance cloud.

5. Configure the following settings.

   - Name
   - Select Cloud CA
   - Description
   - Enter URL
   - Enter Username
   - Enter Password
   - Group
   - Cache Identities on Ivanti Neurons for MDM



Create a Cloud Certificate Authority

Name	Entrust
Select Cloud CA	Entrust
Description	
Enter URL	
Enter Username	
Enter Password	
Group	

☑ Cache Identities on Ivanti Neurons for MDM
Full identities will be stored on Ivanti Neurons for MDM instead of being generated each time

Name

Enter a friendly name for Entrust CA within Ivanti Neurons MDM.

Mandatory: Yes.

Select Cloud CA

Select **Entrust**.

Mandatory: Yes.

Description

Add an optional description for the Entrust CA.

Mandatory: Yes.

Enter URL

Paste the **SCEP URL** value that was obtained in section Configuring Ivanti in PKIaaS.

Mandatory: Yes.

Enter Username

Paste the **User Name** that was used to create a credential in section Configuring Ivanti in PKIaaS.

Enter Password

Paste the password that was obtained after creating a credential in section Configuring Ivanti in PKIaaS.

Mandatory: Yes.

Group

Skip this field, as groups are not evaluated for certificate authorities.

Mandatory: Yes.

Cache Identities on Ivanti Neurons for MDM

Keep this option enabled.

⚠ Disabling this option will result in certificates being regenerated each time they are needed.

Mandatory: Yes.

Adding the PKIaaS issuing and root CA certificates in Ivanti Neurons MDM

Repeat the steps below to add the certificates of the following certificate authorities.

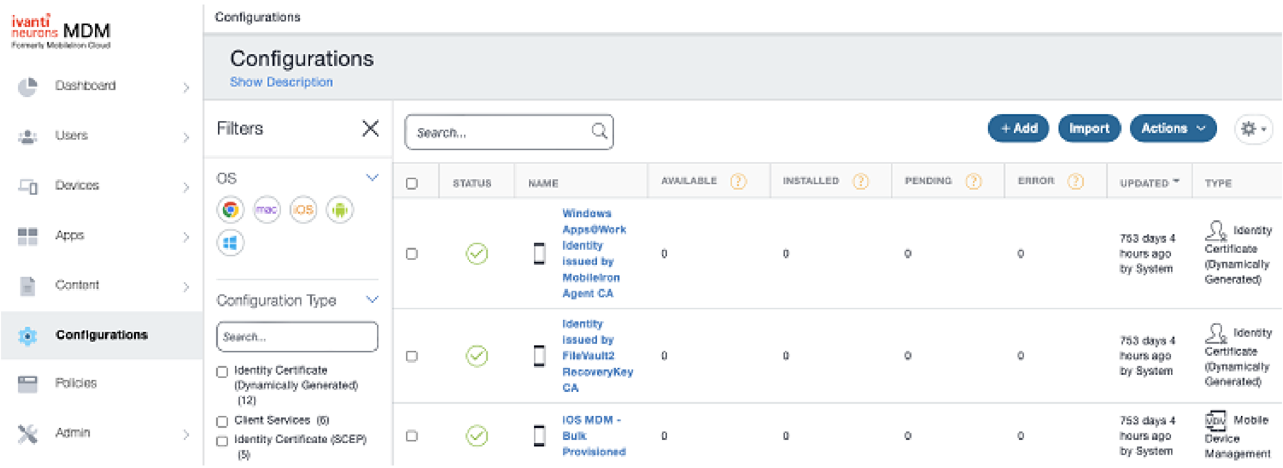
- The issuing CA described in Adding a PKIaaS issuing CA to Ivanti Neurons MDM.
- The root CA of this issuing CA.

ℹ See Downloading a CA certificate for how to download both certificates.

To add a CA certificate in Ivanti Neurons MDM:

1. Log in to the Ivanti Neurons portal.

2. Select **Configurations** in the navigation sidebar and click **Add**.

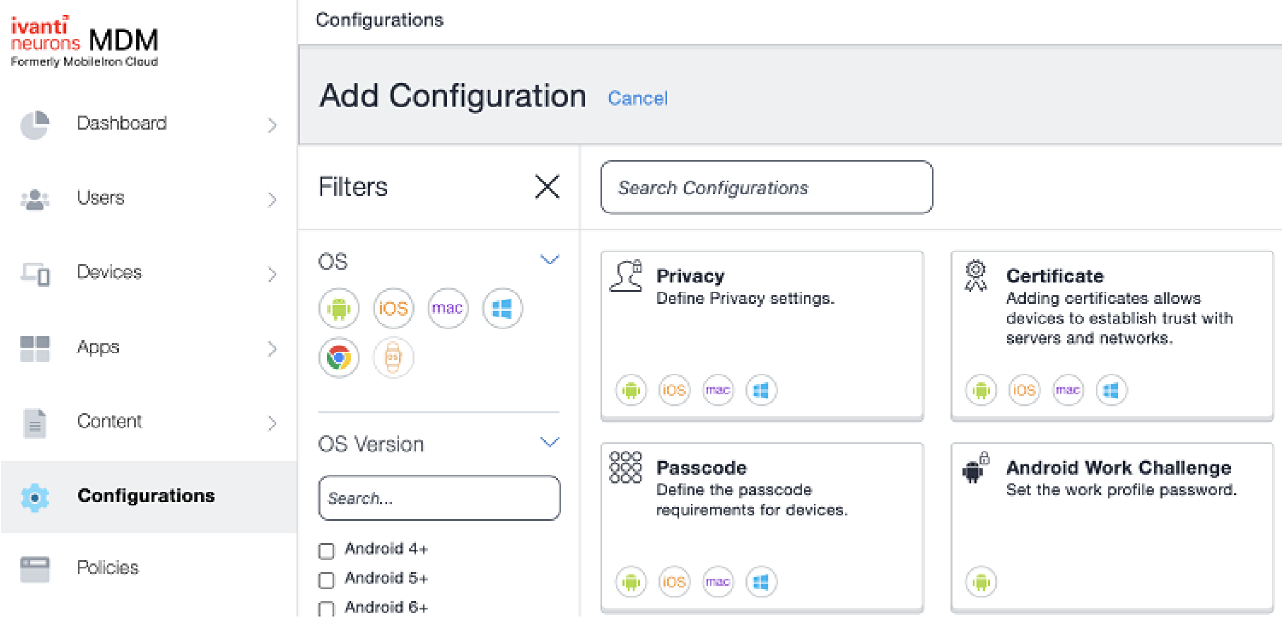


Configurations

□ Identity Certificate (Dynamically Generated) (12)
□ Client Services (6)
□ Identity Certificate (SCEP) (5)

□	STATUS	NAME	AVAILABLE	INSTALLED	PENDING	ERROR	UPDATED	TYPE
□	✓	Windows Apps@Work Identity issued by MobileIron Agent CA	0	0	0	0	753 days 4 hours ago by System	Identity Certificate (Dynamically Generated)
□	✓	Identity issued by FileVault2 RecoveryKey CA	0	0	0	0	753 days 4 hours ago by System	Identity Certificate (Dynamically Generated)
□	✓	iOS MDM - Bulk Provisioned	0	0	0	0	753 days 4 hours ago by System	Mobile Device Management

3. Click **Certificate** in the **Add Configuration** pane.



□ Android 4+
□ Android 5+
□ Android 6+

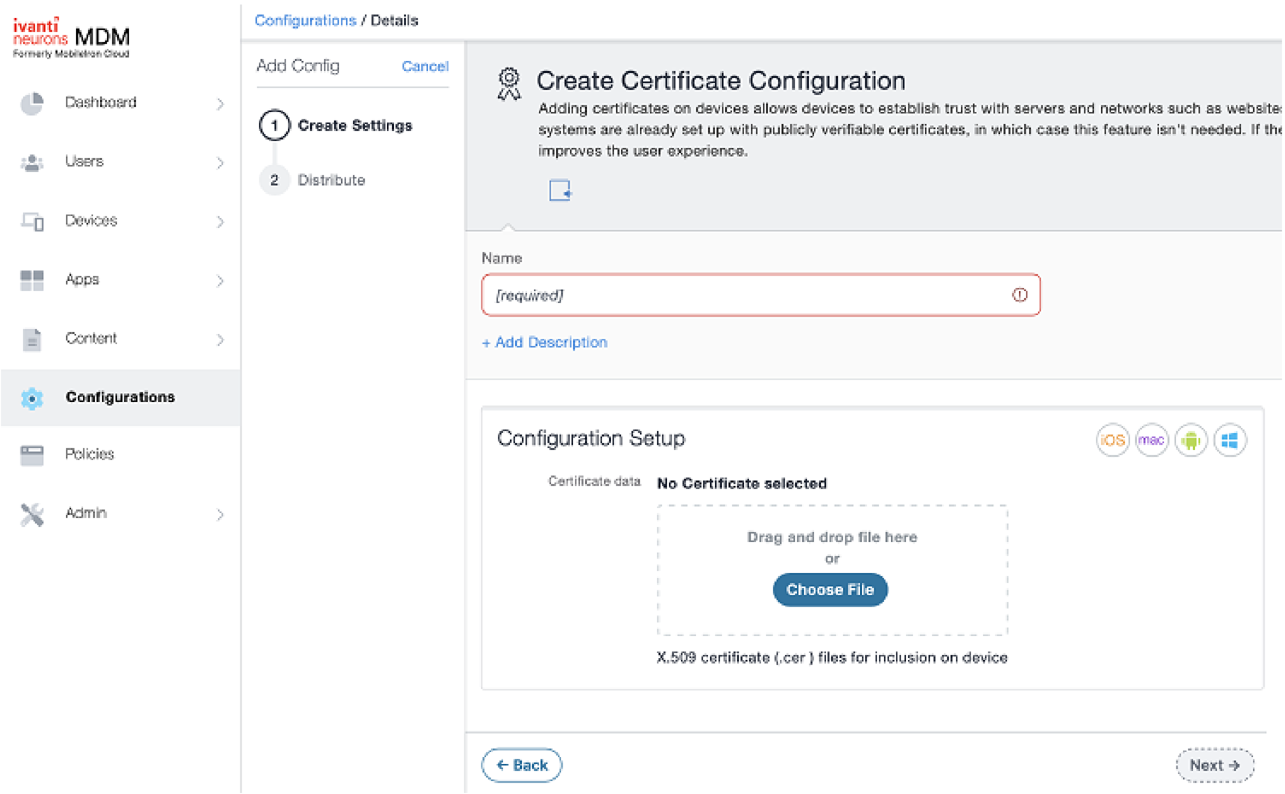
Privacy
Define Privacy settings.

Certificate
Adding certificates allows devices to establish trust with servers and networks.

Passcode
Define the passcode requirements for devices.

Android Work Challenge
Set the work profile password.

4. Enter a friendly name for the CA certificate in the **Name** field.



Create Certificate Configuration

Adding certificates on devices allows devices to establish trust with servers and networks such as website systems are already set up with publicly verifiable certificates, in which case this feature isn't needed. If the improves the user experience.

Name

[required]

+ Add Description

Configuration Setup

Certificate data No Certificate selected

Drag and drop file here

or

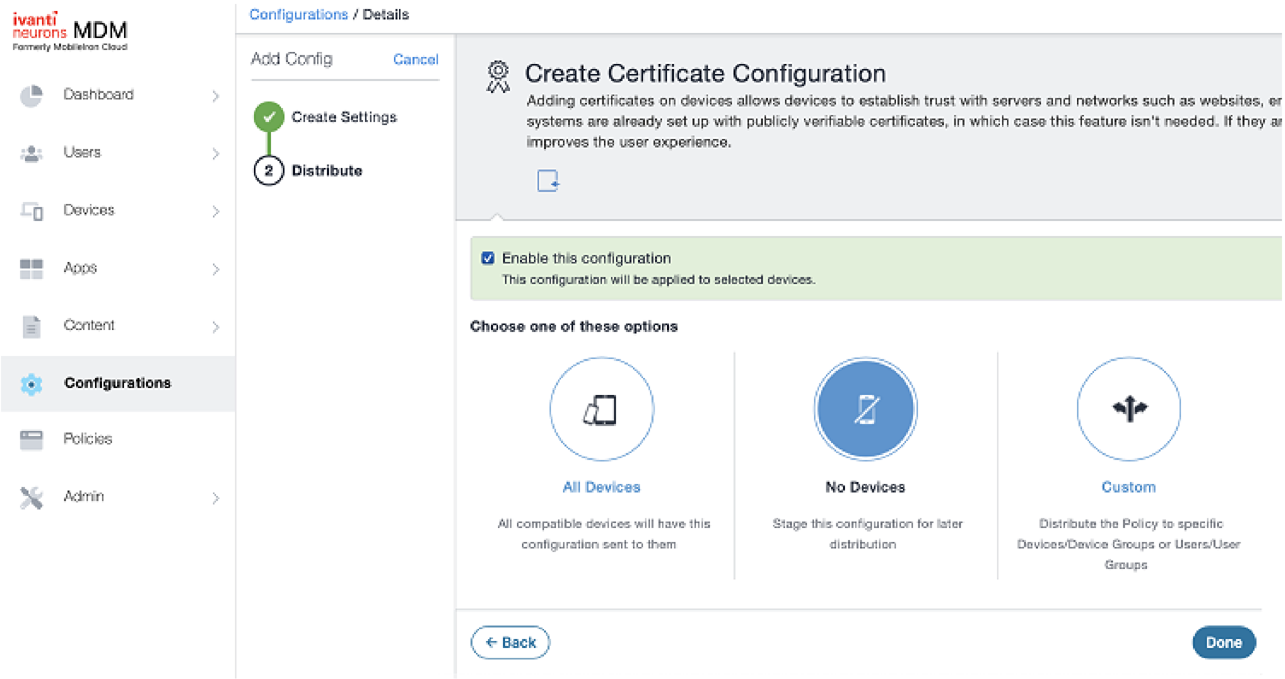
Choose File

X.509 certificate (.cer) files for inclusion on device

5. Click **Choose file** under **Configuration Setup** and import the certificate file.

6. Click **Next**.

7. Select the devices, users, or groups to assign the certificate to.



Create Certificate Configuration

Adding certificates on devices allows devices to establish trust with servers and networks such as websites, er systems are already set up with publicly verifiable certificates, in which case this feature isn't needed. If they ar improves the user experience.

☑ Enable this configuration

This configuration will be applied to selected devices.

Choose one of these options

All Devices

All compatible devices will have this configuration sent to them

No Devices

Stage this configuration for later distribution

Custom

Distribute the Policy to specific Devices/Device Groups or Users/User Groups

8. Click **Done**.

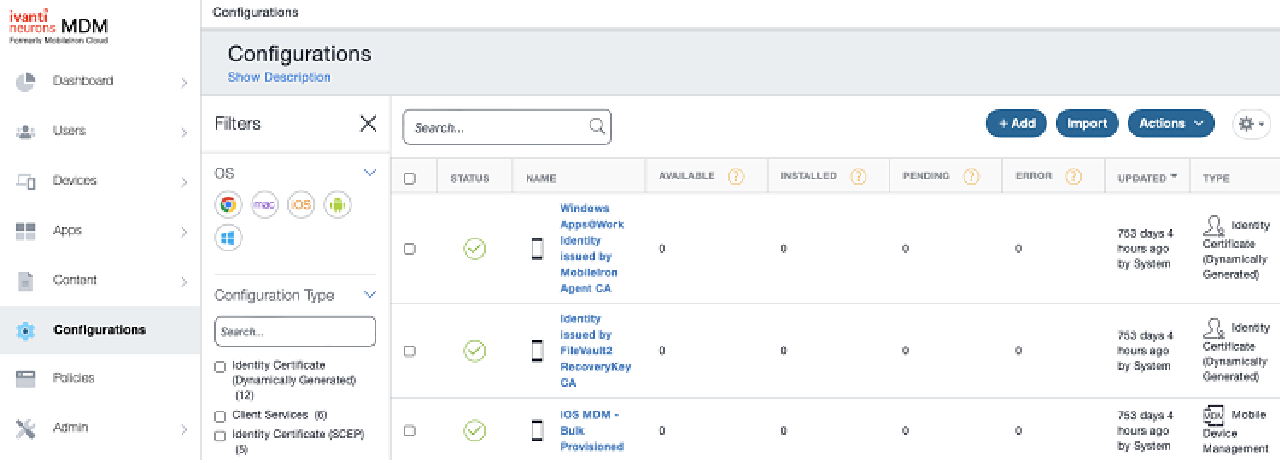
Adding an identity certificate in Ivanti Neurons MDM

Add an identity certificate in Ivanti Neurons to automate MDM enrollment.

To add an identity certificate in Ivanti Neurons:

1. Log in to the Ivanti Neurons portal.

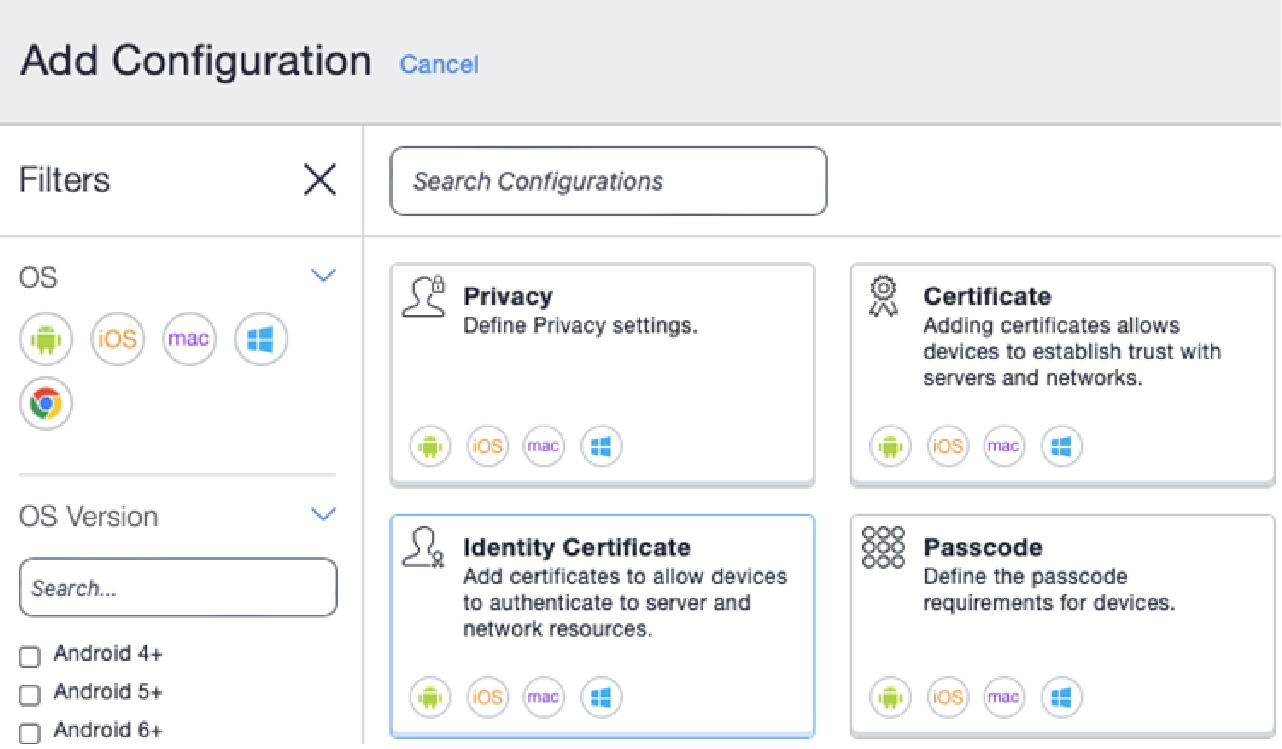
2. Select **Configurations** in the navigation sidebar and click **Add**.



☐ Identity Certificate (Dynamically Generated) (12)
☐ Client Services (6)
☐ Identity Certificate (SCEP) (5)

☐	STATUS	NAME	AVAILABLE	INSTALLED	PENDING	ERROR	UPDATED	TYPE
☐	✓	Windows Apps@Work Identity issued by MobileIron Agent CA	0	0	0	0	753 days 4 hours ago by System	Identity Certificate (Dynamically Generated)
☐	✓	Identity issued by FileVault2 RecoveryKey CA	0	0	0	0	753 days 4 hours ago by System	Identity Certificate (Dynamically Generated)
☐	✓	iOS MDM - Bulk Provisioned	0	0	0	0	753 days 4 hours ago by System	Mobile Device Management

3. Click **Identity certificate** in the **Add Configuration** pane.



☐ Android 4+
☐ Android 5+
☐ Android 6+

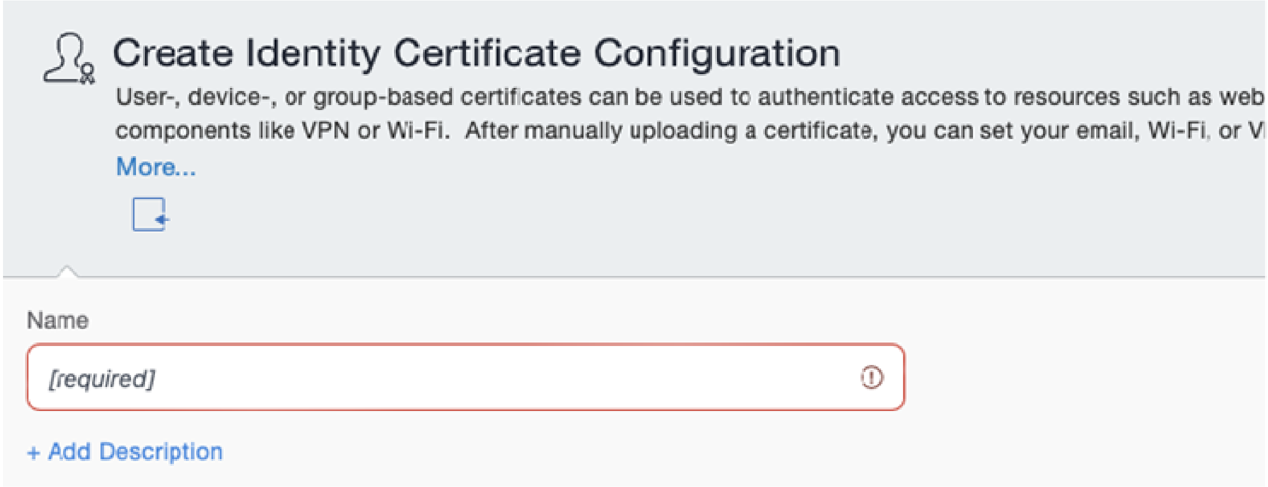
Privacy
Define Privacy settings.

Certificate
Adding certificates allows devices to establish trust with servers and networks.

Identity Certificate
Add certificates to allow devices to authenticate to server and network resources.

Passcode
Define the passcode requirements for devices.

4. Enter a friendly name for the identity certificate in the **Name** field.



Create Identity Certificate Configuration

User-, device-, or group-based certificates can be used to authenticate access to resources such as web components like VPN or Wi-Fi. After manually uploading a certificate, you can set your email, Wi-Fi, or V

More...

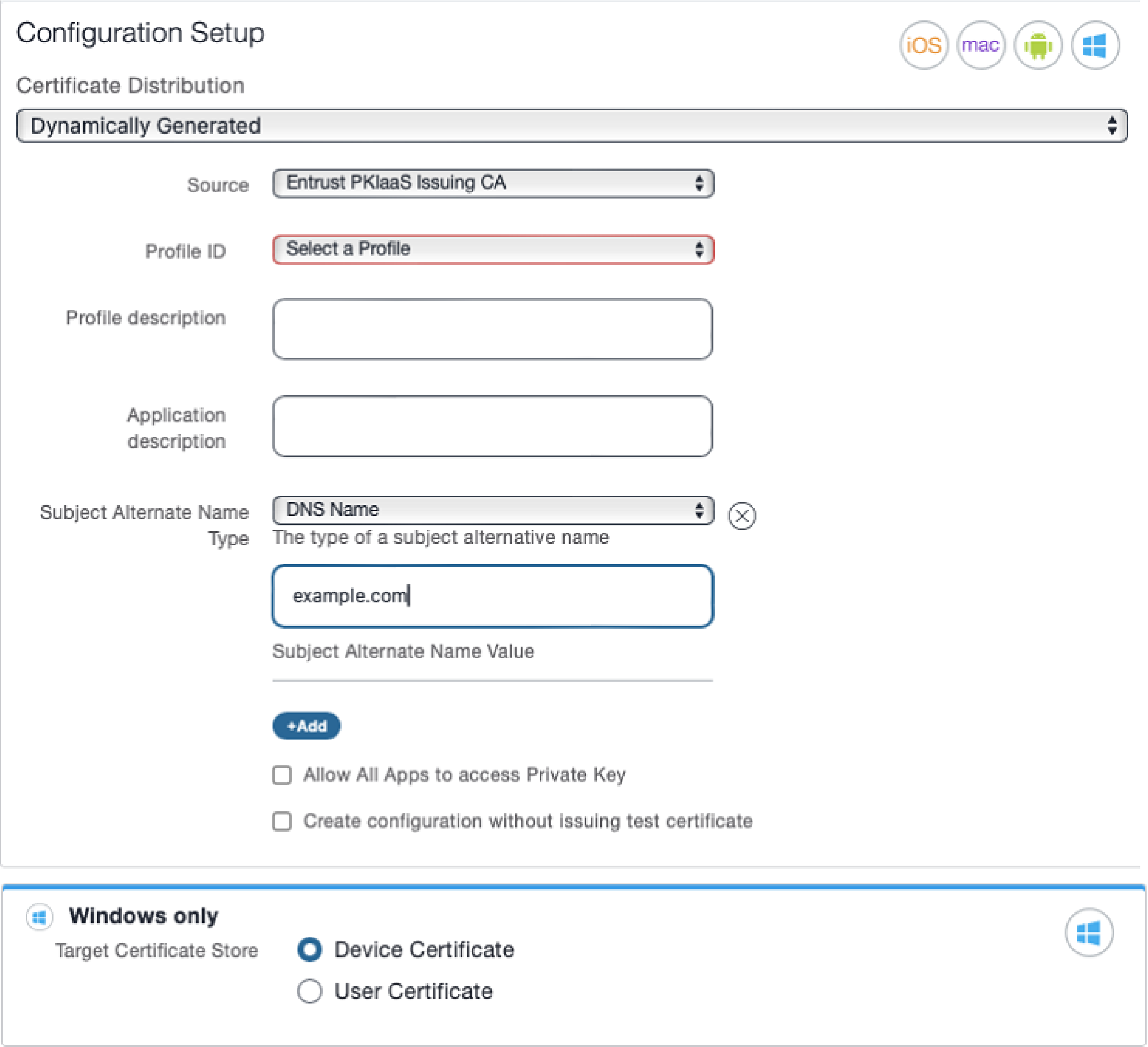
Name

[required]

+ Add Description

5. Select the following values under **Configuration Setup**.

   - Certificate Distribution
   - Source
   - Profile ID
   - Profile description
   - Application description
   - Subject Alternate Name Type
   - Subject Alternative Name Value
   - Target Certificate Store



Configuration Setup

Certificate Distribution: Dynamically Generated

Source: Entrust PKIaaS Issuing CA

Profile ID: Select a Profile

Profile description

Application description

Subject Alternate Name Type: DNS Name

The type of a subject alternative name

example.com

Subject Alternate Name Value

□ Allow All Apps to access Private Key

□ Create configuration without issuing test certificate

Windows only

Target Certificate Store

● Device Certificate

○ User Certificate

Certificate Distribution

Select **Dynamically Generated**.

Mandatory: Yes

Source

Select the certificate authority described in Adding a PKIaaS issuing CA to Ivanti Neurons MDM.

Mandatory: Yes

Profile ID

Select the same **Profile ID** value that was used to create a digital identifier in section Configuring Ivanti in PKIaaS.

Mandatory: Yes

Profile description

Enter a description of the enrollment profile.

Mandatory: No

Application description

Enter a description of the intended application for the identity certificate.

Mandatory: No

Subject Alternate Name Type

Select a format for the Subject Alternative Name field in the enrolled certificates.

Mandatory: Select **None** if the enrolled certificates do not require a Subject Alternative Name field.

Subject Alternative Name Value

Enter a value for the Subject Alternative Name field in the enrolled certificates.

Mandatory: When selecting a value other than **None** in **Subject Alternate Name Type**.

Target Certificate Store

When enrolling Windows devices, select the store for installing the certificates.

Option	Certificate store
Device Certificate	The store of the â□□local machine
User Certificate	The store of the current user

Mandatory: When enrolling certificates for Windows devices.

Automating MDM IBM MaaS360 enrollment

Configure PKIaaS to process MDM IBM MaaS360 enrollment requests with PKIaaS Certification Authorities.

- MDM IBM MaaS360 requirements
- Configuring MDM IBM MaaS360 in PKIaaS
- Configuring MDM automation in IBM Cloud

MDM IBM MaaS360 requirements

You must meet the following requirements to automate MDM IBM MaaS360 enrollment with a PKIaaS gateway.

- PKIaaS account requirements
- Operating system requirements
- TLS Cipher requirements

PKIaaS account requirements

You need an Entrust PKIaaS account with privileges to create an issuing certificate authority.

Operating system requirements

Enrollment integration for this release is tested and validated on the following operating system versions.

OS	Version
iPad	TBD
iPhone	TBD
macOS	TBD
Windows	TBD
Android	TBD
ChromeOS	TBD

Other devices and operating systems listed in the MDM vendor support documents should work, but have not been tested.

TLS Cipher requirements

Enrollment URLs support the following TLS Ciphers.

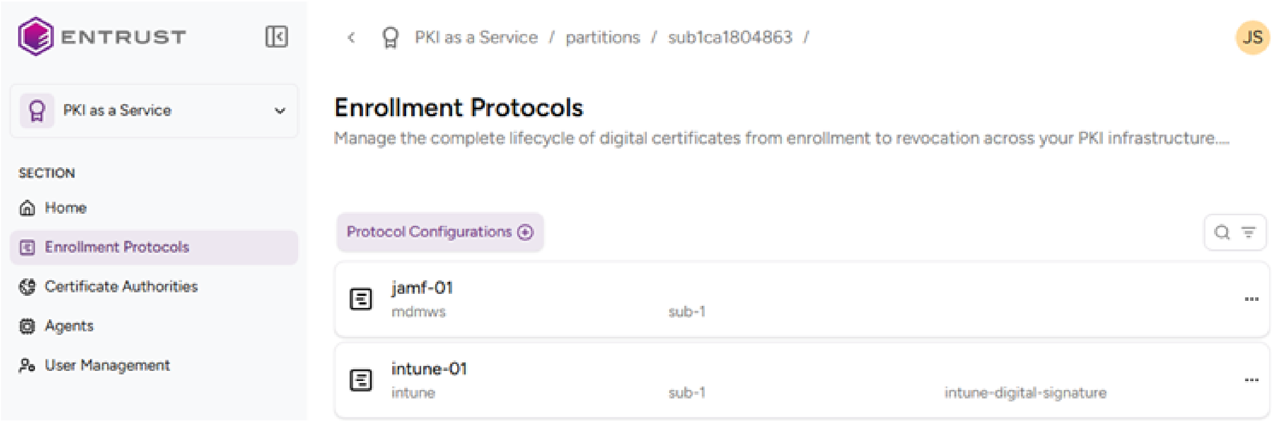
- `ECDHE-RSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES256-GCM-SHA384`

Configuring MDM IBM MaaS360 in PKIaaS

Configure a PKIaaS workflow to process MDM (Mobile Device Management) IBM MaaS360 enrollment requests with PKIaaS Certification Authorities.

To configure an MDM IBM MaaS360 workflow in PKIaaS:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
    - Owners
    - CA Administrators
2. Click **Enrollment Protocols** in the sidebar.



Enrollment Protocols

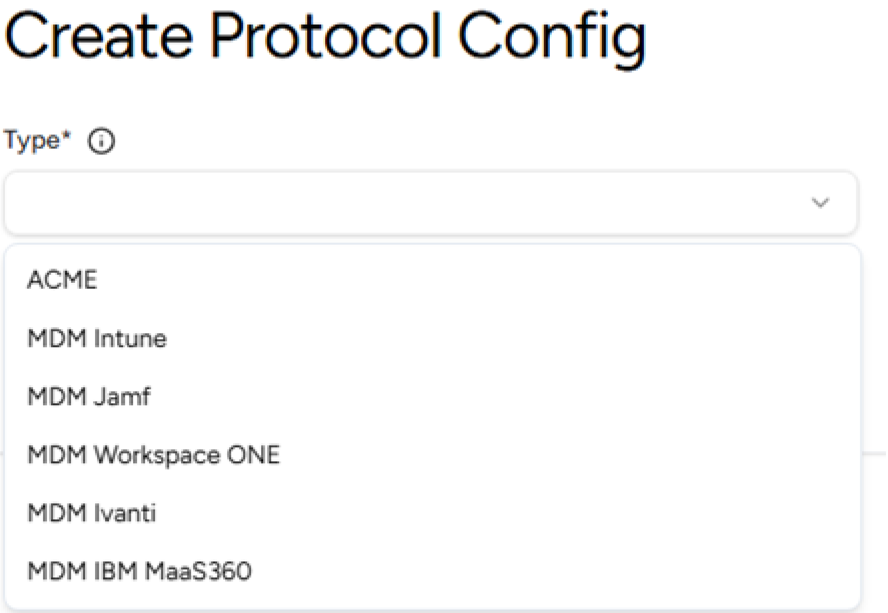
Manage the complete lifecycle of digital certificates from enrollment to revocation across your PKI infrastructure....

jamf-01 mdmws	sub-1	
intune-01 intune	sub-1	intune-digital-signature

3. Click **Create**.

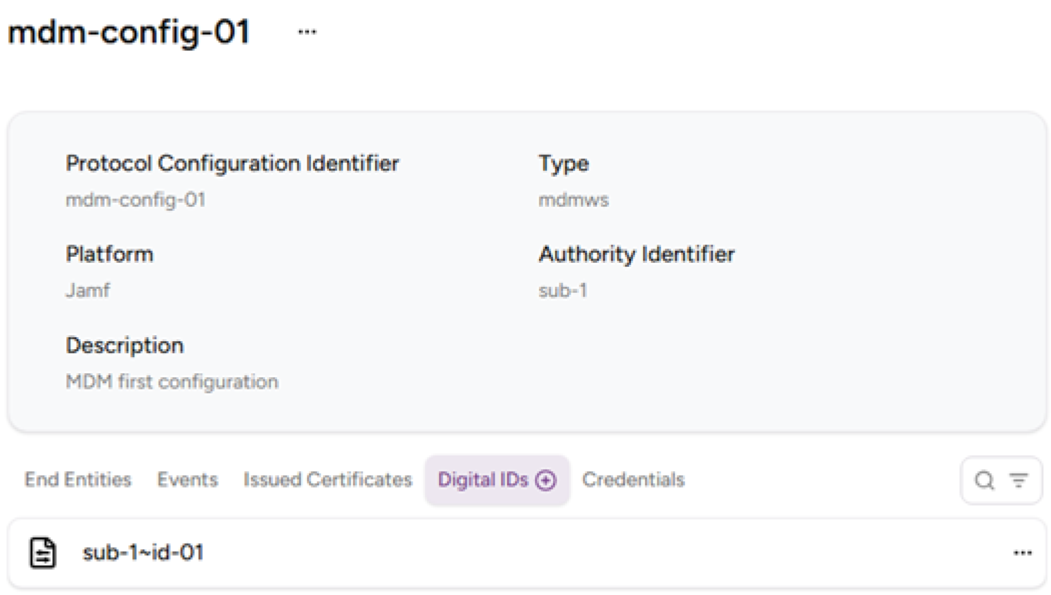
4. Configure the following values in the **Create Protocol Config** dialog.

Field	Value
Type	Select **MDM IBM MaaS360**
Protocol Configuration Identifier	Enter a unique identifier for the new configuration in your PKI. This identifier: Must be 2-18 characters long, can only include lowercase letters, numbers, hyphens ('-'), and underscores ('_').
Description	Enter an optional description of the protocol purpose.
CA Identifier	Select an issuing subordinate authority with profiles of the mdmws group.


Create Protocol Config

5. Click **Create**.

6. In the confirmation window, select the **Digital IDs** tab.



mdm-config-01

Protocol Configuration Identifier
mdm-config-01

Type
mdmws

Platform
Jamf

Authority Identifier
sub-1

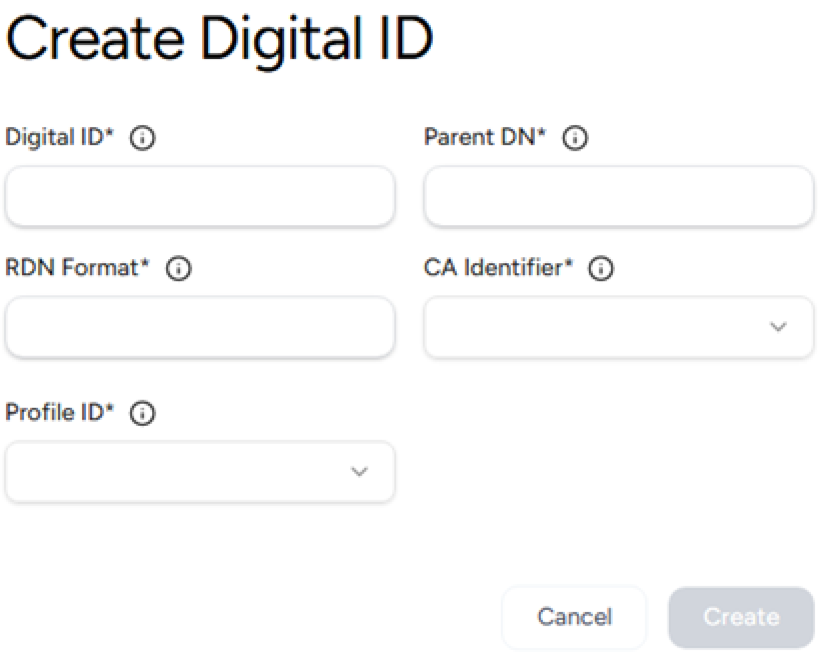
Description
MDM first configuration

sub-1~id-01

7. Click **CREATE**.

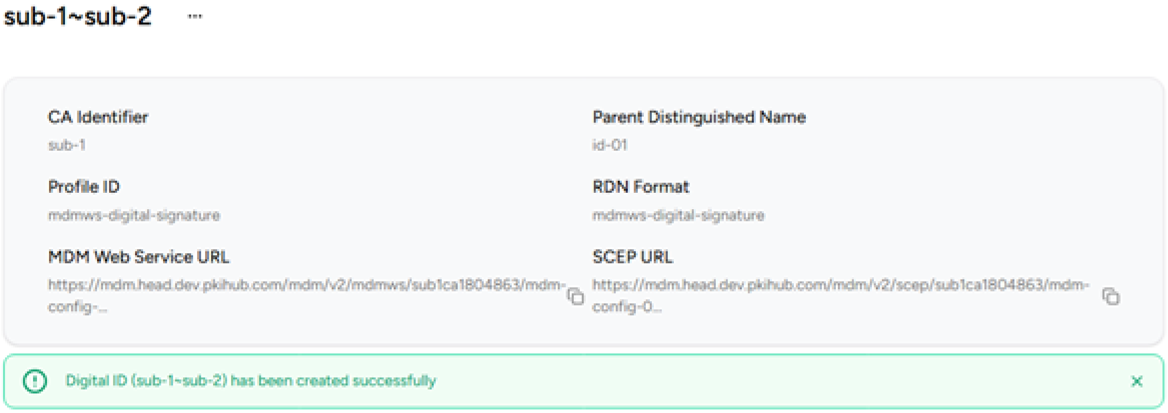
8. Configure the following values in the **Digital identifier** dialog.

Field	Value
Digital ID	Enter a unique name of the new digital identifier.
Parent DN	Enter the parent Distinguished Name (DN) for building the RDN of a certificate. This value is appended to the end of the Subject DN after the **RDN Format** variables have been processed.
RDN Format	Enter the Relative Distinguished Name (RDN) format to build certificate Subject Names.
CA Identifier	Select an issuing subordinate authority with profiles of the mdmws group.
Profile ID	Select the mdmws profile to process the enrollment requests.



9. Click **Create**.

10. Copy the URLs under the **Web Service URL** and **SCEP URL** fields of the confirmation dialog.



sub-1~sub-2 ···

CA Identifier
sub-1

Parent Distinguished Name
id-01

Profile ID
mdmws-digital-signature

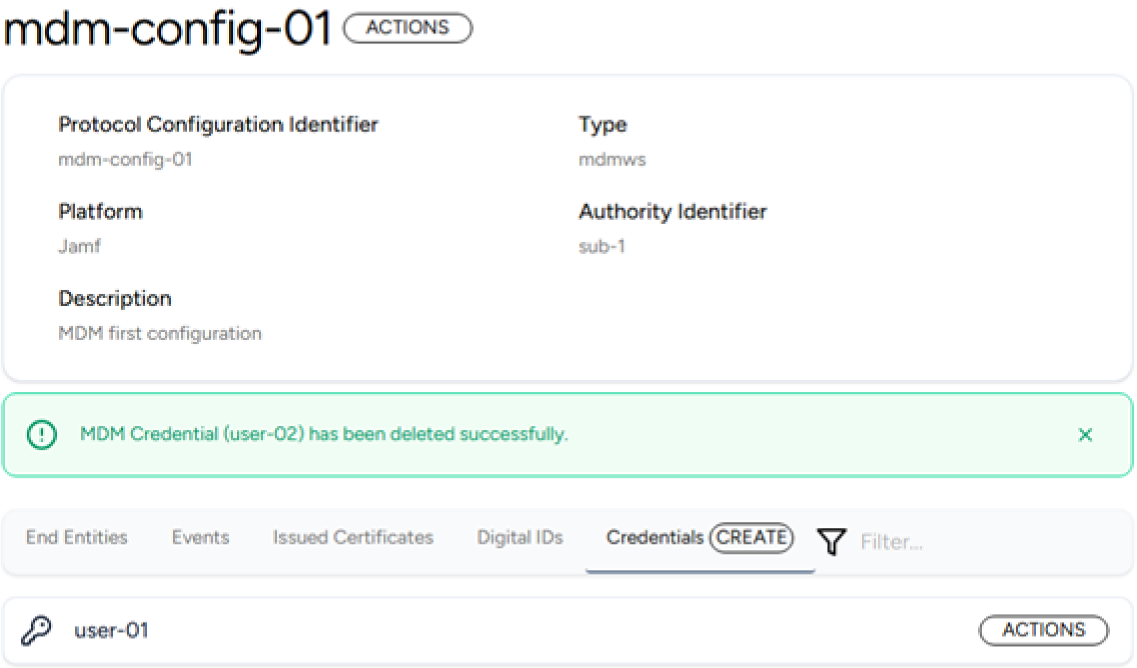
RDN Format
mdmws-digital-signature

MDM Web Service URL
https://mdm.head.dev.pkihub.com/mdm/v2/mdmws/sub1ca1804863/mdm-config-...

SCEP URL
https://mdm.head.dev.pkihub.com/mdm/v2/scep/sub1ca1804863/mdm-config-0...

Digital ID (sub-1~sub-2) has been created successfully

11. Select the **Credentials** tab.



mdm-config-01

Protocol Configuration Identifier
mdm-config-01

Type
mdmws

Platform
Jamf

Authority Identifier
sub-1

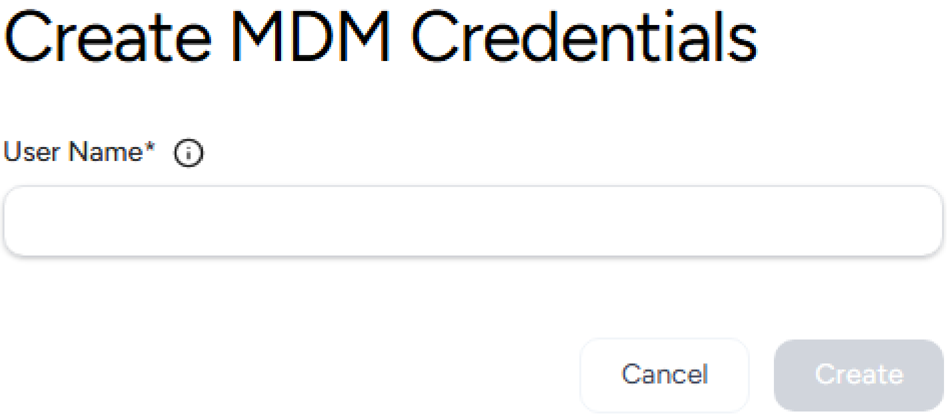
Description
MDM first configuration

MDM Credential (user-02) has been deleted successfully.

user-01

12. Click **CREATE**.

13. In the **Create MDM Credentials** dialog, enter a username that is 2-18 characters long and only includes lowercase letters, numbers, hyphens (â□□-â□□), and underscores (â□□_â□□).

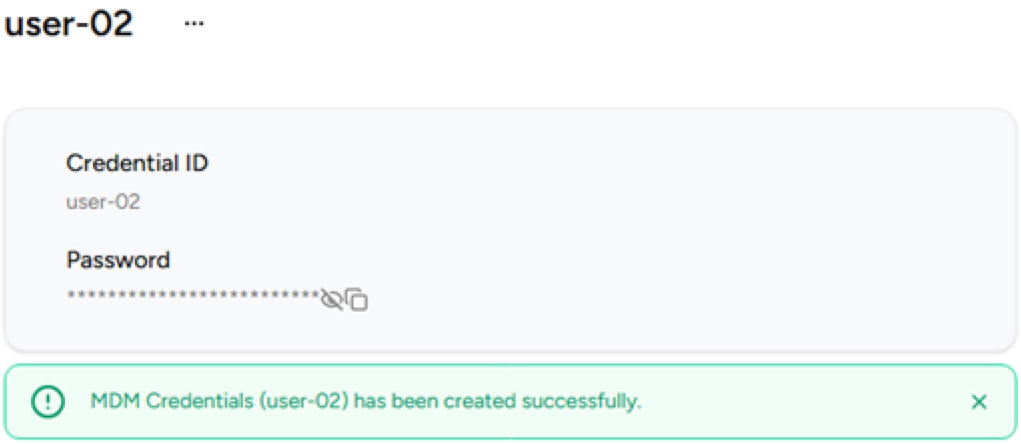


Create MDM Credentials

User Name*

14. Click **Create**.

15. Copy the **Password** value displayed in the confirmation dialog.



user-02

Credential ID
user-02

Password
****

MDM Credentials (user-02) has been created successfully.

⚠ As stated in the confirmation dialog before leaving this page, Entrust PKIaaS will not display the credential password again.

Configuring MDM automation in IBM Cloud

See below for configuring IBM Cloud as an MDM provider.

- Requirements for MDM automation in IBM Cloud
- Configuring MDM automation with Cloud Extender

Requirements for MDM automation in IBM Cloud

See below the requirements for configuring IBM Cloud as an MDM provider.

- Certificate Authority
- Credentials
- IBM MaaS360 Cloud Extender

Certificate Authority

Follow the steps in Managing certificate authorities to:

1. Create a CA hierarchy that includes an issuing subordinate CA.
2. Enable at least one P12 mdmws profile in the issuing subordinate CA.

Credentials

Follow the steps described in Configuring MDM IBM MaaS360 in PKIaaS to create a Digital ID and a credential.

⚠ Make sure the **CA Identifier** value matches the identifier of the issuing subordinate CA.

IBM MaaS360 Cloud Extender

Download and install IBM MaaS360 Cloud Extender as explained in:

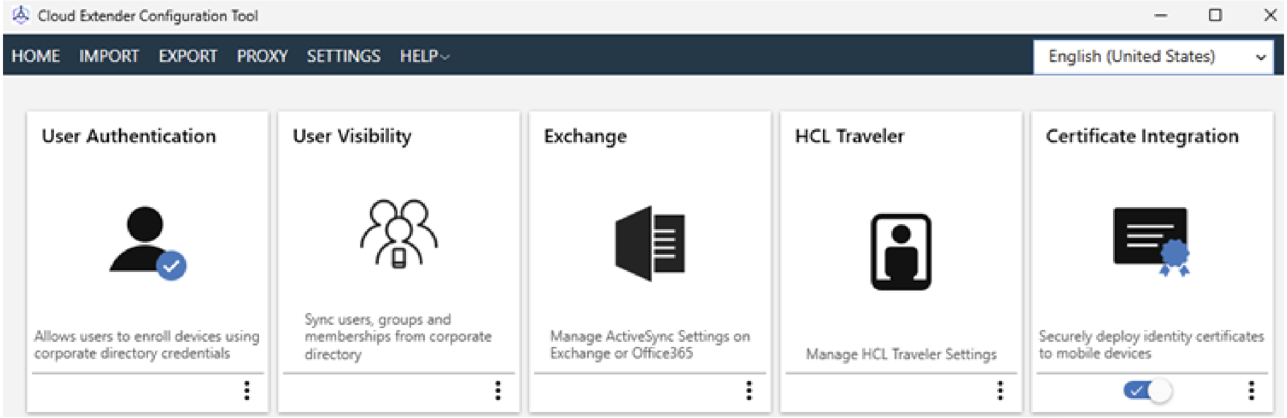
https://www.ibm.com/docs/en/maas360?topic=guide-configuring-cloud-extender

Configuring MDM automation with Cloud Extender

After downloading and installing IBM MaaS360 Cloud Extender, run the Cloud Extender Configuration Tool to configure MDM integration.

To configure IBM Cloud as an MDM provider:

1. In the Cloud Extender Configuration Tool, click **Certificate Integration**.



Cloud Extender Configuration Tool
HOME IMPORT EXPORT PROXY SETTINGS HELP
English (United States)

User Authentication

Allows users to enroll devices using corporate directory credentials

User Visibility

Sync users, groups and memberships from corporate directory

Exchange

Manage ActiveSync Settings on Exchange or Office365

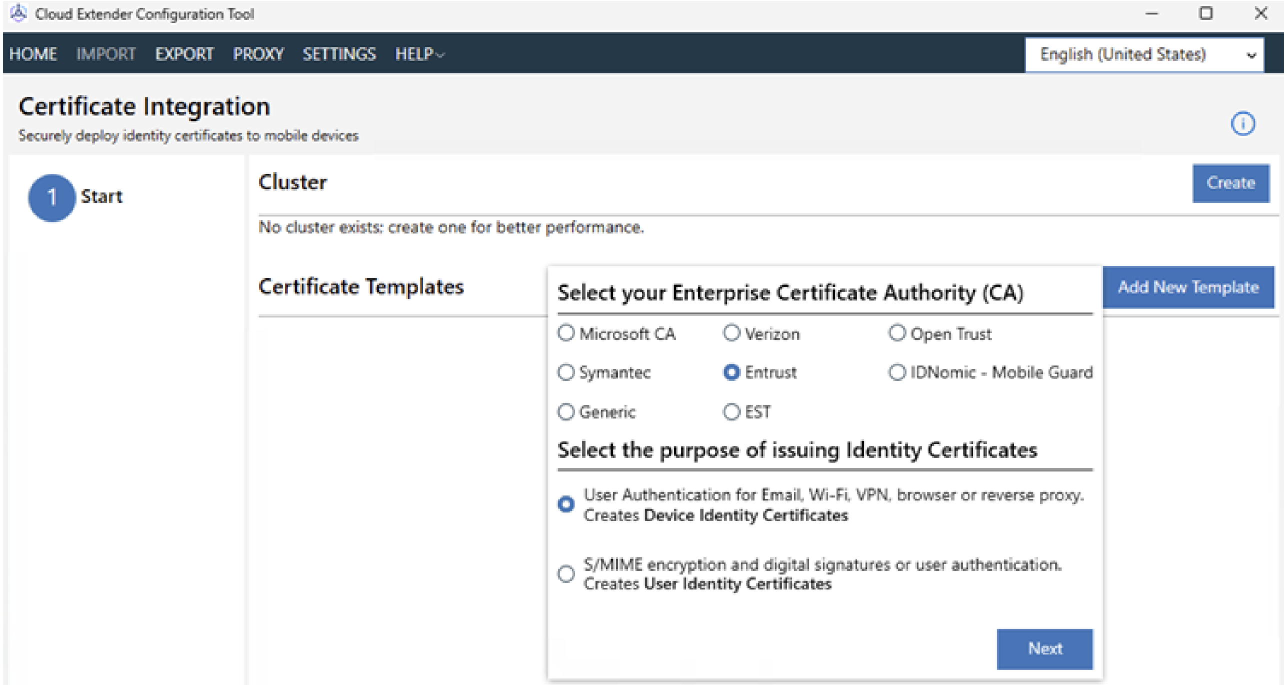
HCL Traveler

Manage HCL Traveler Settings

Certificate Integration

Securely deploy identity certificates to mobile devices

2. Click **Add New Template** to deploy the certificate template options.



Cloud Extender Configuration Tool
HOME IMPORT EXPORT PROXY SETTINGS HELP
English (United States)
1 Start
Create
Add New Template
Next

Certificate Integration

Securely deploy identity certificates to mobile devices

Cluster

No cluster exists: create one for better performance.

Certificate Templates

Select your Enterprise Certificate Authority (CA)

○ Microsoft CA ○ Verizon ○ Open Trust

○ Symantec ● Entrust ○ IDNomic - Mobile Guard

○ Generic ○ EST

Select the purpose of issuing Identity Certificates

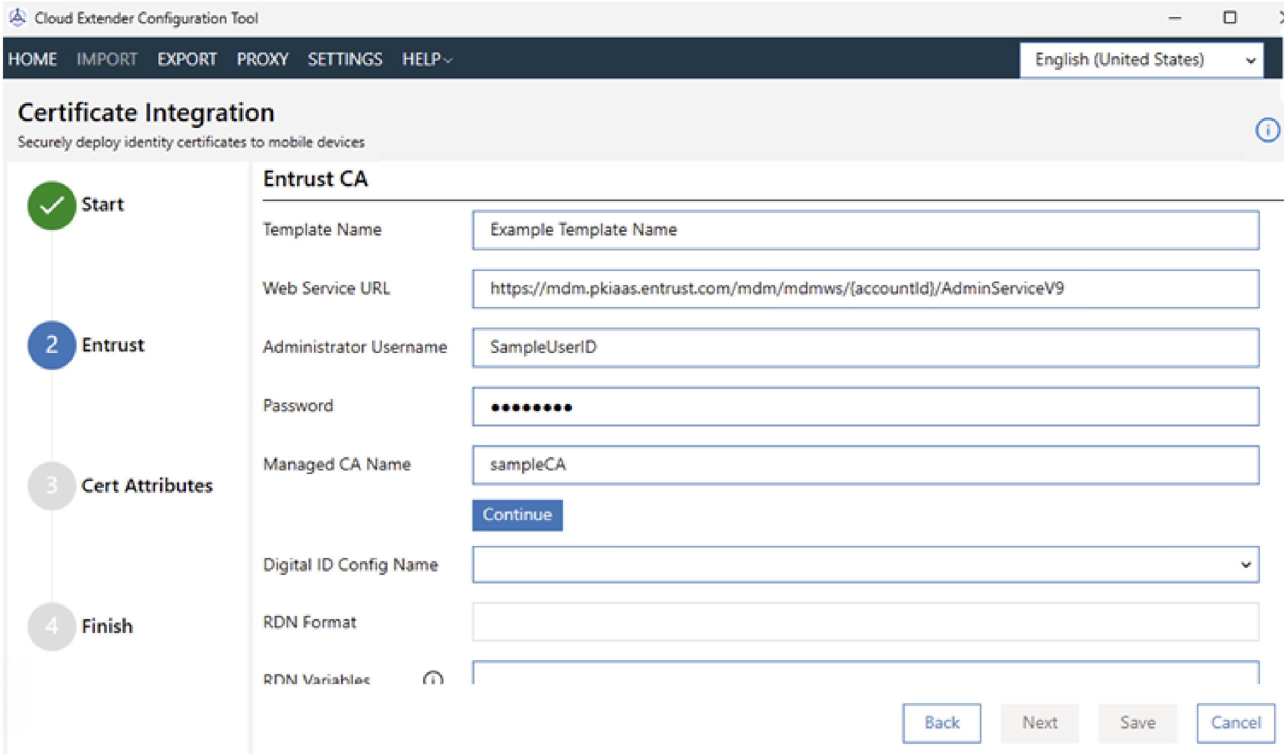
● User Authentication for Email, Wi-Fi, VPN, browser or reverse proxy. Creates **Device Identity Certificates**

○ S/MIME encryption and digital signatures or user authentication. Creates **User Identity Certificates**

3. Under **Select your Enterprise Certificate Authority (CA)**, select "Entrust".

4. Under **Select the purpose of the issuing Identity Certificates**, select "Creates **Device Identity Certificate**".

5. Click **Next** to configure the Entrust CA settings.



Certificate Integration

Securely deploy identity certificates to mobile devices

Entrust CA

Template Name	Example Template Name
Web Service URL	https://mdm.pkiaas.entrust.com/mdm/mdmws/{accountId}/AdminServiceV9
Administrator Username	SampleUserID
Password	••••••••
Managed CA Name	sampleCA
Digital ID Config Name	
RDN Format	
RDN Variables	

6. Fill in the following fields.

Field	Value
Template	Enter a user-friendly name for this configuration
Web Service URL	Enter the **Web Service URL** value obtained in section Configuring MDM IBM MaaS360 in PKIaaS. Make sure this URL ends with "AdminServiceV9".
Administrator Username	Enter the same **User Name** that was used for creating a credential in section Configuring MDM IBM MaaS360 in PKIaaS.
Password	Enter the password obtained after generating a credential in section Configuring MDM IBM MaaS360 in PKIaaS.
Managed CA Name	Enter the same credential **CA Identifier** selected in section Configuring MDM IBM MaaS360 in PKIaaS.

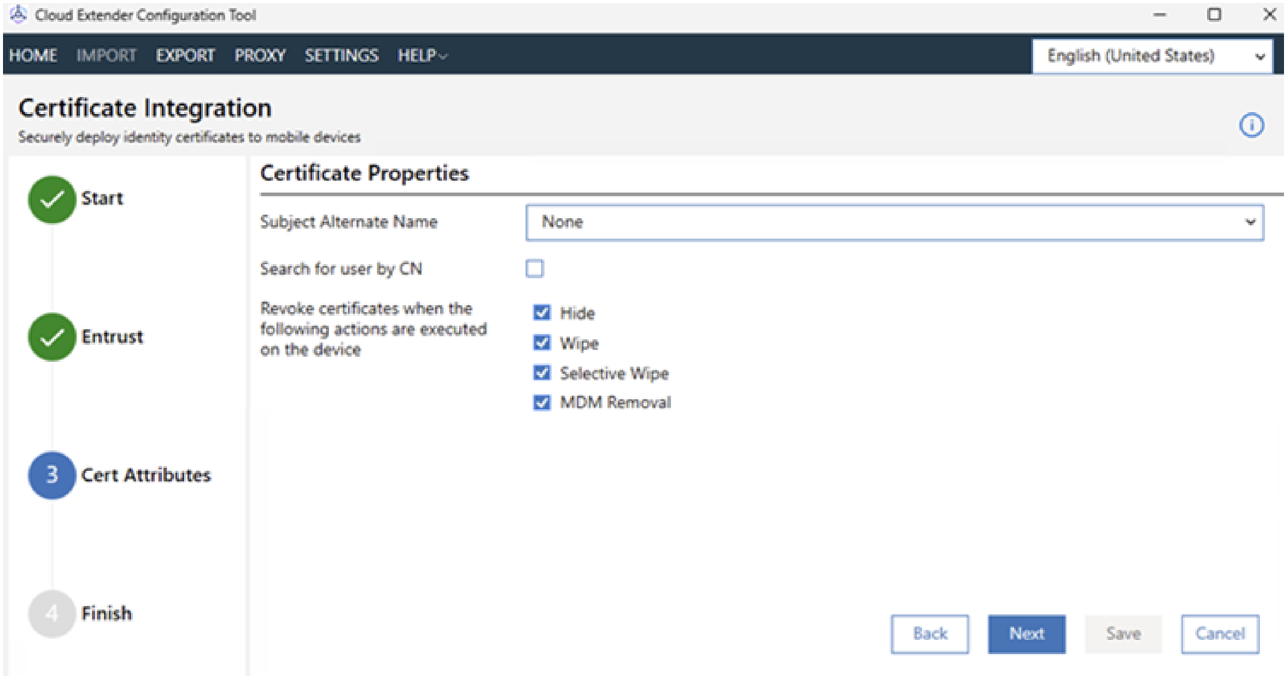
7. Click **Continue** to populate the **Digital ID** list of Digital ID configurations.

8. Select a Digital ID configured to use a PKIaaS CA with an mdmws certificate profile that supports P12.

i Selecting a Digital ID will automatically populate the **RDN Format** and the **RDN Variables** fields.

9. In the **RDN Format** and the **RDN Variables** fields, replace every occurrence of %REPLACE% with the Subject Name variables described at: https://www.ibm.com/docs/en/maas360?topic=integration-configuring-certificate-template-entrust

10. Click **Next** to configure the certificate properties.



Certificate Integration

Securely deploy identity certificates to mobile devices

Certificate Properties

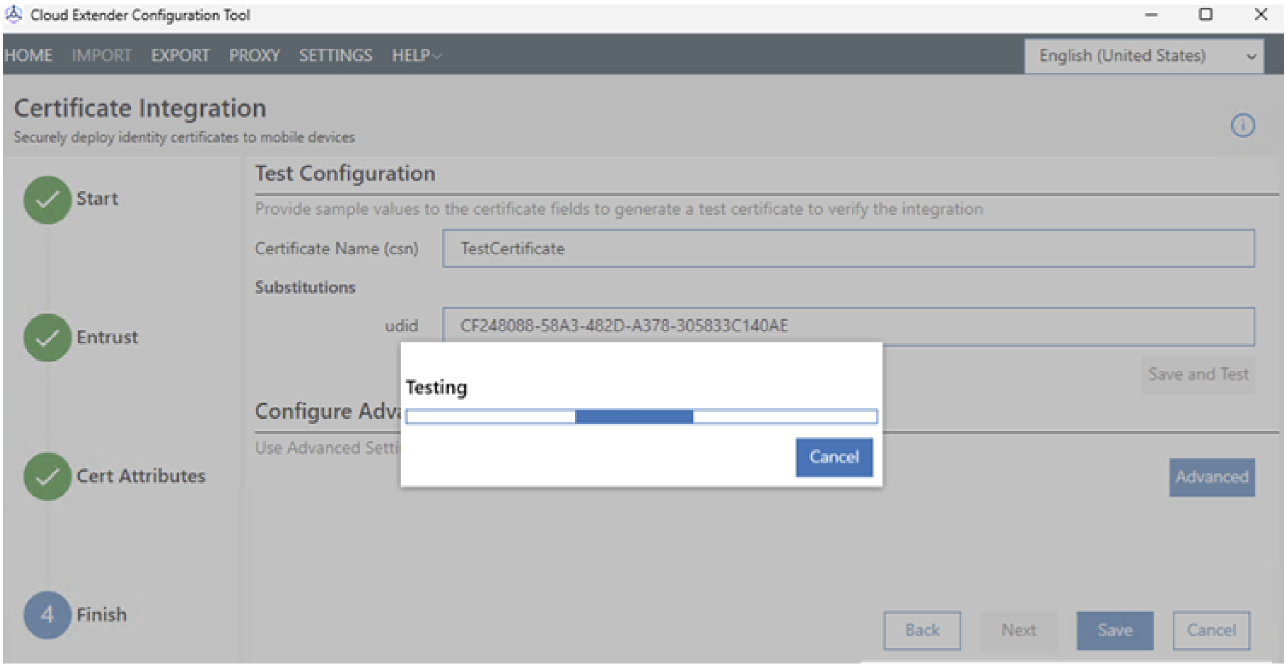
Subject Alternate Name: None

Search for user by CN ☐

Revoke certificates when the following actions are executed on the device: ☑ Hide ☑ Wipe ☑ Selective Wipe ☑ MDM Removal

11. Enable all four revocation-related checkboxes to automatically revoke certificates (recommended).

12. Click **Next** to configure a test certificate request.



Certificate Integration

Securely deploy identity certificates to mobile devices

Test Configuration

Provide sample values to the certificate fields to generate a test certificate to verify the integration

Certificate Name (csn): TestCertificate

Substitutions

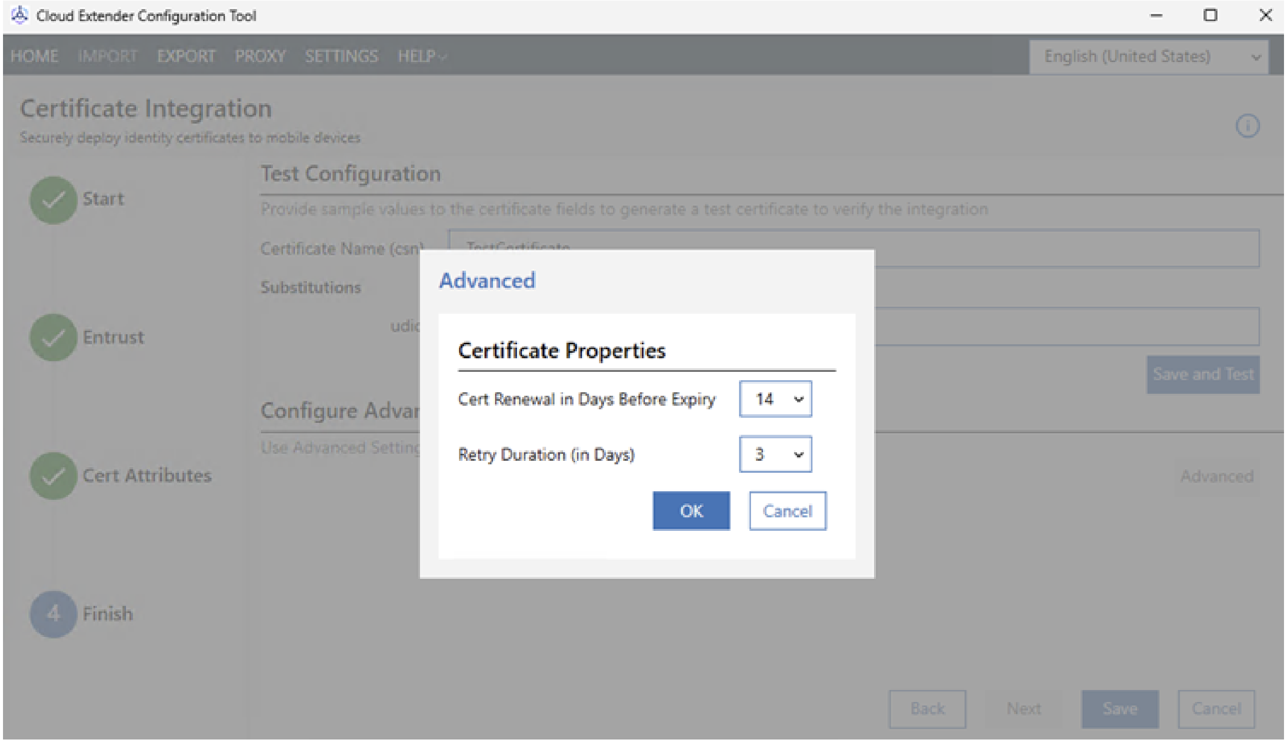
udid: CF248088-58A3-482D-A378-305833C140AE

13. Configure the following values under **Test Configuration**.

Field	Value
Certificate Name (csn)	Enter a name for the new certificate.
Substitutions	Enter a value for each variable configured in the **RDN Format** and **RDN Variables** fields.

14. Click **Save and Test** and wait while the test certificate is issued.

15. Click **Advanced** and configure the renewal settings.



Cert Renewal in Days Before Expiry: 14

Retry Duration (in Days): 3

16. Click **OK** to close the **Advanced** dialog.

17. Click **Save**.

Automating WSTEP enrollment

Configure PKIaaS to process Microsoft WSTEP enrollment requests with PKIaaS Certification Authorities.

- WSTEP integration requirements
- Planning your WSTEP deployment
- Preparing the Active Directory forest for WSTEP
- Downloading an agent
- Installing an agent
- Configuring WSTEP automation in PKIaaS
- Enabling WSTEP for users and devices
- Managing certificate templates
- Managing on-premise Agents
- Troubleshooting WSTEP enrollment issues

WSTEP integration requirements

See below the requirements for automating WSTEP enrollment with a PKIaaS gateway.

- Enrollment protocol requirements
- TLS Cipher requirements
- Agent requirements
- Windows requirements

Enrollment protocol requirements

Entrust PKIaaS integrates into Microsoft Active Directory environments and automates enrollment using the following Microsoft protocols.

- MS-XCEP
- MS-WSTEP

MS-XCEP

MS-XCEP (â□□X.509 Certificate Enrollment Policy Protocol) defines the interactions between a requesting client and a responding server to exchange a certificate enrollment policy.

ℹ A certificate enrollment policy is a collection of certificate templates and certificate issuers available to the requestor for X.509 certificate enrollment.

See https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-xcep for details on this protocol.

MS-WSTEP

MS-WSTEP (WS-Trust X.509v3 Token Enrollment Extensions) defines the message formats and server behavior to manually or automatically enroll X.509 certificates for users and computers.

See https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-wstep for details on this protocol.

TLS Cipher requirements

Enrollment URLs support the following TLS Ciphers.

- `ECDHE-RSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES256-GCM-SHA384`

Agent requirements

Automating Windows Auto Enrollment (WSTEP) requires installing an Entrust PKIaaS On-premises agent on your Local Area Network (LAN). See below for the requirements of this machine.

- Agent network requirements
- Agent Azure requirements
- Agent VMware requirements

⚠ You may use the agent for integrating the on-premises Windows infrastructure of a User with your cloud-based PKIaaS instance. You may only use agent in connection with your validly licensed use of Entrust PKIaaS. You are expected to keep reasonable records relating to at least the number of copies of the software that you have made, used and distributed, and the environments where they have been deployed.

Agent network requirements

The agent has the following network requirements.

- Agent connection settings
- Agent outbound access to Active Directory
- Agent outbound access to ssl.com
- Agent outbound access to the Oracle Yum server
- Agent outbound access to the PKIaaS package repository
- Agent outbound access to PKIHub

Agent connection settings

The connection of the agent requires a DHCP server with a configured DNS.

Agent outbound access to Active Directory

Grant the agent outbound access to:

- The Active Directory DNS servers (to query SRV DNS records for the FQDN of Active Directory Domain controllers).
- The Active Directory LDAP or LDAPS service (to look up information on Microsoft certificate templates, Active Directory users, and Active Directory machines).

See below for the required outbound ports.

Target port	Protocol	Application	Target service
53	TCP/UDP	DNS	Active Directory DNS
389	TCP	LDAP	Active Directory secured with StartTLS
636	TCP	LDAPS	Active Directory

⚠ If an attempted LDAPS connection fails, the agent switches to LDAP port 389 and attempts to use StartTLS (because plaintext LDAP is not supported).

Agent outbound access to ssl.com

Grant the agent the outbound access to the ssl.com services.

URI	Target port	Protocol	Application
`ocsp.ssl.com`	443	TCP	HTTPS
`crls.ssl.com`	443	TCP	HTTPS

Agent outbound access to the Oracle Yum server

Grant the agent the following outbound access to the Oracle Yum server.

URI	Target port	Protocol	Application
`yum.oracle.com`	443	TCP	HTTPS

Agent outbound access to the PKIaaS package repository

Grant the agent access to the package repository.

Region	URI	Target port	Protocol	Application
EU	`pkihub-eu-prod-rpm.s3.eu-central-1.amazonaws.com`	443	TCP	HTTPS
US	`pkihub-prod-rpm.s3.us-east-1.amazonaws.com`	443	TCP	HTTPS

Agent outbound access to PKIHub

Grant the agent access to the PKIHub services.

Region	URI	Target port	Protocol	Application
EU	`idp.eu.pkihub.entrust.com`	443	TCP	HTTPS
	`satellite.eu.pkihub.entrust.com`	443	TCP	HTTPS
	`wstep.eu.pkihub.entrust.com`	443	TCP	HTTPS
US	`idp.pkihub.entrust.com`	443	TCP	HTTPS
	`satellite.pkihub.entrust.com`	443	TCP	HTTPS
	`wstep.pkihub.entrust.com`	443	TCP	HTTPS

Agent Azure requirements

To run the agent on Azure, use a dedicated machine with at least the following resources.

VM size	vCPUs	RAM (GiB)	Data disk	Max IOPS	Local storage (GiB)
â□□B2s	2	4	4	1280â□□	8 (SCSI)â□□

Agent VMware requirements

VMware virtualization platforms must meet the following requirements to run the agent.

- VMware version for running the agent
- VMware machine requirements for running the agent

VMware version for running the agent

You need an environment that supports Virtual Hardware version 14. The following VMware products are compatible with this version.

- ESXi 6.7
- Fusion 10.x
- Workstation Pro 14.x

- Workstation Player 14.x

VMware machine requirements for running the agent

The OVA file of the agent requires the following resources:

- 2 cores
- 8 GB of RAM
- 10 GB of disk space

Make sure the VMware environment running the agent provides these resources.

Windows requirements

The Windows environment of the enrolled devices must meet the following requirements.

- Windows user requirements
- Windows network requirements
- Active Directory requirements

Windows user requirements

For Installing the default set of certificate templates, you will need to log into the root domain of the forest as a user belonging to the following groups.

- Domain Admins
- Enterprise Admins

Windows network requirements

See below for the network requirements for all Windows devices in an Active Directory forest.

- Device outbound access to the Entrust WSTEP service
- Device outbound access to the Entrust certificate validation services

ℹ Connection to the Windows domain is not a requirement for certificate enrollment. After fulfilling the requirements below, domain-joined devices can enroll for certificates even when not connected to the same network as the Windows domain.

Device outbound access to the Entrust WSTEP service

Grant any device access to Entrust PKIaaS.

Region	URI	Target port	Protocol	Application
EU	`wstep.eu.PKIaaS.entrust.com`	443	TCP	HTTPS
US	`wstep.PKIaaS.entrust.com`	443	TCP	HTTPS

Device outbound access to the Entrust certificate validation services

Grant any device access to the following Entrust certificate validation services

Service	Target port	Protocol	Application
Entrust PKIaaS Certificate Revocation Lists	80	TCP	HTTP
Entrust PKIaaS OCSP service	80	TCP	HTTP

Active Directory requirements

Each Windows Active Directory (AD) forest must meet the following requirements.

- LDAPS TLS certificate requirements for AD domain controllers
- SRV record requirements for AD LDAP services

LDAPS TLS certificate requirements for AD domain controllers

In each Active Directory domain controller, the TLS certificate for LDAPS must meet the requirements described in:

https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/enable-ldap-over-ssl-3rd-certification-authority#requirements-for-an-ldaps-certificate

Specifically, this certificate:

- Must be stored in the NT Directory Services (NTDS) personal certificate store.
- Must contain the FQDN (Fully Qualified Domain Name) of the Domain Controller as a DNS SAN (Subject Alternative Name).
- Must use the RSA algorithm.
- Must include Server Authentication (`1.3.6.1.5.5.7.3.1`) as Enhanced Key Usage.

SRV record requirements for AD LDAP services

Service Location (SRV) resource records for the LDAP Service must be valid for all domains in the forest. Verify this requirement as explained at:

https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/verify-srv-dns-records-have-been-created

---

ℹ SRV records do not require extra configuration steps as Active Directory automatically creates and updates them.

Planning your WSTEP deployment

WSTEP integration requires installing an agent virtual machine on-premises in the customer's LAN. Once installed, this virtual machine:

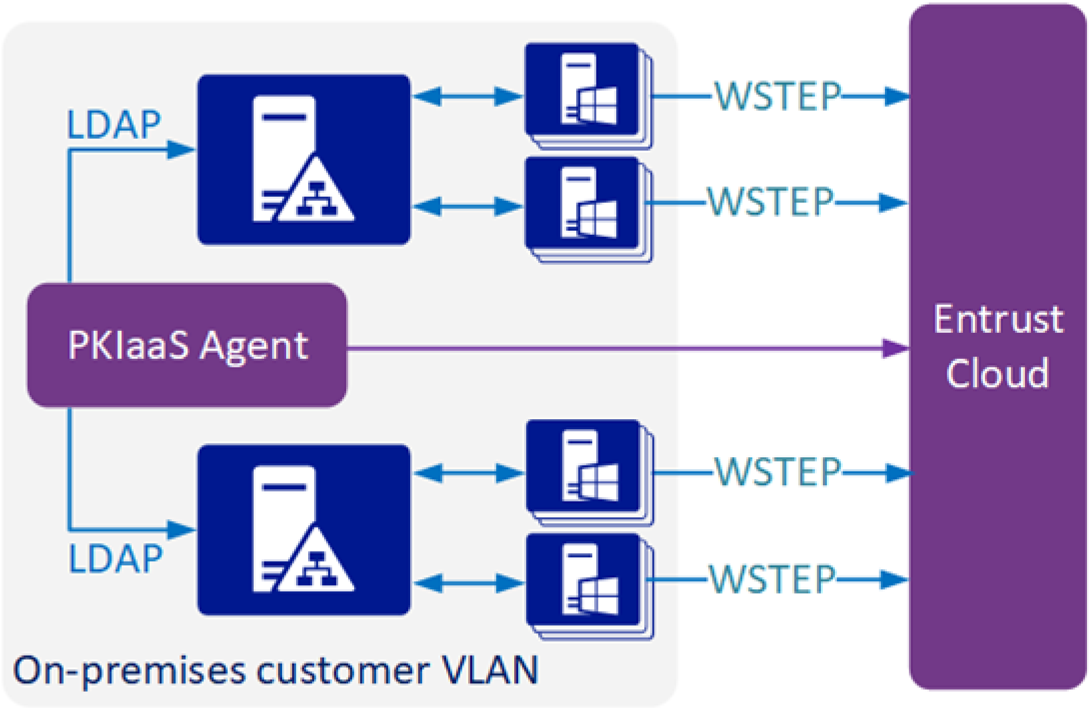
- Performs LDAPS queries against the Domain Controllers in an Active Directory forest.
- Establishes an outbound connection with the Entrust Cloud.

The Windows devices send WSTEP requests directly to the Entrust PKIaaS service hosted in the Entrust cloud. See below for the main integration scenarios.

- Deploying a single agent for multiple Active Directory forests
- Deploying multiple agents for Active Directory forests in different networks

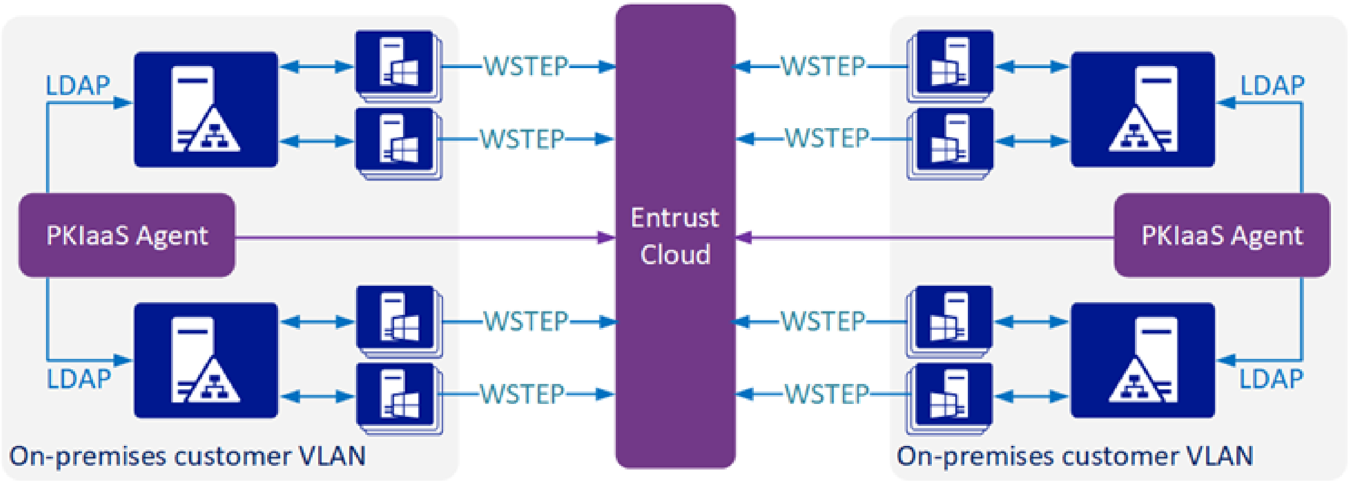
Deploying a single agent for multiple Active Directory forests

A single agent can handle any number of Active Directory forests, provided it can connect with each one.



Deploying multiple agents for Active Directory forests in different networks

As illustrated by the diagram below, multiple agents are required when a single agent cannot communicate with all forests.



In any case, configuring multiple Active Directory forests:

- Requires preparing the domain controllers of each Windows forest as explained in this document.
- Requires adding the root domain of each Windows Forest to the Entrust PKIaaS portal.

- Does not require two-way transitive trusts.

Preparing the Active Directory forest for WSTEP

To prepare for WSTEP enrollment, perform the following operations in the domain controller of the Windows Active Directory forest's root domain.

- Creating a WSTEP service account
- Installing the default set of certificate templates
- Downloading the certificate chain
- Setting up LDAPS on domain controllers

Creating a WSTEP service account

Create a WSTEP service account for the WSTEP agent and WSTEP server to authenticate all incoming requests from WSTEP clients.

ℹ Each root domain in the Active Directory forest requires a separate WSTEP service account, as each Active Directory forest must be configured separately.

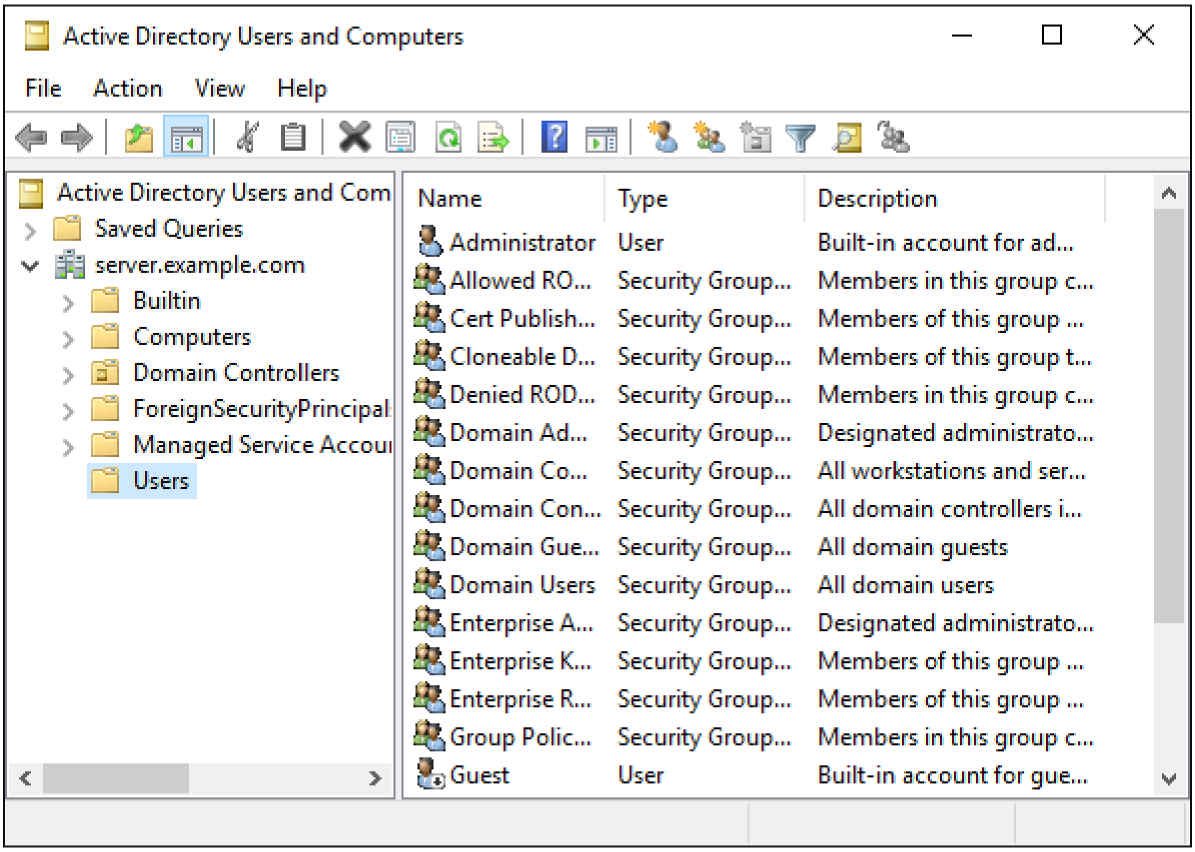
To create a WSTEP service account:

1. Log in to a domain controller of the Active Directory forest's root domain as a user who is a member of both the Domain Admins and Enterprise Admins groups.

   ⚠ The service account created for the agent must have read permissions on certificate templates, user objects, and computer objects in LDAP.

   ---

2. Select **Start** > **Windows Administrative Tools** > **Active Directory Users and Computers** to open the **Active Directory Users and Computers** dialog box.



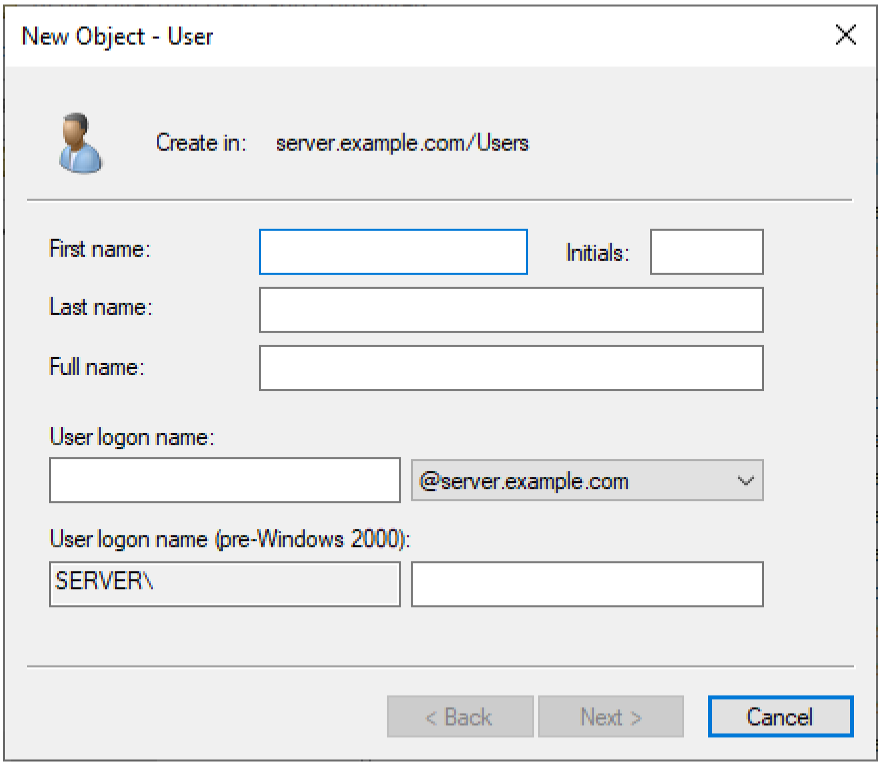
Active Directory Users and Computers

- Active Directory Users and Com
  - Saved Queries
  - server.example.com
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal
    - Managed Service Accou
    - Users

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...

3. Right-click the folder where you want to create the new account.

4. Select **New > User** to open the **New Object â□□ User** dialog box.



New Object - User

Create in: server.example.com/Users

First name:

Initials:

Last name:

Full name:

User logon name:

@server.example.com

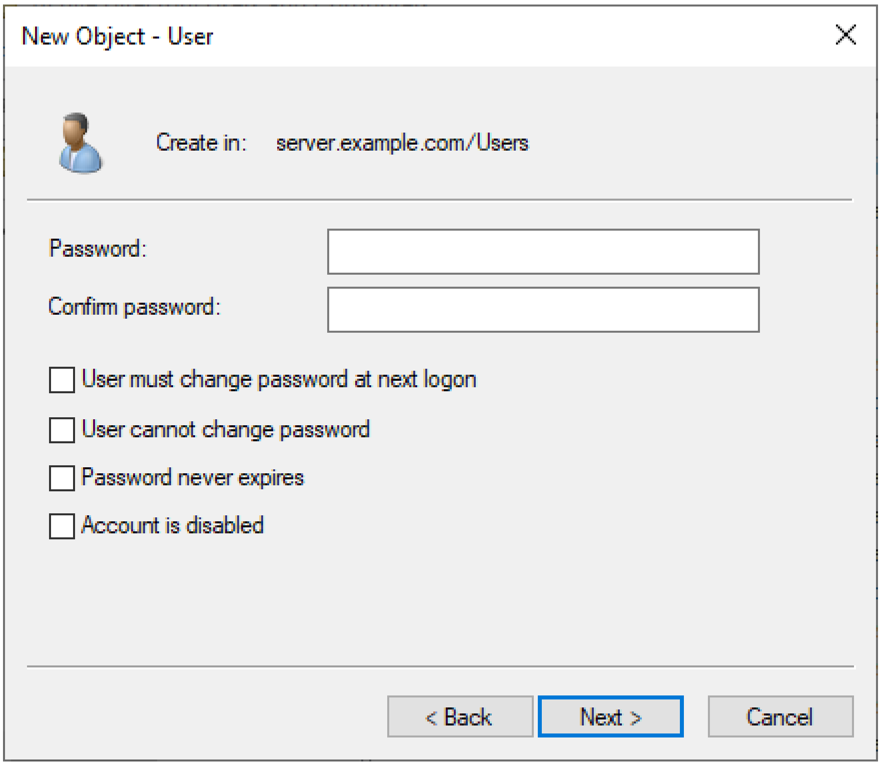
User logon name (pre-Windows 2000):

SERVER\

5. Enter the **First name**, **Last name**, and **Full name** for the new user account.

6. Enter a Windows **User logon name** for the user account. Optionally, enter a **User logon name (pre-Windows 2000)** for pre-Windows 2000 computers.

7. Click **Next** to display the password options.



Create in: server.example.com/Users

Password:

Confirm password:

□ User must change password at next logon

□ User cannot change password

□ Password never expires

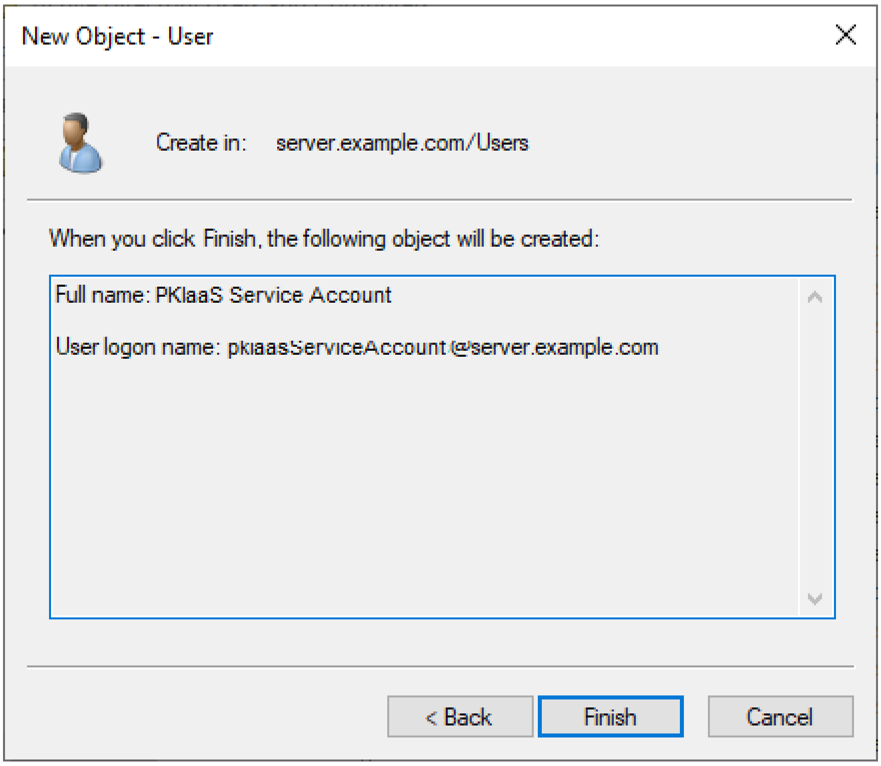
□ Account is disabled

8. Enter a **Password** for the user account.

9. Enter the password again in the **Confirm password** field.

10. Deselect **User must change password at next logon**.

11. Click **Next** to display the confirmation dialog.



Create in: server.example.com/Users

When you click Finish, the following object will be created:

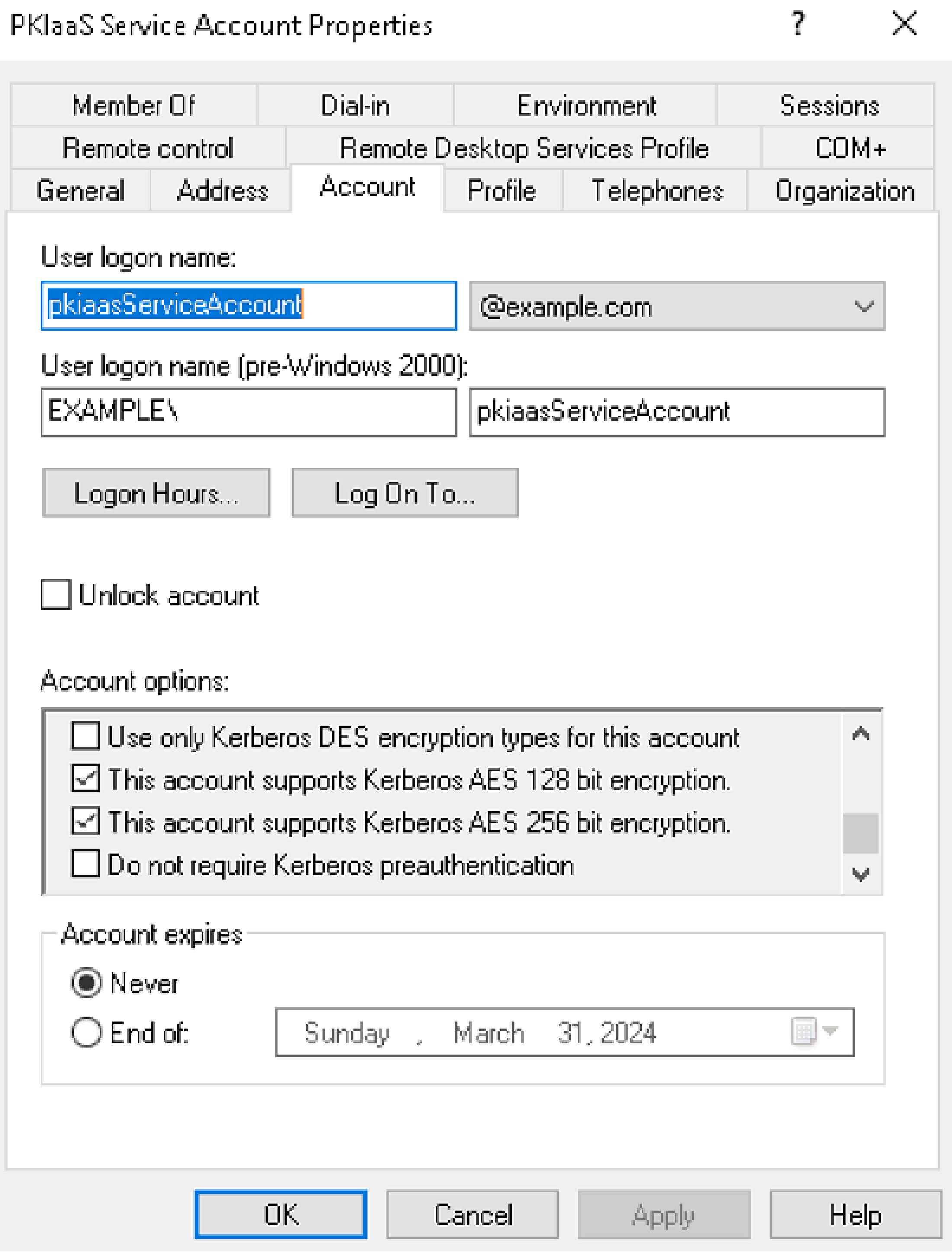
Full name: PKIaaS Service Account

User logon name: pkiaasServiceAccount@server.example.com

12. Record the user logon name of the account. You will use this logon name later to add a Service Principal Name (SPN) mapping for Kerberos.

13. Click **Finish**.

14. Double-click the account you just created to display the properties dialog box.



User logon name: pkiaasServiceAccount @example.com

User logon name (pre-Windows 2000): EXAMPLE\ pkiaasServiceAccount

□ Unlock account

Account options:

□ Use only Kerberos DES encryption types for this account
☑ This account supports Kerberos AES 128 bit encryption.
☑ This account supports Kerberos AES 256 bit encryption.
□ Do not require Kerberos preauthentication

Account expires
● Never
○ End of: Sunday , March 31, 2024

15. In the Account tab, check the following boxes under **Account options**.

   - **This account supports Kerberos AES 128 bit encryption**
   - **This account supports Kerberos AES 256 bit encryption**

16. Click **OK**.

Installing the default set of certificate templates

If not installed, install the default set of Microsoft certificate templates, as described in the following sections.

- Enabling the Certificate Templates snap-in

- Installing the default set of Microsoft Certificate Templates using the snap-in

---

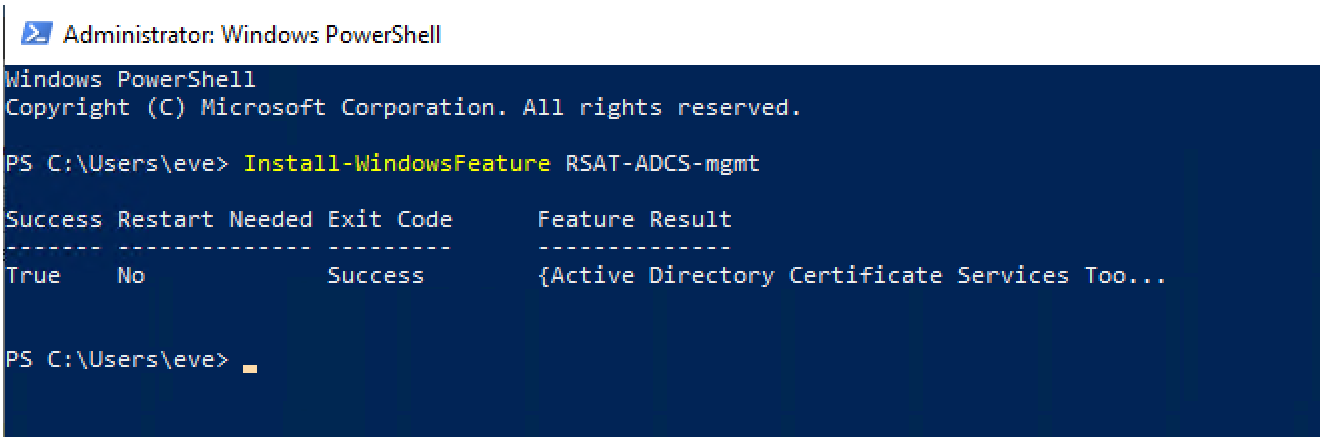
ℹ This section is mainly for new Microsoft Active Directory forest deployments, as they do not include a set of Microsoft certificate templates.

Enabling the Certificate Templates snap-in

You can enable the Certificate Templates snap-in by simply running the following PowerShell command.

```
Install-WindowsFeature RSAT-ADCS-mgmt
```

For example:

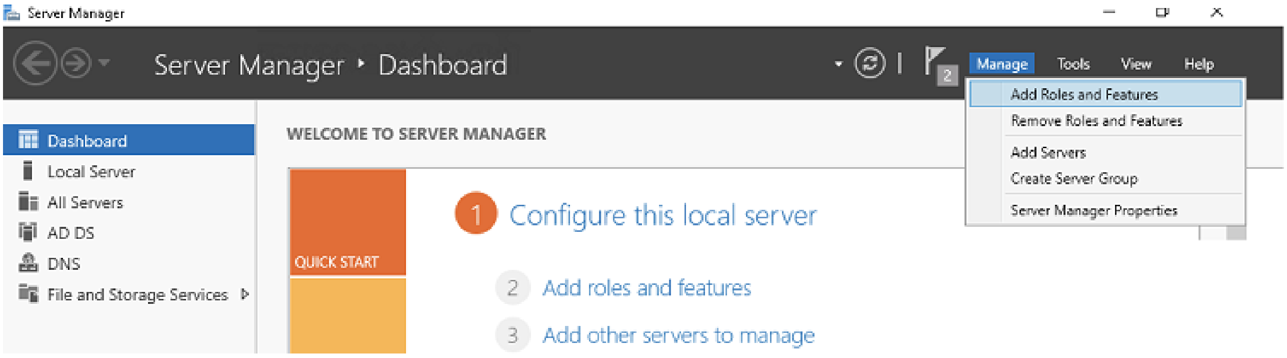


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\eve> Install-WindowsFeature RSAT-ADCS-mgmt

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Certificate Services Too...


PS C:\Users\eve> _
```

Alternatively, you can enable the Certificate Templates snap-in using the Windows Server Manager wizard.

To enable the Certificate Templates snap-in with the Windows Server Manager:

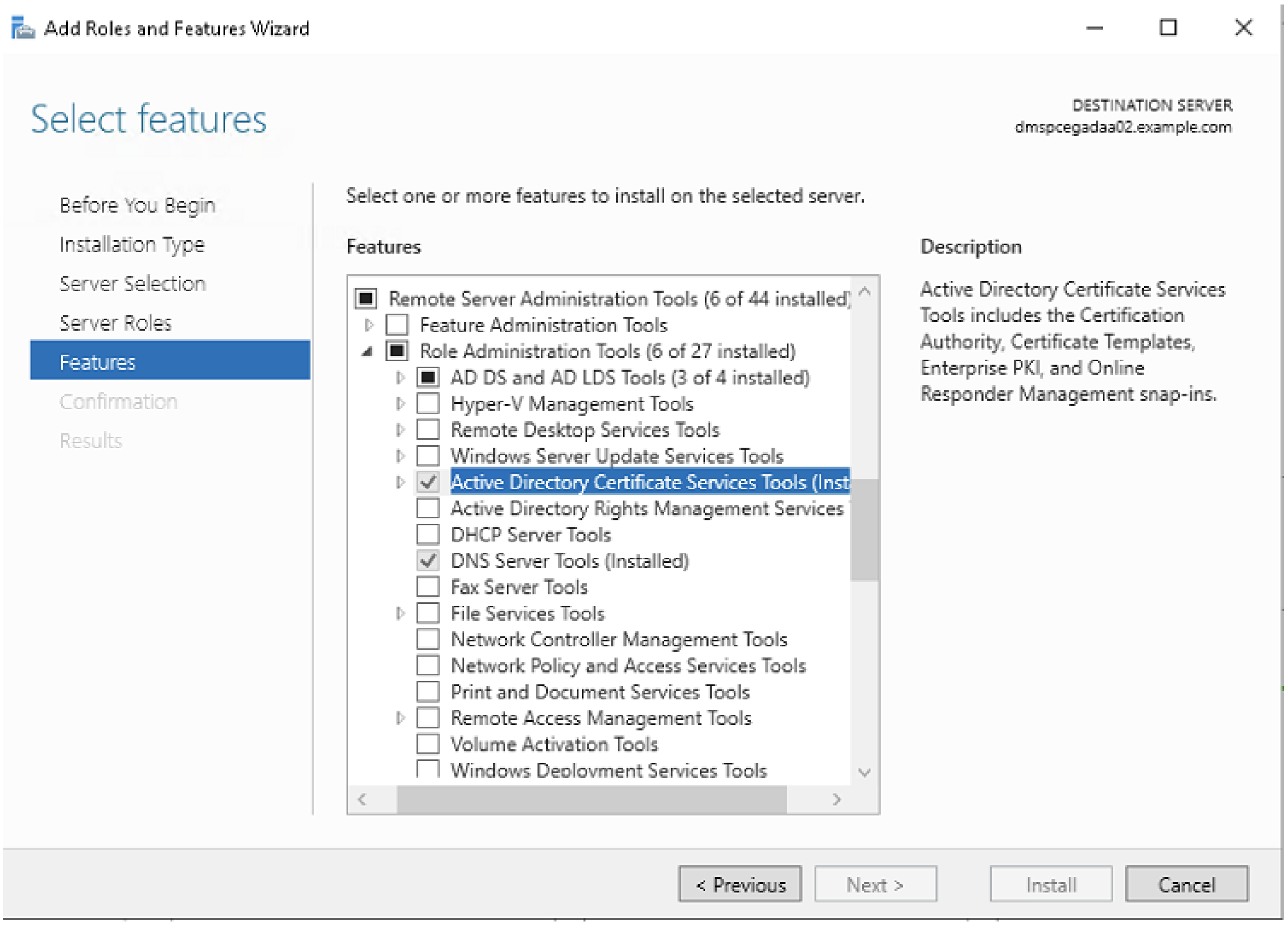
1. Open the Windows Server Manager â for example, by pressing the Windows key on the keyboard and typing "Server Manager" in the search box.



Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
1 Configure this local server
2 Add roles and features
3 Add other servers to manage

2. On the top-right of the window, click **Manage > Add Roles and Features**.

3. In the **Select Features** dialog, click **Next** until the **Features** section is displayed.



Select one or more features to install on the selected server.

Features

- ■ Remote Server Administration Tools (6 of 44 installed)
  - □ Feature Administration Tools
  - ■ Role Administration Tools (6 of 27 installed)
    - ■ AD DS and AD LDS Tools (3 of 4 installed)
    - □ Hyper-V Management Tools
    - □ Remote Desktop Services Tools
    - □ Windows Server Update Services Tools
    - ☑ Active Directory Certificate Services Tools (Inst
    - □ Active Directory Rights Management Services
    - □ DHCP Server Tools
    - ☑ DNS Server Tools (Installed)
    - □ Fax Server Tools
    - □ File Services Tools
    - □ Network Controller Management Tools
    - □ Network Policy and Access Services Tools
    - □ Print and Document Services Tools
    - □ Remote Access Management Tools
    - □ Volume Activation Tools
    - □ Windows Deployment Services Tools

Description

Active Directory Certificate Services Tools includes the Certification Authority, Certificate Templates, Enterprise PKI, and Online Responder Management snap-ins.

4. Check the following box: **Remote Server Administration Tools / Remote Administration Tools / Active Directory Certificate Services Tools**.

5. Click **Next** until the **Install** button appears, and click the Install button.

6. Wait while the installation is complete before proceeding to the next step.

Installing the default set of Microsoft Certificate Templates using the snap-in

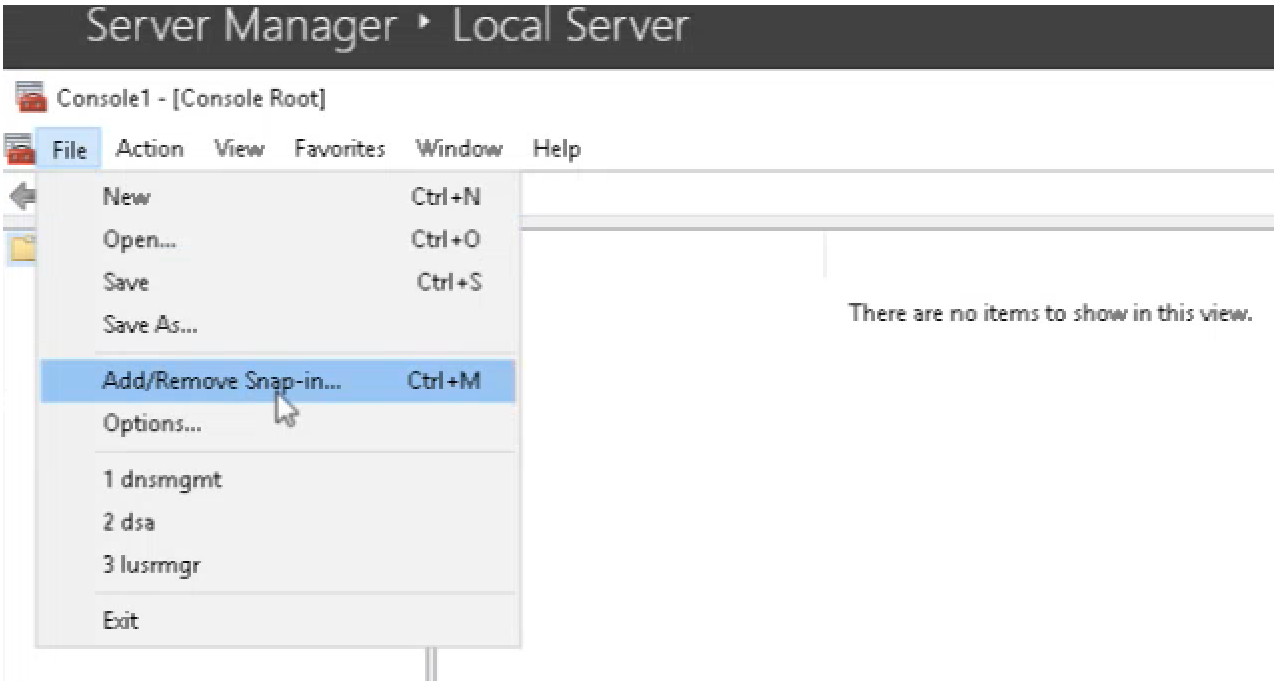
After Enabling the Certificate Templates snap-in, add the snap-in to install the default set of Microsoft Certificate Templates.

To install the default set of Microsoft Certificate Templates using the snap-in:

1. Log in to the root Active Directory Domain of the Windows forest as a member of both the Enterprise Admins and Domain Admin groups.

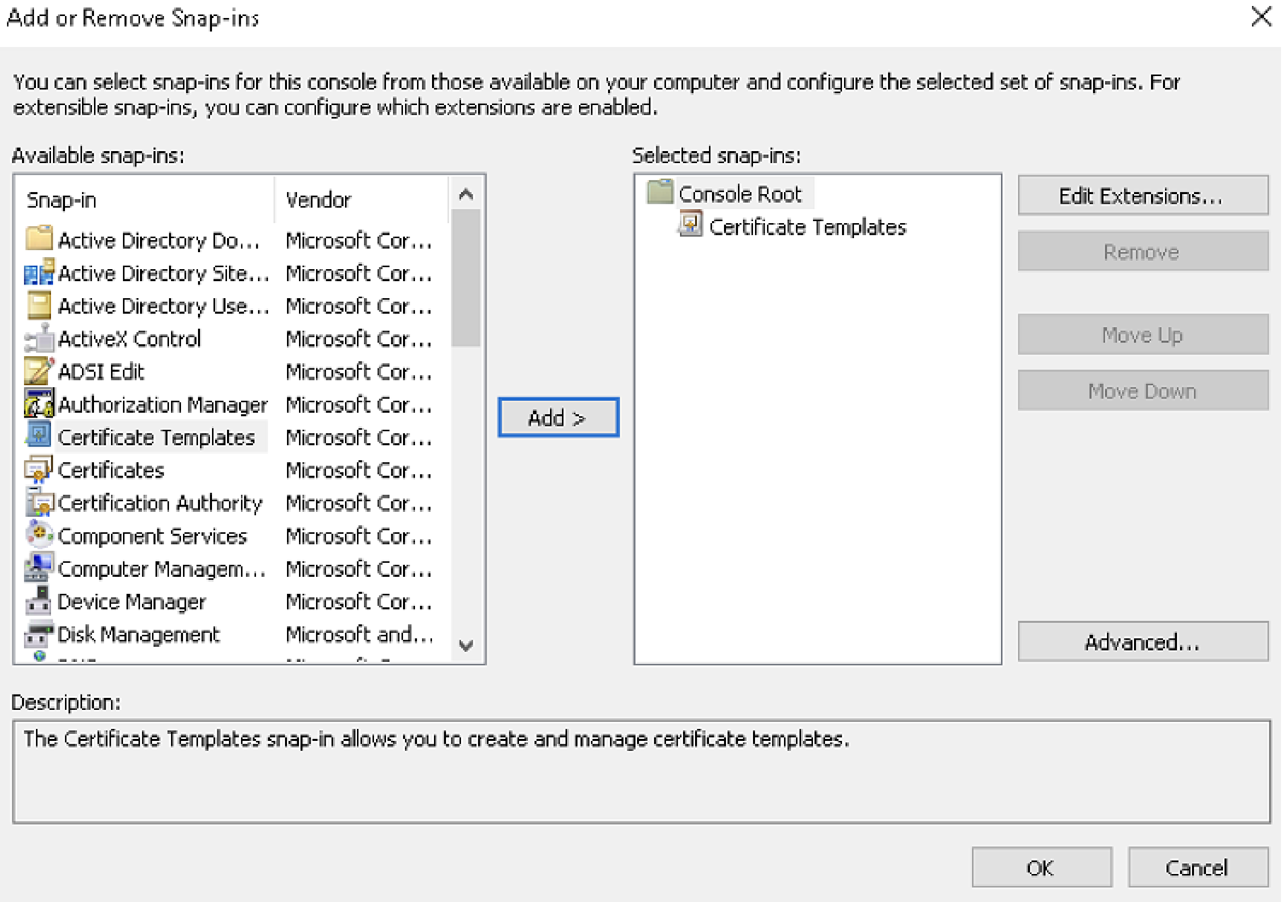
   ⚠ Users without these privileges cannot access the dialog options described in this section.

2. Open Microsoft Management Console (MMC) â□□ for example, by pressing the Windows key on the keyboard and typing "MMC." (ending with a period) in the search box.


Server Manager ▸ Local Server
Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 dnsmgmt
2 dsa
3 lusrmgr
Exit
There are no items to show in this view.

3. Select **File > Add/Remove Snap-in**.

4. In the **Available snap-ins** column, select **Certificate Templates**.


Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...

Selected snap-ins:

- Console Root
  - Certificate Templates

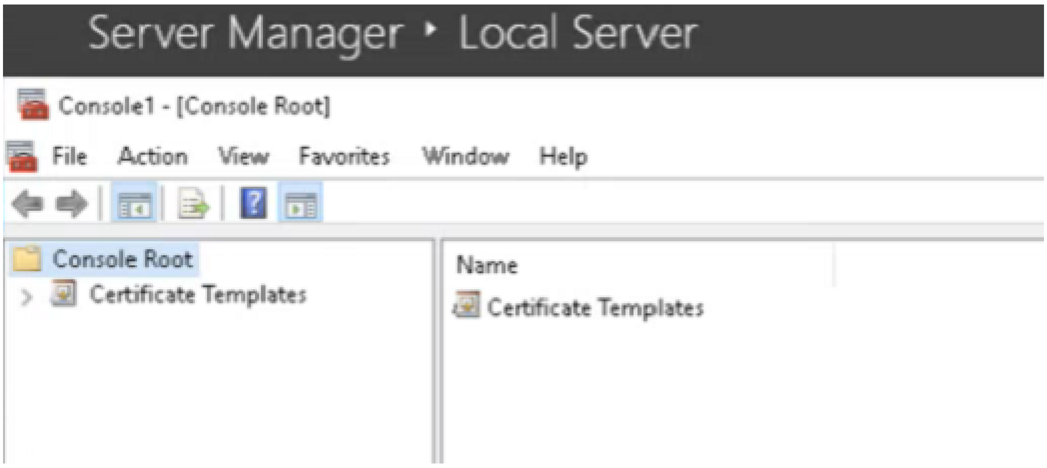
Description:

The Certificate Templates snap-in allows you to create and manage certificate templates.

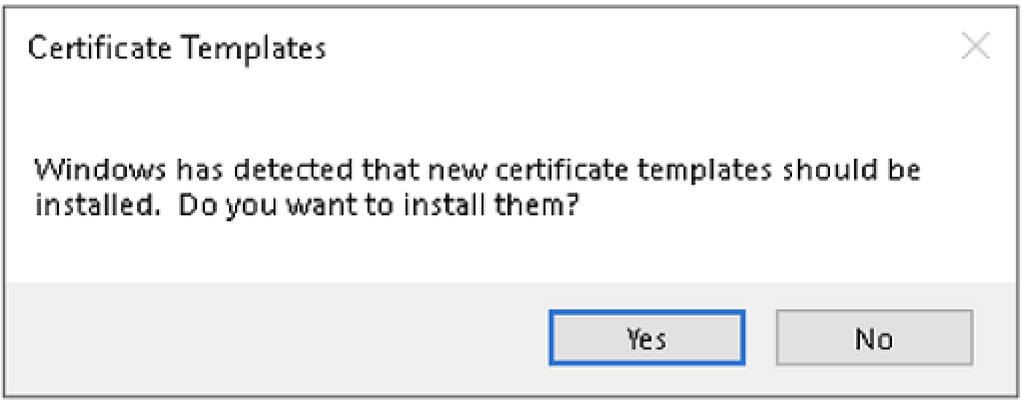
5. Click **Add** to move the **Certificate Templates** snap-in to the **Selected snap-ins** column.

6. Click **OK** to close the **Add or Remove Snap-ins** wizard and return to the Microsoft Management Console.

7. In the Microsoft Management Console, click **Certificate Templates** under **Console Root**.



8. Click **Yes** in the confirmation dialog.



Windows has detected that new certificate templates should be installed. Do you want to install them?

⚠ If you accidentally click No in the confirmation dialog, remove the Active Directory Certificate Services Tools and repeat all the steps explained in Installing the default set of Microsoft Certificate Templates.

Downloading the certificate chain

Follow the steps described in Downloading a CA certificate to download the certificate chain of the following certificates:

- The LDAPS TLS certificates
- The WSTEP-enrolled certificates

Specifically, you must download:

- The certificate of the issuing certificate authority.
- The certificate of the root certificate authority

When not issued by the same certificate authority, you must download separately the certificate chains of the LDAPS TLS and WSTEP certificates

Setting up LDAPS on domain controllers

Follow the steps below if the LDAPS connections with the Active Directory domain controllers are not configured or you want to replace the current TLS certificates.

- Establishing trust of the LDAPS TLS chain
- Generating the LDAPS TLS certificates
- Installing the LDAPS TLS certificates
- Validating the LDAPS configuration

If you want to maintain an existing LDAPS configuration, remember to add the root CA certificate of the LDAPS TLS certificates when Configuring an issuing CA for WSTEP.

Establishing trust of the LDAPS TLS chain

Before generating the LDAPS TLS certificates, configure the Active Directory Forest to trust the certificate chain. Otherwise, there is a risk of breaking the LDAP communications between the various domain controllers. As explained below, the recommended method to configure the LDAPS certificate chain trust is to create a GPO (Group Policy Object) linked to all domains in the Active Directory Forest.

- Creating a Group Policy Object for the LDAPS TLS certificate chain
- Importing the LDAPS TLS certificate chain into the Group Policy Object
- Linking the TLS LDAPS Group Policy Object to all domains

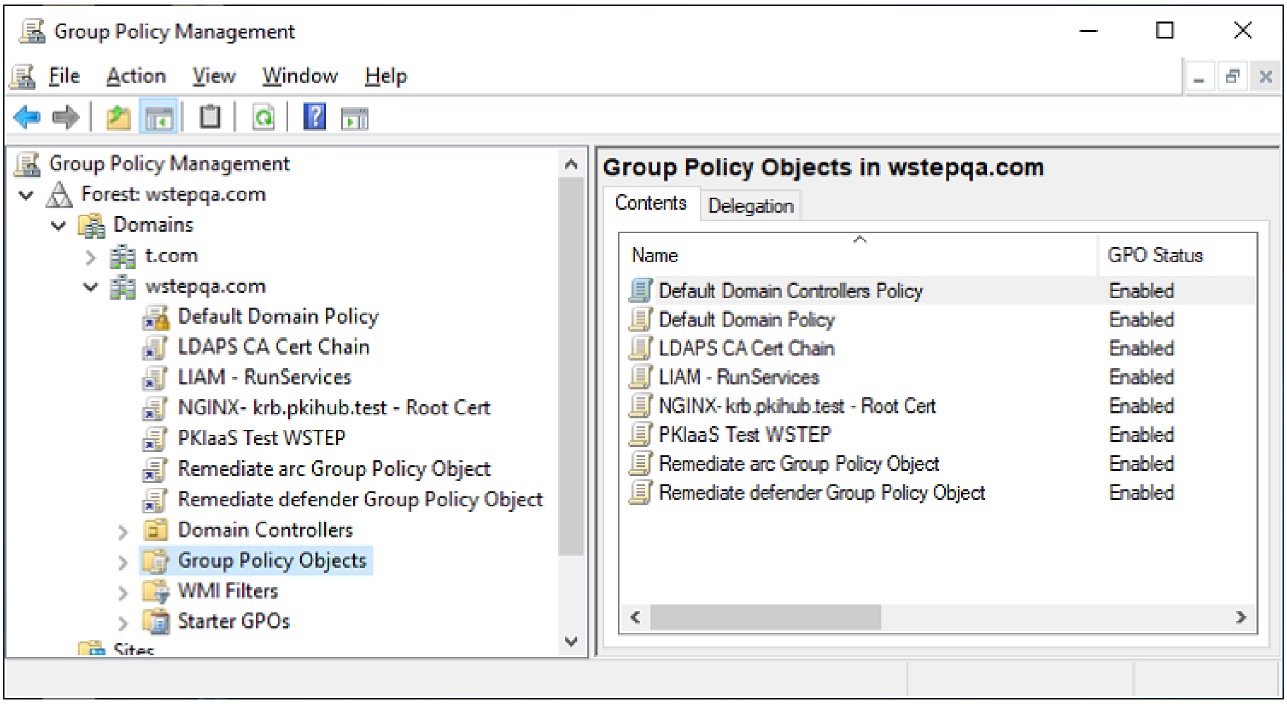
Creating a Group Policy Object for the LDAPS TLS certificate chain

The recommended method to configure a certificate chain trust is to create a Group Policy Object (GPO) linked to all domains in the Active Directory forest.

To create a Group Policy Object:

1. Log in to the root Active Directory of the forest as an Active Directory administrator.

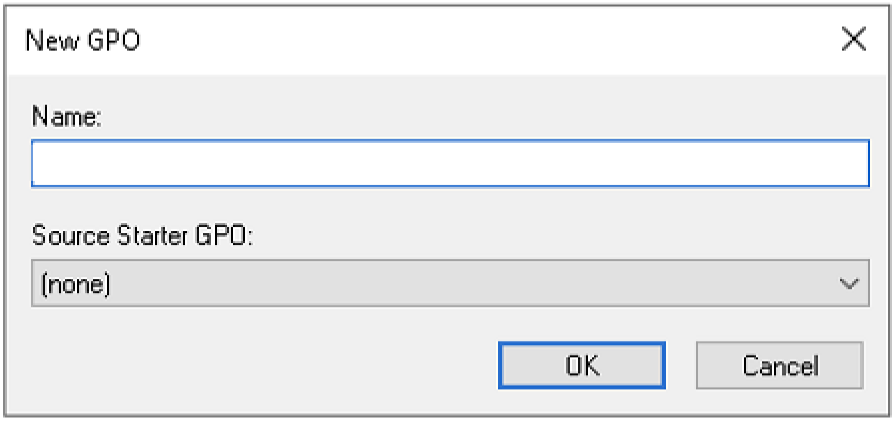
2. Select **Start** > **Windows Administrative Tools** > **Group Policy Management** to open the **Group Policy Management** dialog.



Group Policy Objects in wstepqa.com

Name	GPO Status
Default Domain Controllers Policy	Enabled
Default Domain Policy	Enabled
LDAPS CA Cert Chain	Enabled
LIAM - RunServices	Enabled
NGINX- krb.pkihub.test - Root Cert	Enabled
PKIaaS Test WSTEP	Enabled
Remediate arc Group Policy Object	Enabled
Remediate defender Group Policy Object	Enabled

3. Under the root domain, right-click the **Group Policy Objects** folder and select **New** to display the **New GPO** dialog.



4. Provide a new **Name** for the GPO and click **OK**.

Importing the LDAPS TLS certificate chain into the Group Policy Object

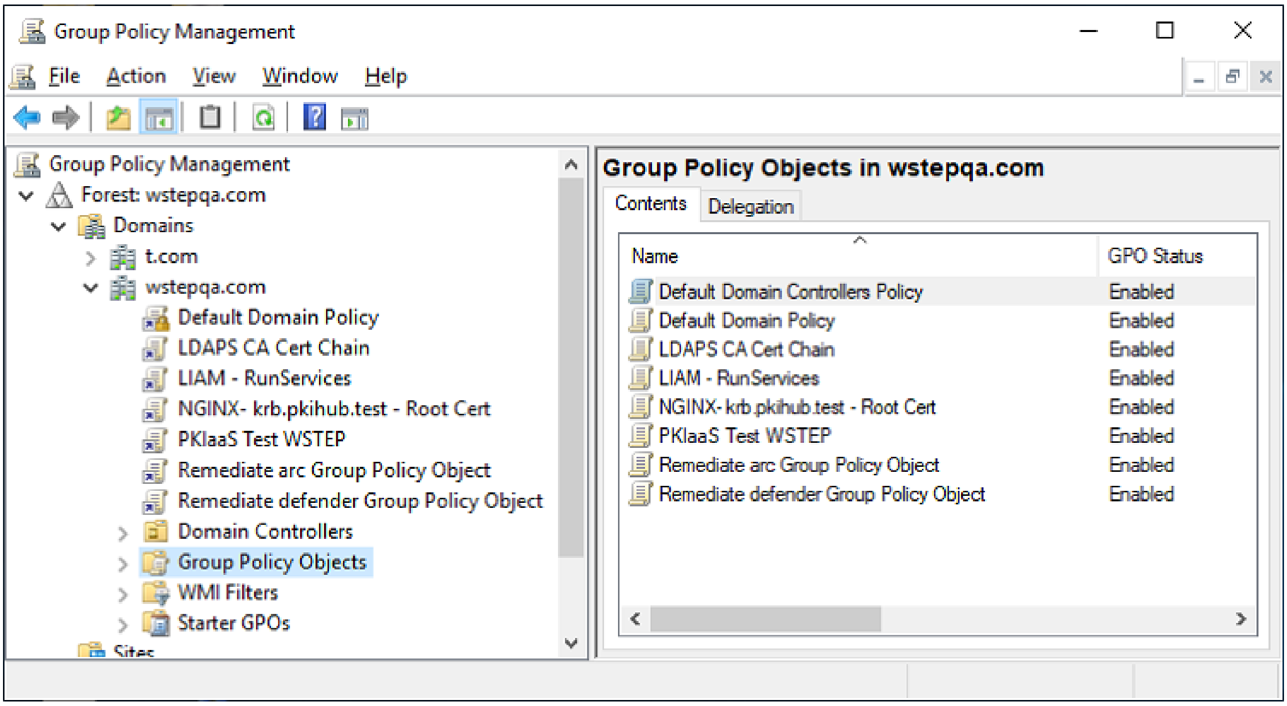
Import the LDAPS TLS certificate chain into the GPO previously created in Creating a Group Policy Object for the LDAPS TLS certificate chain.

ℹ See Downloading the certificate chain for how to download the required certificates.

To import the certificate chain into the GPO:

1. Log in to the root Active Directory of the forest as an Active Directory administrator.

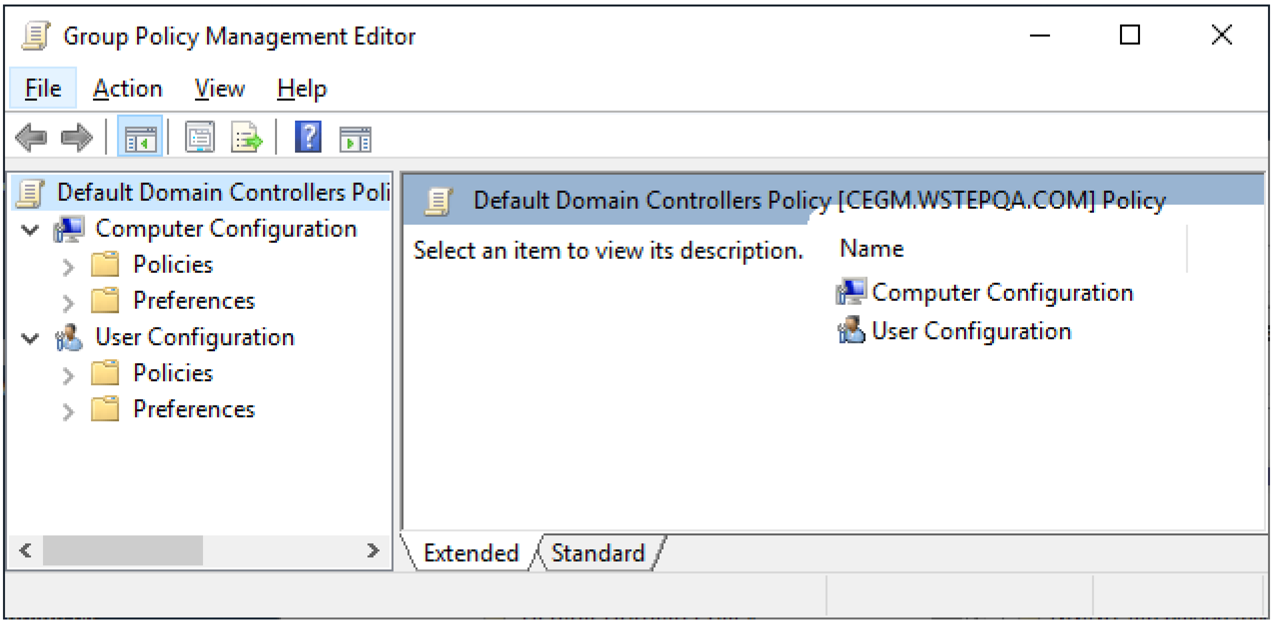
2. Select **Start > Windows Administrative Tools > Group Policy Management** to open the **Group Policy Management** dialog.



Name	GPO Status
Default Domain Controllers Policy	Enabled
Default Domain Policy	Enabled
LDAPS CA Cert Chain	Enabled
LIAM - RunServices	Enabled
NGINX- krb.pkihub.test - Root Cert	Enabled
PKIaaS Test WSTEP	Enabled
Remediate arc Group Policy Object	Enabled
Remediate defender Group Policy Object	Enabled

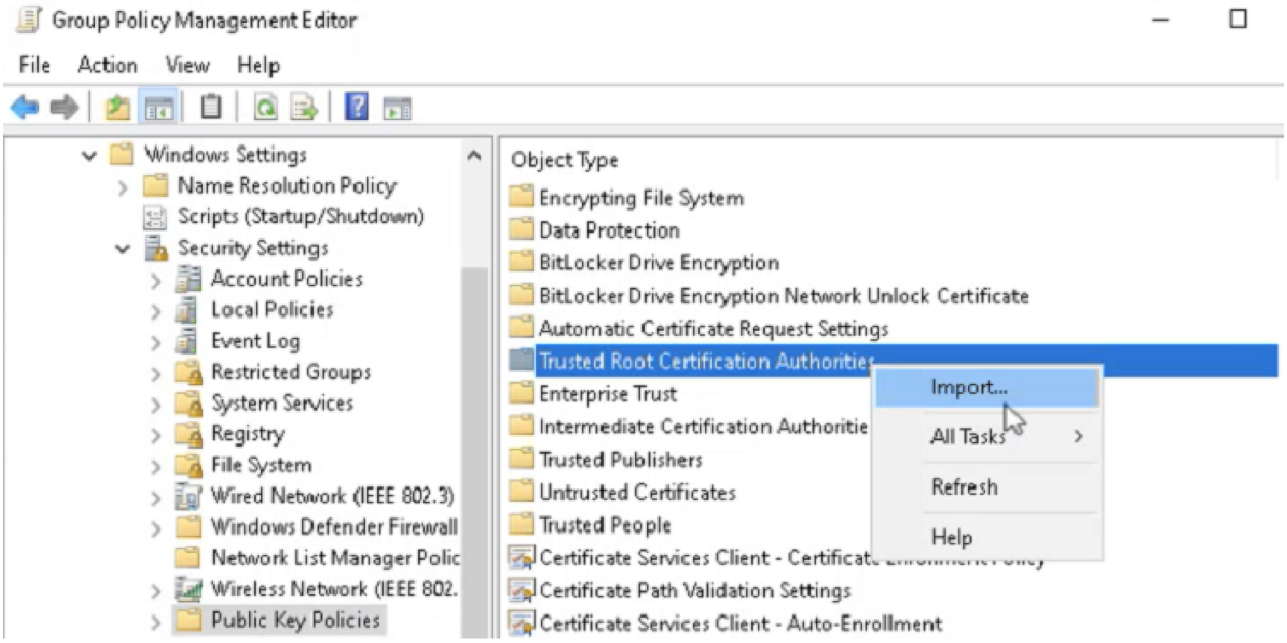
3. Right-click the Group Policy Object.

4. Select **Edit** to display the **Group Policy Management Editor**.


Group Policy Management Editor
File Action View Help
Default Domain Controllers Poli
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Default Domain Controllers Policy [CEGM.WSTEPQA.COM] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration
Extended
Standard

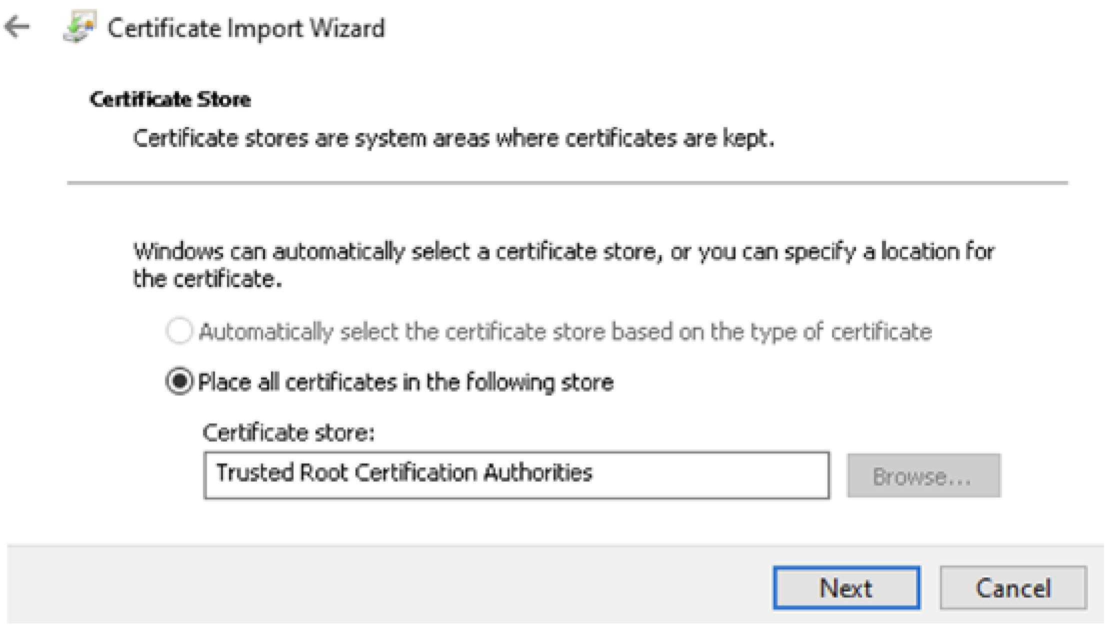
5. Navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**.

6. Right-click **Trusted Root Certificate Authorities** and select **Import**.


Group Policy Management Editor
File Action View Help
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3)
Windows Defender Firewall
Network List Manager Polic
Wireless Network (IEEE 802.
Public Key Policies
Object Type
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock Certificate
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authoritie
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificat
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment
Import...
All Tasks
Refresh
Help

7. In the **Certificate Import Wizard**, click **Next** and select the root CA certificate file to import.

8. Click **Next** to reveal the **Certificate Store** settings.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

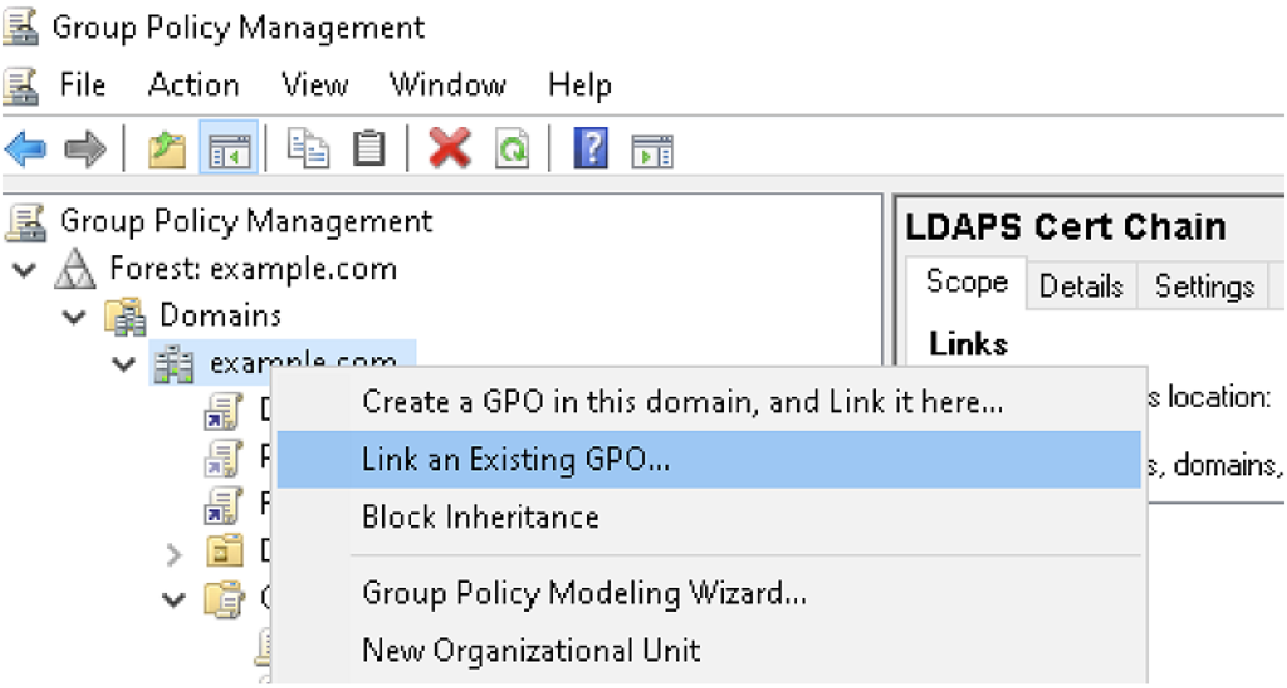
9. Verify that the selected certificate store is **Trusted Root Certification Authorities**.
10. Click **Next** to display the **Completing the Certificate Import Wizard**.
11. Click **Finish** to return to the **Group Policy Management** dialog.
12. In the **Group Policy Managemen**t dialog, navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**.
13. Right-click **Intermediate Certificate Authorities** and select **Import** to display the **Certificate Import Wizard**.
14. Click **Next** and select the issuing CA certificate file to import.
15. Click **Next** to reveal the Certificate Store settings.
16. Verify that the selected certificate store is **Trusted Root Certification Authorities**.
17. Click **Finish**.
18. Select **File** > **Exit** to close the **Group Policy Management Editor**.

Linking the TLS LDAPS Group Policy Object to all domains

Repeat the following procedure in each domain of the Active Directory forest to link the Group Policy Object created for the LDAPS TLS certificate chain.

To link a Group Policy Object with a domain:

1. Log in to the root Active Directory of the forest as an Active Directory administrator.
2. Select **Start** > **Windows Administrative Tools** > **Group Policy Management** to open the **Group Policy Management** dialog.



3. Right-click the domain name and select Link an existing GPO... to display the **Select GPO** dialog.

4. Select the Group Policy Object.

5. Click **OK**.

Generating the LDAPS TLS certificates

You can use Entrust PKIaaS to generate LDAPS TLS certificates for each domain. Follow the steps in Issuing a certificate in a PKCS #12 and select the following values.

Setting	Value
â□□Certificate Authority	Select a certificate authority like the one described in Configuring an issuing CA for WSTEP.
Certificate Profile	Select the `multiuse-p12-key-encipherment-client-server` certificate profile of the multiuse group.
Subject DN	Enter a Common Name (CN) matching the FQDN of the Domain Controller — for example: `dc.example.com`.
Certificate Expiry	Enter a period not exceeding 397 days.
Subject Alternate Names	All Subject Alternative Names must include a DNS matching the FQDN of the Domain Controller.

⚠ If you generate the LDAPS TLS certificates with a non-Entrust PKIaaS authority, ensure they are SHA-2, as SHA-1 certificates are not allowed due to their vulnerabilities.

Installing the LDAPS TLS certificates

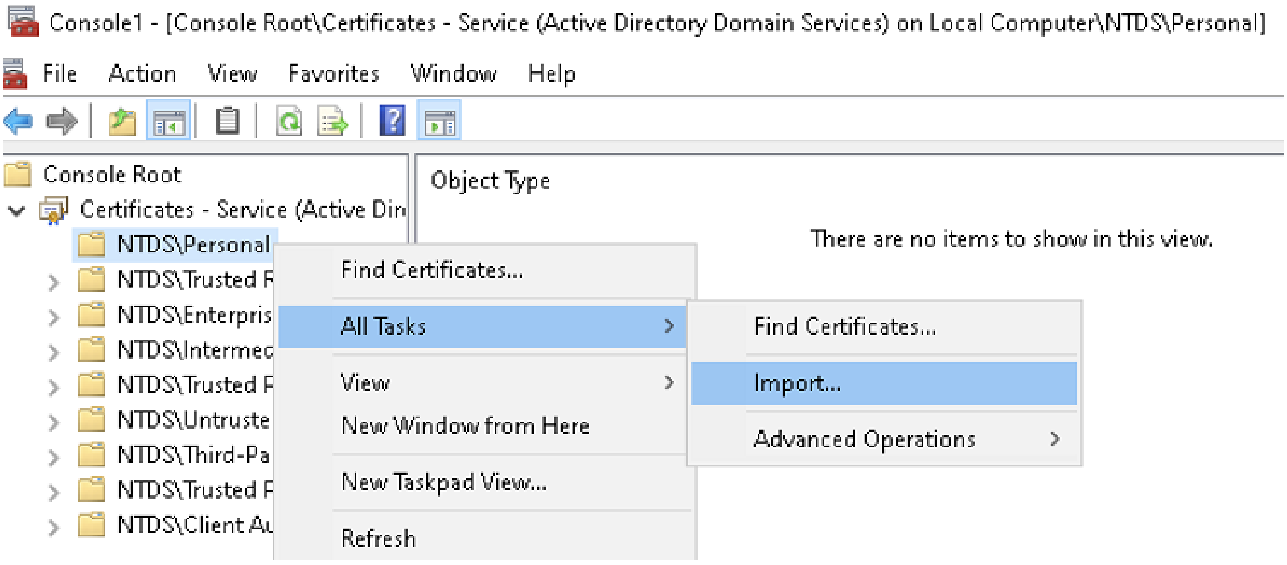
Repeat the following steps in each domain controller to install the LDAPS TLS certificate in the NTDS personal certificate store.

To install the LDAPS TLS certificate in a Domain Controller:

1. In the Domain Controller machine, copy the P12 file obtained when Generating the LDAPS TLS certificates.

2. If not already installed, install the Certificate Templates snap-in as explained in Enabling the Certificate Templates snap-in.

3. In the management console, right-click **NTDS Personal** under **Certificates**.



4. Select **All Tasks > Import** to display the **Certificate Import Wizard**.

5. Follow the wizard instructions to import the certificate file, enter the password, and install the certificate in the **NTDS ersonal** certificate store.

Validating the LDAPS configuration

After completing the LDAPS TLS configuration, open a command shell on any machine with OpenSSL installed and run the following command for each Domain Controller.

```
openssl s_client -connect <DOMAIN-FQDN>:636 -showcerts
```

Where `<DOMAIN-FQDN>` is the Fully Qualified Domain Name of the Domain Controller — for example:

```
openssl s_client -connect dc1.example.com:636 -showcerts
```

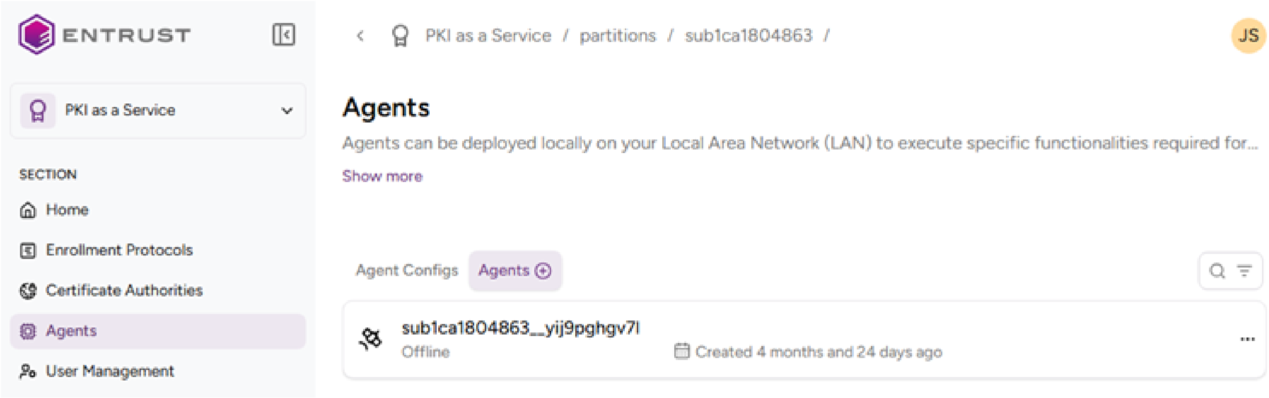
If LDAPS is appropriately configured, this command will display the LDAPS certificate for the selected domain controller

Downloading an agent

Download a virtual machine to operate as a WSTEP agent on your Windows domain.

To download an agent virtual machine:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
    - Owners
    - CA Administrators
2. Click **Agents** in the sidebar.
3. Select the **Agents** tab.



Agents

Agents can be deployed locally on your Local Area Network (LAN) to execute specific functionalities required for...

Show more

sub1ca1804863__yij9pghgv7l
Offline
Created 4 months and 24 days ago

4. Click **REGISTER**.
5. Click the download link corresponding to your corporate platform.
    - VMware vSphere
    - Azure
    - AWS
6. Click **Agree** in the **License Terms and Conditions** dialog to start the image file download.

Installing an agent

Once downloaded, install the agent virtual machine in your preferred virtualization infrastructure.

- Installing on Amazon Web Services
- Installing on Azure
- Installing on VMware vSphere

ℹ The agent virtual machine is stateless and stores all configuration settings on the Entrust cloud.

Installing on Amazon Web Services

See below for installing an agent virtual machine on the Amazon Web Services (AWS) cloud.

ℹ Refer to https://docs.aws.amazon.com for advanced configurations not covered in this guide, like selecting the machine DNS.

To install an agent virtual machine on Amazon Web Services:

1. Log in to https://console.aws.amazon.com as a user with permission to:
    - Create and manage S3 buckets, roles, policies, snapshots, images, and EC2 instances.
    - Run AWS CLI commands using a locally installed AWS CLI or the AWS ShellCloud.
2. Perform the steps explained below.
    - Creating an S3 bucket
    - Configuring an IAM policy
    - Creating an IAM role
    - Uploading the OVA file
    - Creating an AMI import configuration file
    - Preparing the command-line interface
    - Importing the AMI
    - Creating an EC2 instance
    - Opening a session on AWS

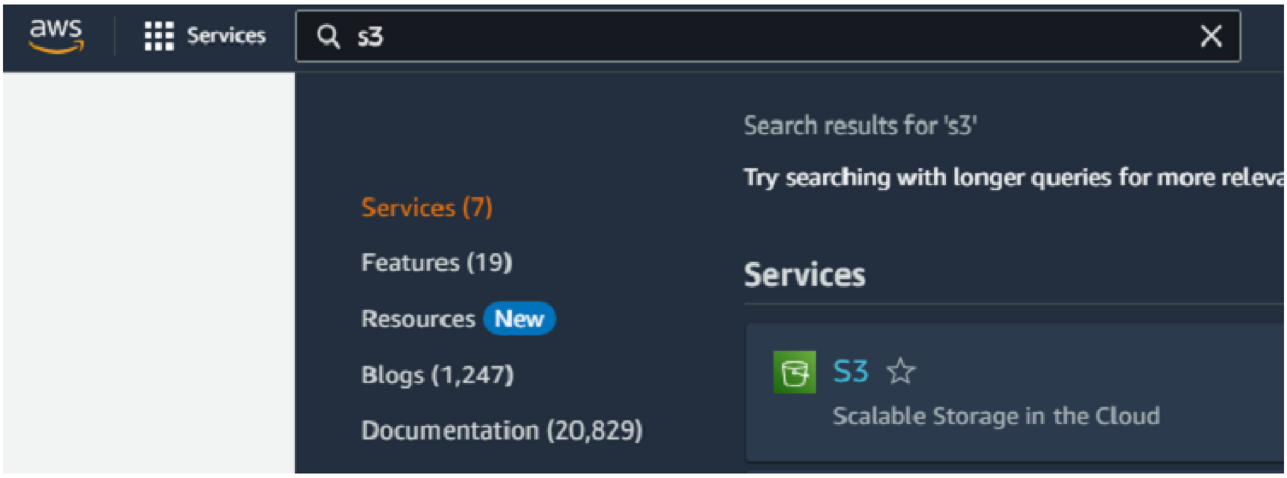
Creating an S3 bucket

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

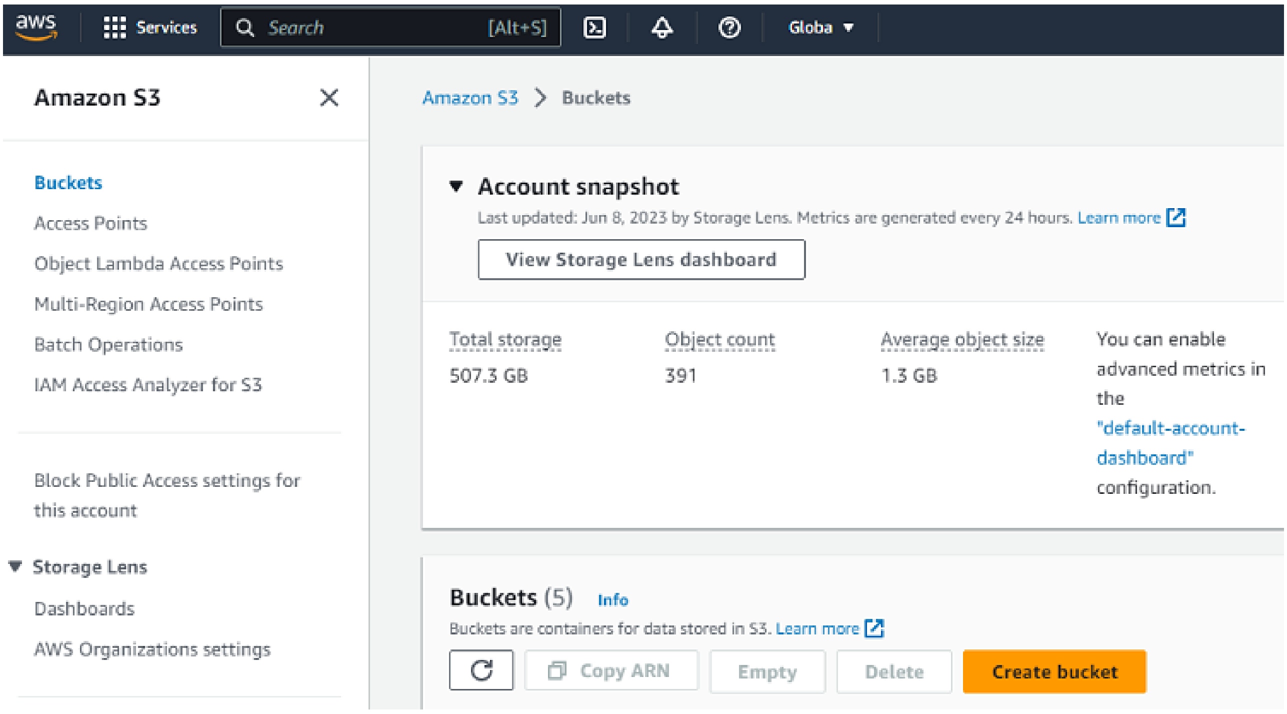
ℹ Skip this step if the bucket was already created for a previous deployment.

To create an S3 bucket:

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



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



Last updated: Jun 8, 2023 by Storage Lens. Metrics are generated every 24 hours. Learn more

Total storage	Object count	Average object size
507.3 GB	391	1.3 GB

You can enable advanced metrics in the "default-account-dashboard" configuration.

Buckets are containers for data stored in S3. Learn more

3. Click **Create a bucket**.

4. Enter a name for the new bucket.

5. Select an AWS region for the bucket.

⚠ All the resources created to deploy the agent in Amazon Web Services must share the same region.

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

7. Click **Create bucket**.

Configuring an IAM policy

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

- Creating a new IAM policy
- Updating an existing IAM policy

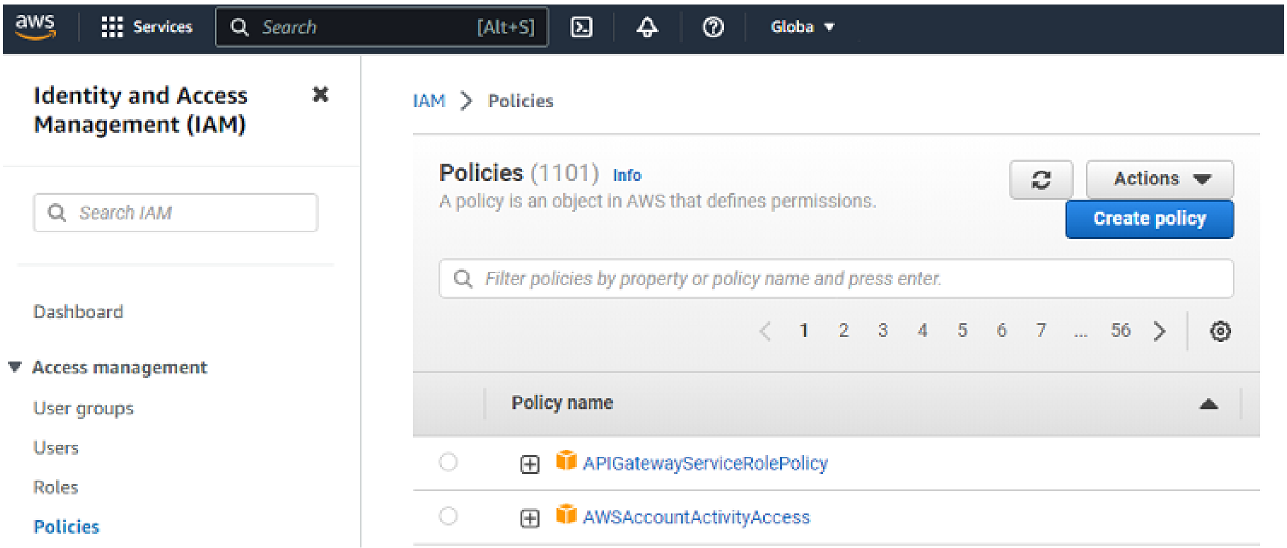
ℹ Skip this step if the policy was already configured for a previous deployment.

Creating a new IAM policy

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

To create an IAM policy:

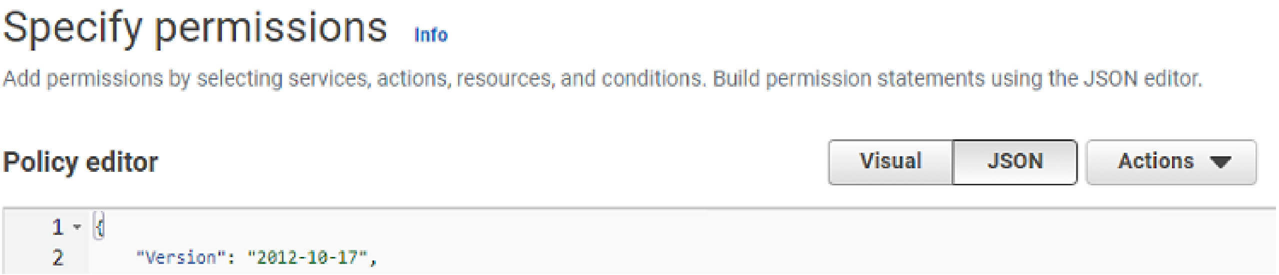
1. Type "IAM" in the AWS console search box.
2. Select **IAM** in the search results to display the IAM dashboard.



A policy is an object in AWS that defines permissions.

Policy name
APIGatewayServiceRolePolicy
AWSAccountActivityAccess

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



Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

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

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::$S3_BUCKET_NAME",
                "arn:aws:s3:::$S3_BUCKET_NAME/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifySnapshotAttribute",
                "ec2:CopySnapshot",
                "ec2:RegisterImage",
                "ec2:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

7. In the JSON code, replace $S3_BUCKET_NAME with the name of the S3 bucket selected when Creating an S3 bucket.

8. Click **Next**.

9. Enter a name and an optional description for the new policy.

10. Click **Create policy**.

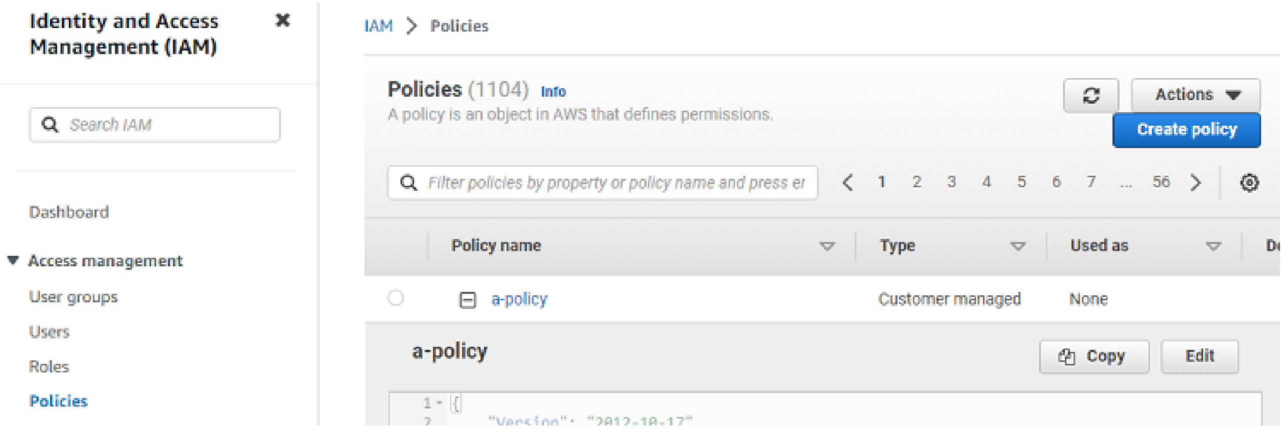
Updating an existing IAM policy

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

To update an IAM policy:

1. Type "IAM" in the AWS console search box.

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



A policy is an object in AWS that defines permissions.

Policy name	Type	Used as
a-policy	Customer managed	None

```
{
    "Version": "2012-10-17"
```

3. Select **Access management > Policies** in the navigation sidebar.

4. In the content pane, click the ✚ expand button for an existing IAM policy.

5. Click **Edit**.

6. In the policy editor field, add the following code to the `Resource` array.

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

7. In the code, replace `$S3_BUCKET_NAME` with the name of the S3 bucket selected when Creating an S3 bucket.

8. Click **Next**.

9. Click **Save changes**.

Creating an IAM role

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

ℹ Skip this step if the role was already created for a previous deployment.

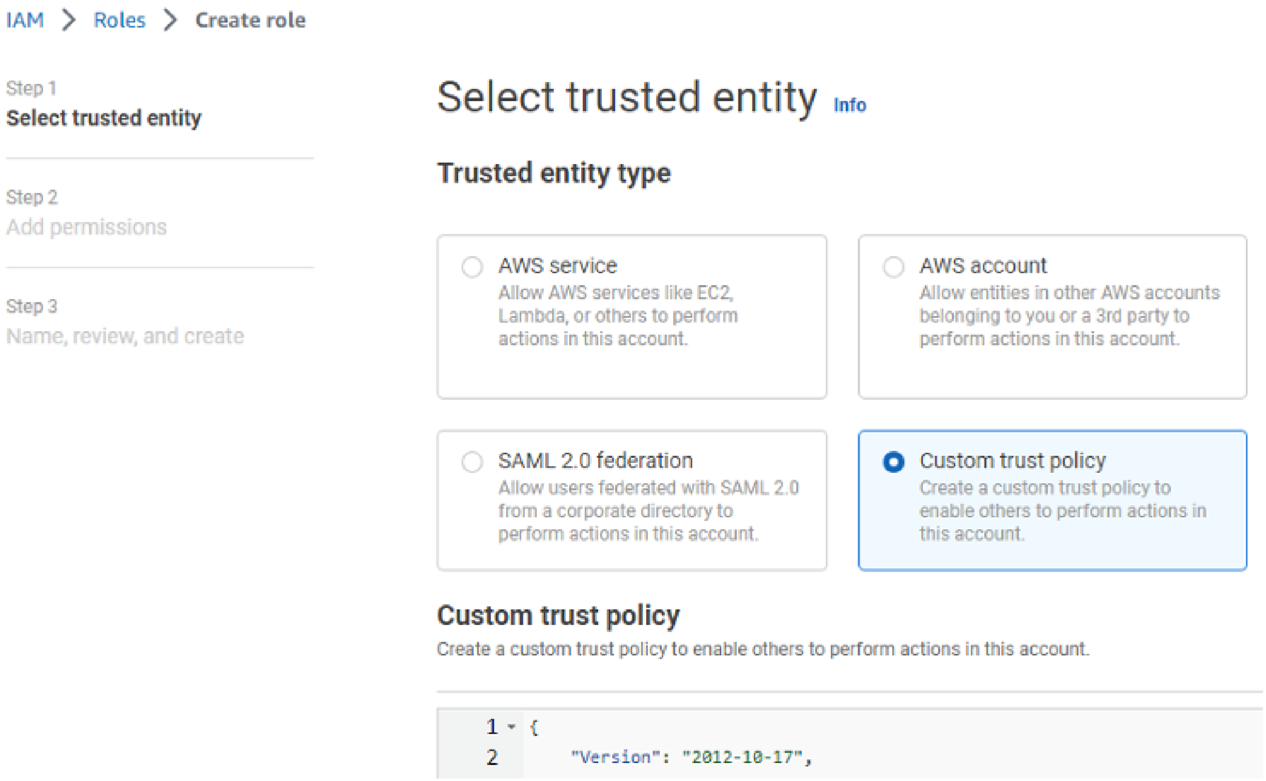
To create an IAM role:

1. Type "IAM" in the search box.

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

3. Select **Access management> Roles** in the navigation sidebar.

4. Click **Create role** to display the **Select trusted entity** page.



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

● Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

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

5. Under **Trusted entity type**, click **Custom trust policy**.

6. Paste the following code under **Custom trust policy**.

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

7. Click **Next**.

8. In the **Add permissions** page, select the policy described in Configuring an IAM policy.

9. Click **Next** to display the **Role details** page.

10. In the **Role name** field, type `vmimport`.

11. Click **Create role**.

Uploading the OVA file

Upload the OVA (Open Virtualization Format) image file of the agent.

---

i See Downloading an agent to obtain this file.

To upload the OVA file:

1. Navigate to the **Amazon S3 page > Buckets** page of the AWS console.
2. Click the name of an S3 bucket. As explained in Creating an S3 bucket, you can select an existing bucket or create a new one.
3. In the S3 bucket details page, click **Upload**.
4. Select the agent image file with the `.ova` extension and wait while the file uploads.

Creating an AMI import configuration file

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

```
[
    {
        "Description": "Agent AMI file",
        "Format": "ova",
        "UserBucket": {
        "S3Bucket": "$AWS_S3_BUCKET",
        "S3Key": "$OVA_FILE"
        }
    }
]
```

In the file contents, replace:

- `$AWS_S3_BUCKET` with the name of the S3 bucket described in Creating an S3 bucket.
- `$OVA_FILE` with the name of the OVA file selected when Uploading the OVA file.

For example:

```
[
    {
        "Description": "Agent AMI file",
        "Format": "ova",
        "UserBucket": {
            "S3Bucket": "PKIaaS-vm",
            "S3Key": "PKIaaS-vm-prod-us.ova"
        }
    }
]
```

Preparing the command-line interface

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

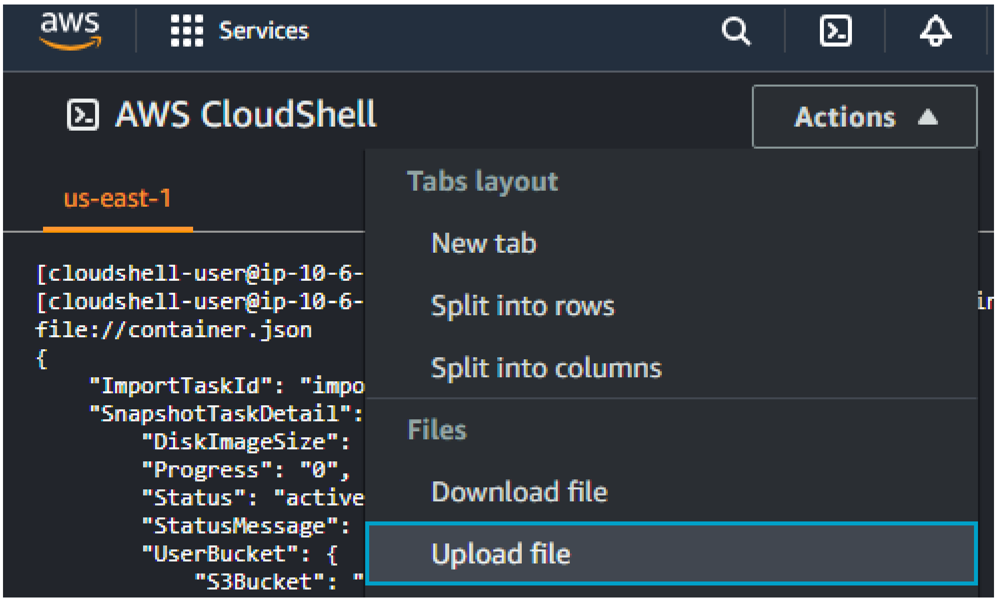
https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html

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

To upload the AMI import configuration file:

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

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



```
[cloudshell-user@ip-10-6-
[cloudshell-user@ip-10-6-
file://container.json
{
    "ImportTaskId": "impo
    "SnapshotTaskDetail":
        "DiskImageSize":
        "Progress": "0",
        "Status": "active
        "StatusMessage":
        "UserBucket": {
            "S3Bucket": "
```

3. In the options menu, select **Actions > Upload** file.

4. Select the `containers.json` file described in Creating an AMI import configuration file.

5. Click **Upload**.

Importing the AMI

Run the following AWS command to import the agent OVA as an EC2 AMI.

```
aws ec2 import-image --disk-containers file://containers.json
```

For example:

```
$ aws ec2 import-image --disk-containers file://containers.json
{
    "ImportTaskId": "import-ami-0c0ccaaab21ee1ce5",
    "Progress": "1",
    "SnapshotDetails": [
        {
            "Description": "Agent AMI file",
            "DiskImageSize": 0.0,
            "Format": "OVA",
            "Url": "s3://PKIaaS-vm/PKIaaS-vm-prod-us.ova",
            "UserBucket": {
                "S3Bucket": "PKIaaS-vm",
                "S3Key": "PKIaaS-vm-prod-us.ova"
            }
        }
    ],
    "Status": "active",
    "StatusMessage": "pending"
}
```

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

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

For example:

```
{
    "ImportImageTasks": [
        {
            "Architecture": "x86_64",
            "ImageId": "ami-0844eae6801fff32a",
            "ImportTaskId": "import-ami-0c0ccaaab21ee1ce5",
            "LicenseType": "BYOL",
            "Platform": "Linux",
            "SnapshotDetails": [
                {
                    "DeviceName": "/dev/sda1",
                    "DiskImageSize": 1538403840.0,
                    "Format": "VMDK",
                    "SnapshotId": "snap-0a6deaf4b94eb2b36",
                    "Status": "completed",
                    "Url": "s3://PKIaaS-vm/PKIaaS-vm-prod-us.ova",
                    "UserBucket": {
                        "S3Bucket": "PKIaaS-vm",
                        "S3Key": "PKIaaS-vm-prod-us.ova"
                    }
                }
            ],
            "Status": "completed",
            "Tags": []
        }
    ]
}
```

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

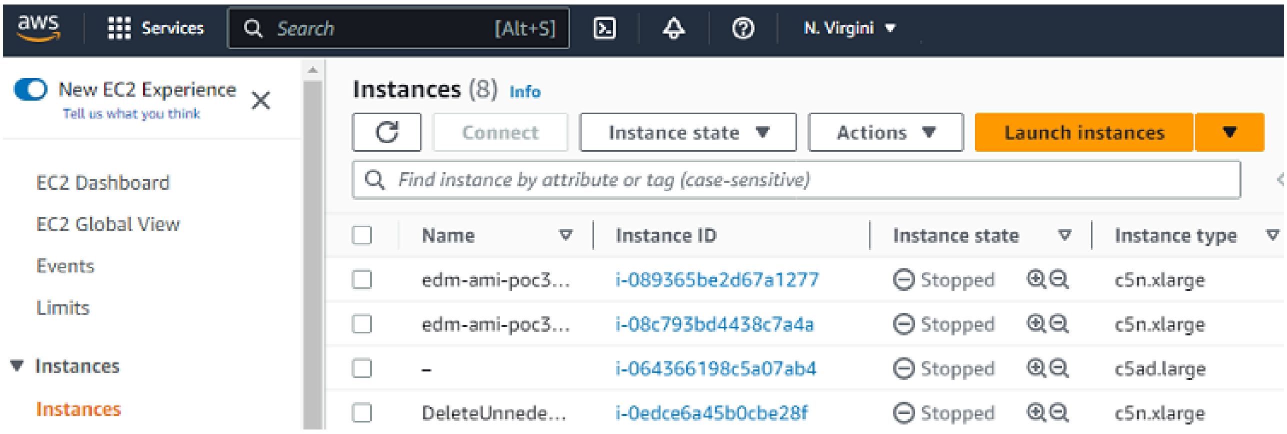
Status	Description	Required action
`active`	The import process is still running	Rerun the command after 5 minutes to recheck the status
`completed`	The import process has already finished	Copy the `ImageId` value you will later use for Creating an EC2 instance

Creating an EC2 instance

Create an EC2 instance for running the agent virtual machine image.

To create the EC2 instance:

1. Type "EC2" in the search box.
2. Select **EC2** in the search results to display the EC2 dashboard.



□	Name	Instance ID	Instance state	Instance type
□	edm-ami-poc3...	i-089365be2d67a1277	Stopped	c5n.xlarge
□	edm-ami-poc3...	i-08c793bd4438c7a4a	Stopped	c5n.xlarge
□	–	i-064366198c5a07ab4	Stopped	c5ad.large
□	DeleteUnnede...	i-0edce6a45b0cbe28f	Stopped	c5n.xlarge

3. Select **Instances > Instance** in the navigation sidebar.
4. Click Launch instance in the options menu.
5. Configure the following settings.
    - Name and tags > Name
    - Application and OS Images (Amazon Machine Image)
    - Instance type
    - Key pair (login)
    - Network settings > Firewall (security groups)
    - Configure storage
6. Click **Launch instance**.

Name and tags > Name

Enter a name for the new EC2 instance.

Application and OS Images (Amazon Machine Image)

Under the **My AMIs** tab, select the image previously imported in Importing the AMI.

Instance type

Select an EC2 instance built on the AWS Nitro System:

https://docs.aws.amazon.com/ec2/latest/instancetypes/ec2-nitro-instances.html

---

⚠ The minimum recommended instance type is **c5a.large**.

Key pair (login)

Select "Proceed without a key pair" as the SSH connection won't be used.

Network settings > Firewall (security groups)

Select or create a security group with permission to open the ports described in Agent network requirements.

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

Configure storage

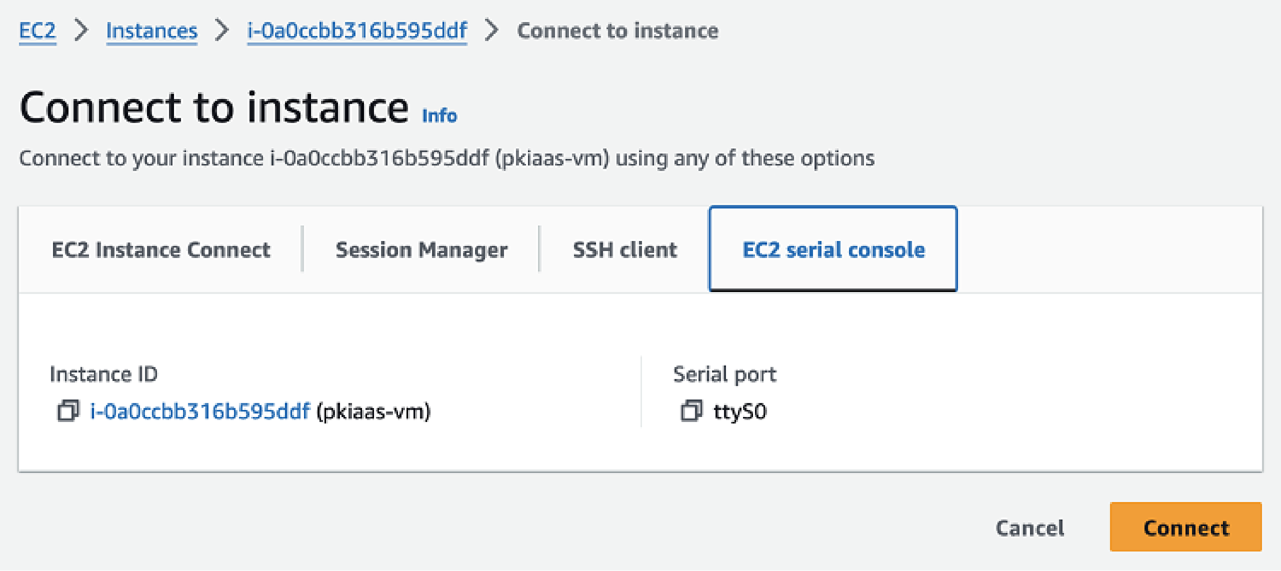
Select the default volume size.

Opening a session on AWS

After Creating an EC2 instance, refresh the EC2 instance list until the instance status is **Running**, and then open a session into the agent.

To open an agent session on AWS:

1. Select the Entrust PKIaaS agent in the instances list.
2. Click **Connect** in the options menu.
3. Navigate to the **EC2 serial console** tab.
4. Click **Connect**.



EC2 > Instances > i-0a0ccbb316b595ddf > Connect to instance

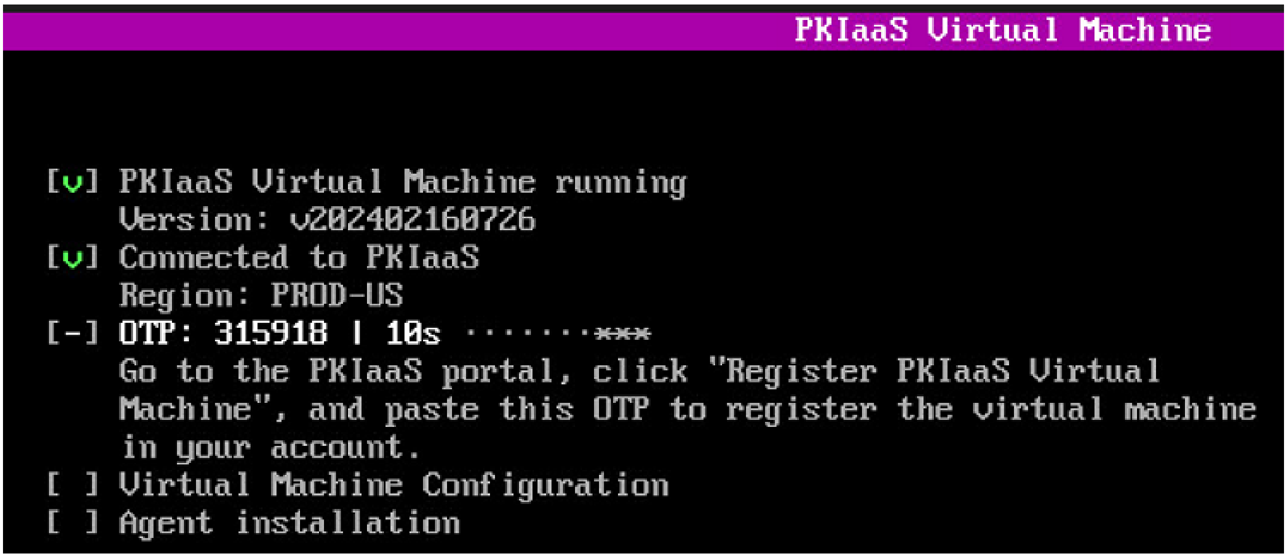
Connect to instance Info

Connect to your instance i-0a0ccbb316b595ddf (pkiaas-vm) using any of these options

Instance ID
i-0a0ccbb316b595ddf (pkiaas-vm)

Serial port
ttyS0

5. Wait a few seconds after the serial console appears.
6. Press the Enter key on your keyboard to launch the agent interface.



```
                                                    PKIaaS Virtual Machine


 [v] PKIaaS Virtual Machine running
     Version: v202402160726
 [v] Connected to PKIaaS
     Region: PROD-US
 [-] OTP: 315918 | 10s ·······***
     Go to the PKIaaS portal, click "Register PKIaaS Virtual
     Machine", and paste this OTP to register the virtual machine
     in your account.
 [ ] Virtual Machine Configuration
 [ ] Agent installation
```

7. Take note of the One-time Password (OTP) the agent displays on start. You will need this OTP for Registering an agent.

⚠ The agent refreshes the OTP every 30 seconds.

Installing on Azure

See below for installing an agent on Microsoft Azure.

ℹ Refer to https://learn.microsoft.com/azure for advanced configurations not covered in this guide, like selecting the machine DNS.

To install an agent in Azure:

1. Log in to https://portal.azure.com as a user with permission to create and manage:
   - Storage accounts
   - Images
   - Network rules
   - SSH keys
   - Virtual machines
2. Perform the steps described below.
   - Creating an Azure storage account
   - Uploading the VHD image
   - Creating an Azure image
   - Creating Azure network rules
   - Creating the agent on Azure
   - Opening a session on Azure

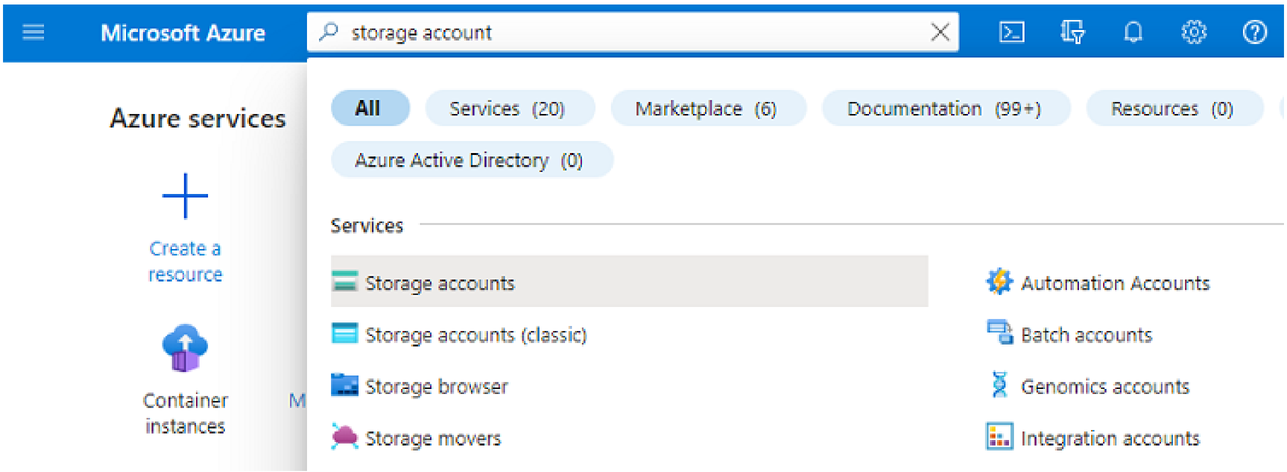
Creating an Azure storage account

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

ℹ Skip this step if the storage was already created for a previous deployment.

To create an Azure storage account:

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



2. Select **Storage accounts** in the search results.

3. Click **+ Create** on the **Storage accounts** page.

4. Configure the following settings on the **Create a storage account** page.
   - Subscription
   - Resource group
   - Storage account name
   - Region

5. Click **Review** to display the configured settings.

6. Click **Create** to create the storage account.

Subscription

Select your Azure user subscription.

Resource group

Select an existing resource group or create a new one.

⚠ All the resources created to deploy an agent in Azure must share the same resource group.

Storage account name

Enter a name for the new storage account.

Region

Select a region for the new storage account.

⚠ All the resources created in Azure must share the same region.

Uploading the VHD image

Upload the agent image file with the `.vdh` extension to Azure.

ℹ See Downloading an agent to obtain this file.

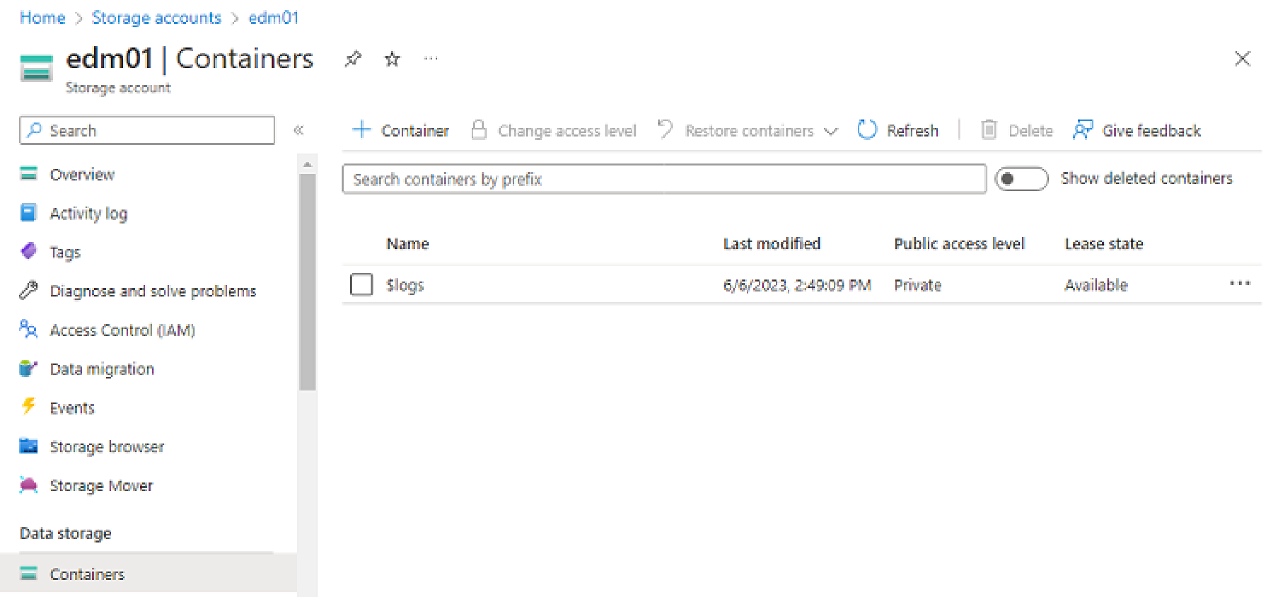
To upload the VHD image file:

1. Extract the contents of the Azure zipped image.

   ⚠ Extracting the Azure zipped VHD image requires at least 11 GB of disk space.

   ---

2. In the Azure Portal, select the storage account described in Creating an Azure storage account.



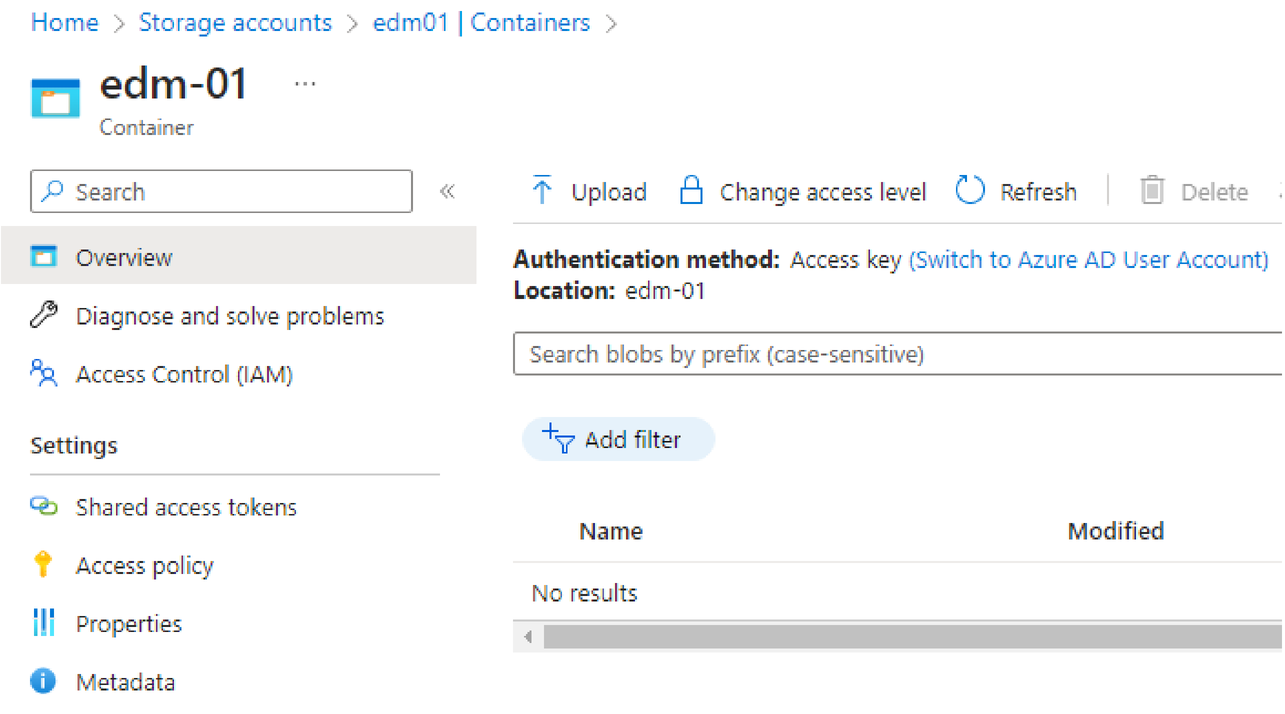
Name	Last modified	Public access level	Lease state
□ $logs	6/6/2023, 2:49:09 PM	Private	Available

3. In the sidebar menu of the storage settings page, select **Data storage** > **Containers**.

4. On the **Containers** page, click **+ Container**.

5. Enter a name for the new container and click **Create**.

6. On the **Containers** page, click the name of the new container to display the container details.



Authentication method: Access key (Switch to Azure AD User Account)
Location: edm-01

7. On the container details page, click **Upload**.

8. Select the agent image file with the `.vdh` extension and wait while the file uploads.

Creating an Azure image

See below for how to create the agent image using the Azure Portal.

To create the image in the Azure Portal:

1. Type "images" in the Azure Portal search bar.

2. Click **Images** on the search results.

3. Click **+ Create** on the **Images** page.

4. Configure the following settings in the **Create an image** page.
   - Project details
   - Instance details
   - OS disk

5. Click Review + create to validate the image settings.

6. Click Create to create the new image.

Project details

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

Setting	Value
Subscription	Select your Azure subscription.

Setting	Value
Resource group	Select the same resource group selected when Creating an Azure storage account.

Instance details

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

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

OS disk

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

Setting	Value
OS type	Select **Linux**
VM generation	Select **Gen 1**
Storage blob	Select the VHD image described in Uploading the VHD image
Account type	Select **Standard SSD**
Host caching	Select **Read-only**

Creating Azure network rules

Create a Network Security Group with rules granting access to the ports listed in Agent network requirements.

Creating the agent on Azure

Set the following configuration when creating the agent on Azure.

- Basics
- Disk
- Networking

Basics

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

Setting	Value
Project details / Subscription	Select your Azure subscription.
â□□Project details / Resource group	Select the resource group described in Creating an Azure storage account.

Setting	Value
Instance details / Virtual machine name	Enter a name for the new virtual machine.
Instance details / Region	Select the region shared by the rest of the Azure resources.
Instance details / Image	Select the image described in Creating an Azure image.
Instance details / Size	Select **Standard_B2s** or greater.
Administrator account / Authentication type	Select **SSH public key**.
Administrator account / SSH public key source	Generate a new one or use an existing one. The Azure VM creation process requires this step, but the key won't be used in the agent, as there is no SSH connection.
Inbound port rules / Public inbound ports	Select **None**.
Licensing type / License type	Select **Other**.

Disk

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

Setting	Value
OS disk / OS disk type	Select **Premium SSD (locally-redundant storage)** or higher.

Networking

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

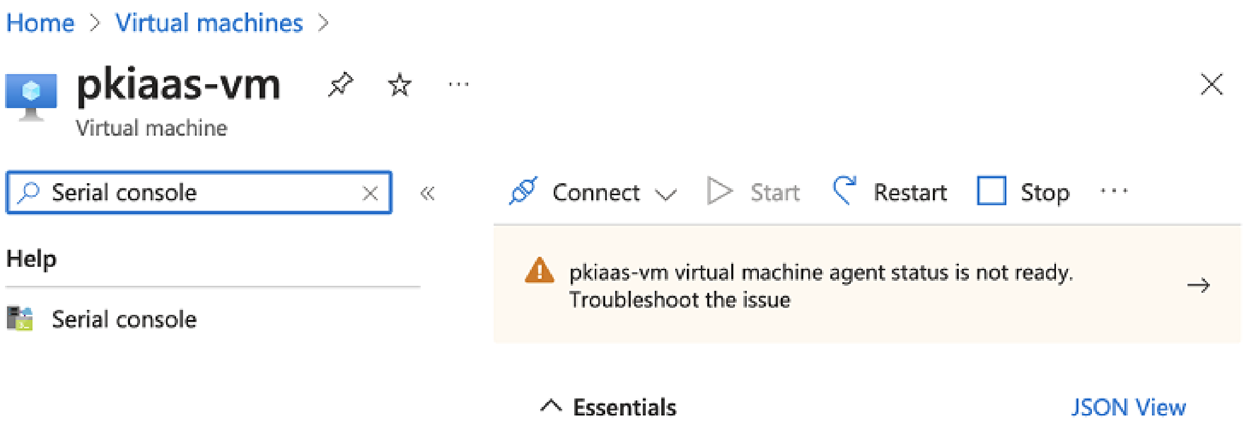
Setting	Value
NIC network security group	Select **Advanced**.
Configure network security group	Select the network security group described in Creating Azure network rules.

Opening a session on Azure

After Creating the agent on Azure, wait until the machine status changes from **Deployment is in progress** to **Your deployment is complete**, and open a session into the agent.

To open an agent session on Azure:

1. Select the agent in the **Agents** list.



pkiaas-vm virtual machine agent status is not ready.
Troubleshoot the issue

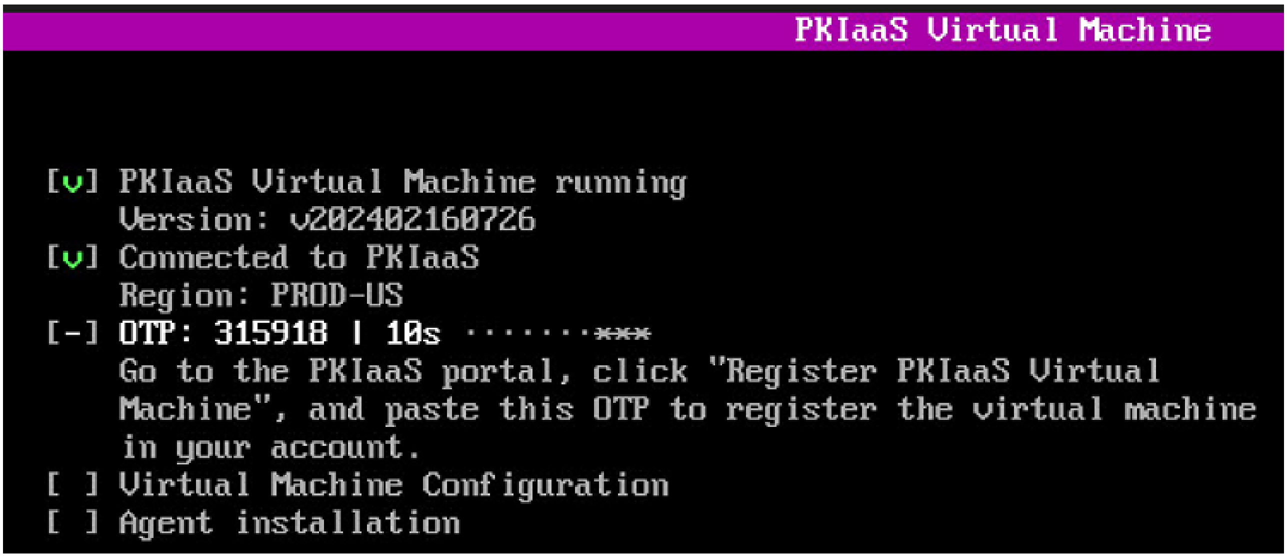
2. If displayed, ignore the "Agent status is Not ready" warning.

3. Type "Serial console" In the search box.

4. Click the **Serial console** result under the search box.

5. Wait until the serial connection is established and the "Press ENTER to continue" message appears.

6. Press the Enter key on your keyboard to launch the agent interface.



```
                                         PKIaaS Virtual Machine


  [✓] PKIaaS Virtual Machine running
      Version: v202402160726
  [✓] Connected to PKIaaS
      Region: PROD-US
  [-] OTP: 315918 | 10s ·······***
      Go to the PKIaaS portal, click "Register PKIaaS Virtual
      Machine", and paste this OTP to register the virtual machine
      in your account.
  [ ] Virtual Machine Configuration
  [ ] Agent installation
```

7. Take note of the One-time Password (OTP) the agent displays on start. You will need this OTP for Registering an agent.

ℹ The agent refreshes the OTP every 30 seconds.

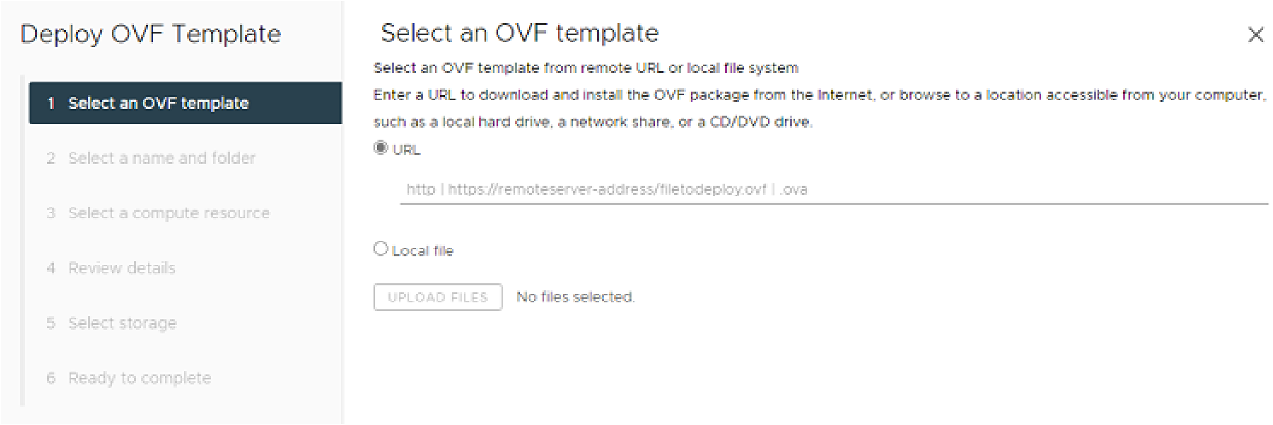
Installing on VMware vSphere

Use either the download link or the `.ova` image file to install an agent in VMware Workstation.

ℹ See Downloading an agent to obtain this file.

To install an agent in VMware vSphere:

1. Log in to your VMware vSphere portal.
2. Right-click on a folder of the navigation tree.
3. Select the **Deploy OVF Template** command to display the machine creation wizard.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

● URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

○ Local file

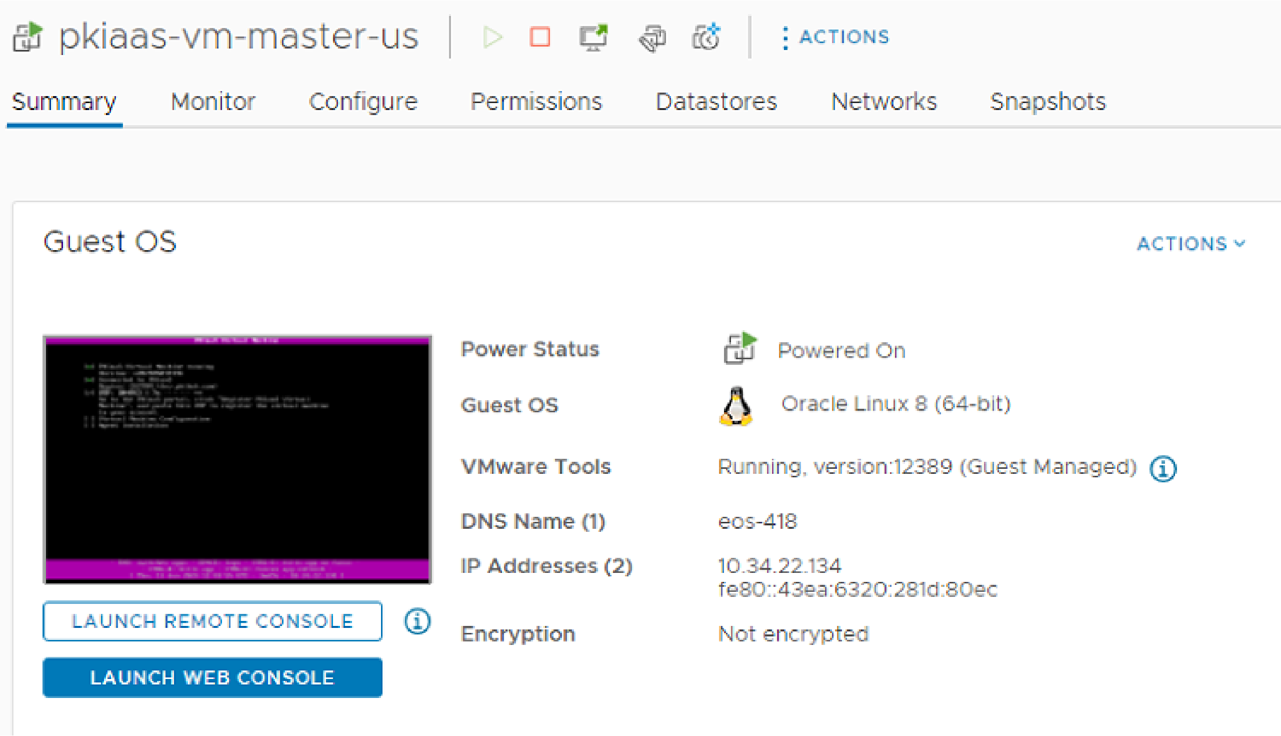
UPLOAD FILES No files selected.

4. In the **Select an OVF template** page, click **URL** to paste the download link, or **Local** file to import the `.ova` image file.
5. In the **Select a name and folder** page, select a name and a folder for the new virtual machine.
6. In the **Select a compute resource** page, select a computing resource for the new virtual machine.
7. In the **Review details** page, review the settings already selected for the new virtual machine.
8. In the **Select storage** page, select a storage resource for the new virtual machine.

⚠ Do not enable the Encrypt this virtual machine option.

---

9. In the **Select networks** page, select a network meeting the Agent network requirements.
10. In the **Ready to complete page**, review all the machine settings.
11. Click **Finish** and wait while VMware vSphere creates the machine.
12. Select the newly created machine in the navigation tree.
13. Click the **â□¶** icon to power the machine, and wait while the machine starts.



Power Status: Powered On

Guest OS: Oracle Linux 8 (64-bit)

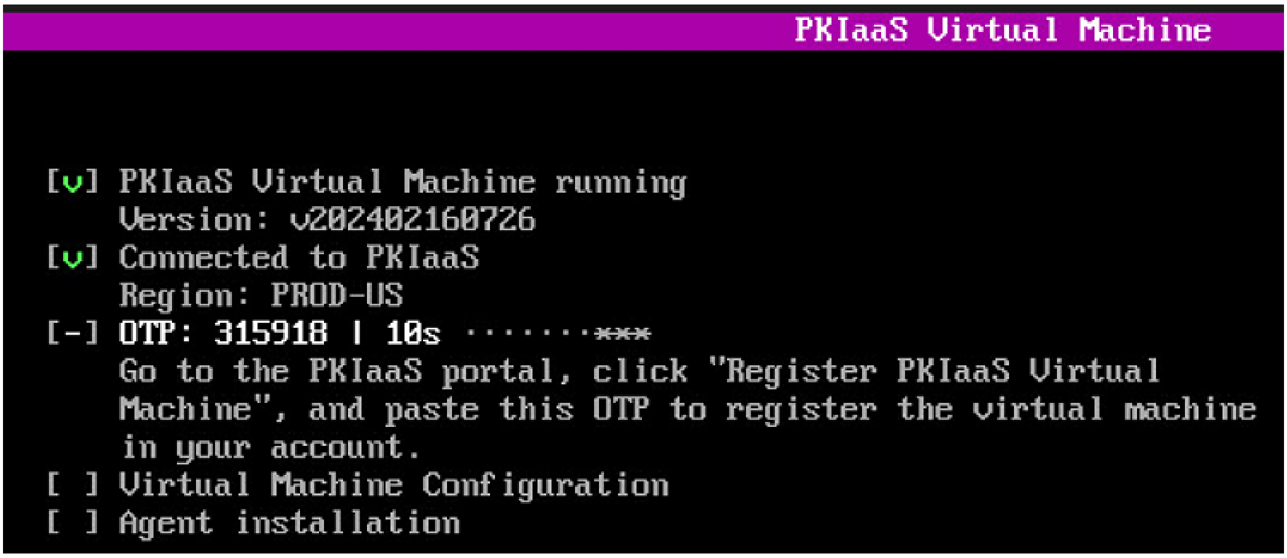
VMware Tools: Running, version:12389 (Guest Managed)

DNS Name (1): eos-418

IP Addresses (2): 10.34.22.134
fe80::43ea:6320:281d:80ec

Encryption: Not encrypted

14. Click **LAUNCH WEB CONSOLE** to display the machine prompt in your web browser.



```
                                              PKIaaS Virtual Machine


 [v] PKIaaS Virtual Machine running
     Version: v202402160726
 [v] Connected to PKIaaS
     Region: PROD-US
 [-] OTP: 315918 | 10s ········***
     Go to the PKIaaS portal, click "Register PKIaaS Virtual
     Machine", and paste this OTP to register the virtual machine
     in your account.
 [ ] Virtual Machine Configuration
 [ ] Agent installation
```

15. Take note of the One-time Password (OTP) the agent displays on start. You will need this OTP for Registering an agent.

⚠ The agent refreshes the OTP every 30 seconds.

Configuring WSTEP automation in PKIaaS

Configure PKIaaS to process WSTEP enrollment requests with PKIaaS Certification Authorities.

- Configuring an issuing CA for WSTEP
- Registering an agent
- Creating an agent configuration
- Linking an agent to a configuration

- Adding Active Directory nodes
- Getting the enrollment URL
- Enabling WSTEP for Active Directory nodes

Configuring an issuing CA for WSTEP

You need a subordinate or *certificate issuing* certificate authority with profiles of the wstep or multiuse groups. You can either:

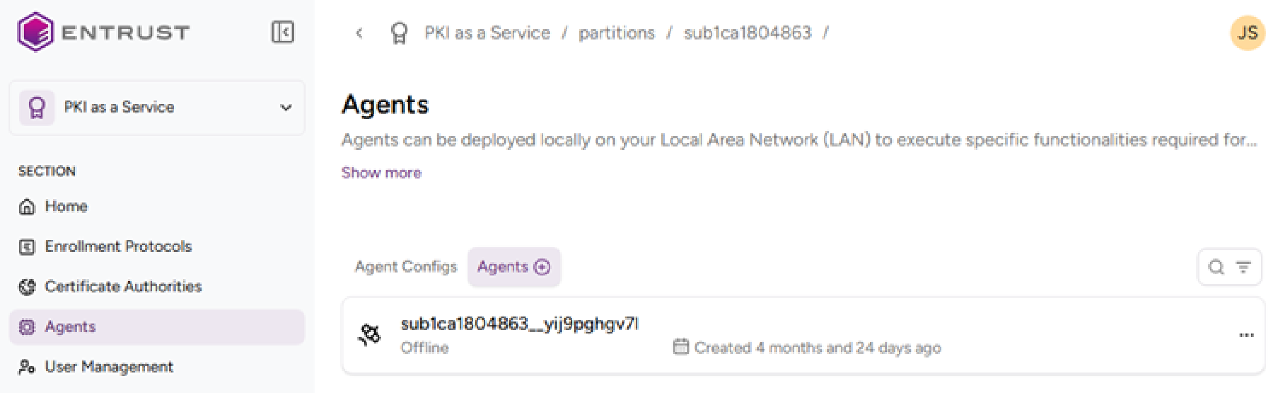
- Create an issuing subordinate CA with these profiles, as explained in Creating an issuing subordinate CA.
- Add these profiles to an existing CA, as explained in Selecting CA profiles.

Registering an agent

Once installed on your premises, register the agent in the Entrust PKIaaS portal.

To register an agent:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the following roles:
    - Owners
    - Protocol Operators
2. Click **Agents** in the sidebar.
3. Select the **Agents** tab.



Agents

Agents can be deployed locally on your Local Area Network (LAN) to execute specific functionalities required for...

Show more

sub1ca1804863__yij9pghgv7l
Offline
Created 4 months and 24 days ago

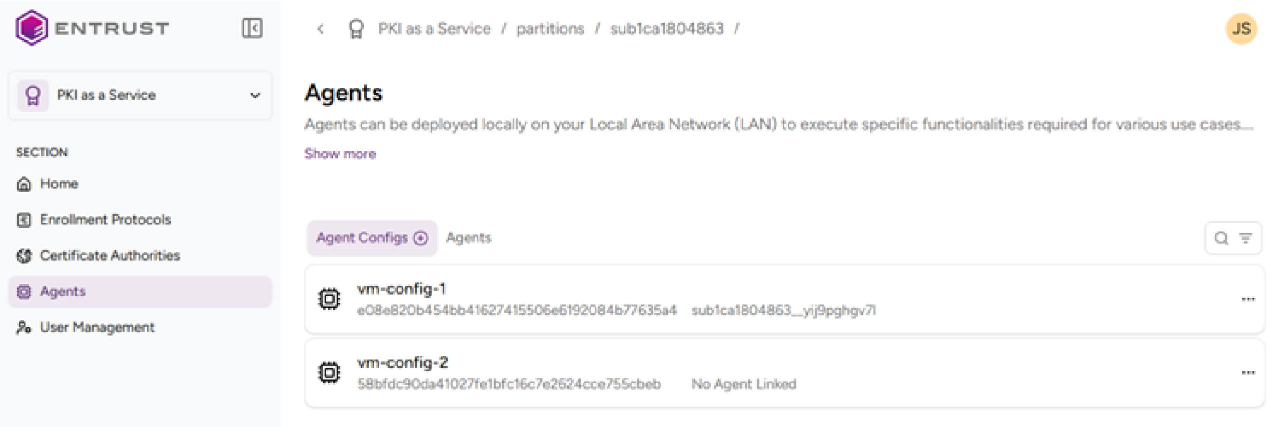
4. Click the plus **+** icon to the right of **Agents**.
5. In the **Register Agent** dialog, enter the one-time password you obtained when completing the installation on the selected platform.
    - Opening a session on AWS
    - Opening a session on Azure
    - Installing on VMware vSphere
6. Click **Register**.

Creating an agent configuration

Create a configuration for your agent.

To create an agent configuration:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the following roles:
    - Owners
    - Protocol Operators
2. Click **Agents** in the sidebar.
3. Click the three dots to the right of the Agent Configs tab.



Agents

Agents can be deployed locally on your Local Area Network (LAN) to execute specific functionalities required for various use cases...

vm-config-1
e08e820b454bb41627415506e6192084b77635a4 sub1ca1804863__yij9pghgv7l

vm-config-2
58bfdc90da41027fe1bfc16c7e2624cce755cbeb No Agent Linked

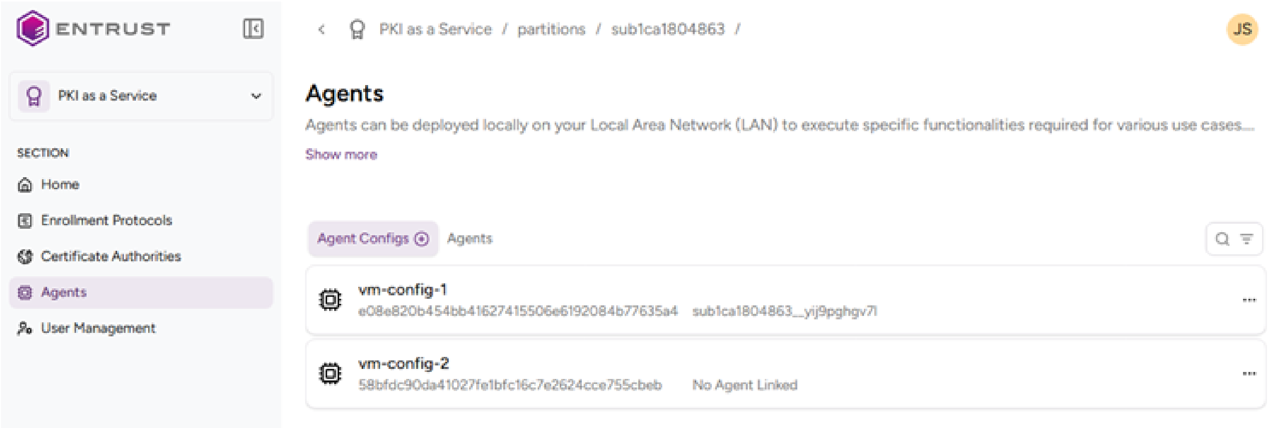
4. In the **Create an agent Configuration** dialog, add a friendly name and optional description for the configuration.
5. Click **Create**.

Linking an agent to a configuration

Link a configuration with your agent.

To link an agent configuration:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the following roles:
    - Owners
    - Protocol Operators
2. Click **Agents** in the sidebar.



Agents

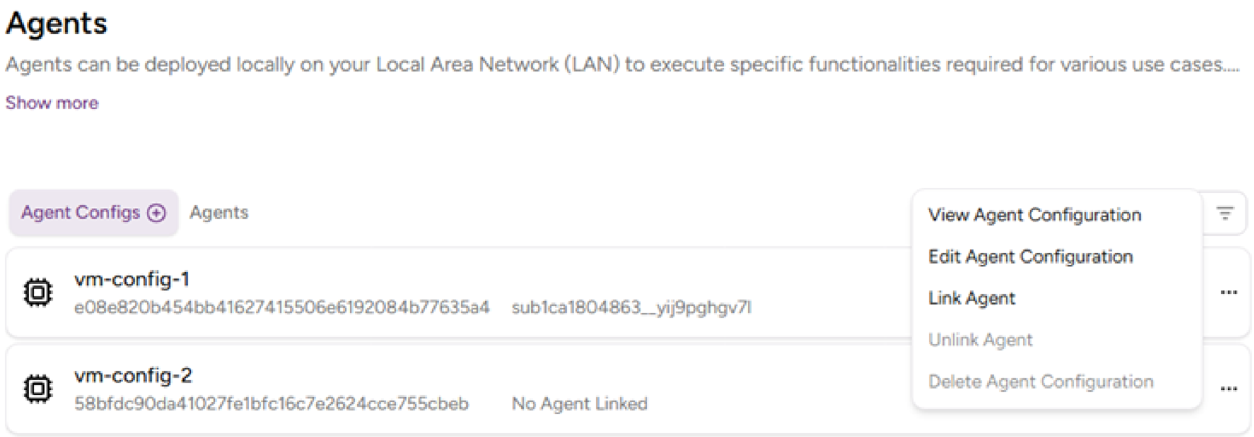
Agents can be deployed locally on your Local Area Network (LAN) to execute specific functionalities required for various use cases....

Show more

vm-config-1
e08e820b454bb41627415506e6192084b77635a4 sub1ca1804863__yij9pghgv7l

vm-config-2
58bfdc90da41027fe1bfc16c7e2624cce755cbeb No Agent Linked

3. In the **Agent Configs** tab, click the three dots to the right of the agent name.



Agents

Agents can be deployed locally on your Local Area Network (LAN) to execute specific functionalities required for various use cases....

Show more

vm-config-1
e08e820b454bb41627415506e6192084b77635a4 sub1ca1804863__yij9pghgv7l

vm-config-2
58bfdc90da41027fe1bfc16c7e2624cce755cbeb No Agent Linked

4. Select one of your registered agents.

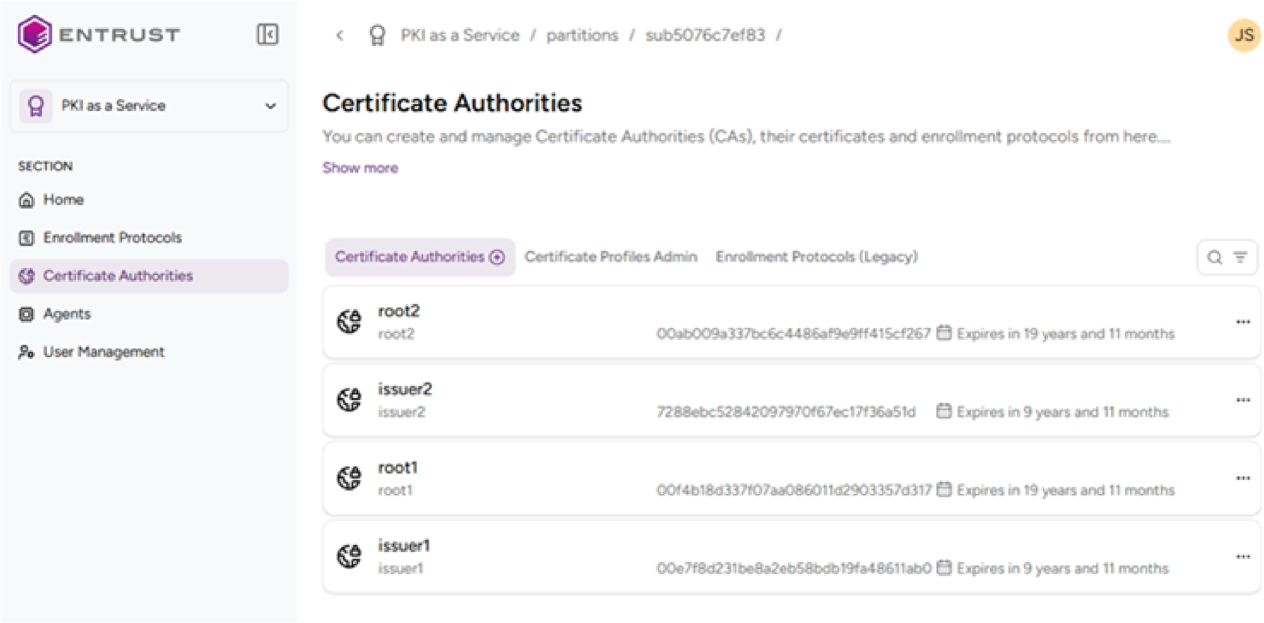
5. Click **Link Agent**.

Adding Active Directory nodes

Add the Windows Active Directory nodes for which to enroll certificates.

To add an Active Directory node:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the following roles:
   - Owners
   - Protocol Operators
2. Click **Certificate Authorities** in the sidebar.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

Show more

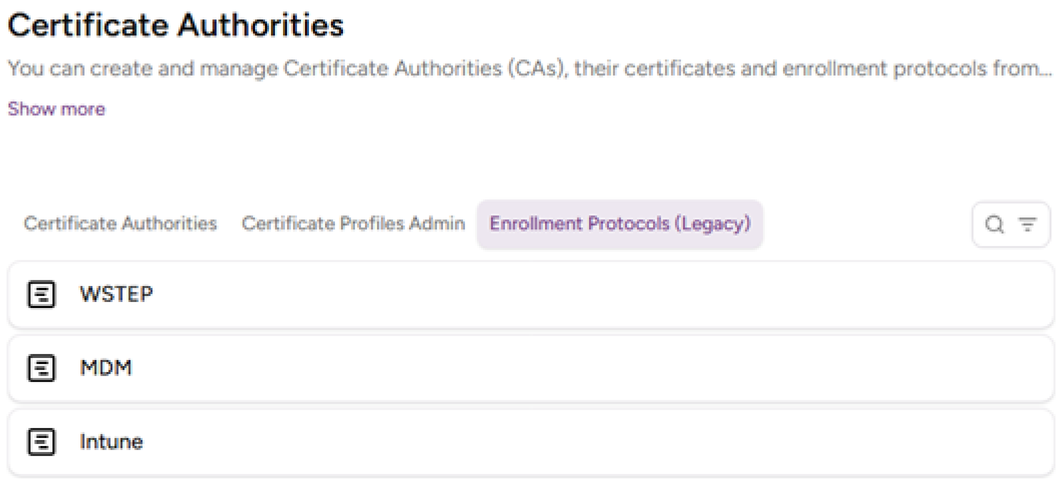
root2
root2 00ab009a337bc6c4486af9e9ff415cf267 Expires in 19 years and 11 months

issuer2
issuer2 7288ebc5284209797 0f67ec17f36a51d Expires in 9 years and 11 months

root1
root1 00f4b18d337f07aa086011d2903357d317 Expires in 19 years and 11 months

issuer1
issuer1 00e7f8d231be8a2eb58bdb19fa48611ab0 Expires in 9 years and 11 months

3. Make sure you have a subordinate CA with a profile of the wstep group. You can either:
    - Create a new issuing subordinate CA with this set, as explained in Creating an issuing subordinate CA.
    - Add this set to an existing CA, as explained in Selecting CA profiles.
4. Select the **Enrollment Protocols (Legacy)** tab.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from...

Show more

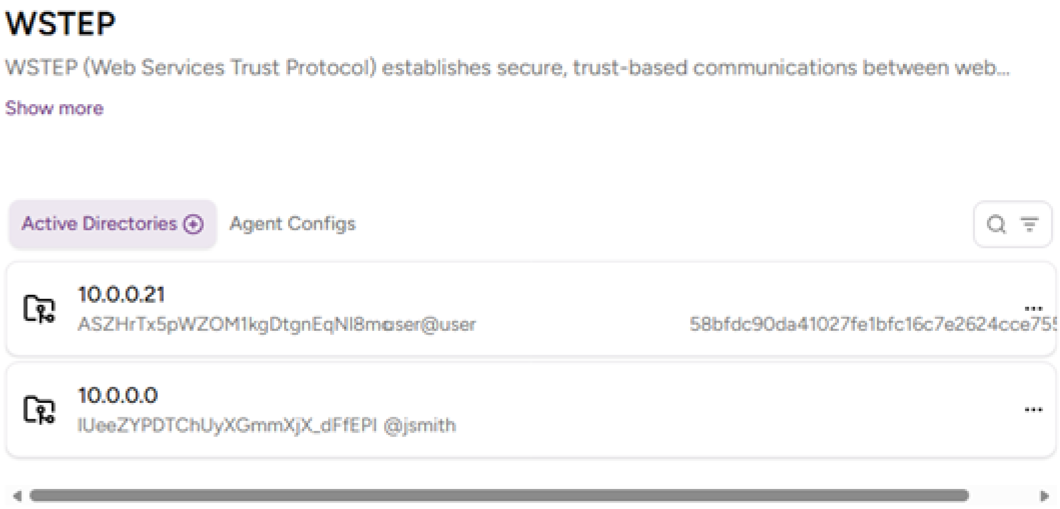
WSTEP

MDM

Intune

i Future releases will move all functionalities on this legacy tab to the **Enrollment Protocols** branch of the navigation tree.

5. Click **WSTEP** in the protocols list.
6. Click the plus **+** icon to the right of the **Active Directories** tab.



WSTEP

WSTEP (Web Services Trust Protocol) establishes secure, trust-based communications between web...

10.0.0.21
ASZHrTx5pWZOM1kgDtgnEqNl8moser@user   58bfdc90da41027fe1bfc16c7e2624cce75

10.0.0.0
lUeeZYPDTChUyXGmmXjX_dFfEPl @jsmith

7. Configure the following values.
   - Server
   - DNS Resolver
   - User
   - Password
   - LDAP Certificate Chain
   - CA Identifier
8. Click **Add**.
9. In the details of the new Active Directory, copy the value under **Certificate Enrollment Policy Server**. You will need this value when Enabling WSTEP for users.

Server

Enter an identifier for the Active Directory.

DNS Resolver

Enter the DNS resolver that the WSTEP agent will use to resolve domain names. Enter the DNS resolver in the following syntax:

```
<ip>[:<port>]
```

Where:

- `<ip>` is the IP address of the DNS server.
- `<port>` is the port of the DNS service (defaults to 53).

User

Enter the name of a user with administrative permissions in the Windows domain.

Password

Enter and confirm the password of the selected user.

LDAP Certificate Chain

Select a file containing the certificate chain of the Active Directory server.

CA Identifier

Select the issuing subordinate CA that will process the WSTEP enrollment requests.

ℹ This list only includes certificate authorities with profiles of the wstep group.

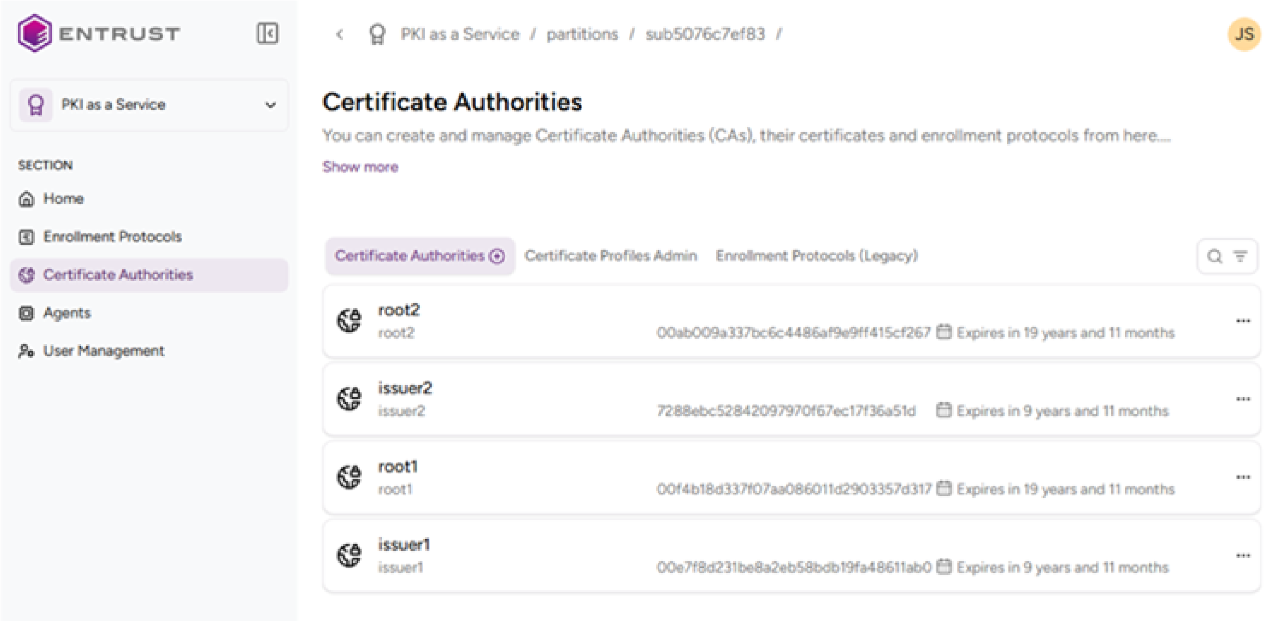
Getting the enrollment URL

When Enabling WSTEP for users on your Windows domain you will need the URL of the Certificate Enrollment Policy Server. See below for how to obtain this URL.

ℹ Skip this section if you already copied this URL when Adding Active Directory nodes.

To get the WSTEP enrollment URL:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the following roles:
   - Owners
   - Protocol Operators
2. Click **Certificate Authorities** in the sidebar.


ENTRUST
PKI as a Service
SECTION
Home
Enrollment Protocols
Certificate Authorities
Agents
User Management
PKI as a Service / partitions / sub5076c7ef83 /
JS
Certificate Authorities ⊕
Certificate Profiles Admin
Enrollment Protocols (Legacy)

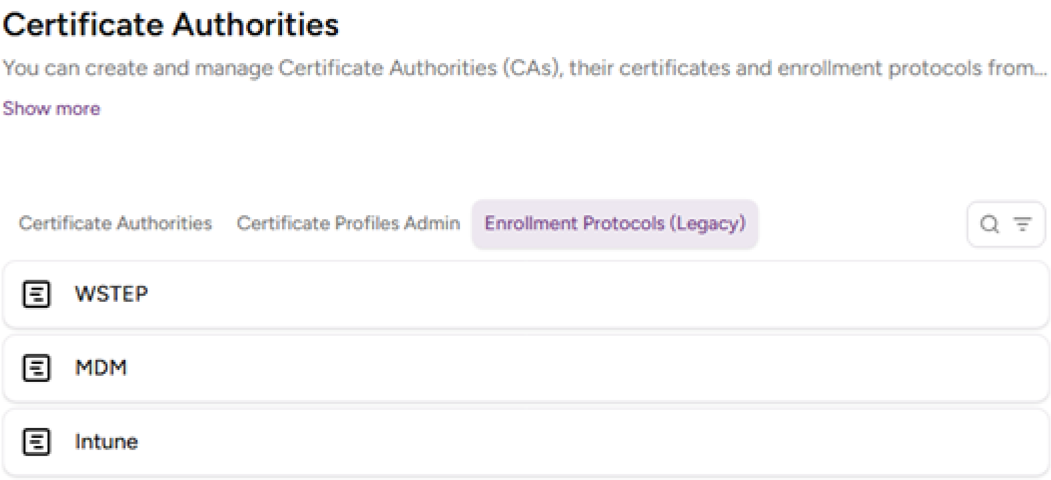
Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

Show more

root2 root2	00ab009a337bc6c4486af9e9ff415cf267	Expires in 19 years and 11 months
issuer2 issuer2	7288ebc52842097970f67ec17f36a51d	Expires in 9 years and 11 months
root1 root1	00f4b18d337f07aa086011d2903357d317	Expires in 19 years and 11 months
issuer1 issuer1	00e7f8d231be8a2eb58bdb19fa48611ab0	Expires in 9 years and 11 months

3. Select the **Enrollment Protocols** tab.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from...

Show more

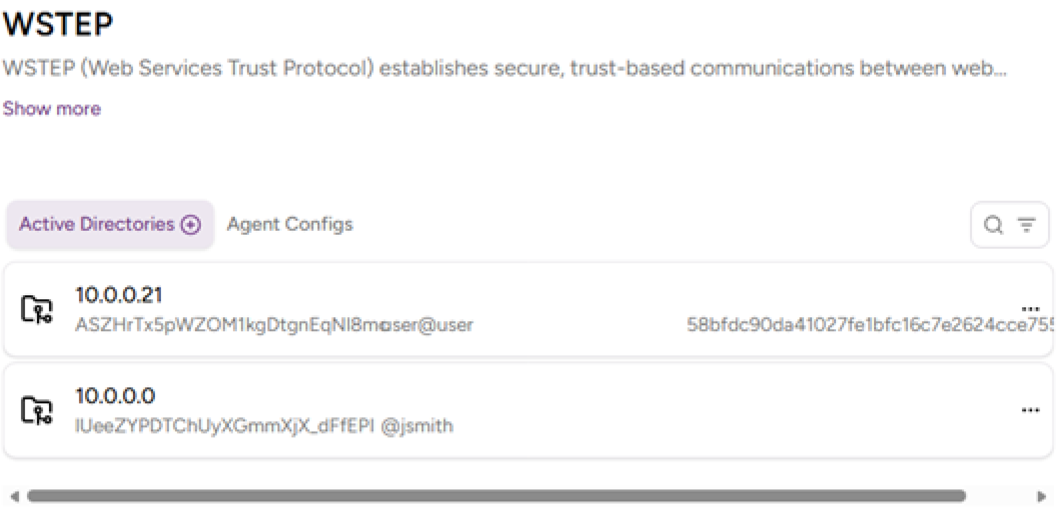
WSTEP

MDM

Intune

4. Click **WSTEP** in the protocols list.

5. In the **Active Directories** tab, click domain the Active Directory for which to obtain the WSTEP enrollment URL.



WSTEP

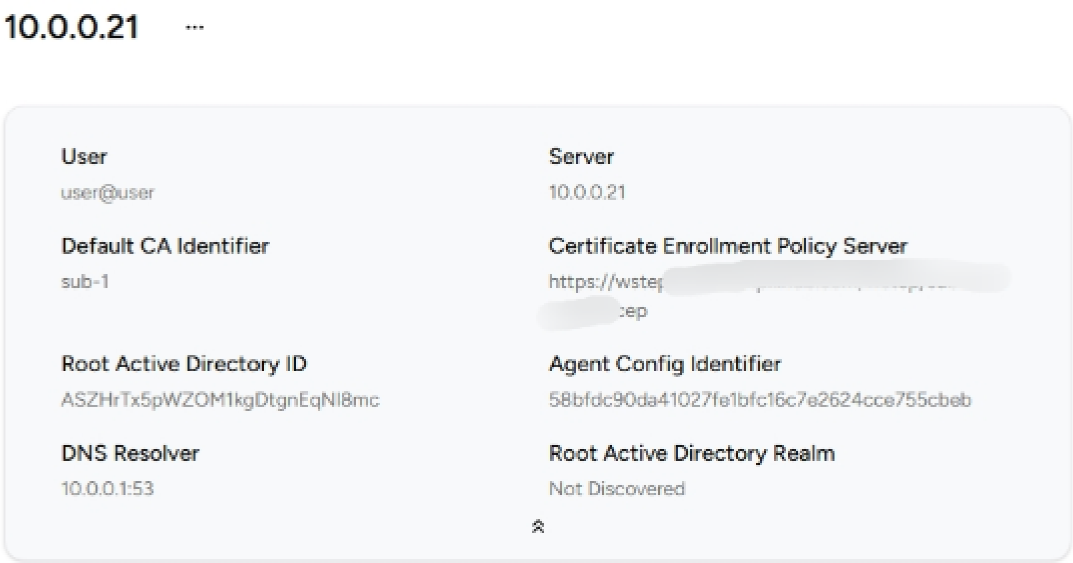
WSTEP (Web Services Trust Protocol) establishes secure, trust-based communications between web...

Show more

10.0.0.21
ASZHrTx5pWZOM1kgDtgnEqNI8mcuser@user 58bfdc90da41027fe1bfc16c7e2624cce75

10.0.0.0
lUeeZYPDTChUyXGmmXjX_dFfEPl @jsmith

6. Expand the domain details and copy the URL under **Certificate Enrollment Policy Server**.



10.0.0.21

User
user@user

Server
10.0.0.21

Default CA Identifier
sub-1

Certificate Enrollment Policy Server
https://wstep[redacted]cep

Root Active Directory ID
ASZHrTx5pWZOM1kgDtgnEqNI8mc

Agent Config Identifier
58bfdc90da41027fe1bfc16c7e2624cce755cbeb

DNS Resolver
10.0.0.1:53

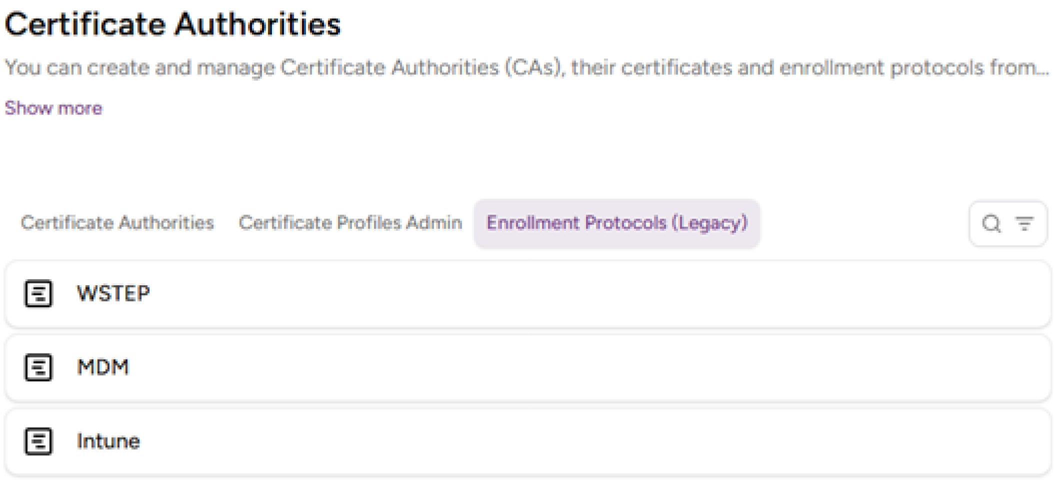
Root Active Directory Realm
Not Discovered

Enabling WSTEP for Active Directory nodes

Enable WSTEP enrollment for the Active Directory nodes configured in Adding Active Directory nodes.

To enable WSTEP for an Active Directory node:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the following roles:
   - Owners
   - Protocol Operators
2. Click **Certificate Authorities** in the sidebar.
3. Select the **Enrollment Protocols** tab.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from...

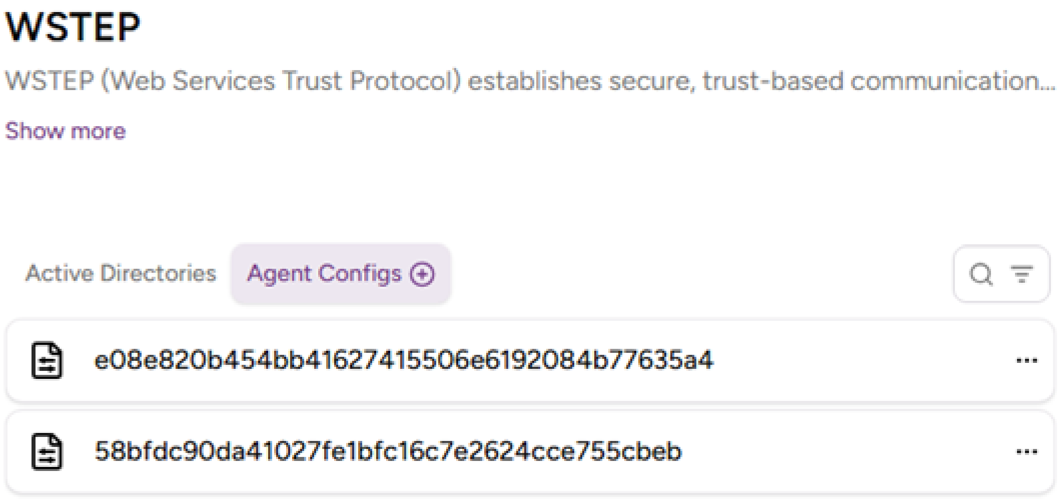
Show more

WSTEP

MDM

Intune

4. Click **WSTEP** in the protocols list.
5. Select the **Agent Configs** tab.



WSTEP

WSTEP (Web Services Trust Protocol) establishes secure, trust-based communication...

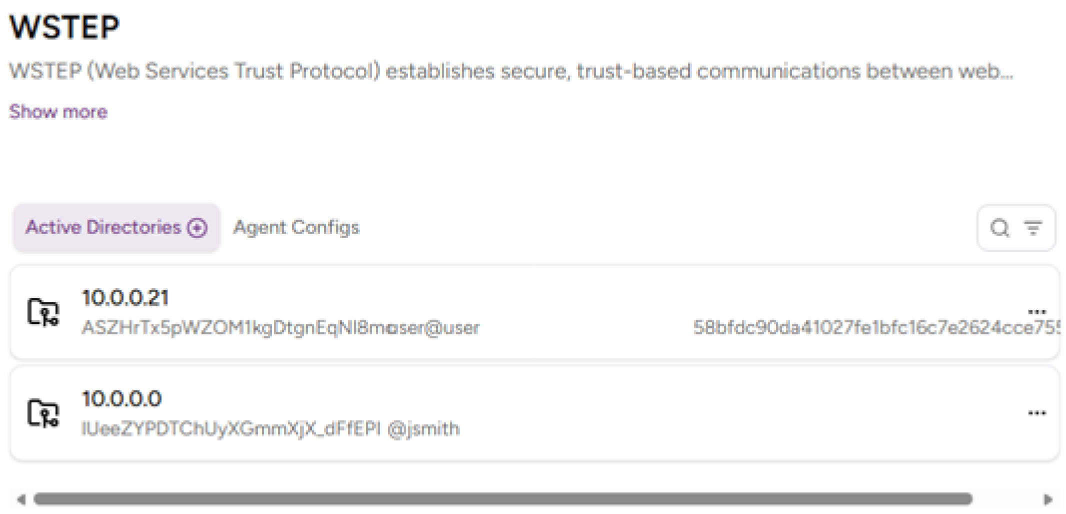
Show more

e08e820b454bb41627415506e6192084b77635a4 ···

58bfdc90da41027fe1bfc16c7e2624cce755cbeb ···

6. Click the plus **+** icon to the right of **Agent Configs**.
7. Select one of the configurations added when Creating an agent configuration.
8. Click **Enable**.

9. Select the **Active Directories** tab.



WSTEP

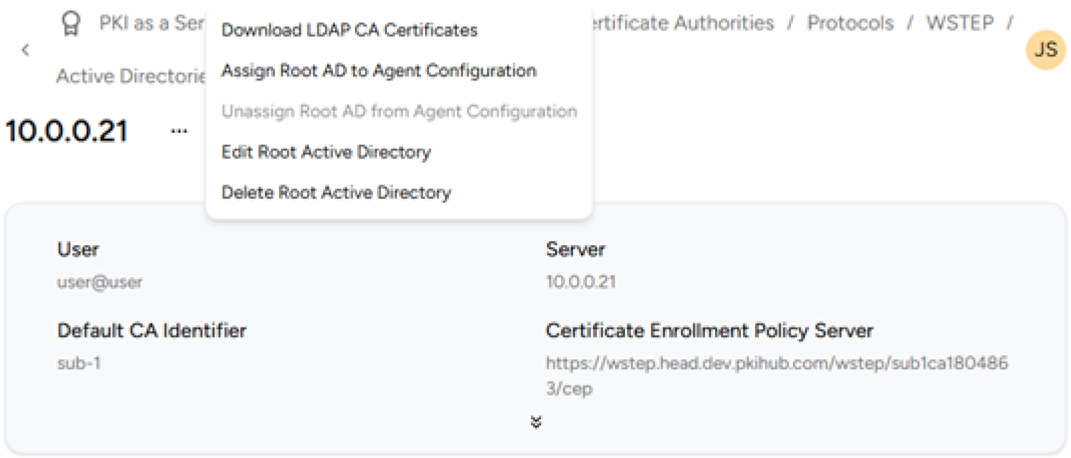
WSTEP (Web Services Trust Protocol) establishes secure, trust-based communications between web...

Show more

10.0.0.21
ASZHrTx5pWZOM1kgDtgnEqNl8mœser@user
58bfdc90da41027fe1bfc16c7e2624cce75

10.0.0.0
lUeeZYPDTChUyXGmmXjX_dFfEPl @jsmith

10. Select the Active Directory node you previously added in Adding Active Directory nodes.



PKI as a Ser
rtificate Authorities / Protocols / WSTEP /
Active Directorie
JS
Download LDAP CA Certificates
Assign Root AD to Agent Configuration
Unassign Root AD from Agent Configuration
Edit Root Active Directory
Delete Root Active Directory

10.0.0.21

User
user@user

Server
10.0.0.21

Default CA Identifier
sub-1

Certificate Enrollment Policy Server
https://wstep.head.dev.pkihub.com/wstep/sub1ca1804863/cep

11. Click the three buttons right to the Active Directory name and select **Assign Root AD to Agent Configuration**.

12. In the **Assign Root AD to Agent Configuration** dialog, select the configuration previously created in Creating an agent configuration.

13. Click **Assign**.

Enabling WSTEP for users and devices

Enable WSTEP enrollment and autoenrollment for users and devices.

- Creating a Group Policy Object
- Importing the WSTEP certificate chain
- Enabling WSTEP for users
- Enabling autoenrollment for users
- Enabling WSTEP for devices
- Enabling autoenrollment for devices
- Linking the WSTEP Group Policy Object

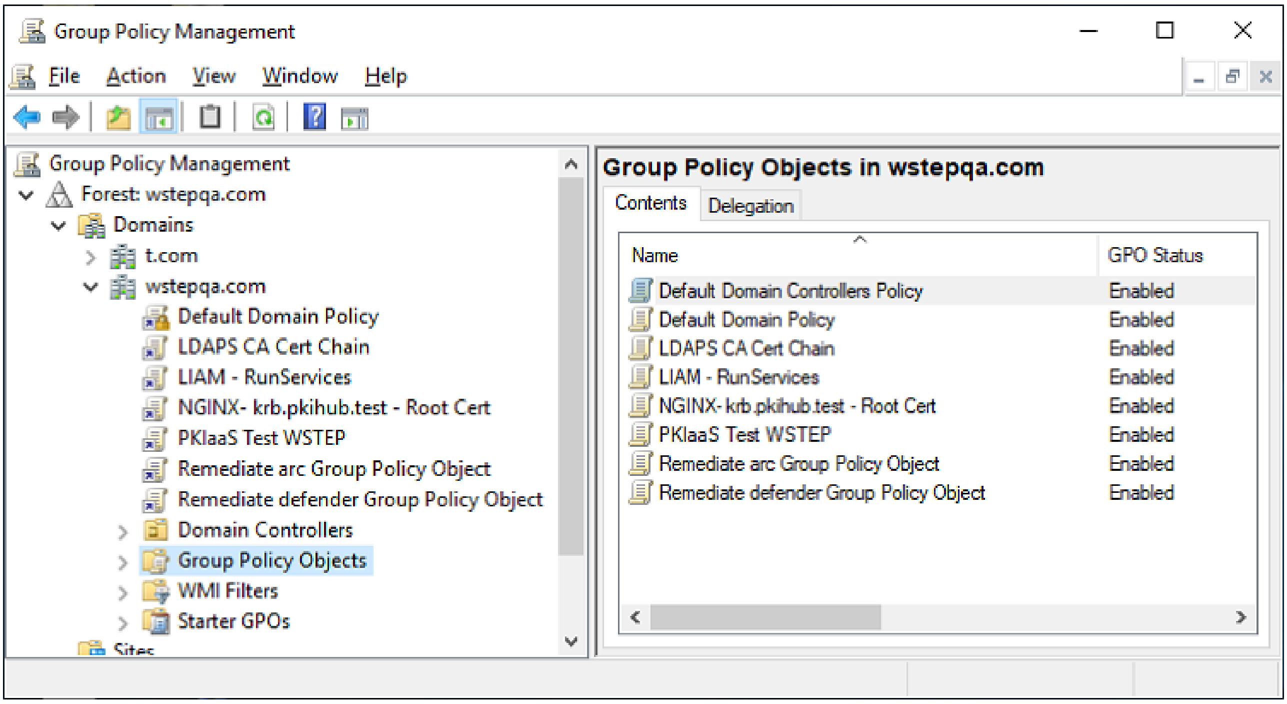
Creating a Group Policy Object

The recommended method to configure a certificate chain trust is to create a Group Policy Object (GPO) linked to all domains in the Active Directory forest.

To create a Group Policy Object:

1. Log in to the root Active Directory of the forest as an Active Directory administrator.

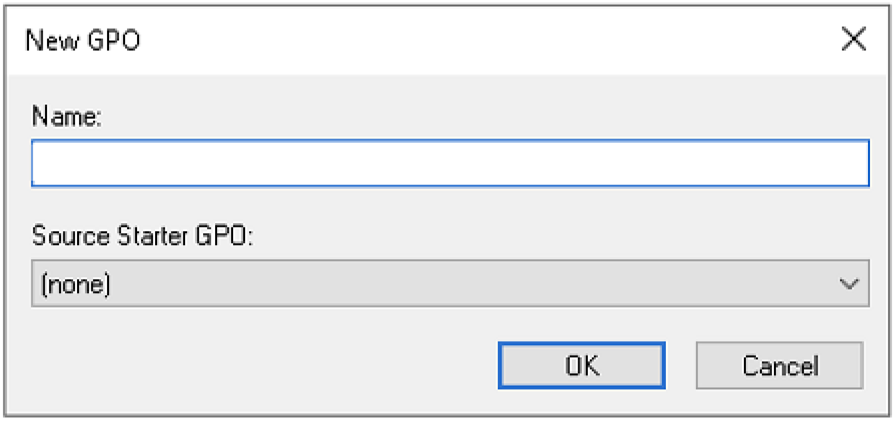
2. Select **Start > Windows Administrative Tools > Group Policy Management** to open the **Group Policy Management** dialog.



Group Policy Objects in wstepqa.com

Name	GPO Status
Default Domain Controllers Policy	Enabled
Default Domain Policy	Enabled
LDAPS CA Cert Chain	Enabled
LIAM - RunServices	Enabled
NGINX- krb.pkihub.test - Root Cert	Enabled
PKIaaS Test WSTEP	Enabled
Remediate arc Group Policy Object	Enabled
Remediate defender Group Policy Object	Enabled

3. Under the root domain, right-click the **Group Policy Objects** folder and select New to display the **New GPO** dialog.



Name:

Source Starter GPO:
(none)

4. Provide a new **Name** for the GPO and click **OK**.

Importing the WSTEP certificate chain

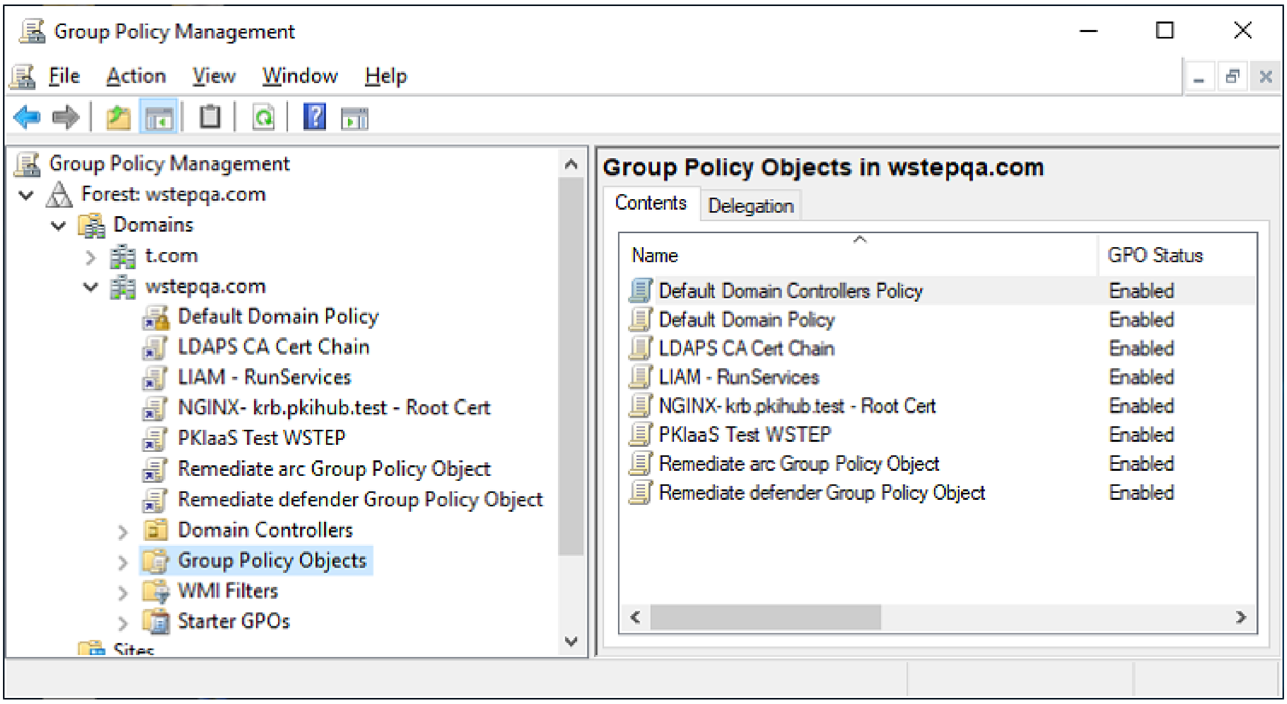
Import the WSTEP certificate chain into the GPO previously created in Creating a Group Policy Object.

ℹ See Downloading the certificate chain for how to download the required certificates.

To import the certificate chain into the GPO:

1. Log in to the root Active Directory of the forest as an Active Directory administrator.

2. Select **Start** > **Windows Administrative Tools** > **Group Policy Management** to open the **Group Policy Management** dialog.



Group Policy Management
Forest: wstepqa.com
Domains
t.com
wstepqa.com
Default Domain Policy
LDAPS CA Cert Chain
LIAM - RunServices
NGINX- krb.pkihub.test - Root Cert
PKIaaS Test WSTEP
Remediate arc Group Policy Object
Remediate defender Group Policy Object
Domain Controllers
Group Policy Objects
WMI Filters
Starter GPOs
Sites

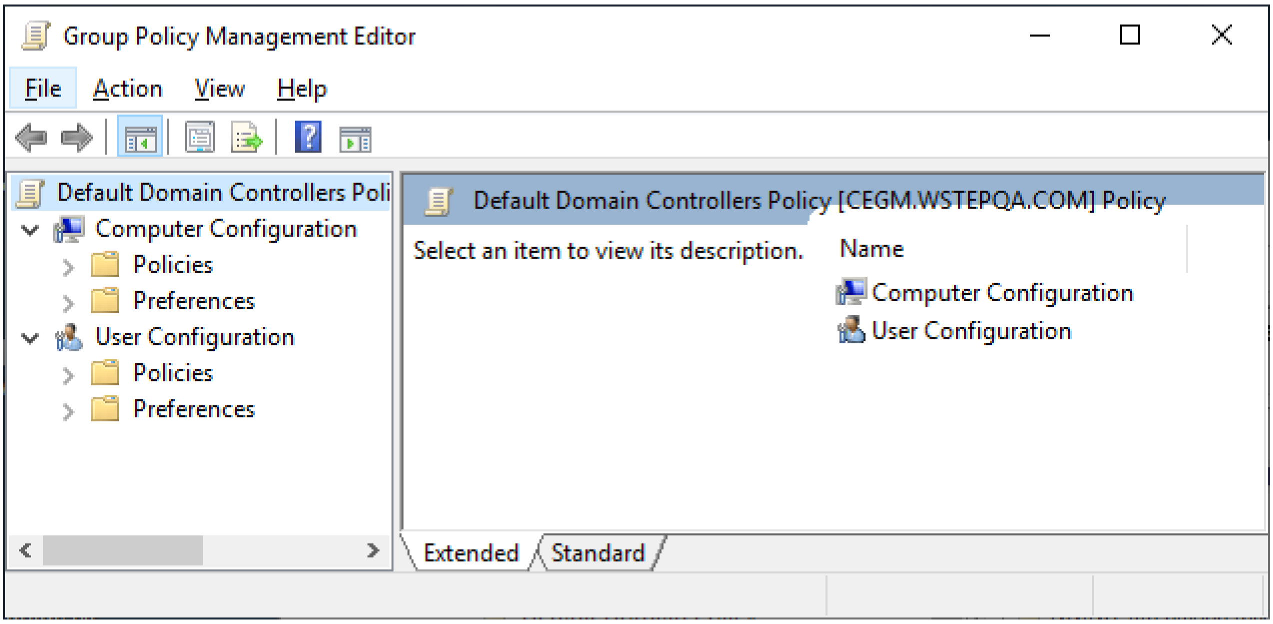
Group Policy Objects in wstepqa.com

Contents | Delegation

Name	GPO Status
Default Domain Controllers Policy	Enabled
Default Domain Policy	Enabled
LDAPS CA Cert Chain	Enabled
LIAM - RunServices	Enabled
NGINX- krb.pkihub.test - Root Cert	Enabled
PKIaaS Test WSTEP	Enabled
Remediate arc Group Policy Object	Enabled
Remediate defender Group Policy Object	Enabled

3. Right-click the Group Policy Object.

4. Select **Edit** to display the **Group Policy Management Editor**.



Default Domain Controllers Poli
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences

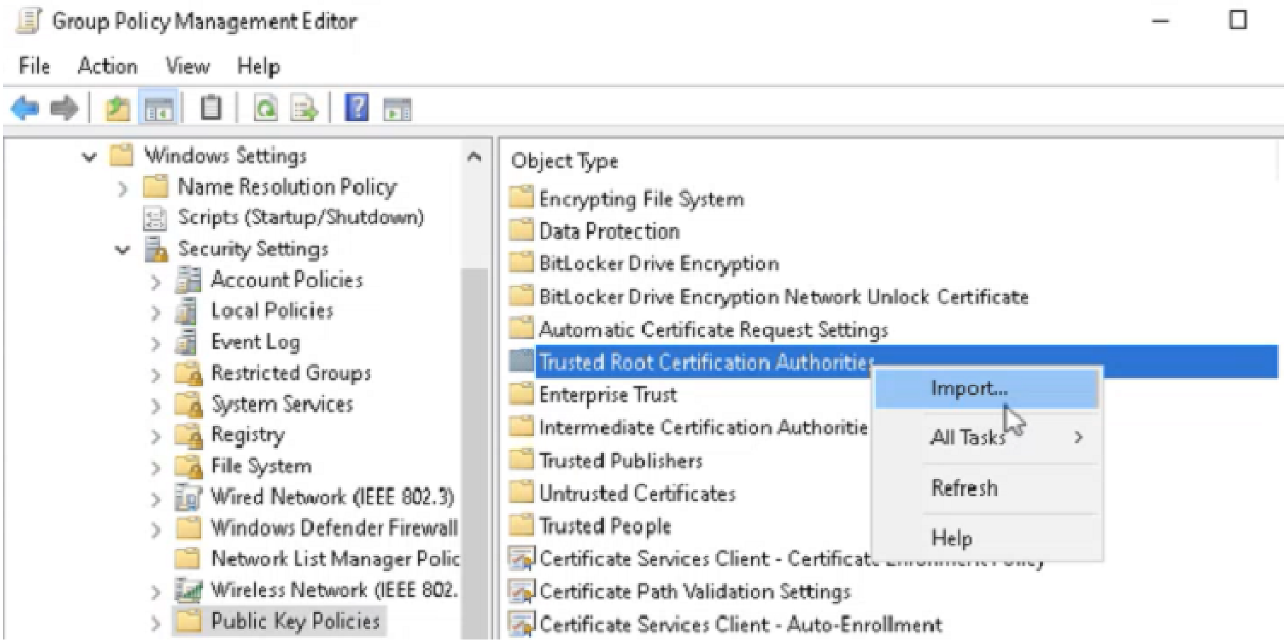
Default Domain Controllers Policy [CEGM.WSTEPQA.COM] Policy

Select an item to view its description.

Name
Computer Configuration
User Configuration

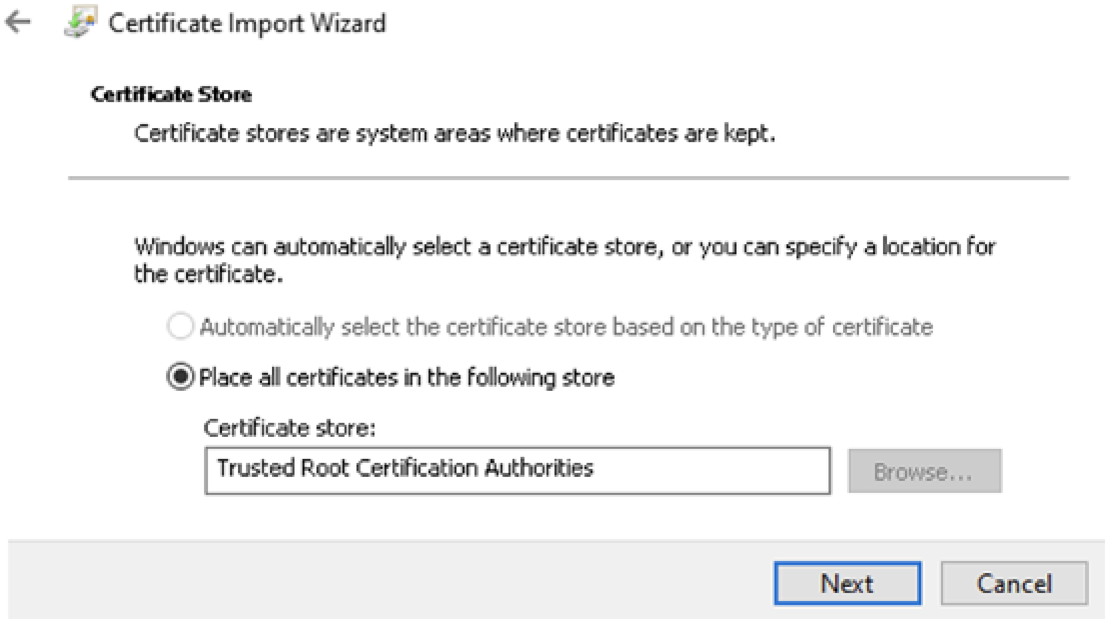
5. Navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**.

6. Right-click **Trusted Root Certificate Authorities** and select **Import**.


Group Policy Management Editor
File
Action
View
Help
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3)
Windows Defender Firewall
Network List Manager Polic
Wireless Network (IEEE 802.
Public Key Policies
Object Type
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock Certificate
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authoritie
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificat
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment
Import...
All Tasks
Refresh
Help

7. In the **Certificate Import Wizard**, click **Next** and select the root CA certificate file to import.

8. Click **Next** to reveal the **Certificate Store** settings.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

9. Verify that the selected certificate store is **Trusted Root Certification Authorities**.

10. Click **Next** to display the **Completing the Certificate Import Wizard**.

11. Click **Finish** to return to the **Group Policy Management** dialog.

12. In the **Group Policy Management** dialog, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.

13. Right-click **Intermediate Certificate Authorities** and select **Import** to display the **Certificate Import Wizard**.

14. Click **Next** and select the issuing CA certificate file to import.

15. Click **Next** to reveal the Certificate Store settings.

16. Verify that the selected certificate store is **Intermediate Certification Authorities**.

17. Click **Finish**.

18. Select **File > Exit** to close the **Group Policy Management Editor**.

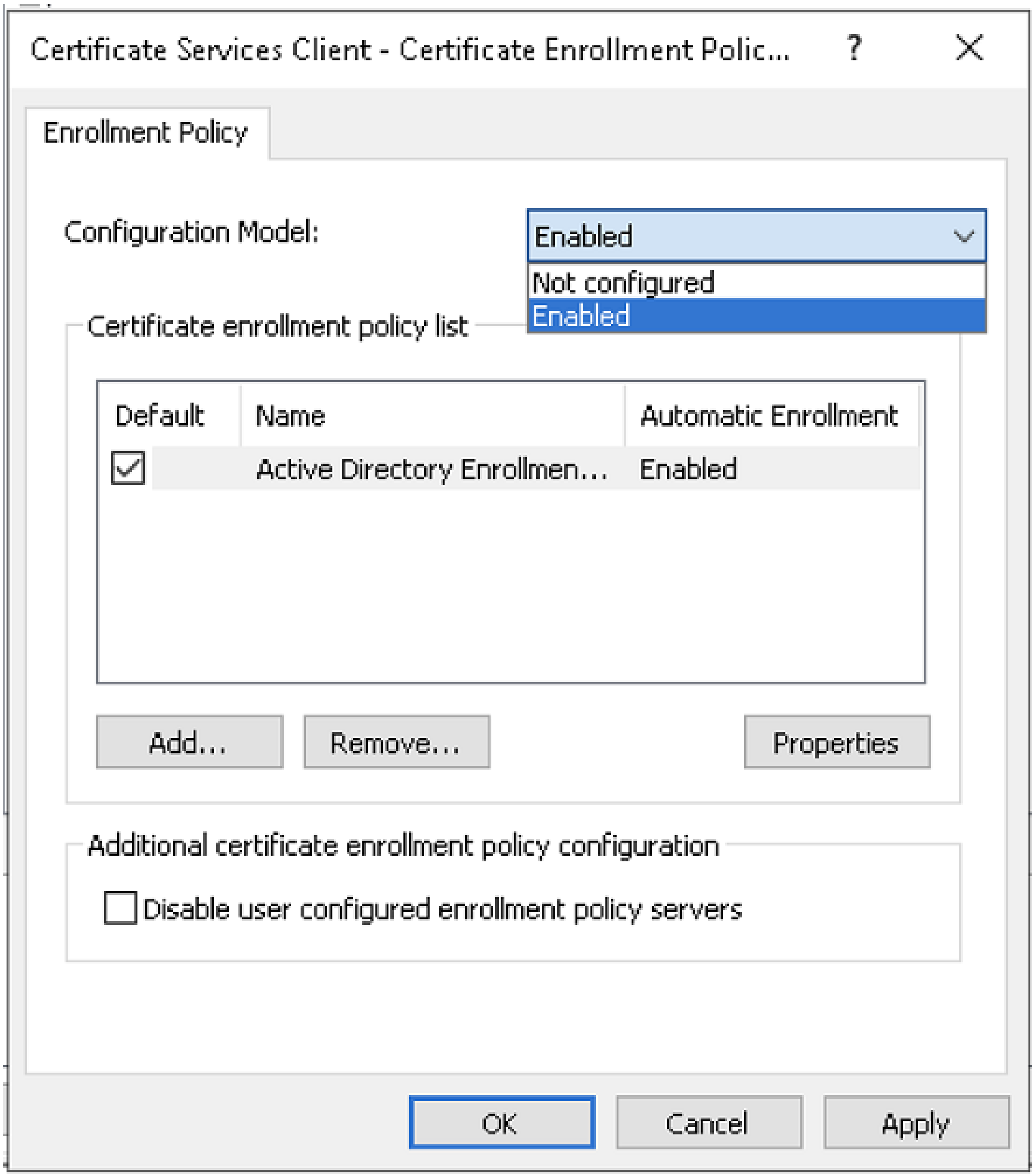
Enabling WSTEP for users

Configure the WSTEP to enable WSTEP for users.

To enable WSTEP for users:

1. In the navigation tree of the new WSTEP Group Policy Object, expand **User Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.

2. In the content pane, right-click **Certificate Services Client - Certificate Enrollment Policy** and select **Properties** to display the **Certificate Services Client - Certificate Enrollment Policy Properties** dialog box.



Certificate Services Client - Certificate Enrollment Polic...

Enrollment Policy

Configuration Model: Enabled

Not configured
Enabled

Certificate enrollment policy list

Default	Name	Automatic Enrollment
☑	Active Directory Enrollmen...	Enabled

Additional certificate enrollment policy configuration

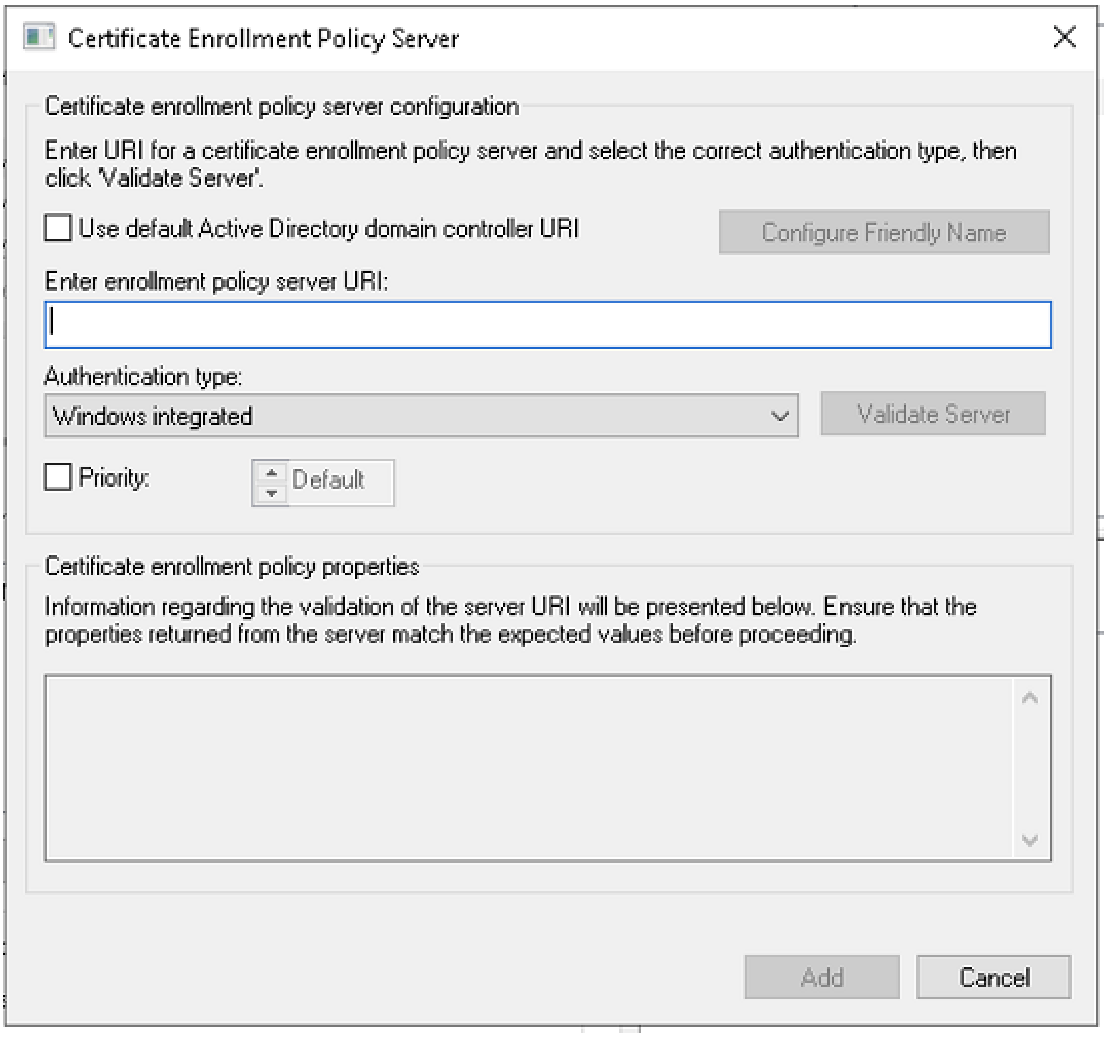
☐ Disable user configured enrollment policy servers

3. Select **Enabled** in the **Configuration Model** drop-down list.

⚠ If you are not installing WSTEP alongside an existing Microsoft CA WSTEP, select **Active Directory Enrollment** in the **Certificate enrollment policy list** pane, and click **Remove**.

---

4. Click **Add** to display the **Certificate Enrollment Policy Server** dialog box.



Certificate Enrollment Policy Server

Certificate enrollment policy server configuration

Enter URI for a certificate enrollment policy server and select the correct authentication type, then click 'Validate Server'.

□ Use default Active Directory domain controller URI

Enter enrollment policy server URI:

Authentication type: Windows integrated

□ Priority: Default

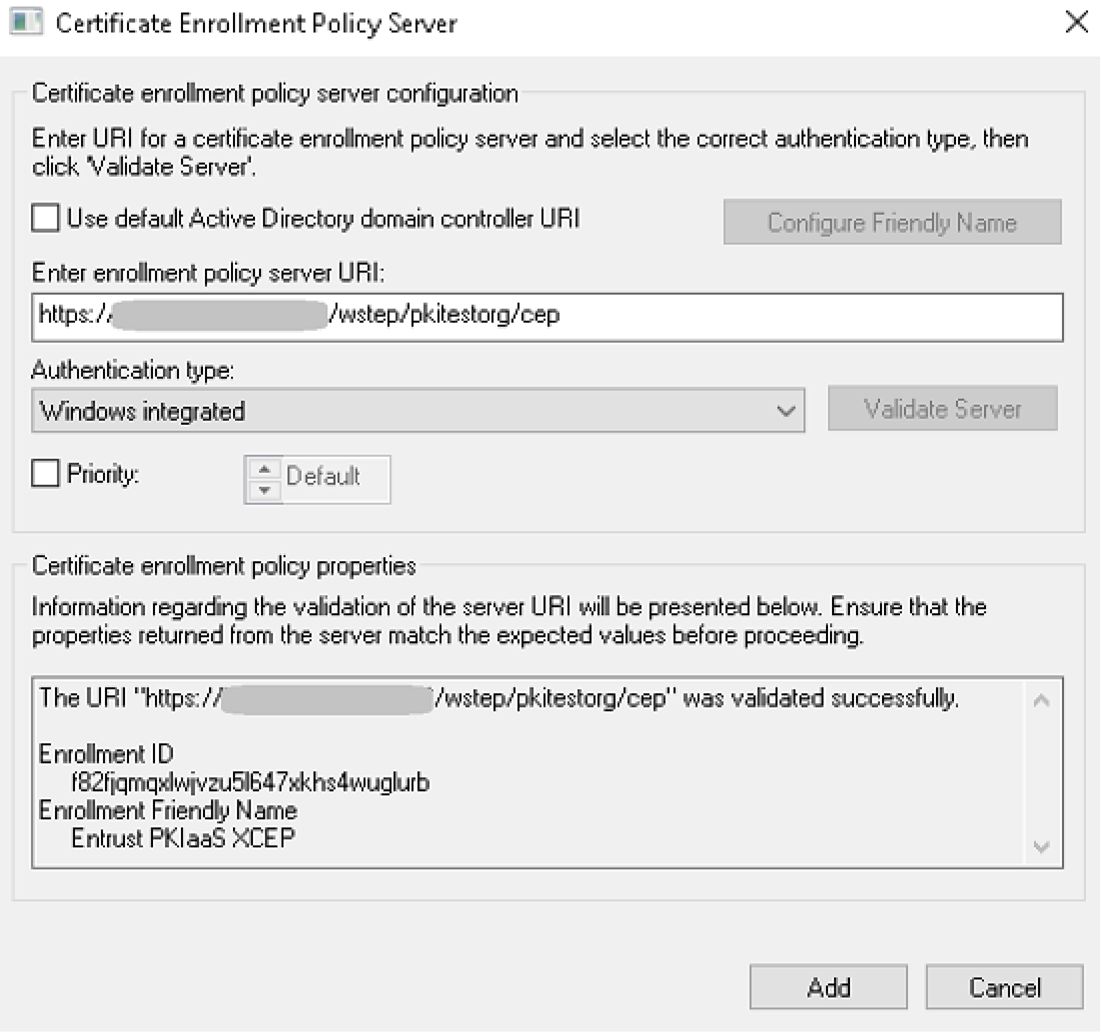
Certificate enrollment policy properties

Information regarding the validation of the server URI will be presented below. Ensure that the properties returned from the server match the expected values before proceeding.

5. In the **Enter enrollment policy server URI** field, enter the WSTEP URI you obtained when either:
   - Adding Active Directory nodes
   - Getting the enrollment URL

6. In the **Authentication type** drop-down list, select the same "Windows Integrated" option (should be selected by default).

7. Click **Validate Server** and check the URI validation results.



Certificate Enrollment Policy Server

Certificate enrollment policy server configuration

Enter URI for a certificate enrollment policy server and select the correct authentication type, then click 'Validate Server'.

□ Use default Active Directory domain controller URI

Enter enrollment policy server URI:

https://[redacted]/wstep/pkitestorg/cep

Authentication type: Windows integrated

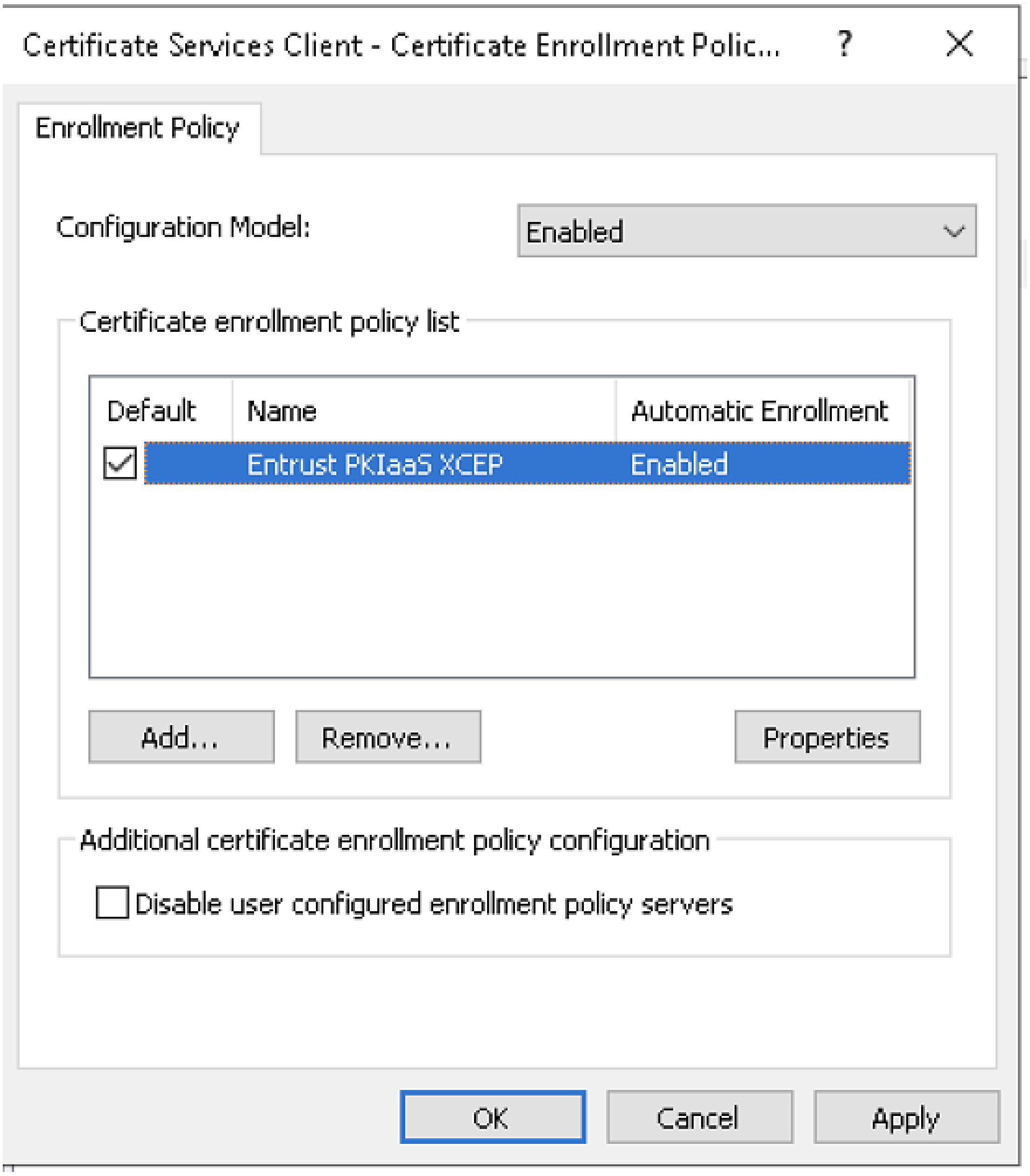
□ Priority: Default

Certificate enrollment policy properties

Information regarding the validation of the server URI will be presented below. Ensure that the properties returned from the server match the expected values before proceeding.

```
The URI "https://[redacted]/wstep/pkitestorg/cep" was validated successfully.

Enrollment ID
    f82fjqmqxlwjvzu5l647xkhs4wuglurb
Enrollment Friendly Name
    Entrust PKIaaS XCEP
```

8. Click **Add** to add the new WSTEP service to the **Certificate enrollment policy list** pane.



Certificate Services Client - Certificate Enrollment Polic...

Enrollment Policy

Configuration Model: Enabled

Certificate enrollment policy list

Default	Name	Automatic Enrollment
☑	Entrust PKIaaS XCEP	Enabled

Additional certificate enrollment policy configuration

□ Disable user configured enrollment policy servers

9. In the **Certificate enrollment policy** list pane, check the box of the new **Entrust PKIaaS XCEP** certificate enrollment policy to make it the default one.

10. Click **OK**.

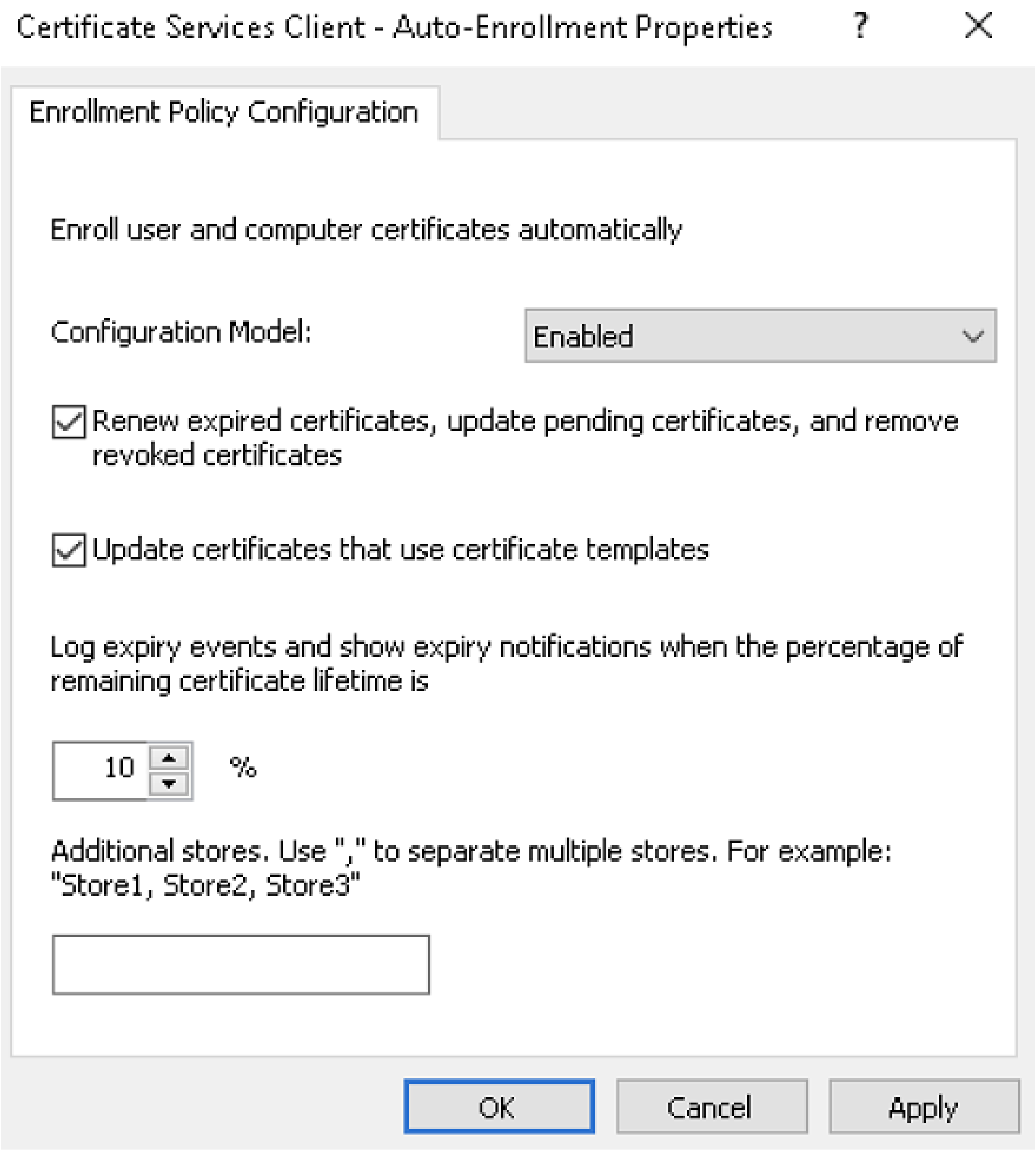
Enabling autoenrollment for users

Configure the WSTEP Group Policy Object to enable autoenrollment for users.

To enable autoenrollment for users:

1. In the navigation tree of the new WSTEP Group Policy Object, expand **User Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**.

2. In the content pane, right-click **Certificate Services Client Auto Enrollment** and select **Properties to display the Certificate Services Client Auto-Enrollment Properties** dialog box.



Certificate Services Client - Auto-Enrollment Properties

Enrollment Policy Configuration

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

☑ Update certificates that use certificate templates

Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is

10 %

Additional stores. Use "," to separate multiple stores. For example: "Store1, Store2, Store3"

3. Select **Enabled** in the **Configuration Model** drop-down list.

4. Check the following boxes:

   - **Renew expired certificates, update pending certificates, and remove revoked certificates**
   - **Update certificates that use certificate templates**

5. Optionally, change the percentage under **Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is**.

6. Click **OK**.

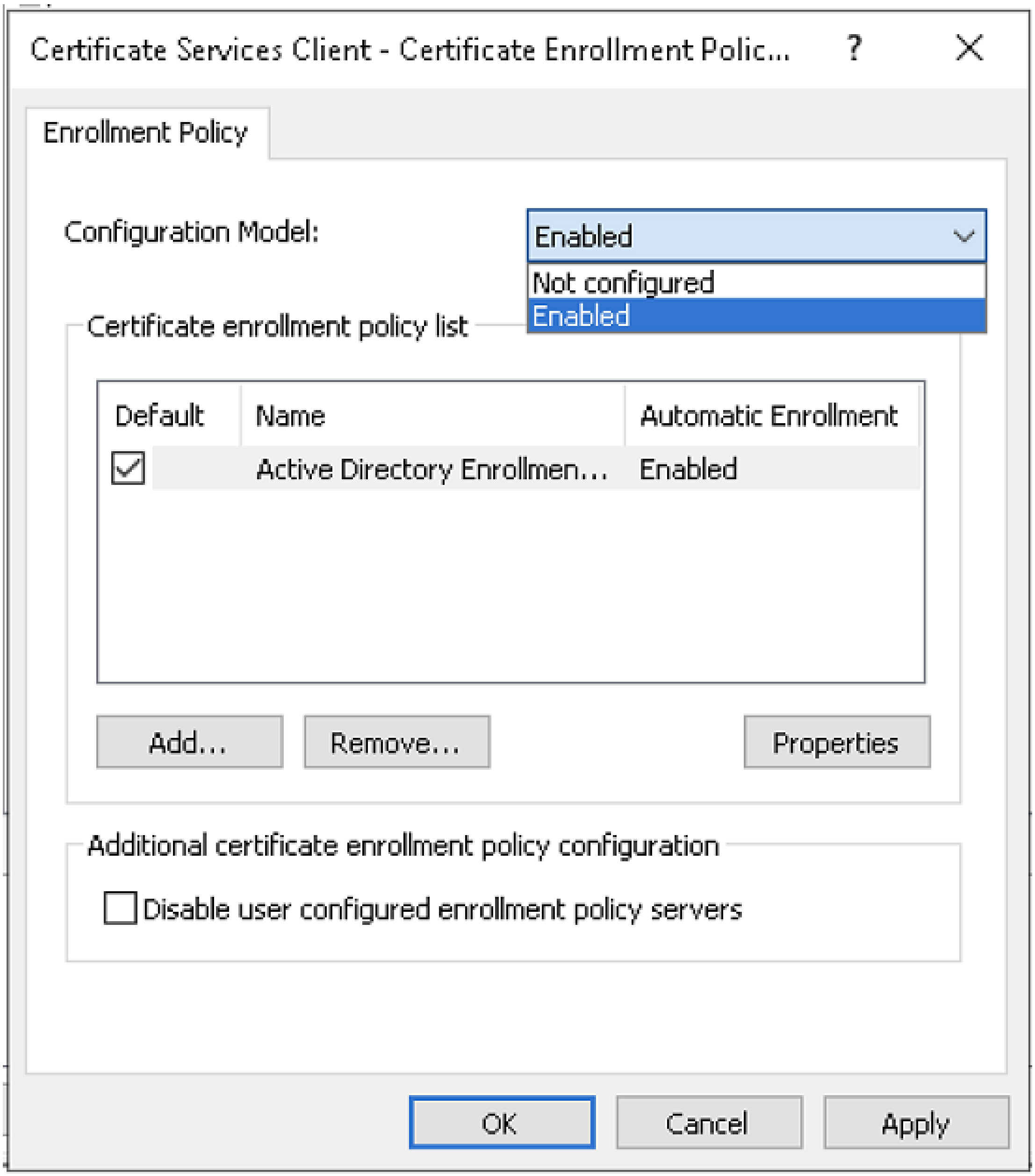
Enabling WSTEP for devices

Configure the Entrust PKIaaS WSTEP to enable WSTEP for devices.

To enable WSTEP for devices:

1. In the navigation tree of the new Entrust PKIaaS WSTEP Group Policy Object, expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**.

2. In the content pane, right-click **Certificate Services Client - Certificate Enrollment Policy** and select **Properties** to display the **Certificate Services Client - Certificate Enrollment Policy Properties** dialog box.



Certificate Services Client - Certificate Enrollment Polic...

Enrollment Policy

Configuration Model: Enabled

Certificate enrollment policy list

Default	Name	Automatic Enrollment
☑	Active Directory Enrollmen...	Enabled

Additional certificate enrollment policy configuration

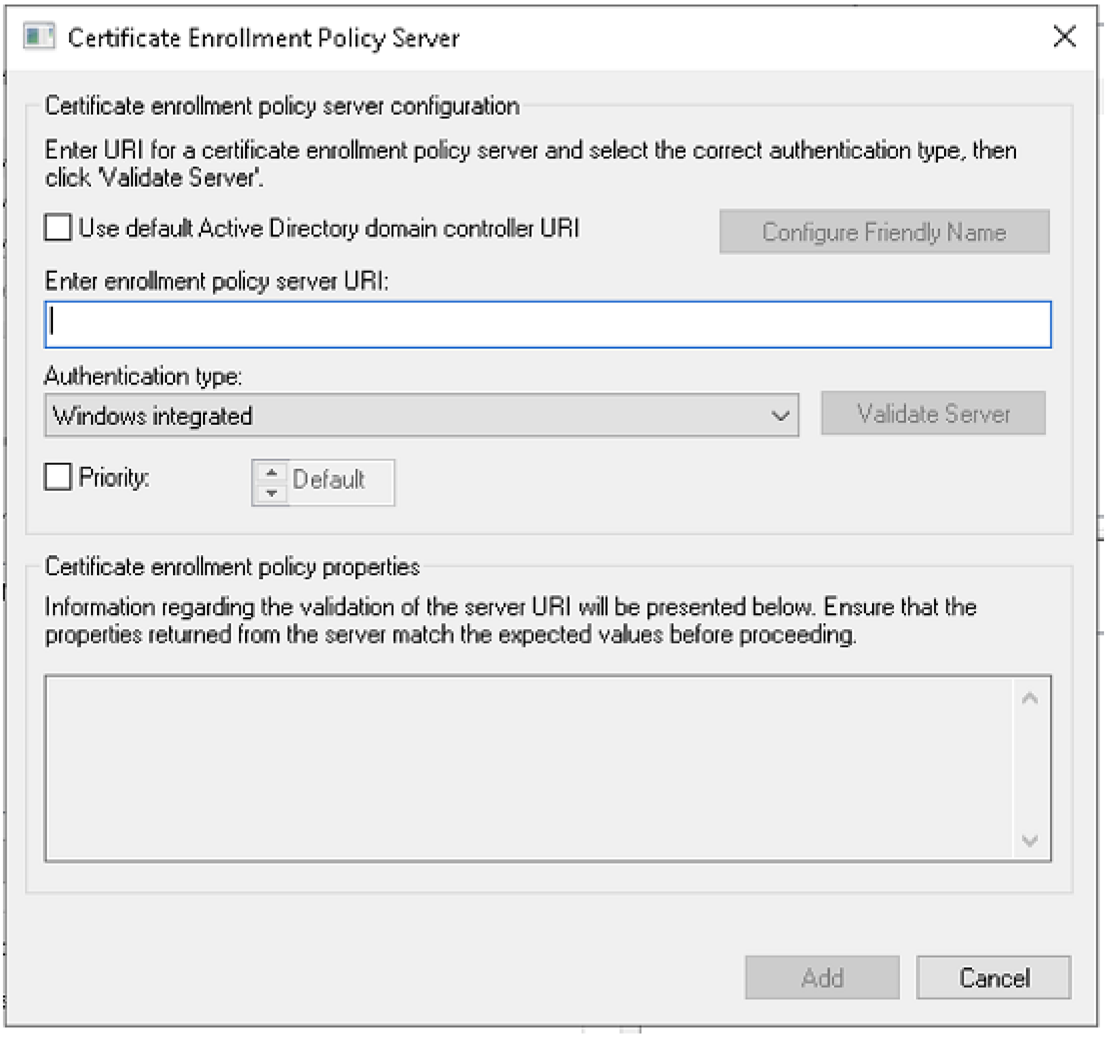
□ Disable user configured enrollment policy servers

3. Select **Enabled** in the **Configuration Model** drop-down list.

⚠ If you are not installing WSTEP alongside an existing Microsoft CA WSTEP, select **Active Directory Enrollment** in the **Certificate enrollment policy list** pane, and click **Remove**.

---

4. Click **Add** to display the **Certificate Enrollment Policy Server** dialog box.



Certificate Enrollment Policy Server

Certificate enrollment policy server configuration

Enter URI for a certificate enrollment policy server and select the correct authentication type, then click 'Validate Server'.

□ Use default Active Directory domain controller URI

Enter enrollment policy server URI:

Authentication type: Windows integrated

□ Priority: Default

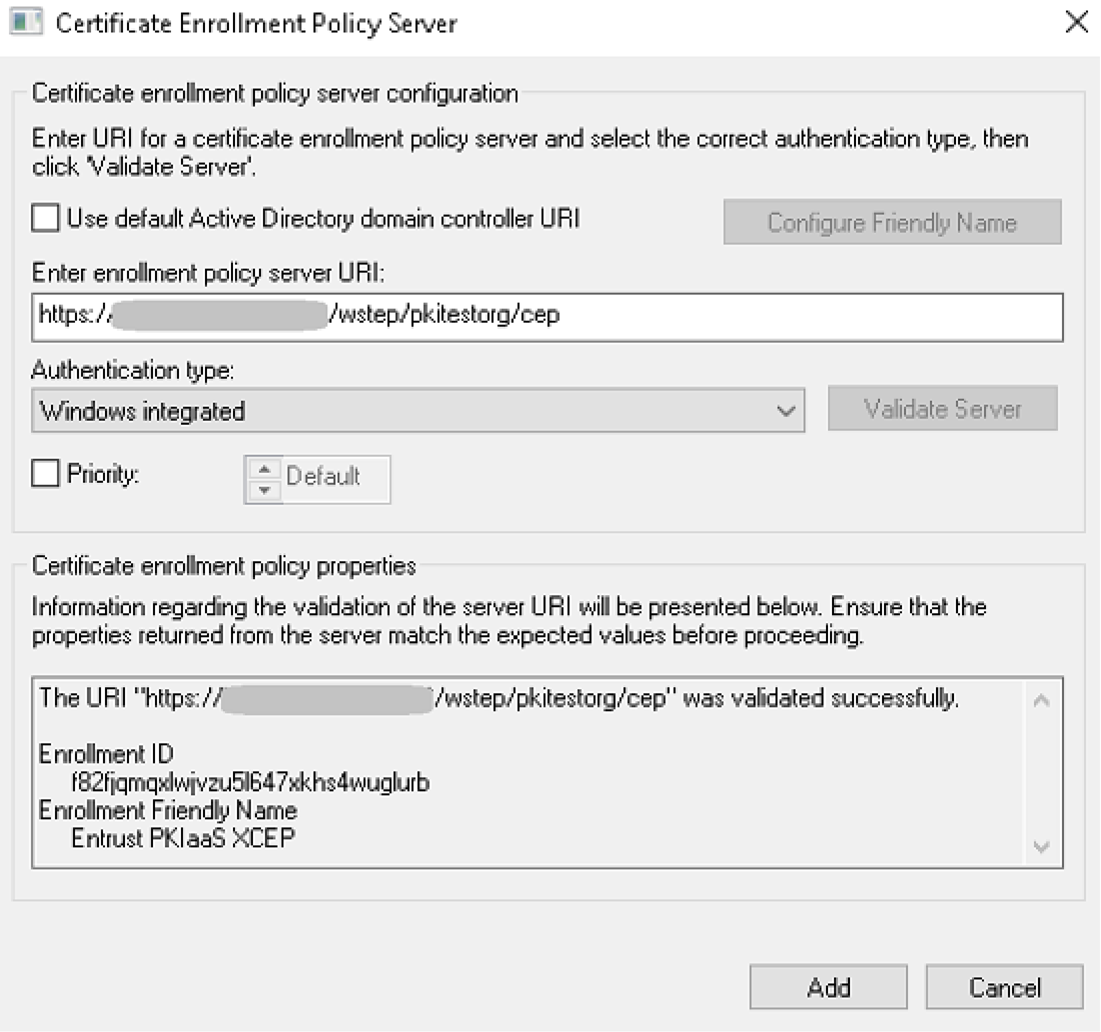
Certificate enrollment policy properties

Information regarding the validation of the server URI will be presented below. Ensure that the properties returned from the server match the expected values before proceeding.

5. In the **Enter enrollment policy server URI** field, enter the WSTEP URI provided on the PKIaaS portal for device enrollment.

6. In the **Authentication type** drop-down list, select the same "Windows Integrated" option (should be selected by default).

7. Click **Validate Server** and check the URI validation results.



Certificate Enrollment Policy Server

Certificate enrollment policy server configuration

Enter URI for a certificate enrollment policy server and select the correct authentication type, then click 'Validate Server'.

□ Use default Active Directory domain controller URI

Enter enrollment policy server URI:
https://[redacted]/wstep/pkitestorg/cep

Authentication type:
Windows integrated

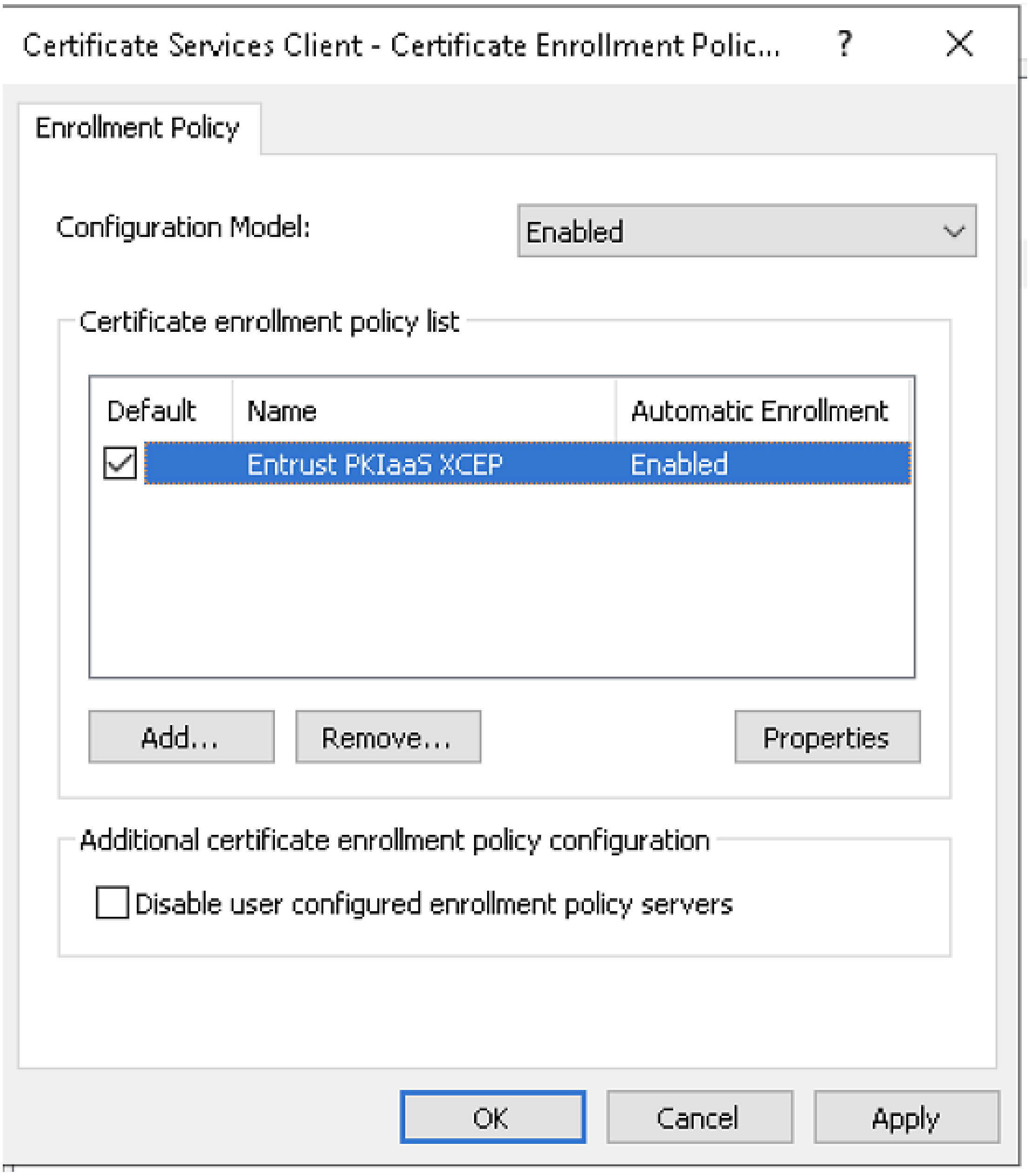
□ Priority: Default

Certificate enrollment policy properties

Information regarding the validation of the server URI will be presented below. Ensure that the properties returned from the server match the expected values before proceeding.

```
The URI "https://[redacted]/wstep/pkitestorg/cep" was validated successfully.

Enrollment ID
    f82fjqmqxlwjvzu5l647xkhs4wuglurb
Enrollment Friendly Name
    Entrust PKIaaS XCEP
```

8. Click **Add** to add the new WSTEP service to the **Certificate enrollment policy list** pane.



Certificate Services Client - Certificate Enrollment Polic...
?
Enrollment Policy

Configuration Model: Enabled

Certificate enrollment policy list

Default	Name	Automatic Enrollment
☑	Entrust PKIaaS XCEP	Enabled

Add...
Remove...
Properties

Additional certificate enrollment policy configuration

□ Disable user configured enrollment policy servers

9. In the **Certificate enrollment policy list** pane, check the box of the new WSTEP service to make it the default Certificate Enrollment Policy.

10. Click **OK**.

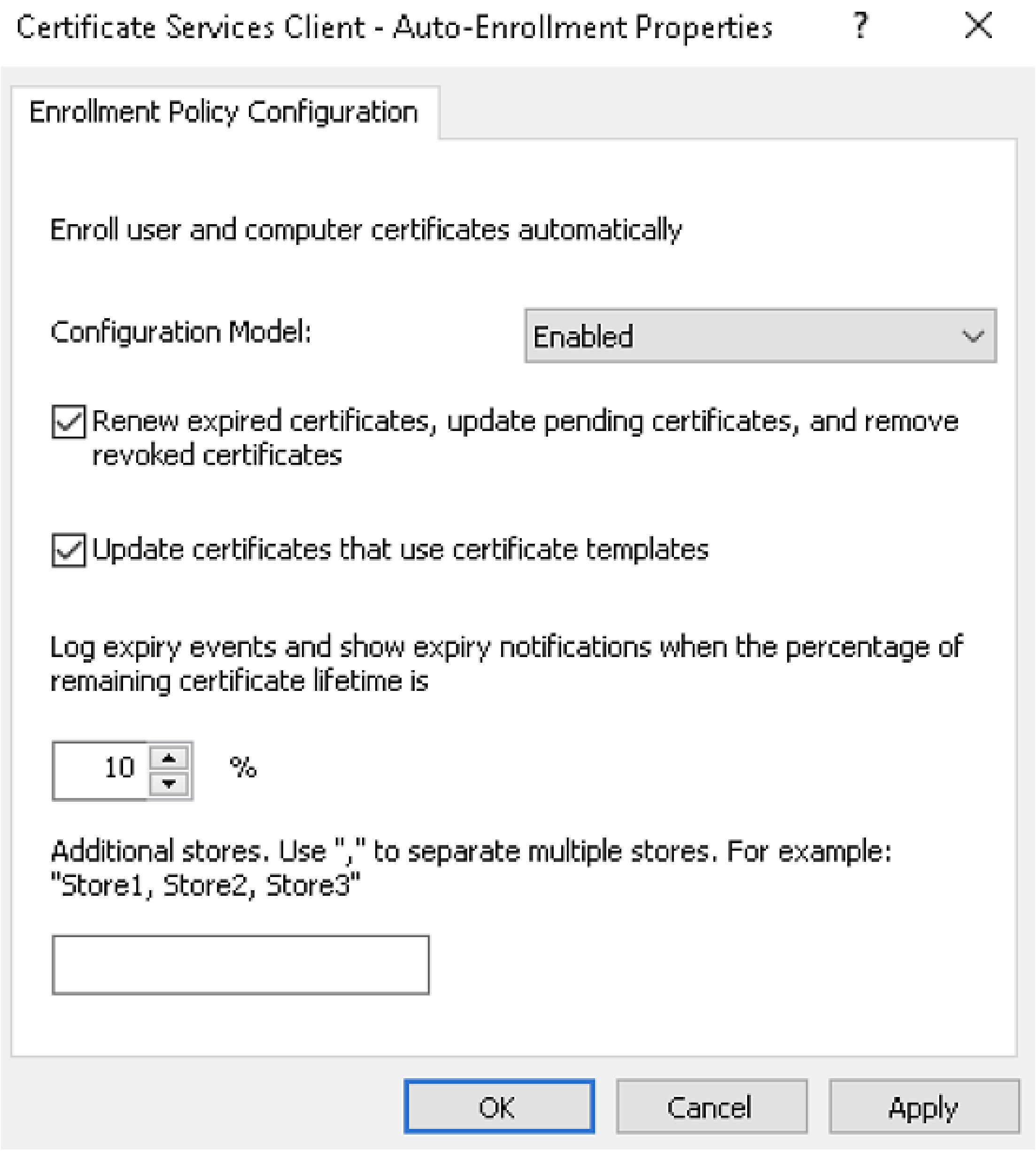
Enabling autoenrollment for devices

Configure the WSTEP Group Policy Object to enable autoenrollment for devices.

To enable autoenrollment for devices:

1. In the navigation tree of the new WSTEP Group Policy Object, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.

2. In the content pane, right-click **Certificate Services Client Auto Enrollment** and select **Properties** to display the **Certificate Services Client Auto-Enrollment Properties** dialog box.



Certificate Services Client - Auto-Enrollment Properties

Enrollment Policy Configuration

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

☑ Update certificates that use certificate templates

Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is

10 %

Additional stores. Use "," to separate multiple stores. For example: "Store1, Store2, Store3"

3. Select **Enabled** in the **Configuration Model** drop-down list.
4. Check the following boxes:
   - **Renew expired certificates, update pending certificates, and remove revoked certificates**
   - **Update certificates that use certificate templates**
5. Optionally, change the percentage under **Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is**.
6. Click **OK**.

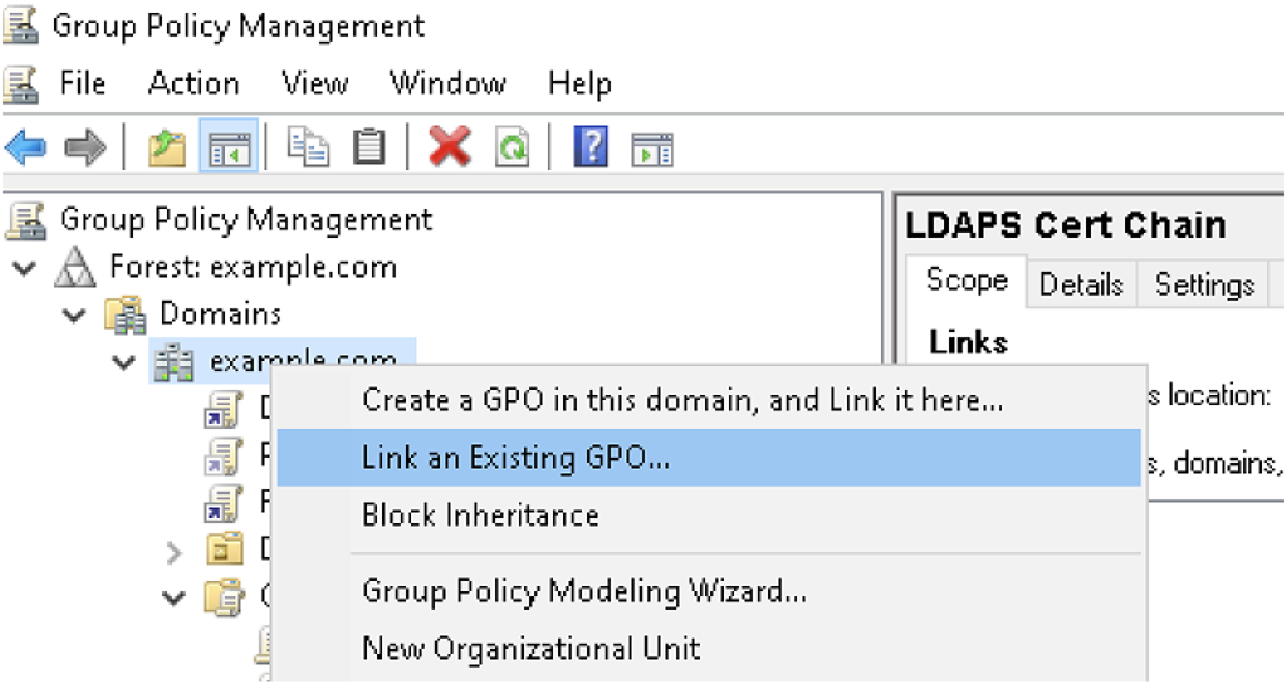
Linking the WSTEP Group Policy Object

Repeat the following procedure in each domain of the Active Directory forest to link the Group Policy Object created for the WSTEP certificate chain.

To link a Group Policy Object with a domain:

1. Log in to the root Active Directory of the forest as an Active Directory administrator.

2. Select **Start > Windows Administrative Tools > Group Policy Management** to open the Group **Policy Management** dialog.



3. Right-click the domain name and select **Link an existing GPO...** to display the **Select GPO** dialog.

4. Select the Group Policy Object.

5. Click **OK**.

Managing certificate templates

See below for adding and managing the Microsoft certificate templates in Active Directory for WSTEP enrollment and autoenrollment.

- Creating and configuring certificate templates
- Selecting CAs for certificate templates
- Disabling certificate templates

Creating and configuring certificate templates

In your Active Directory, create and configure Windows certificate templates for WSTEP enrollment.

To create and configure a Windows certificate template:

1. If not already installed, install the **Certificate Templates** snap-in as explained in Installing the default set of Microsoft Certificate Templates using the snap-in.

2. Select the existing certificate template that most closely meets your desired specs.

3. Right-click on the existing template and select **Duplicate template**.

4. Configure the settings in the following tabs of the **Properties of the New Template** dialog.

    - Compatibility
    - Cryptography

  - Extensions
  - General
  - Issuance requirements
  - Key Attestation
  - Request Handling
  - Security
  - Server
  - Superseded Templates

5. Click **OK**.

Superseded Templates

If you want the new certificate template to replace an existing one:

1. Select the **Superseded Template** tab of the **Properties of the New Template** dialog.
2. Click the **Add** button.
3. Select the name of the existing certificate template.

Selecting CAs for certificate templates

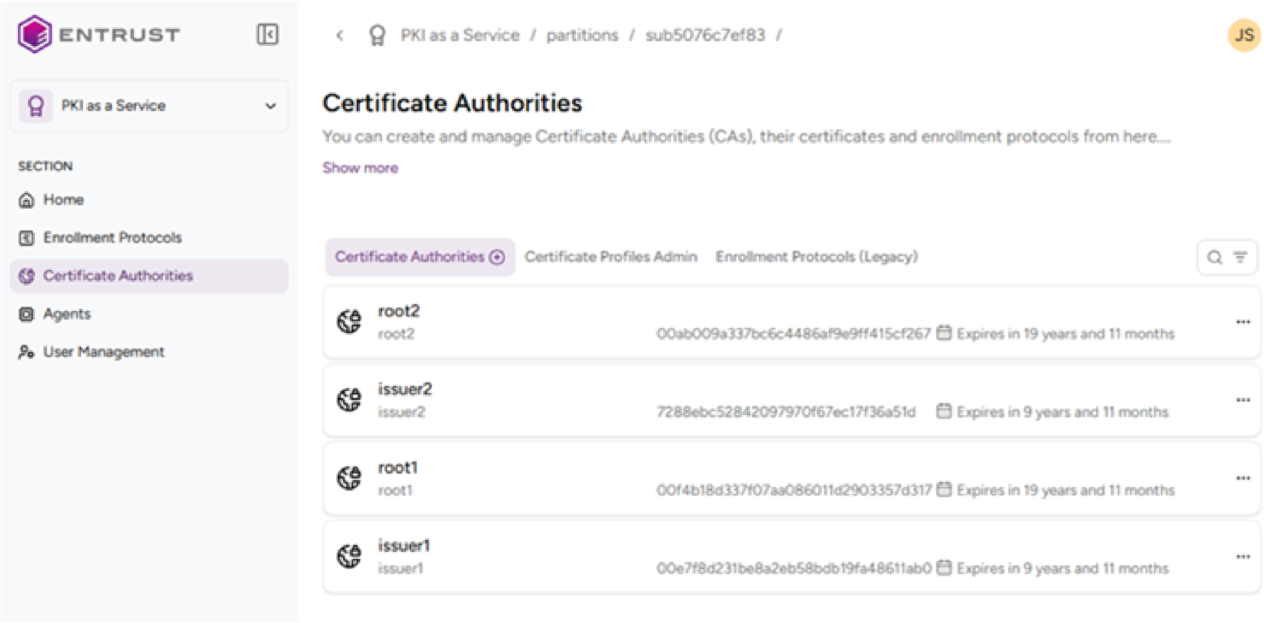
Once started, the on-premises agent discovers:

- The Microsoft Windows domains for each Active Directory node (see Adding Active Directory nodes).
- The Microsoft certificate templates configured on each domain

See below for how to select the PKIaaS certificate authority that will issue certificates for each template.

To select a CA for a certificate template:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
   - Owners
   - CA Administrators
2. Click **Certificate Authorities** in the sidebar.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from here....

Show more

Certificate Authorities ⊕ Certificate Profiles Admin Enrollment Protocols (Legacy)

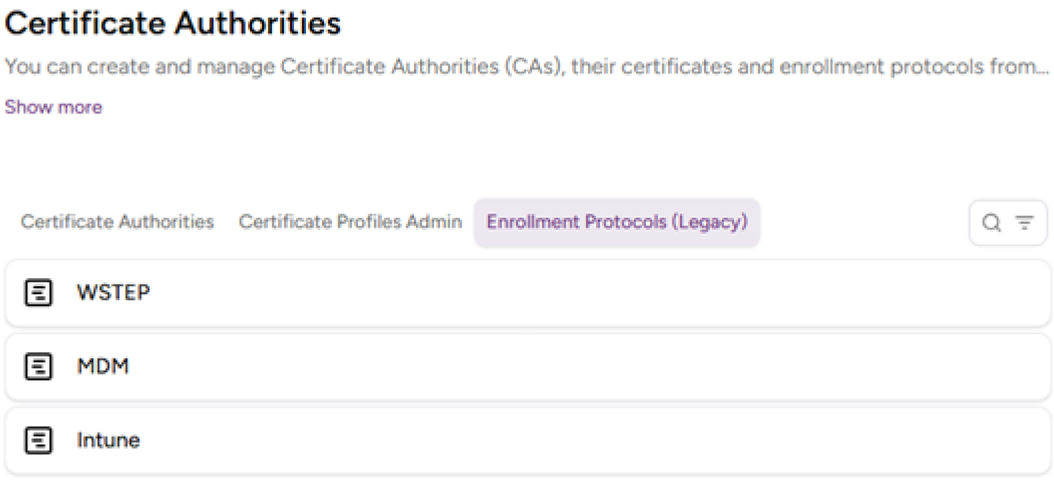
root2
root2 00ab009a337bc6c4486af9e9ff415cf267 Expires in 19 years and 11 months

issuer2
issuer2 7288ebc52842097970f67ec17f36a51d Expires in 9 years and 11 months

root1
root1 00f4b18d337f07aa086011d2903357d317 Expires in 19 years and 11 months

issuer1
issuer1 00e7f8d231be8a2eb58bdb19fa48611ab0 Expires in 9 years and 11 months

3. Select the **Enrollment Protocols** tab.



Certificate Authorities

You can create and manage Certificate Authorities (CAs), their certificates and enrollment protocols from...

Show more

Certificate Authorities Certificate Profiles Admin Enrollment Protocols (Legacy)

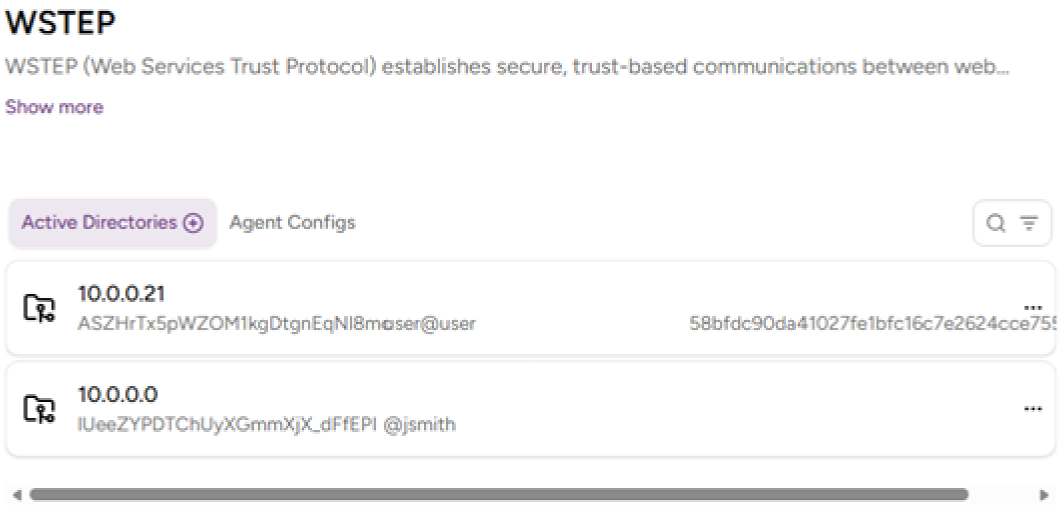
WSTEP

MDM

Intune

4. Click **WSTEP** in the protocols list.

5. In the **Active Directories** tab, click on an Active Directory name.



WSTEP

WSTEP (Web Services Trust Protocol) establishes secure, trust-based communications between web...

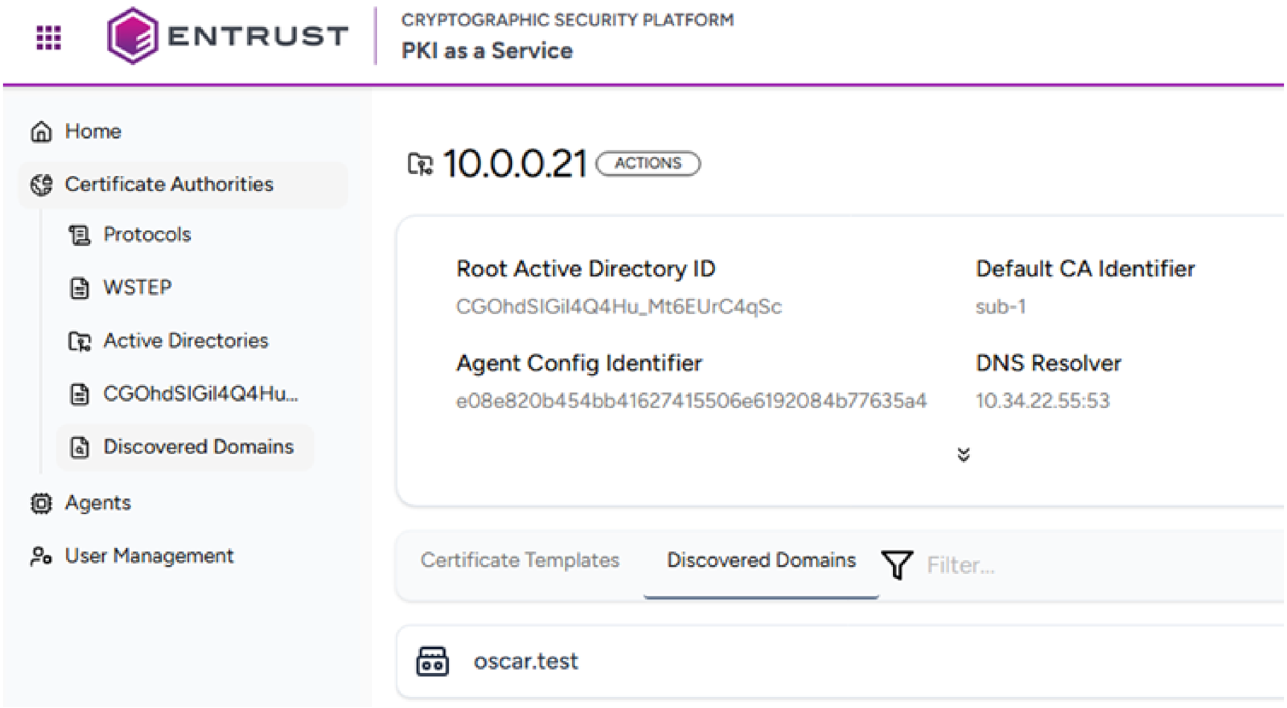
Show more

Active Directories ⊕ Agent Configs

10.0.0.21
ASZHrTx5pWZOM1kgDtgnEqNI8maser@user 58bfdc90da41027fe1bfc16c7e2624cce75!

10.0.0.0
lUeeZYPDTChUyXGmmXjX_dFfEPI @jsmith

6. On the **Discovered Domains** tab, check the domains discovered by the agent for the Active Directory.



10.0.0.21

Root Active Directory ID
CGOhdSIGil4Q4Hu_Mt6EUrC4qSc

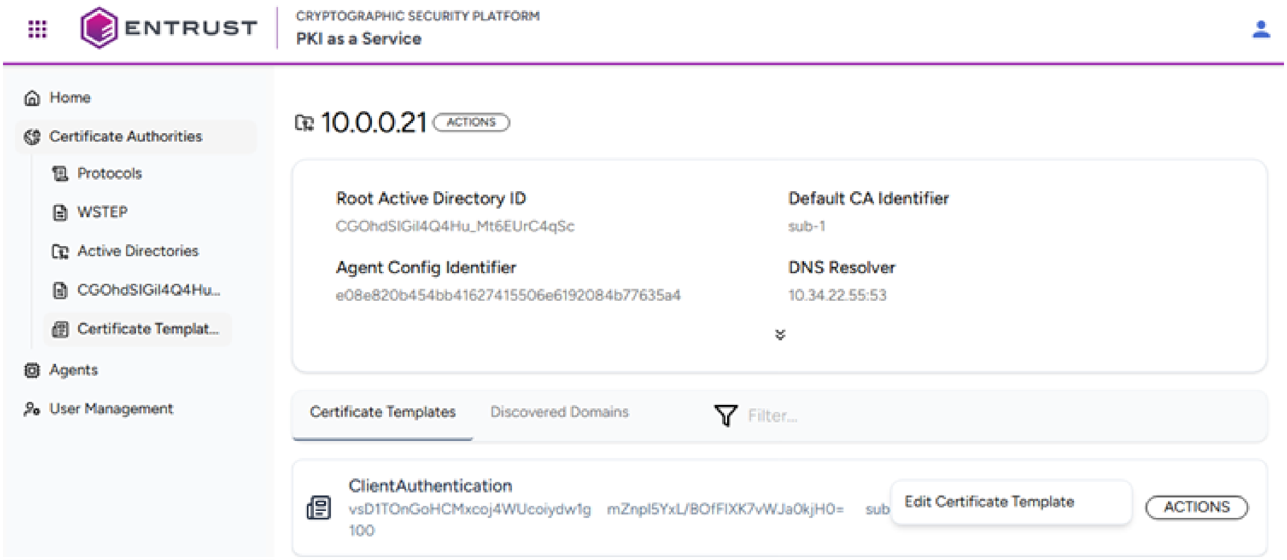
Default CA Identifier
sub-1

Agent Config Identifier
e08e820b454bb41627415506e6192084b77635a4

DNS Resolver
10.34.22.55:53

oscar.test

7. On the Certificate Templates tab, select **Actions > Edit Certificate Template** for a certificate template.



10.0.0.21

Root Active Directory ID
CGOhdSIGil4Q4Hu_Mt6EUrC4qSc

Default CA Identifier
sub-1

Agent Config Identifier
e08e820b454bb41627415506e6192084b77635a4

DNS Resolver
10.34.22.55:53

ClientAuthentication
vsD1TOnGoHCMxcoj4WUcoiydw1g mZnpl5YxL/BOfFIXK7vWJa0kjH0= sub
100

8. Select one of the certificate authorities described in Configuring an issuing CA for WSTEP and click **Edit**.

Disabling certificate templates

In some situations, you may want to disable a particular certificate template for WSTEP enrollments. You can either:

- Open the Microsoft certificate template properties dialog, select the Security tab, and disable the **Read** permission for the WSTEP service account.
- Log in to PKIaaS and unassign the CA previously assigned in Selecting CAs for certificate templates.

ℹ While disabled, certificate templates remain defined in Active Directory but can no longer be used to enroll certificates.

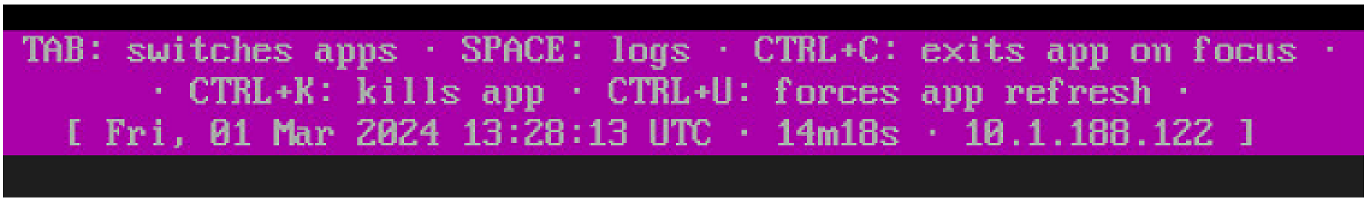
Managing on-premise Agents

As explained in Installing an agent, the agent virtual machine prompts for a registration OTP when launched. See below for additional information.

- Keyboard shortcuts
- Browsing logs
- Adding an agent for disaster recovery

Keyboard shortcuts

The ribbon at the bottom displays the keyboard shortcuts for managing the agent.



```
TAB: switches apps · SPACE: logs · CTRL+C: exits app on focus ·
     · CTRL+K: kills app · CTRL+U: forces app refresh ·
  [ Fri, 01 Mar 2024 13:28:13 UTC · 14m18s · 10.1.188.122 ]
```

As detailed in the following table, not all these shortcuts are currently supported by the agent.

Shortcut	Action	Supported
TAB	Switch tab	Yes
Space	Display detailed logs on the current tab	Yes
CTRL+C	Restart the application running on the current tab. Restarting the whole agent can only be done from the VMware Host Client	Yes
CTRL+K	Kill the application running on the current tab	No
CTRL+U	Refresh the application running on the current tab	No

Browsing logs

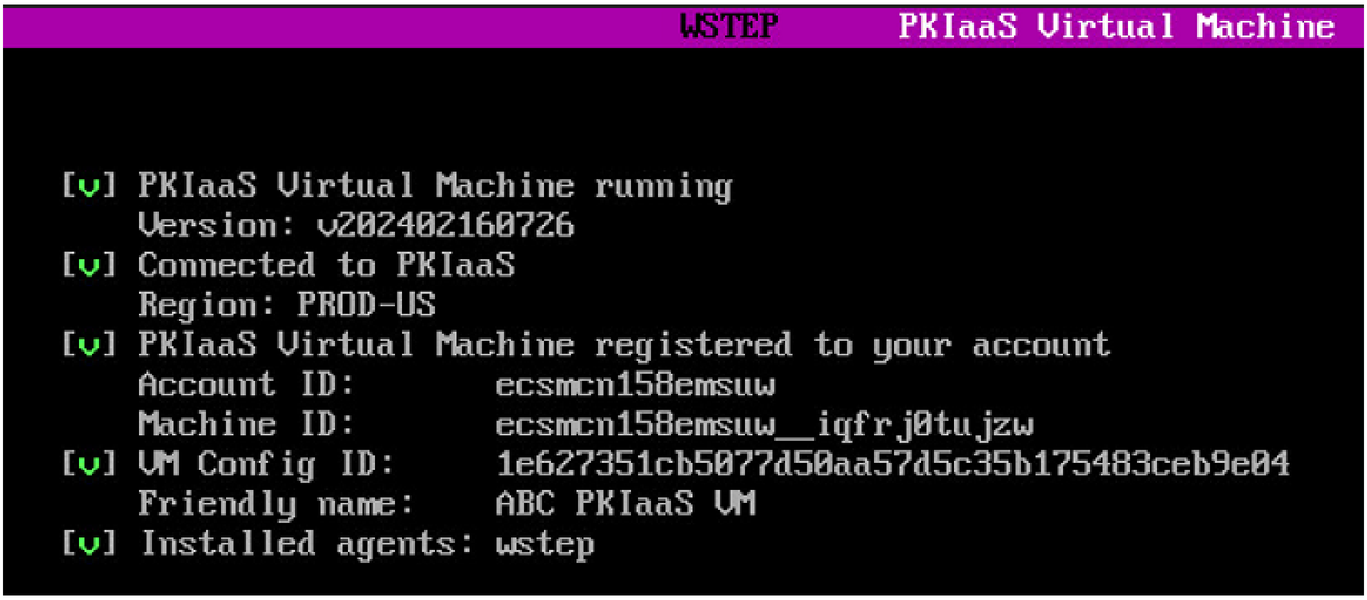
Browse the following logs on the agent prompt.

- Browsing agent startup logs
- Browsing WSTEP enrollment logs

ℹ The agent does not currently support SIEM integration.

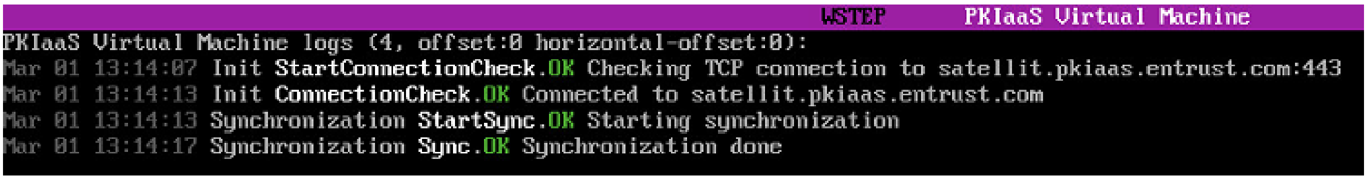
Browsing agent startup logs

The **Agent** tab of the agent prompt displays information on each startup step.



```
                                          WSTEP     PKIaaS Virtual Machine


  [v] PKIaaS Virtual Machine running
      Version: v202402160726
  [v] Connected to PKIaaS
      Region: PROD-US
  [v] PKIaaS Virtual Machine registered to your account
      Account ID:      ecsmcn158emsuw
      Machine ID:      ecsmcn158emsuw__iqfrj0tujzw
  [v] VM Config ID:    1e627351cb5077d50aa57d5c35b175483ceb9e04
      Friendly name:   ABC PKIaaS VM
  [v] Installed agents: wstep
```

Press the space bar to display more detailed logs.



```
                                                                WSTEP      PKIaaS Virtual Machine
PKIaaS Virtual Machine logs (4, offset:0 horizontal-offset:0):
Mar 01 13:14:07 Init StartConnectionCheck.OK Checking TCP connection to satellit.pkiaas.entrust.com:443
Mar 01 13:14:13 Init ConnectionCheck.OK Connected to satellit.pkiaas.entrust.com
Mar 01 13:14:13 Synchronization StartSync.OK Starting synchronization
Mar 01 13:14:17 Synchronization Sync.OK Synchronization done
```

See the following table for a description of each step.

Step	Step information	Step completion
Agent Running	The versionâ□□ of the agent	When the machine is running
Connected to Entrust PKIaaS	The region hosting the Entrust PKIaaS services.	When the machine is running
Entrust PKIaaS Gateway registered to your account	A registration confirmation message and details on the registered machine	After Registering an agent
Node ID	The internal Entrust PKIaaS identifier of the agent	After Registering an agent
Installed agents	The "WSTEP" name of the installed agent.	After Installing an agent

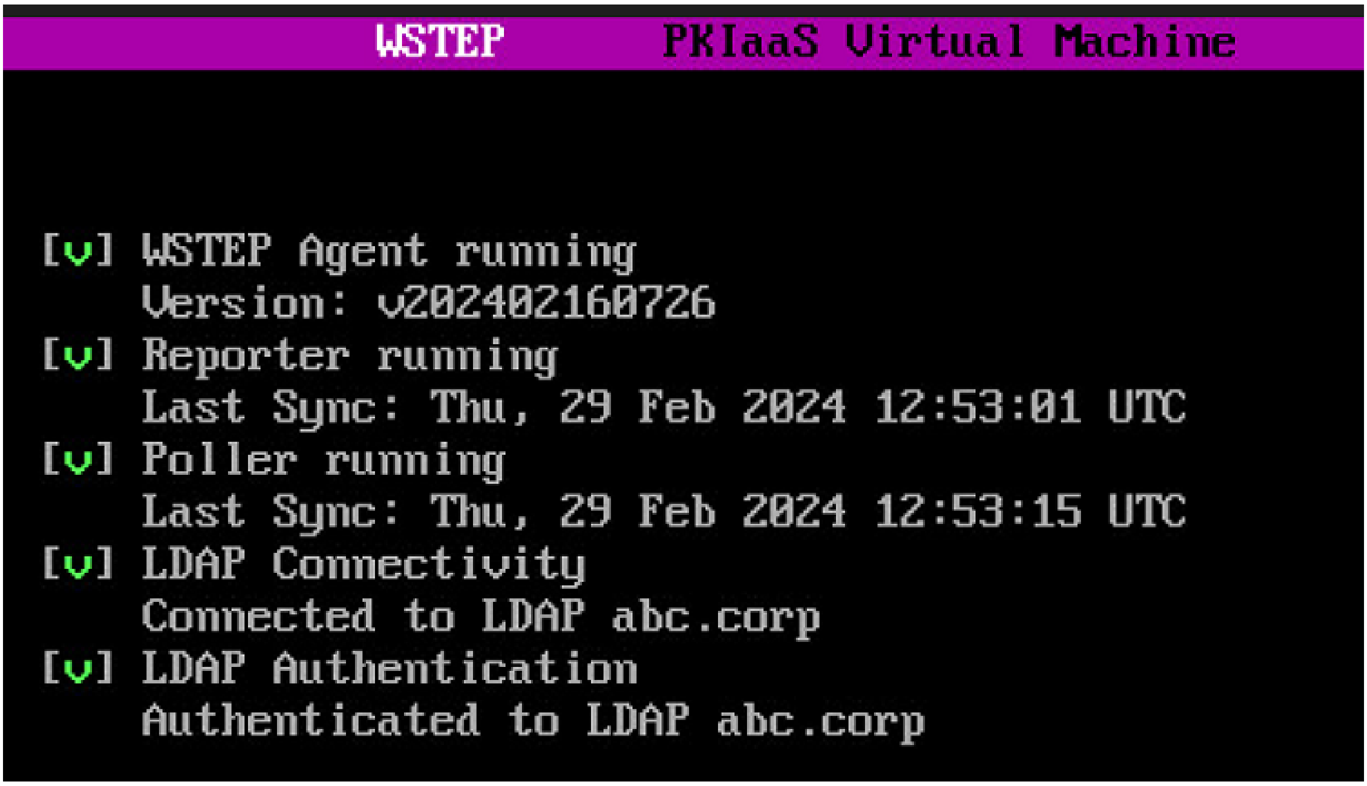
For each step, the prompt displays the following status symbols.

Symbol	Step status
â□□[ ]	Not yet startedâ□□
[\]	In progress
[v]	Completed

Symbol	Step status
[x]	Failed

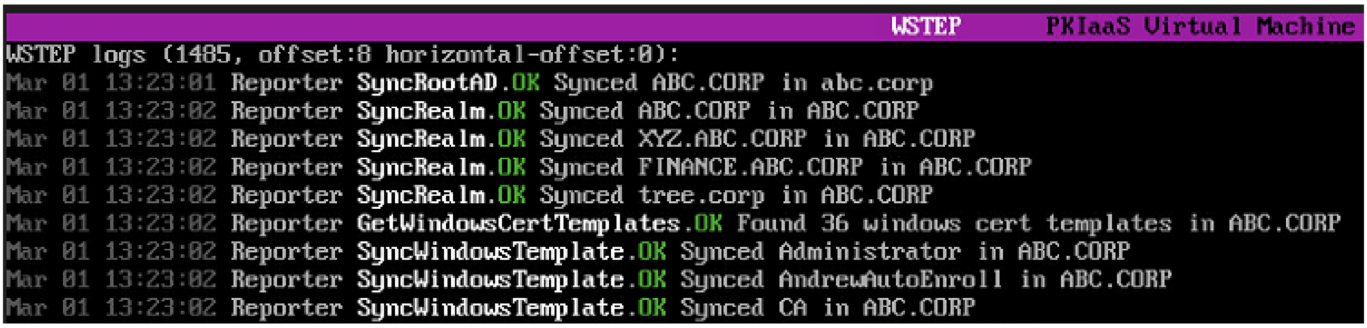
Browsing WSTEP enrollment logs

When completing the startup process, press the tab key to switch to the **WSTEP** tab and browse logs on the WSTEP agent.



```
            WSTEP       PKIaaS Virtual Machine



[v] WSTEP Agent running
    Version: v202402160726
[v] Reporter running
    Last Sync: Thu, 29 Feb 2024 12:53:01 UTC
[v] Poller running
    Last Sync: Thu, 29 Feb 2024 12:53:15 UTC
[v] LDAP Connectivity
    Connected to LDAP abc.corp
[v] LDAP Authentication
    Authenticated to LDAP abc.corp
```

Press the space bar to display more detailed logs.



```
                                                                   WSTEP       PKIaaS Virtual Machine
WSTEP logs (1485, offset:8 horizontal-offset:0):
Mar 01 13:23:01 Reporter SyncRootAD.OK Synced ABC.CORP in abc.corp
Mar 01 13:23:02 Reporter SyncRealm.OK Synced ABC.CORP in ABC.CORP
Mar 01 13:23:02 Reporter SyncRealm.OK Synced XYZ.ABC.CORP in ABC.CORP
Mar 01 13:23:02 Reporter SyncRealm.OK Synced FINANCE.ABC.CORP in ABC.CORP
Mar 01 13:23:02 Reporter SyncRealm.OK Synced tree.corp in ABC.CORP
Mar 01 13:23:02 Reporter GetWindowsCertTemplates.OK Found 36 windows cert templates in ABC.CORP
Mar 01 13:23:02 Reporter SyncWindowsTemplate.OK Synced Administrator in ABC.CORP
Mar 01 13:23:02 Reporter SyncWindowsTemplate.OK Synced AndrewAutoEnroll in ABC.CORP
Mar 01 13:23:02 Reporter SyncWindowsTemplate.OK Synced CA in ABC.CORP
```

The displayed WSTEP enrollment logs:

- Do not contain any sensitive information.
- Are stored alongside the WSTEP service in the cloud for troubleshooting purposes.
- Cannot be manually exported.

Adding an agent for disaster recovery

After completing the installation, registration, and configuration of the agent, it is recommended to deploy an additional agent for disaster recovery.

To create an additional agent for disaster recovery:

1. Repeat the steps described in Installing an agent to create a new agent. Use the same file obtained when Downloading an agent.
2. Register the new agent as explained in Registering an agent.
3. Keep the machine running.

Troubleshooting WSTEP enrollment issues

See below for how to solve the main issues related to WSTEP enrollment configuration and execution.

- Troubleshooting agent onboarding issues
- Troubleshooting agent configuration issues
- Troubleshooting Group Policy Object configuration issues
- Troubleshooting enrollment and certificate template issues

Troubleshooting agent onboarding issues

If you are having problems connecting the on-premises agent to the Entrust PKIaaS cloud:

1. Check the error log as explained in Browsing logs.
2. Take a screenshot of the error log.
3. Attach the screenshot to a support ticket.

Troubleshooting agent configuration issues

The steps described in Configuring WSTEP automation in PKIaaS require adding and configuring a WSTEP agent. See below for how to solve any issue you might encounter.

- DNS Server unreachable
- Invalid LDAP credentials
- LDAP timeout
- TLS handshake failed
- Unknown LDAP host

See Browsing WSTEP enrollment logs for browsing logs in the WSTEP tab of the on-premises agent.

DNS Server unreachable

While configuring an Active Directory in the agent, you may encounter the **ErrorDialURL** error on the **WSTEP** tab of the on-premises agent.

```
LDAP Result Code 200 "Network Error": dial tcp: lookup <DOMAIN-NAME>: i/o timeout
```

See below for a list of possible causes and the corresponding solutions.

- Firewall rules blocking access
- Invalid DNS settings in the agent configuration

Firewall rules blocking access

Firewall rules may block connections from the IP address of the agent to the DNS server on port 53.

ℹ See Agent network requirements for all the port access requirements.

Issue resolution: Edit the firewall rules to allow access.

Invalid DNS settings in the agent configuration

The DNS server settings were not properly defined when Adding Active Directory nodes.

Issue resolution: Edit the agent configuration to update the DNS settings.

Invalid LDAP credentials

While Adding Active Directory nodes, you may encounter the **ErrorLDAPAuthentication** error on the **WSTEP** tab of the on-premises agent.

```
LDAP Result Code 49 "Invalid Credentials": 80090308: LdapErr: DSID-0C090439,
comment: AcceptSecurityContext error, data 52e, v4563
```

The cause of this error is an invalid LDAP username or password.

Issue resolution:

1. Edit the Active Directory created when Adding Active Directory nodes.
2. Enter a valid username and user password.

LDAP timeout

While Adding Active Directory nodes, you may encounter the **ErrorDialURL** error on the **WSTEP** tab of the on-premises agent.

```
ldap://<DOMAIN-CONTROLLER>
LDAP Result Code 200 "Network Error": dial tcp dc1.example.com:389: i/o timeout
```

See below for a list of possible causes and the corresponding solutions.

- Domain Controller powered off
- Orphaned Domain Controller
- Incorrect IP address

Domain Controller powered off

The `<DOMAIN-CONTROLLER>` might be powered off.

Issue resolution: Power on the Domain Controller.

Orphaned Domain Controller

The `<DOMAIN-CONTROLLER>` Domain Controller mentioned in the error might be orphaned. This issue might occur if the Domain Controller was accidentally or incorrectly removed from an Active Directory forest.

Issue resolution: Remove the orphaned Domain Controller as explained in https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/remove-orphaned-domains

Incorrect IP address

The DNS Entry for the `<DOMAIN-CONTROLLER>` Domain Controller might point to an incorrect IP address. This issue can occur if:

- A Domain Controller was erroneously deployed using a DHCP-assigned IP address instead of a static IP address.
- Mistakes were made while deliberately changing the IP address of a Domain Controller.

Issue resolution:

1. Check the `<DOMAIN-CONTROLLER>` DNS entry in the Microsoft DNS manager.
2. Verify the listed IP Address.
3. If the IP address in the Microsoft DNS Manager is correct and differs from the IP address in the logs, another DNS record must be fixed.

TLS handshake failed

While Adding Active Directory nodes, you may encounter the **ErrorDialURL** error on the **WSTEP** tab of the on-premises agent.

```
url: ldap://<DOMAIN-CONTROLLER-FQDN>LDAP Result Code 200 "Network Error": TLS
handshake failed (tls: either ServerName or InsecureSkipVerify must be specified
in the tls.Config)
```

See below for a list of possible causes and the corresponding solutions.

Missing LDAPS TLS certificate

The Domain Controller is missing a TLS certificate for LDAPS.

Issue resolution:

1. Run the command described in Validating the LDAPS configuration.
2. If the command output does not contain an LDAPS TLS certificate, follow the steps described in Setting up LDAPS on domain controllers.

Invalid LDAPS TLS certificate

The Domain Controller does not have a valid TLS certificate for LDAPS connections.

Issue resolution: Check the following.

- The certificate meets the requirements described in Generating the LDAPS TLS certificates.
- The certificate chain has been imported as explained in Creating a Group Policy Object for the LDAPS TLS certificate chain.

LDAPS TLS certificate not trusted

The root CA certificate of the LDAPS TLS certificate chain is not trusted.

Issue resolution: Verify that the root CA certificate in the root Active Directory domain matches the root CA certificate imported when configuring an Active Directory in the agent.

Incorrect DNS entries

The DNS server on your network might have an incorrect IP address for the Active Directory domain controller.

Issue resolution: Verify that the IP address of the Active Directory domain controller is properly configured in the DNS server.

Unknown LDAP host

While configuring an Active Directory in the agent, you may encounter the **ErrorDialURL** error on the **WSTEP** tab of the on-premises agent.

```
ldap://<DOMAIN-CONTROLLER>
LDAP Result Code 200 "Network Error": dial tcp lookup <DOMAIN-CONTROLLER> on <DNS-
RESOLVER-IP-ADDRESS>:53 no such host
```

See below for a list of possible causes and the corresponding solutions.

- Orphaned Domain Controller
- Missing DNS record

Orphaned Domain Controller

The `<DOMAIN-CONTROLLER>` Domain Controller mentioned in the error might be orphaned. This issue might occur if the Domain Controller was accidentally or incorrectly removed from an Active Directory forest.

Issue resolution: Remove the orphaned Domain Controller as explained in https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/remove-orphaned-domains

Missing DNS record

The DNS server running on `<DNS-RESOLVER-IP-ADDRESS>:53` does not have a DNS Record for `<DOMAIN-CONTROLLER>`. This error might occur after following the Microsoft documentation to solve the orphaned

Domain Controller issue mentioned above.

Issue resolution: Adding the missing DNS record.

Troubleshooting Group Policy Object configuration issues

Issues may arise while Creating a Group Policy Object. See below for how to solve them.

- Access denied by remote endpoint
- Remote endpoint not reachable

Access denied by remote endpoint

When Enabling WSTEP for users and devices, the Windows machine can display the following error.

```
Error: Access was denied by the remote endpoint.
080300005 (-2143485947 WS_E_ENDPOINT_ACCESS-DENIED)
```

See below for a list of possible causes and the corresponding solutions.

- Invalid enrollment URL
- Invalid agent configuration
- Invalid root Active Directory username

Invalid enrollment URL

The CEP URL provided to the Group Policy Manager may contain a typo.

Issue resolution: Check that the entered URL matches the URL displayed on the welcome page of the Entrust PKIaaS UI.

Invalid agent configuration

The WSTEP agent configuration is not valid.

Issue resolution: Check the following.

1. The WSTEP agent runs with a valid configuration before the PKIaaS CEP URL can be defined in a Group Policy Object.
2. The WSTEP agent on the agent completes an initial synchronization of the Kerberos data (SPN, KVNO) from the root Active Directory before the Microsoft Group Policy Manager can validate the PKIaaS CEP URL.

See Troubleshooting agent configuration issues for solving agent-related issues.

Invalid root Active Directory username

The username defined on the Entrust PKIaaS UI for the root Active Directory RootAD does not have a properly configured SPN (Service Principal Name) or UPN (User Principal Name).

Issue resolution: Run the following command to fix the root Active Directory username.

```
ktpass -mapuser <USER> -princ HTTP/<PKIaaS-WSTEP-URL>@<UPPERCASE-DOMAIN-NAME> -
pass <PASS> -ptype KRB5_NT_PRINCIPAL /Target <UPPERCASE-DOMAIN-NAME> /crypto ALL
```

Remote endpoint not reachable

When Enabling WSTEP for users and devices, the Windows machine can display the following error.

```
Error: The remote endpoint was not reachable.
0x005de01a (-2143485936 WS_E_ENDPOINT_UNREACHABLE)
```

See below for a list of possible causes and the corresponding solutions.

- Invalid enrollment URL
- Network issues

Invalid enrollment URL

The CEP URL provided to the Group Policy Manager may contain a typo.

Issue resolution: Check that the entered URL matches the URL displayed on the welcome page of the Entrust PKIaaS UI.

Network issues

Network issues prevent the Microsoft server from accessing the PKIaaS WSTEP URLs.

Issue resolution: Verify the following.

- The entrust PKIaaS WSTEP URL is reachable.
- The firewall rules do not block traffic to the PKIaaS WSTEP URL.

Troubleshooting enrollment and certificate template issues

See below for solving issues related to enrollment, autoenrollment, and certificate template management.

- Certificate template not enrolling or autoenrolling
- Missing certificate template
- Unexpected behavior of certificate enrollment

Certificate template not enrolling or autoenrolling

Once configured, a Windows certificate template may not enroll or autoenroll devices. See below for the possible causes and corresponding solutions.

- Missing Group Policy Object
- Missing permissions

Missing Group Policy Object

The Group Policy Object to enable Autoenrollment may not have been created, or may not have been linked to the various domains in the Windows Active Directory forest.

Issue resolution: Configure a Group Policy Object as explained below.

- Enabling autoenrollment for users
- Enabling autoenrollment for devices
- Linking the WSTEP Group Policy Object

Missing permissions

The user or group facing may not have permission to enroll or autoenroll.

Issue resolution: Select the Security to select the users and groups with permission to enroll and autoenroll.

Missing certificate template

When browsing certificate templates (as explained in Selecting CAs for certificate templates), a template may be missing because it contains an unsupported key usage.

Issue resolution: Verify the key usages.

Unexpected behavior of certificate enrollment

Certificate enrollment may not behave as expected when the Windows certificate template includes unsupported settings.

Issue resolution: Verify that the certificate template matches the configuration described in Creating and configuring certificate templates. Specifically, the configuration must not include any of the following unsupported settings.

Tab	Unsupported setting
Extensions	Any key usage combination containing the following key usages: CRL Sign, Decipher Only, Encipher Only, Key Agreement, Key Cert Sign
General	Publish certificate in Active Directory
Issuance requirements	CA certificate manager approvalâ□□
Key Attestation	Required
Request Handling	Archive subject's encryption private key
Server	Do not include revocation information in issued certificates
	Do not store certificates and requests in the CA Database

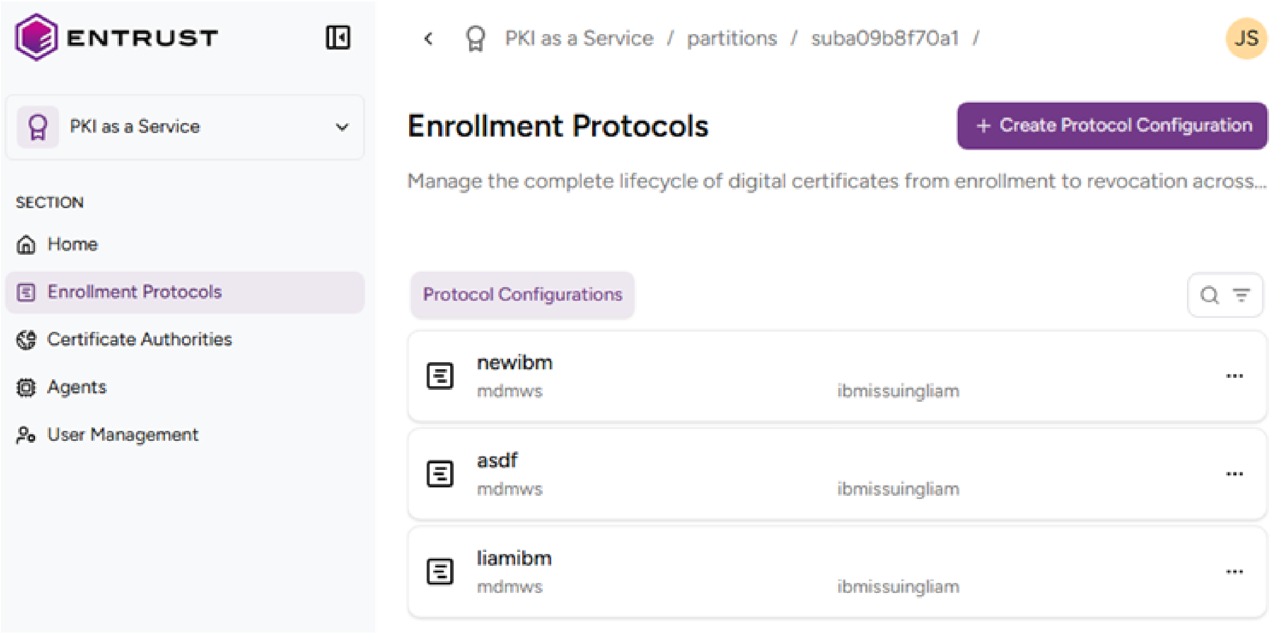
Managing end-entities

As explained in the previous sections, PKIaaS supports automating enrollment with different protocols such as ACME, MDM, IBM, or WSTEP. See below for the PKIaaS options for managing the end-entities requesting certificates.

ℹ This section does not explain integrating end-entities. Refer to the corresponding enrollment automation section for details.

To manage end-entities:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
   - Owners
   - CA Administrators
2. Click **Enrollment Protocols** in the sidebar.



Enrollment Protocols

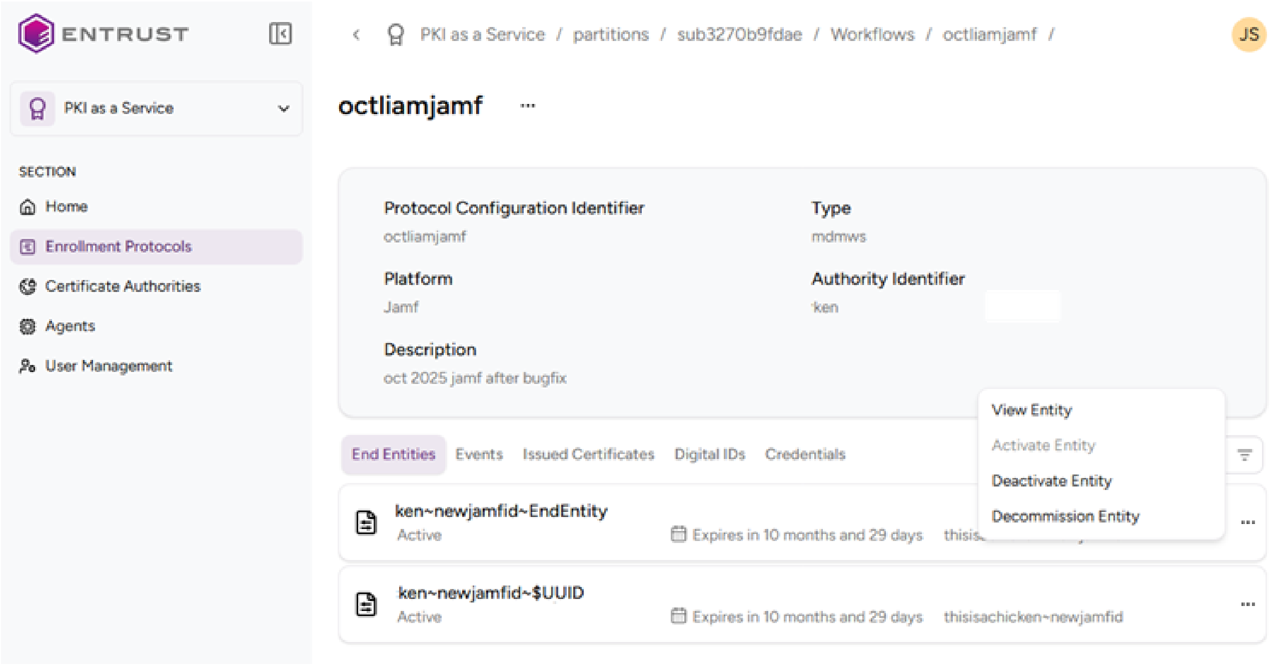
Manage the complete lifecycle of digital certificates from enrollment to revocation across...

newibm
mdmws ibmissuingliam

asdf
mdmws ibmissuingliam

liamibm
mdmws ibmissuingliam

3. Click the name of a enrollment protocol.



Protocol Configuration Identifier: octliamjamf

Type: mdmws

Platform: Jamf

Authority Identifier: ken

Description: oct 2025 jamf after bugfix

ken~newjamfid~EndEntity — Active — Expires in 10 months and 29 days — thisis

ken~newjamfid~$UUID — Active — Expires in 10 months and 29 days — thisisachicken~newjamfid

4. In the **End Entities** tab, browse the following end-entity details.

   - Identifier
   - Activation status
   - Expiration date

5. Click the three dots **...** right to an end entity and select:

   - **View Entity** to display the end-entity details
   - **Activate Entity** to activate a deactivated entity
   - **Deactivate Entity** to deactivate an entity
   - **Decommission Entity** to permanently remove an end-entity

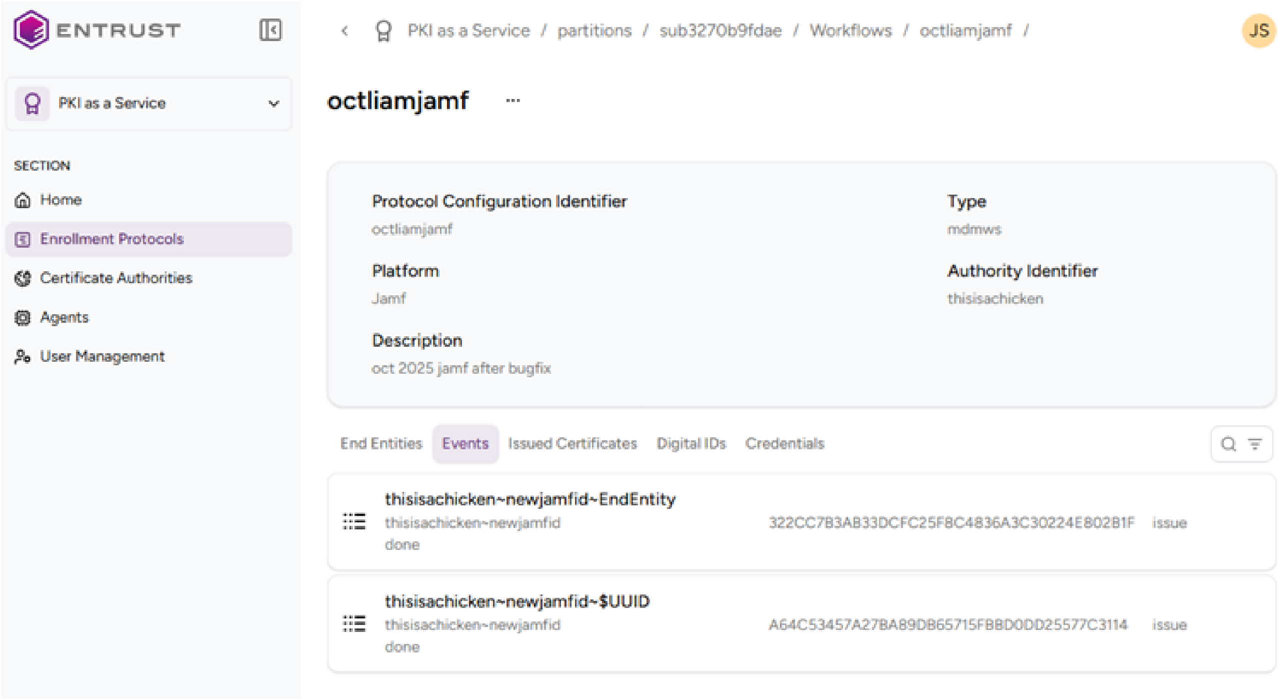
Auditing enrollment events

See below for auditing the enrollment events triggered by remote end-entities.

To audit enrollment events:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of the roles described under Role permissions.

2. Click **Enrollment Protocols** in the sidebar.



octliamjamf

Protocol Configuration Identifier
octliamjamf

Type
mdmws

Platform
Jamf

Authority Identifier
thisisachicken

Description
oct 2025 jamf after bugfix

thisisachicken~newjamfid~EndEntity
thisisachicken~newjamfid 322CC7B3AB33DCFC25F8C4836A3C30224E802B1F issue
done

thisisachicken~newjamfid~$UUID
thisisachicken~newjamfid A64C53457A27BA89DB65715FBBD0DD25577C3114 issue
done

3. In the **Events** tab, browse the following event details.
   - The end-entity triggering the event.
   - The completion status, for example **done**.
   - The event internal identifier, as a hexadecimal string.
   - The event type, for example **issue**.

Migrating an on-prem gateway to PKIaaS

Entrust PKIaaS supports the following migrations from a customer-hosted Certificate Enrollment Gateway to a PKIaaS gateway for the same CA and certificate profile.

- Migrating an Intune on-prem gateway to PKIaaS
- Migrating an MDM Jamf on-prem gateway to PKIaaS
- Migrating a WSTEP on-prem gateway to PKIaaS

Migrating an Intune on-prem gateway to PKIaaS

See below for migrating Intune enrollment from a customer-hosted Enrollment Gateway to a PKIaaS gateway.

To migrate Intune enrollment to PKIaaS:

1. Deploy a PKIaaS Intune gateway as explained in Configuring Intune in PKIaaS.
2. In Microsoft Endpoint, replace the **SCEP Server URLs** of all your Intune SCEP configuration profiles with the values described in Configuring Intune in PKIaaS.
3. Test and validate the new PKIaaS Intune service.

Migrating an MDM Jamf on-prem gateway to PKIaaS

See below for migrating MDM Jamf enrollment from a customer-hosted Enrollment Gateway to PKIaaS.

To migrate MDM Jamf enrollment to PKIaaS:

1. Add the configuration settings described in Configuring Jamf in PKIaaS.

2. When Configuring MDM automation in Jamf, go to **Options / SCEP** and update only the following parameters of your existing Jamf configuration.

   - In URL, paste the **SCEP URL** value obtained when Configuring Jamf in PKIaaS.
   - In Entrust Web Service URL, paste the **MDM Web Service URL** value obtained when Configuring Jamf in PKIaaS.
   - In Administrator Username, paste the **Credential Identifier** value obtained when Configuring Jamf in PKIaaS.
   - In Administrator Password, paste the credential **Password** value generated when Configuring Jamf in PKIaaS.

3. Test and validate the new PKIaaS and MDM service.

Migrating a WSTEP on-prem gateway to PKIaaS

To configure the migration from a WSTEP on-premises Enrollment Gateway to a PKIaaS gateway, follow the steps under Automating WSTEP enrollment. See below for specific considerations on each section.

1. When Planning your WSTEP deployment, determine the required number of Agents based on your current deployment.
2. When evaluating the WSTEP integration requirements, determine the networking requirements based on your current deployment. Make any necessary adjustment to the DNS server and the firewall rules.
3. You can skip section Configuring an issuing CA for WSTEP as WSTEP is already configured for your on-premises deployment.
4. When Preparing the Active Directory forest for WSTEP:
   - Repeat Adding Active Directory nodes for each root Active Directory in every Microsoft Active Directory forest. It is recommended to create a new service account for the PKIaaS WSTEP gateway to allow the existing on-premises WSTEP Enrollment Gateway to continue functioning until decommissioned.
   - You can skip Installing the default set of certificate templates, as the templates should already exist for each Microsoft Active Directory forest.
   - Repeat Setting up LDAPS on domain controllers across the entire Microsoft Active Directory forest. In contrast, the on-premises WSTEP Enrollment Gateway requires LDAPS TLS certificates to be configured only on the root Active Directory domain controllers.
5. When Configuring WSTEP automation in PKIaaS, complete all the steps. When Preparing the Active Directory forest for WSTEP, ensure the selected certificate authority matches the one used for the on-premises WSTEP Enrollment Gateway.
6. When Enabling WSTEP for users and devices, do not reuse the Group Policy Object (GPO) of the on-premises WSTEP Enrollment Gateway. Complete the following steps in order to allow rolling back the process, if needed.
   1. Create a new GPO.
   2. Apply the GPO to a single test user.
   3. Complete the migration testing.
   4. Apply the GPO across the entire forest.
   5. Unlink the existing GPO for the on-premises WSTEP Enrollment Gateway.

⚠ It is recommended to keep the on-premises WSTEP Enrollment Gateway running until the PKIaaS WSTEP gateway is fully deployed and integrated within the Microsoft Active Directory forest.

When completing these configuration steps, perform the following cleanup steps.

- Cleaning up the Windows domain after migrating WSTEP to PKIaaS
- Cleaning up the appliance after migrating WSTEP to PKIaaS

Cleaning up the Windows domain after migrating WSTEP to PKIaaS

Perform the following steps in your Windows domain to complete the migration.

To clean up the Windows domain after migration:

1. Remove all Group Policy Objects (GPOs) for the on-premises WSTEP Enrollment Gateway
2. Run the `gpupdate /force` command to force a group policy update.
3. In the root domains of the Microsoft Active Directory forests, delete the WSTEP Service account for the on-premises WSTEP Enrollment Gateway.
4. Turn off the Microsoft servers with the Certificate Enrollment Policy (CEP) service. If these are virtual machines, you can delete them.
5. Open the ADSI Edit console and remove the Enrollment Service for the on-premises WSTEP Enrollment Gateway.

Cleaning up the appliance after migrating WSTEP to PKIaaS

The required cleanup operations on the appliance vary depending on the following situations.

- The on-premises Entrust Enrollment Gateway runs other enrollment protocols like ACME, MDM, Intune, or SCEP.
- The appliance cluster hosts other solutions like Certificate Hub or CA Gateway.

See the table below for the required cleanup actions on each appliance cluster.

Enrollment protocols	Other solutions	Cleanup solutions
WSTEP	✓	Run the `sudo kubectl delete namespace ceg` command to delete the `ceg` namespace from the appliance. This operation will keep the configuration and the license in case you need to redeploy.
WSTEP	✗	You can shut down or delete the nodes of the appliance cluster.
WSTEP and other protocols	✓	Do nothing.
WSTEP and other protocols	✗	Do nothing.

Integrating third-party tools with the CA Gateway API

Entrust CA Gateway provides the API described at:

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

Of the capabilities documented in this reference, PKIaaS supports natively the ones listed in:

https://api.managed.entrust.com/doc/#operation/caCapabilities

As explained in the following sections, implementing other capabilities requires a third-party tool.

- Managing CA Gateway credentials
- Accessing the CA Gateway API
- Integrating with Ansible
- Integrating with HashiCorp Vault
- Integrating with Venafi

Managing CA Gateway credentials

See below for instructions on managing the PKCS #12 credentials required to connect to the Entrust CA Gateway API.

- Creating CA Gateway credentials
- Renewing CA Gateway credentials

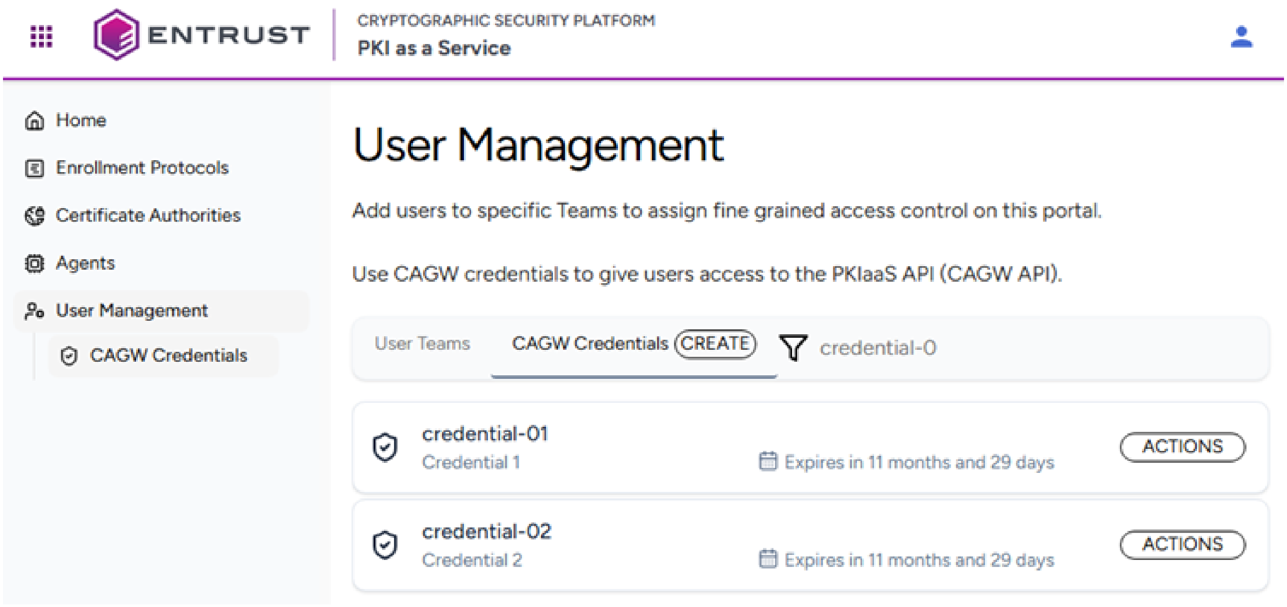
Creating CA Gateway credentials

Create PKCS #12 credentials to connect with the CA Gateway API.

ℹ Unless deleted before expiry, credentials are valid for one year. See Renewing CA Gateway credentials for how to renew them before the expiry date.

To generate a CA Gateway credential:

1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
   - Owners
   - CA Administrators
2. Click **User Management** in the sidebar.
3. Select the **CAGW Credentials** tab.



User Management

Add users to specific Teams to assign fine grained access control on this portal.

Use CAGW credentials to give users access to the PKIaaS API (CAGW API).

credential-01
Credential 1
Expires in 11 months and 29 days

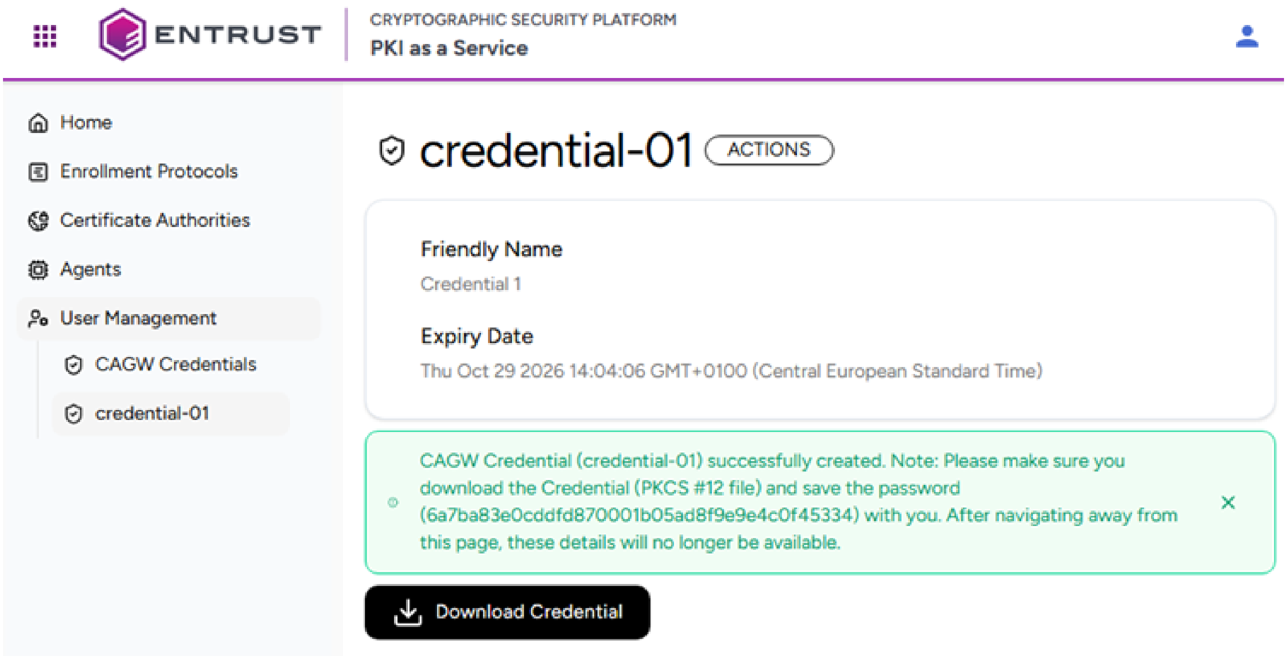
credential-02
Credential 2
Expires in 11 months and 29 days

4. Click **CREATE**.

5. Fill in the **Credential identifier** and **Friendly Name** fields.

6. Click **Create**

7. Check the details of the new PKCS #12 credential.



credential-01

Friendly Name
Credential 1

Expiry Date
Thu Oct 29 2026 14:04:06 GMT+0100 (Central European Standard Time)

CAGW Credential (credential-01) successfully created. Note: Please make sure you download the Credential (PKCS #12 file) and save the password (6a7ba83e0cddfd870001b05ad8f9e9e4c0f45334) with you. After navigating away from this page, these details will no longer be available.

8. Copy the password displayed in the information note.

⚠ You won't be able to copy the password or download the PKCS #12 file after leaving this page.

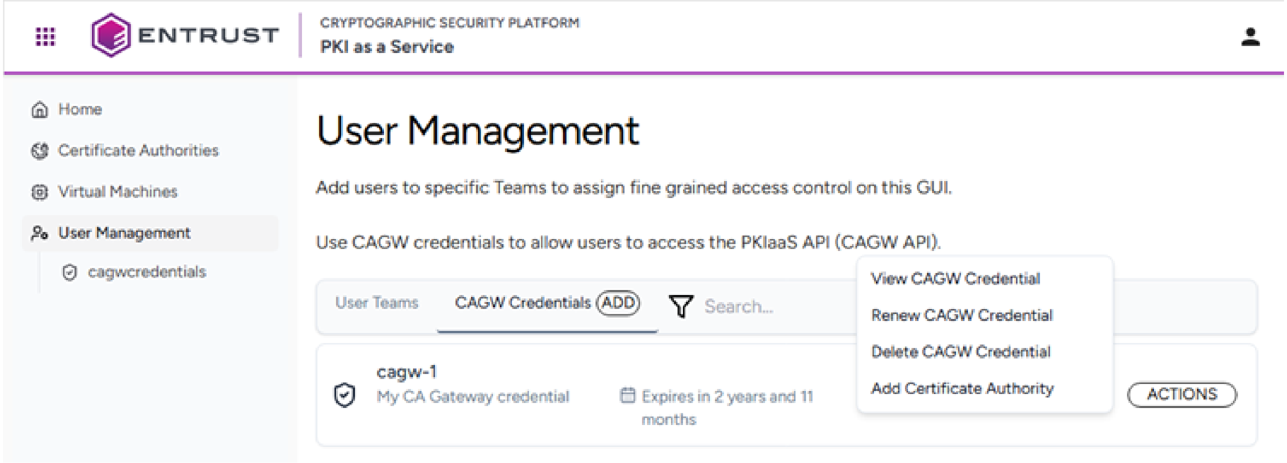
---

9. Click **Download Credential** to download the `pkcs12-<credential>.p12` file, where `<credential>` is the **Credential identifier** value.

10. Click **CAGW Credentials** in the sidebar.

11. Click **Continue** in the **Are you sure you want to leave this page?** dialog.

12. In the **CAGW Credentials** tab, click **ACTIONS** for the new credential.



User Management

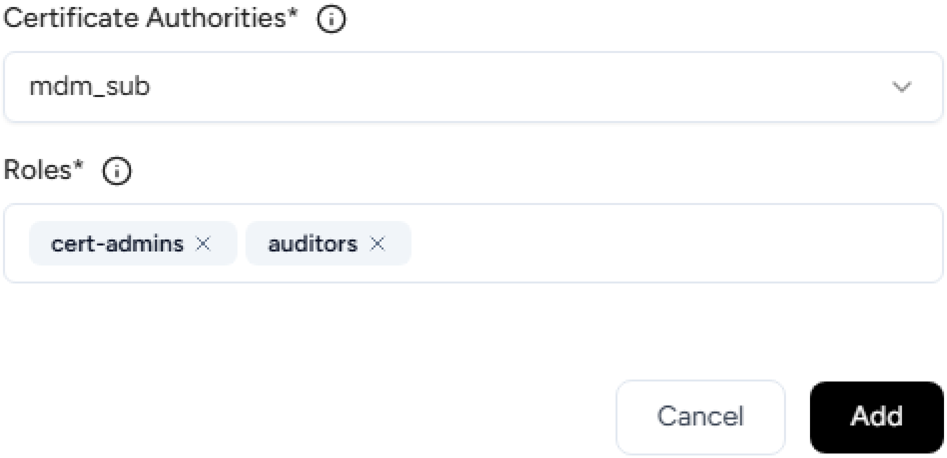
Add users to specific Teams to assign fine grained access control on this GUI.

Use CAGW credentials to allow users to access the PKIaaS API (CAGW API).

cagw-1
My CA Gateway credential
Expires in 2 years and 11 months

13. Select **Add Certificate Authority**.

14. In the **Certificate Authority** list, select the CA on which the credential holders will have permissions.



Certificate Authorities*
mdm_sub

Roles*
cert-admins
auditors

15. In the **Roles** list, select the roles granted to the credential holders in the CA.

---

i See Role permissions for the CA management permissions granted to each role.

---

16. Click **Add**.

Renewing CA Gateway credentials

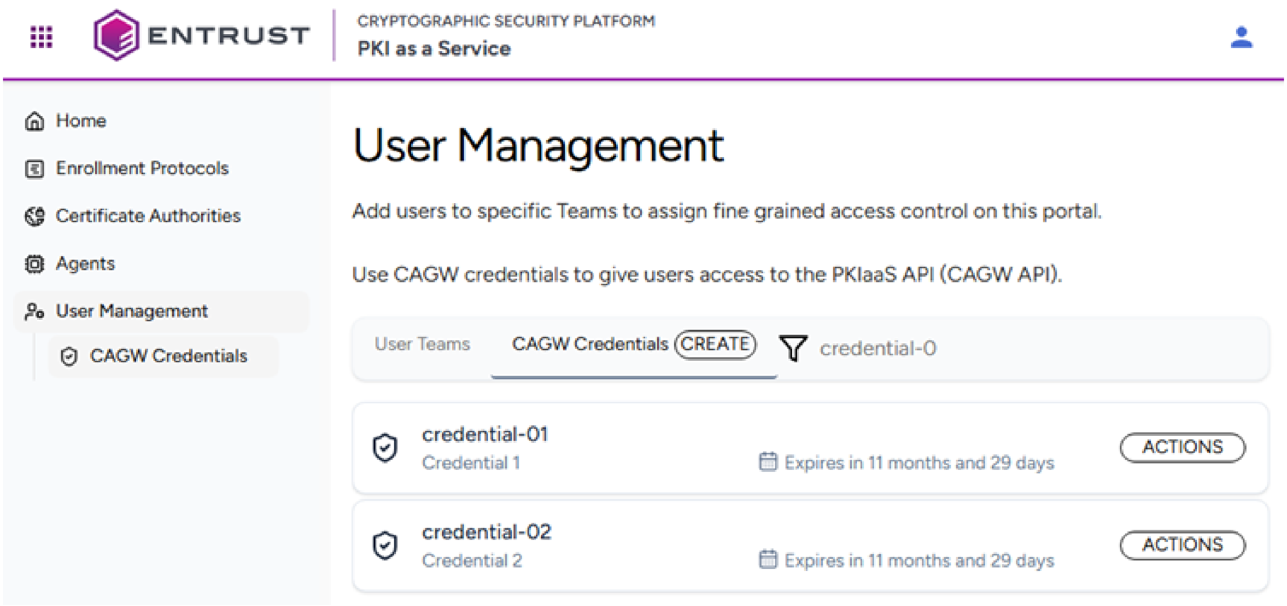
Before the expiry date, you can renew your CA Gateway credentials as explained below.

To renew a CA Gateway credential:

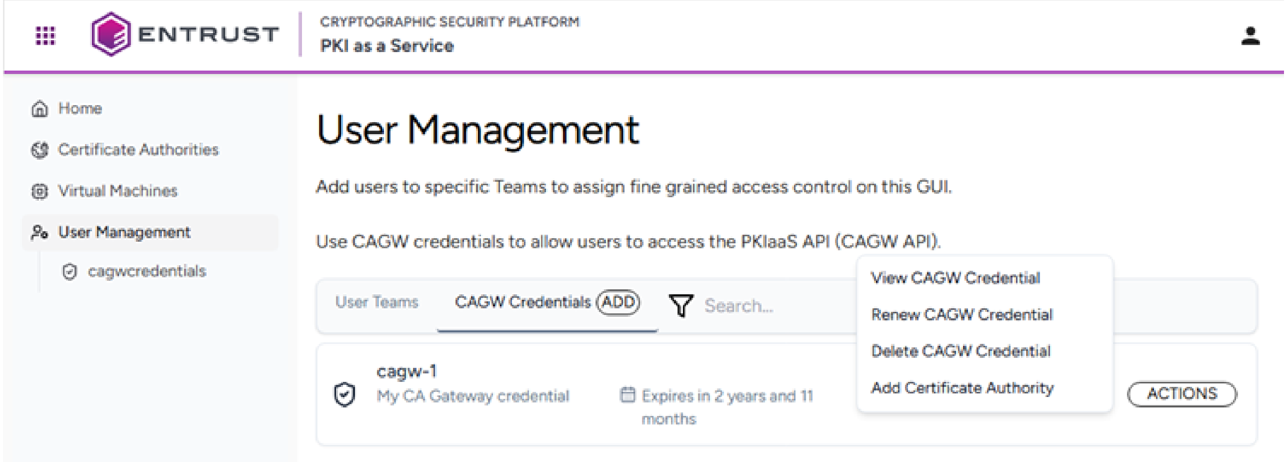
1. Follow the steps described in Accessing your partitions to log into the PKIaaS interface as a user with any of these roles:
    - Owners
    - CA Administrators

2. Click **User Management** in the sidebar.

3. Select the **CAGW Credentials** tab.


ENTRUST
CRYPTOGRAPHIC SECURITY PLATFORM
PKI as a Service
Home
Enrollment Protocols
Certificate Authorities
Agents
User Management
CAGW Credentials
User Management
Add users to specific Teams to assign fine grained access control on this portal.
Use CAGW credentials to give users access to the PKIaaS API (CAGW API).
User Teams
CAGW Credentials
CREATE
credential-0
credential-01
Credential 1
Expires in 11 months and 29 days
ACTIONS
credential-02
Credential 2
Expires in 11 months and 29 days
ACTIONS

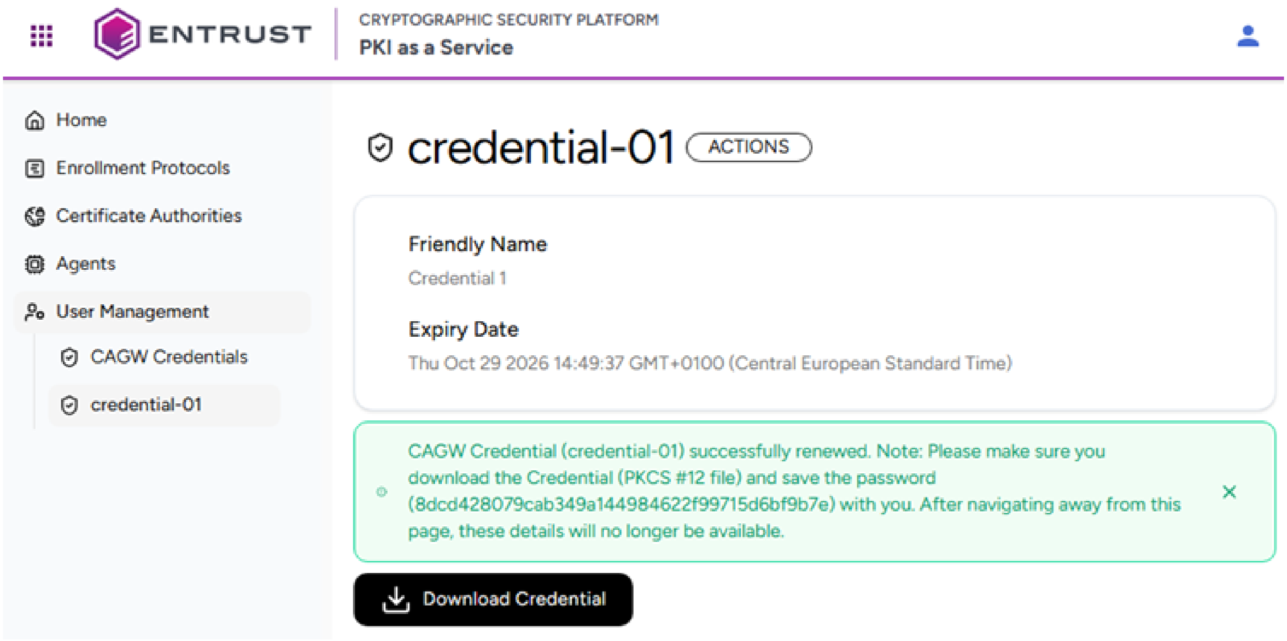
4. In the **CAGW Credentials** tab, click **ACTIONS** for the new credential.



5. Select **Renew CAGW Credential**.

6. Click **Renew**.

7. Check the details of the new PKCS #12 credential.



credential-01

Friendly Name
Credential 1

Expiry Date
Thu Oct 29 2026 14:49:37 GMT+0100 (Central European Standard Time)

CAGW Credential (credential-01) successfully renewed. Note: Please make sure you download the Credential (PKCS #12 file) and save the password (8dcd428079cab349a144984622f99715d6bf9b7e) with you. After navigating away from this page, these details will no longer be available.

8. Copy the password displayed in the information note.

⚠ You won't be able to copy the password or download the PKCS #12 file after leaving this page.

---

9. Click **Download Credential** to download the `pkcs12-<credential>.p12` file, where `<credential>` is the **Credential identifier** value that was used to create the credential.

Accessing the CA Gateway API

After you have installed the Entrust CA Gateway credential on your local machine, you can access the following.

- API endpoints
- Swagger UI

API endpoints

Use the API endpoints for programmatic interaction with the API and integrations with third-party clients.

Region	URL
US	`https://cagw.pkiaas.entrust.com/cagw/v1`
EU	`https://cagw.eu.pkiaas.entrust.com/cagw/v1`

Swagger UI

Use the Swagger UI to manually interact with a web browser or generate curl commands for API endpoints.

Region	URL
US	`https://cagw.pkiaas.entrust.com/cagw/swagger-ui`

Region	URL
EU	`https://cagw.eu.pkiaas.entrust.com/cagw/swagger-ui`

Integrating with Ansible

To integrate Entrust PKIaaS with Ansible, use the open-source client:

https://github.com/EntrustCorporation/entrust-ansible-collection

Integrating with HashiCorp Vault

To integrate Entrust PKIaaS with HashiCorp Vault, use the open-source plug-in:

https://github.com/EntrustCorporation/cagw-vault-plugin

Integrating with Venafi

To integrate Entrust PKIaaS with the Venafi certificate management software, add an Entrust CA as explained in:

https://docs.venafi.com/Docs/current/TopNav/Content/Drivers/r-drivers-Entrust-CAGateway-ConfiguringCATemplateObject.php

Revoking certificates in bulk

You can revoke certificates in bulk using the CA Gateway API provided by Entrust PKIaaS and the following open-source utility:

https://github.com/EntrustCorporation/pki-utilities/tree/main/cagw-shell-util

Obtaining support

See below for getting support on your purchased products.

- Contacting Entrust support
- Obtaining TrustedCare resources

ℹ To contact the Entrust sales department, fill in the form at https://www.entrust.com/contact/sales

Contacting Entrust support

To contact Entrust support, email `support@entrust.com` or call the following phone numbers.

- North America: 1-866-267-9297
- Outside North America: 1-613-270-2680
- Toll-free support numbers for Silver & Gold customers outside of North America: https://www.entrust.com/knowledgebase/ssl/contact-silver-gold-support-numbers

ℹ As explained in entrust-certificate-solutions-hosted-support-schedule-lg.pdf, the availability of the support team depends on your service plan (Silver vs. Platinum).

Obtaining TrustedCare resources

Entrust provides a comprehensive service and support program through the https://trustedcare.entrust.com online portal. This portal allows you to:

- Download software product updates for components you run on your premises or in your cloud.
- Browse product documentation, frequently asked questions, or technical bulletins.
- Open support cases.
- Check on the status of existing cases.