



Administrator's Guide
for
Sectigo® Certificate Manager
24.5

May 2024

Sectigo Certificate Manager

Administrator's Guide, 24.5 SCMAG

Copyright © 2008, 2024, Sectigo.

All rights reserved.

Author: Sectigo

The documentation contains proprietary information; it is provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright and other intellectual and industrial property laws.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to Sectigo in writing. This document is not warranted to be error-free.

Except as may be expressly permitted in your license agreement, the documentation may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

The documentation is produced for general use with a variety of information management applications. It is not produced or intended for use with any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this documentation in conjunction with dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy and other measures to ensure its safe use. Sectigo and its affiliates disclaim any liability for any damages caused by such use of the documentation.

Sectigo, CodeGuard, Icon Labs are registered trademarks of Sectigo Limited and/or its affiliates. Other names may be trademarks of their respective owners.

The documentation may provide links to websites and access to content, products, and services from third parties. Sectigo is not responsible for the availability of, or any content provided on, third-party websites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Sectigo is not responsible for: (a) the quality of third-party products or services; (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Sectigo is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Table of Contents

Preface	
Audience	viii
Related documentation	viii
Conventions	viii
1 Understanding SCM	
Understanding SCM.....	1
Organizations, departments, and domains.....	1
Administrators	1
Certificates	2
Certificate profiles.....	2
Public vs private certificates.....	2
Enrollment options	3
Agents and certificate discovery.....	3
Notifications	3
Getting started with SCM.....	3
How to access SCM	3
Logging into SCM.....	4
Logging out of SCM	4
How to view your notifications.....	4
How to manage your profile.....	5
2 Understanding the SCM dashboard	
The SCM dashboard overview	8
Understanding charts.....	9
The Expiring Certificates chart	10
The Expiring Domain Validation chart	10
The Certificates Requested vs Issued chart.....	11
The Certificate Requests chart.....	11
The SSL Certificate Types (Managed) chart.....	12
The SSL Certificates by Validation Level chart	13
The Certificates by Template chart.....	13
The Certificates by CA chart	14
The Certificates by Duration chart	14
The DCV Status chart.....	15
The Certificates by Organization chart.....	16
The Key Strength chart.....	16
The Signature Algorithms chart	17
The Public Key Algorithms chart	18

3 Managing certificates

Certificate management overview	19
Managing SSL Certificates.....	20
SSL certificate parameters.....	22
How to view or modify SSL certificate details	24
Using the SSL Certificate Details tab.....	27
Using the Certificate Management tab	28
Using the Certificate Chain Of Trust tab	30
Using the Private Key Store to store and manage SSL certificate private keys	31
Editing notification email for issued SSL certificates	32
Restarting Apache server after auto-installation of SSL certificates.....	32
Updating the auto-renewal status	33
How to request and issue SSL certificates to web servers and hosts	33
Using the SSL certificate enrollment form	35
Using the SSL built-in enrollment wizard.....	40
Approving, declining, viewing, and editing certificate requests.....	70
Certificate collection and installation.....	71
How to import SSL certificates	73
SSL certificate CSV file format and importing guidelines	74
Bulk SSL certificate CSV file errors	74
How to renew SSL certificates	76
Certificate renewal by administrators.....	76
Certificate renewal by end-users	76
Automatic certificate renewal scheduling.....	77
How to revoke, replace, and delete SSL certificates	79
Certificate revocation by administrators	79
Certificate revocation by end-users.....	80
Replacing certificates.....	81
Managing Client Certificates	82
How to view end-user Client Certificates	84
How to view or modify Client certificate details	87
How to manage end-users.....	89
Adding end-users manually.....	90
End-user CSV file format and importing guidelines	92
End-user CSV file format and importing guidelines	92
Loading multiple end-users from a CSV file	95
Modifying and deleting end-users.....	96
How to request and issue Client Certificates to end-users.....	98
Enabling the end-user self-enrollment by access code	98
Enabling the end-user self-enrollment by secret identifier.....	103
Enabling the end-user enrollment by invitation	106
How to download private keys from Sectigo Key Vault and Key Escrow	109
How to revoke Client Certificates	109
Managing Code Signing Certificates	111
Modify code signing certificate.....	114
How to request and issue code signing certificates.....	115
Sending code signing certificate invitations	116
Completing the code signing certificate request.....	116
Code signing certificate CSV file format and importing guidelines	118
Managing Device Certificates.....	119
How to view device certificate details.....	121

How to request and issue device certificates	123
Issuing device certificates through SCEP	124
Issuing device certificates through self-enrollment	124
Issuing device certificates manually	127
Approving and declining device certificate requests	129
About device certificate collection.....	129
Resending the device certificate collection email.....	130
Revoking device certificates	130
4 Performing certificate discovery tasks	
Certificate discovery tasks overview	132
Performing network discovery tasks	133
How to add and modify network discovery tasks	135
How to import multiple network discovery tasks from a CSV file.....	138
Network discovery task CSV file format.....	138
How to delete a discovery task.....	139
How to run network discovery scans.....	139
How to view a history of network discovery tasks	140
Performing AD discovery tasks.....	142
How to add and modify MS AD discovery tasks	144
How to delete AD discovery tasks.....	147
How to run AD discovery scans.....	147
How to view a history of AD discovery tasks.....	147
Managing assignment rules	150
Managing certificate buckets.....	153
How to view certificates via certificate buckets	153
How to add and modify certificate buckets.....	154
How to manage authentication credentials in certificate buckets	155
How to manage Client Secret.....	155
Manually assigning certificates to organizations and departments.....	156
How to export MS AD discovery tasks and certificates to CSV from the certificate buckets	156
5 Configuring organizations and domains	
6 Generating reports	
7 Managing enrollments	
How to manage certificate profiles	160
Bulk enrollment of SSL certificates.....	160
Submitting bulk SSL requests	161
Managing bulk SSL requests.....	163
How to map MS AD certificate templates to SCM	166
Configuring enrollment endpoints.....	166
Creating and modifying enrollment form endpoints.....	169
Certificate enrollment authentication types	171
Adding and modifying web form accounts.....	172
How to configure SCEP endpoints	175
Managing SCEP RA certificates.....	176

Adding SCEP endpoints	177
How to add and modify accounts for SCEP endpoints	178
How to configure EST endpoints	180
Adding EST endpoints	180
How to add and modify accounts for REST endpoints	181
8 Using the Sectigo ACME Service	
Sectigo ACME service overview	183
Configuring ACME endpoints.....	185
How to manage ACME accounts	185
How to add and modify accounts for Sectigo public ACME servers	186
How to add and modify accounts for Universal ACME servers.....	187
How to view account details.....	188
Deleting ACME Accounts	189
ACME clients overview	190
How to view ACME clients details.....	190
How to use Certbot.....	191
9 Managing issuers	
CA Backends.....	196
How to manage private CAs.....	196
Requesting and adding a trial private CA	197
10 Using SCM with Microsoft Azure and Intune	
Microsoft Azure configuration overview	203
Configuring Azure for Azure Key Vault.....	204
How to set API permissions for Azure Key Vault.....	204
How to grant an application access to resource groups	207
How to grant an application access to Key Vaults	208
Configuring Azure for Intune SCEP	209
How to set API permissions for Intune SCEP	210
How to add Intune SCEP endpoints in SCM.....	213
How to create trusted certificate profiles	215
How to create SCEP profiles	216
Strong mapping in Microsoft Intune certificates	218
Issues and limitations related to different platforms	218
Configuring Azure for Intune Exporter	218
How to set application API permissions for Intune Exporter.....	219
How to configure Intune to use imported certificates	220
How to configure SCM for Intune Exporter	221
Registering applications in Azure	223
Creating Client Secret.....	224
Adding certificates.....	225
Configuring SCM Azure accounts	226
How to add an Azure account.....	227
How to delegate Azure accounts	228

11 SCM agent integrations

12 Configuring settings

The settings configuration overview.....	231
Configuring organizations, departments, and domains	235
How to define custom fields	235
Configuring notifications.....	235
Configuring notification templates	235
Configuring Key Escrow and encryption.....	236
About the master key requirements for issuing Client Certificates.....	236
How to configure Key Escrow for an organization or department.....	237
How to view and configure encryption settings.....	238
How to encrypt private keys.....	238
How to re-encrypt private keys.....	239
How to recover an end-user's private key from Escrow.....	241
Configuring access control	241
Configuring a Private Key Store	241
Managing SCM agents	242
Configuring assignment rules.....	242
Using Sectigo Key Vault	242
How to download an end-user's Private Key from Sectigo Key Vault.....	242
How to configure Sectigo Key Vault for use with iOS.....	243
Configuring Azure integration	245
Managing General settings.....	245

13 Managing administrators

Appendix A: CSV import format requirements

SSL certificate CSV file format and importing guidelines.....	B-2
End-user CSV file format and importing guidelines.....	B-4
Code signing certificate CSV file format and importing guidelines	B-7

Appendix B: Sectigo root and intermediate certificates

Sectigo root and intermediate certificates	C-1
Importing the Sectigo root certificate.....	C-1
Importing the Sectigo intermediate certificates.....	C-2

Preface

The *Sectigo Certificate Manager Administrator's Guide* explains how to use Sectigo Certificate Manager (SCM) to perform a variety of administrative tasks that largely depend on your security role.

Audience

The *Sectigo Certificate Manager Administrator's Guide* is intended for administrators working with SCM.

This document assumes that you are familiar with concepts related to security certificates issuance and management.

This document also assumes that you are familiar with your operating system. The general operation of any operating system is described in the user documentation for that system, and is not repeated in this manual.

Related documentation

- *SCM Release Notes*
- *SCM REST API Reference*

Conventions

The following text conventions are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles and emphasis.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, or text that appears on the screen.
< <i>text</i> >	Italic type with chevron brackets indicates the required insertion of user or company specific text.

Understanding SCM

Sectigo Certificate Manager (SCM) centralizes and streamlines the life-cycle management of web server, client, code signing, and device authentication certificates through a unified interface.

This chapter describes the following topics:

- [Understanding SCM](#)
- [Getting started with SCM](#)

1.1 Understanding SCM

The following sections provide an overview of the key concepts and features you should understand to be able to use SCM to efficiently manage your PKI infrastructure.

1.1.1 Organizations, departments, and domains

In SCM, organizations and departments are created by administrators for the purpose of requesting, issuing, and managing certificates for domains and employees.

Depending on the complexity of your enterprise, you can create multiple organizations, and each organization can have multiple departments. Once created, you can assign domains and administrators to specific organizations or departments.

Any certificate ordered through SCM must be assigned to an organization. Before you can request SSL, client, code signing, or device certificates, you must also create domains and delegate them to organizations or departments. To issue publicly trusted certificates, the delegated public domains must further pass domain control validation (DCV) to prove that you are the owner of the domain. Although, privately trusted certificates do not require a validated domain. Domains can be delegated to multiple organizations and departments.

To issue OV SSL certificates for organizations and their departments, the organizations must further be validated by Sectigo. The validation process for newly created organizations can be initiated from SCM.

At a minimum, your SCM configuration will include 1 organization, and if your account is configured for OV SSL certificates, the organization will be validated by Sectigo.

1.1.2 Administrators

There are three administrator roles in SCM:

- Master Registration Authority Officer (MRAO)
- Registration Authority Officer (RAO)

- Department Registration Authority Officer (DRAO)

Organizations are typically managed by a RAO, while departments are typically managed by a DRAO. An MRAO can manage all organizations and all departments.

At a minimum, your SCM configuration will include 1 MRAO. An MRAO can add administrators of any role (including other MRAOs).

1.1.3 Certificates

Depending on the features enabled for your account, SCM can be used to request and manage the following types of certificates:

- **SSL certificates** are used to secure communications between a website, host or server and end-users that are connecting to that server. An SSL certificate confirms the identity of the organization that is operating the website, encrypts all information passed between the site and the visitor, and ensures the confidentiality and integrity of all transmitted data.
- **Client certificates** (aka S/MIME) are issued to individuals and can be used to encrypt and digitally sign email messages, documents, and files, as well as to authenticate the identity of an individual prior to granting them access to secure online services.
- **Code signing certificates** are used to digitally sign software executables and scripts. Doing so helps ensure that the software is authentic by verifying the content source (authentication of the publisher of the software) and its integrity, as well as ensuring that the software has not been modified, corrupted or hacked since the time it was originally signed.
- **Device certificates** are issued to desktop and mobile devices to authenticate those devices to networks and Virtual Private Networks (VPNs).

1.1.3.1 Certificate profiles

Certificate profiles are used to provide an additional level of customization for your organizations and departments when ordering certificates from Sectigo. Using templates specified by Sectigo, you can customize features of your certificates, such as the validity period of the certificate, the allowed key types, and so on.

Every certificate created is based on a certificate profile, so at least one certificate profile of a certificate type is required to issue certificates of that type (e.g., at least one SSL certificate profile must be configured before you can request SSL certificates). Typically, your account will include several certificate profiles pre-configured by Sectigo.

1.1.3.2 Public vs private certificates

SCM can be used to issue publicly or privately trusted certificates.

Publicly trusted certificates can only be issued by Sectigo for validated domains belonging to validated organizations.

Privately trusted certificates can be issued on your own authority, and can be used to secure enterprise infrastructure, such as:

- Internal servers—Issue and manage private SSL certificates to secure internal web servers, user access, connected devices, and applications.
- Corporate email—Issue and manage private client certificates.

In SCM, privately trusted certificates are issued using a private CA. A private CA is required to issue device certificates. If your account includes private CA, the CA will be configured for you by Sectigo.

1.1.3.3 Enrollment options

Whether from a public or private CA, certificates can be enrolled in a variety of ways, depending on the features enabled for your account:

- Manually—Certificates can be ordered by administrators directly from SCM.
- Self-enrollment—External users can order certificates via enrollment endpoints, which can be accessed at a publicly accessible address that you communicate to the user.
- Programmatically—SCM provides Representational State Transfer (REST) and Simple Object Access Protocol (SOAP) APIs. For more information, see the *SCM REST API Reference* and *SCM Web Service SSL API* guides.
- ACME—SCM supports the Automatic Certificate Management Environment (ACME) protocol (RFC 8555) for issuing SSL certificates. The protocol automates interactions between web servers and CAs, including certificate installation, renewal, and domain validation.
- SCEP—SCM supports the Simple Certificate Enrollment Protocol (SCEP) for issuing client and device certificates.
- EST—SCM supports Enrollment over Secure Transport (EST).

1.1.4 Agents and certificate discovery

You may already have a variety of certificates issued by Sectigo or other vendors. To assign these existing certificates to SCM, you can use network agents to scan publicly accessible servers and internal networks and import any discovered certificates into SCM.

Agents can also be used for automatic installation and renewal of certificates.

1.1.5 Notifications

A wide range of organization- and department-specific email notifications can be set up to alert personnel to changes in certificate status, changes to domain status, discovery scan summaries, administrator creation, and so on.

1.2 Getting started with SCM

The following sections describe how to log in, get started, and manage your profile.

1.2.1 How to access SCM

SCM can be accessed through your organization's unique SCM URL. This URL must be communicated to you by Sectigo or by another administrator in your organization. By default, the format of this URL is similar to the following:

```
https://cert-manager.com/customer/<customer_uri>/
```

NOTE: For European customers, please use `https://eu.cert-manager.com/customer/<customer_uri>/` to access the SCM UI.

Where `<customer_uri>` is a path segment specific to your company. This identifier, often referred to as your URI in the context of this guide, is used in various parts of SCM.

Once you have access to your organization SCM login URL, you can log into SCM using the credentials provided by your account manager or, if configured, using an Identity Provider (IdP) for single sign-on (SSO) functionality.

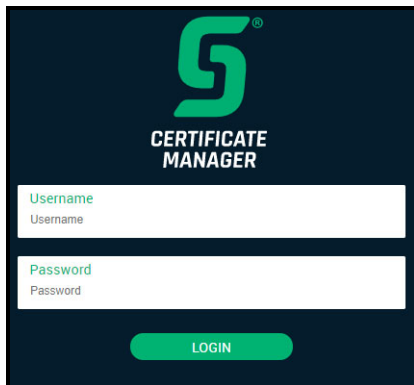
Alternatively, a direct IdP login URL may have been communicated to you, in which case a link to the IdP on the SCM login page does not appear.

NOTE: Your account may be configured to only allow logging in from your IdP and not from SCM directly.

1.2.2 Logging into SCM

To log into SCM, do the following:


1. Navigate to your SCM URL.



2. Validate your identity using one of the following methods:
 - Enter your SCM credentials and click **Login**.
 - If configured, click the name of your identity provider and enter your SSO credentials.
3. Depending on how your account was set up, you may be prompted to change your password after your first login. You will also see the license agreement.


1.2.3 Logging out of SCM

To log out of SCM, do the following:

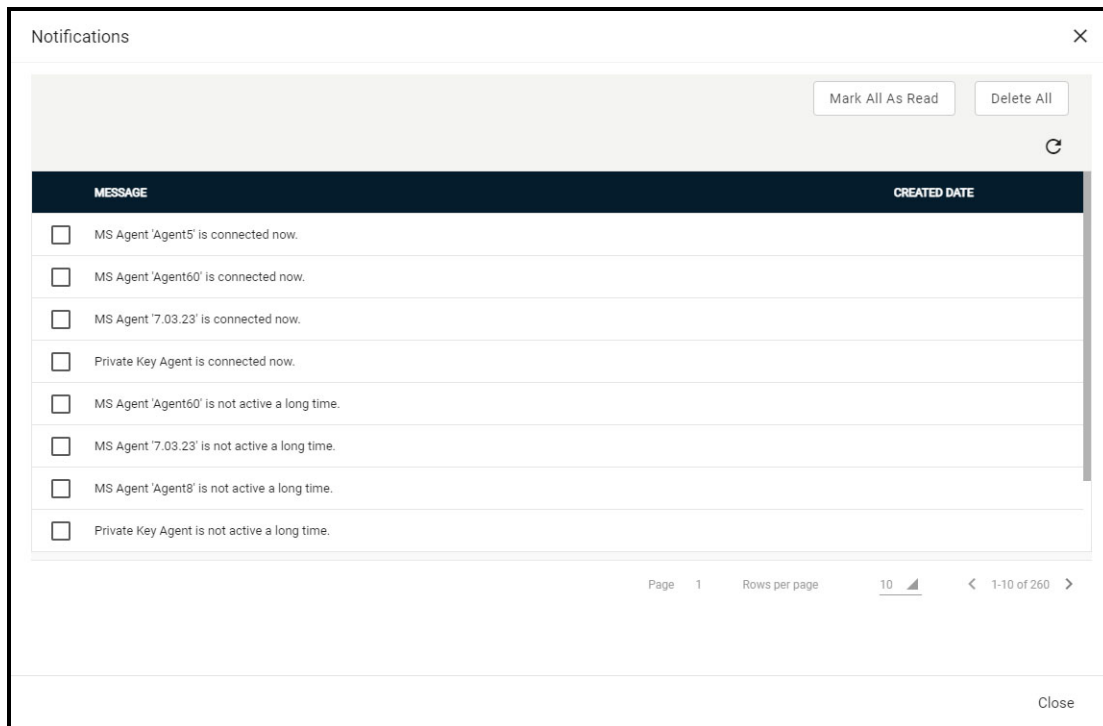
1. In the top-right corner of SCM, click the down arrow, and then click **Logout** .
2. Click **OK**.

1.2.4 How to view your notifications

The **Notifications** dialog provides you with notifications that are important to your administrative role. The types of messages displayed are related to validation, agents, and so on.

- To view your notifications, in the top-right corner of SCM, click  to display the **Notifications** dialog. Select a notification and click **Details**.
- To remove a notification from the list, select it and click **Delete**.

- Click **Delete All** to delete all notifications.
- Your unread messages are displayed in **bold**.
- Click **Mark All As Read** to mark them as read.



1.2.6 How to manage your profile

The **My Profile** dialog contains the details and personal settings of your profile. You can view or edit information about your account. The administrator details are also available via the **Admins** page.

You can access your profile by clicking your username in the top-right corner of SCM and selecting **My Profile**.

My Profile ✕

Username	admin
Name	admin mrao
Email	autotest@ccmqa.com
Role	MRAO Admin
Title	<input type="text"/>
Telephone Number	<input type="text"/>
Street Locality	<input type="text"/>
Zip / Postal Code	<input type="text"/>
Country	<input type="text"/>
Relationship	<input type="text"/>
Current locale	en
Password	<input type="button" value="Change"/>
Grid settings	<input type="button" value="Reset To Default"/>
Recent Activity	<input type="button" value="Show"/>

The following table outlines the fields and controls available in the **My Profile** dialog.

Field	Description
Username	The profile used to log into SCM (read only).
Name	The name associated with your profile (read only)
Email	The email address associated with your profile (read only)
Role	The SCM administrator role associated with your profile (read only)
Title	Your official or preferred title (e.g., Mr., Mrs.)
Telephone Number	Your contact telephone number
Street, Locality, State/ Province, Postal Code, Country	Your address, including the street, city (Locality), state or province, postal code, and country
Relationship	Your relationship with the company (e.g., employee, third party). Used when requesting and approving EV certificates
Current Locale	This enables you to change the SCM interface language. The settings take effect the next time you log in
Password	Click Change to change your password
Grid settings	Click Reset to default to revert all column widths and sorting preferences in SCM back to the default values
Recent Activity	Click Recent Activity to view a list of successful logins on your account. This list shows various information about each specific login

Understanding the SCM dashboard

This chapter describes how to use the SCM dashboard for viewing data on various parameters of certificates.

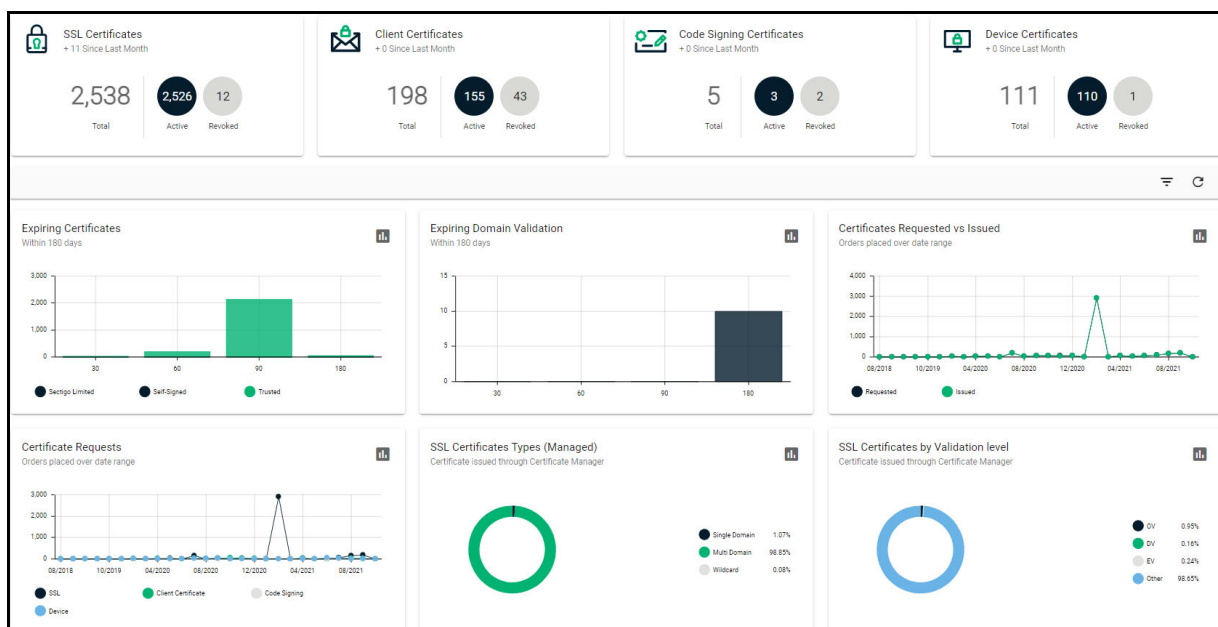
This chapter describes the following topics:


- [The SCM dashboard overview](#)
- [Understanding charts](#)

2.1 The SCM dashboard overview

The SCM dashboard shown in the following illustration is displayed by default when you log in to SCM. The dashboard provides an overview of all SSL, client, code signing, and device certificates on the network. The charts present a combination of the key lifecycle information, such as certificates approaching expiry, certificates issued and requested, as well as the DCV status. In addition, the charts provide important technical information, such as a number of servers that have support for perfect forward secrecy, renegotiation and RC4 suites. The chart data is updated in real time.

The row at the top of the dashboard displays an up-to-date summary of active and revoked certificates.



Clicking the chart icon  in the upper right corner of a chart displays a report with the breakdown of the chart statistics. Hovering the cursor over a legend or chart sector displays additional information.

The chart data presentation depends on your administrative security role, as follows:

- MRAO administrators can view charts for all certificate types, domains, and web servers pertaining to all organizations and departments.
- RAO SSL, RAO Client Certificate, and RAO Code Signing administrators can view charts relevant to the certificate types, domains, and web servers of the organizations and their subordinate departments that have been delegated to these administrators.
- DRAO SSL, DRAO Client Certificate, and DRAO Code Signing administrators can view charts relevant to the certificate types, domains, and web servers of the departments that have been delegated to these administrators.

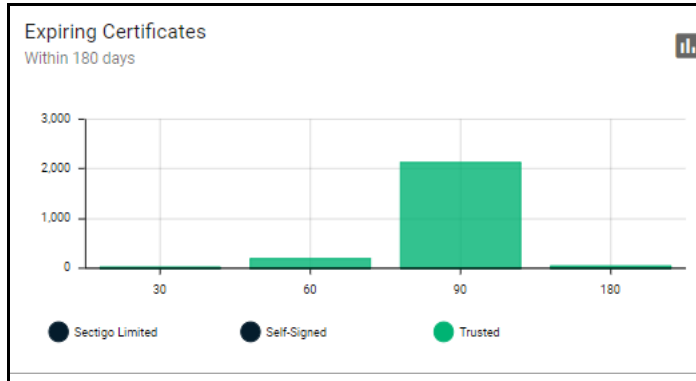
2.2 Understanding charts

The following charts are available through the dashboard:

- **Expiring Certificates**—Certificates expiring within the next 180 days per each certificate issuer.
- **Expiring Domain Validation**—Domains for which domain control validation expires within the next 180 days.
- **Certificates Requested vs Issued**—Certificate requests and how many of these requests have been issued, over time.
- **Certificate Requests**—Requested certificates, by certificate type, over time.
- **SSL Certificates Types (Managed)**—Managed certificates on your network by type (i.e., single domain, wildcard, multi domain, etc).
- **SSL Certificates by Validation Level**—Certificates by validation level, such as Domain Validated (DV), Organization Validated (OV), and Extended Validation (EV) levels.
- **Certificates by Template**—Certificates issued through SCM broken down by brand names (certificate profiles) such as Instant SSL, Premium SSL, and EV SSL.
- **Certificates by CA**—Certificates issued by different CAs, such as Sectigo, VeriSign, GoDaddy, Thawte, and self-signed.
- **Certificates By Duration**—Certificates issued for a specific duration, such as 1 year, 2 years, and 3 years.
- **DCV Status**—The current stage in the DVC process held by the certificate-hosting domains.
- **Certificates by Organization**—Certificates divided by the organizations to which these certificates have been issued.
- **Key Strength**—The strength of key with which the certificates were signed, such as 1024 bit, and 2048 bit.
- **Signature Algorithm**—Hashing and signing algorithms used, such as SHA1withRSA.
- **Public Key Algorithm**—Encryption algorithm used, such as RSA, and DSA.

2.2.1 The Expiring Certificates chart

The **Expiring Certificates** chart shown in the following illustration displays the number of certificates expiring within the next 30, 60, 90, and 180 days. These certificates are further broken down according to their signer. Trusted certificates are those from other CAs.

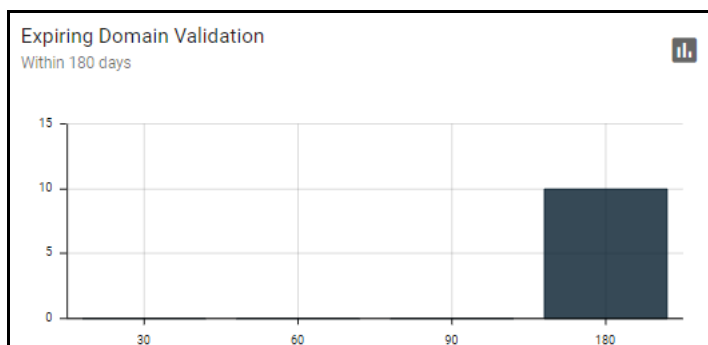


The following information is available:

- **Common Name**—the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- **Organization**—name of the organization that has been issued the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank if a department has not been delegated as the controlling entity.
- **Expires**—the expiration date of the certificate.

2.2.2 The Expiring Domain Validation chart

The **Expiring Domain Validation** chart shown in the following illustration indicates how many of your domains are within 30, 60, 90, and 180 days of the DCV expiry. Since the DCV validity lasts for one year, it is possible the DCV might be approaching expiry even though your certificate is not. If DCV is allowed to expire, it does not mean your certificate becomes invalid or stops functioning. However, your next application for that public domain would need to pass DCV again.



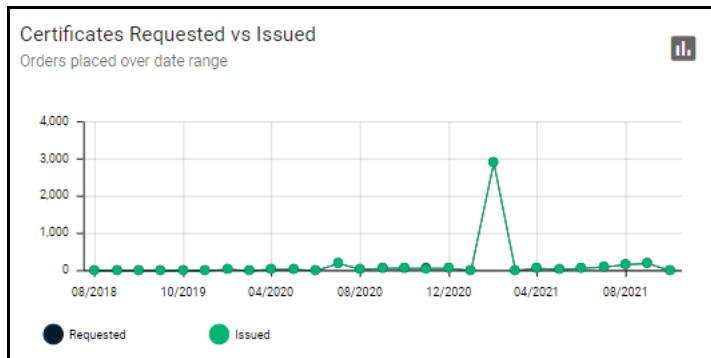
The following information is available:

- **Name**—the domain name.

- **Delegation Status**—indicates whether domain is active or inactive.
- **Date Requested**—the date on which the domain was requested.
- **DCV Status**—the request and approval status of the domain.

2.2.3 The Certificates Requested vs Issued chart

The **Certificates Requested vs Issued** chart shown in the following illustration enables you to compare the statistics of certificate issuance against certificate requests over time.

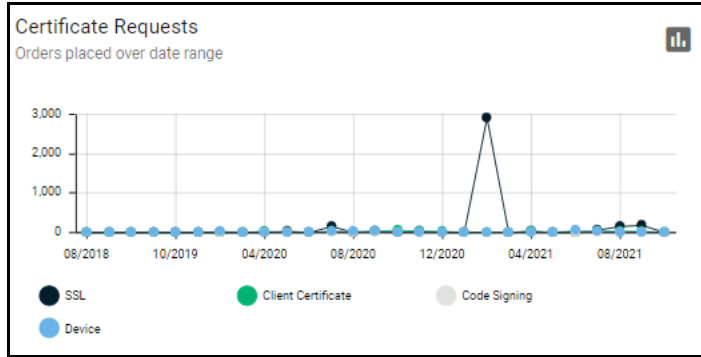


The following information is available:

- **Certificate Type**—the type of the issued or requested certificate.
- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Order Number**—the number assigned by the CA for the request.
- **Serial Number**—the unique identifier of the certificate.
- **Term**—the length of time for which the certificate is valid, starting from the time of issuance. For certificates that have not yet been approved, this is the certificate life time that was requested during the application process.
- **Status**—the current status of the certificate.
- **Requested**—the date when the certificate was requested by the end-user or administrator.
- **Collected**—the date when the certificate was collected by the end-user or administrator.
- **Expires**—the certificate expiry date.

2.2.4 The Certificate Requests chart

The **Certificates Requests** chart shown in the following illustration displays the number of SCM orders placed over time for SSL, client, code signing, and device certificates.

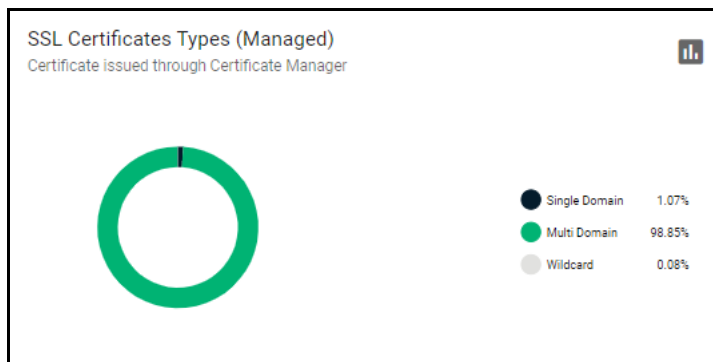


The following information is available:

- **Certificate Type**—the type of the issued or requested certificate.
- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Order Number**—the number assigned by the CA for the request.
- **Serial Number**—the unique identifier of the certificate.
- **Term**—the length of time for which the certificate is valid, starting from the time of issuance. For certificates that have not yet been approved, this is the certificate life time that was requested during the application process.
- **Status**—the current status of the certificate.
- **Requested**—the date when the certificate was requested by the end-user or administrator.
- **Collected**—the date when the certificate was collected by the end-user or administrator.
- **Expires**—the certificate expiry date.

2.2.5 The SSL Certificate Types (Managed) chart

The **SSL Certificate Types (Managed)** chart shown in the following illustration summarizes the different types of SSL certificates issued through SCM and installed on servers within your network, such as single domain, multi domain, wildcard, or private.



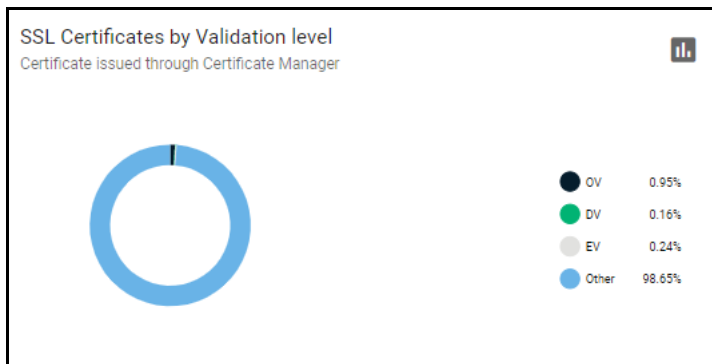
The following information is available:

- **Common Name**—the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.

- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Sub Type**—the sub type of each certificate.
- **Certificate Profile**—the certificate profile associated with the certificate.

2.2.6 The SSL Certificates by Validation Level chart

The **SSL Certificates by Validation Level** chart shown in the following illustration displays the composition of your certificate portfolio according to the certificate validation level, including the number of DV, OV, and EV certificates on your network.

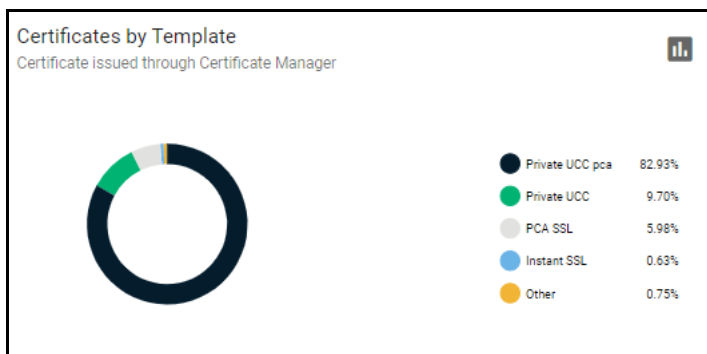


The following information is available:

- **Common Name**—the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Sub Type**—the sub type of the certificate.

2.2.7 The Certificates by Template chart

The **Certificates by Template** chart shown in the following illustration details the quantities of SSL certificates issued by SCM according to the certificate profile used.



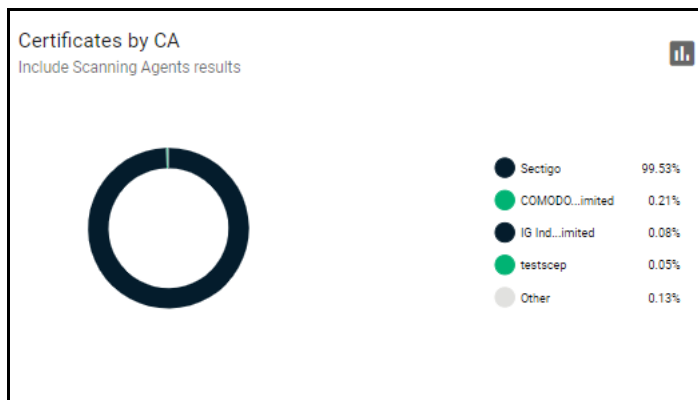
The following information is available:

- **Common Name**—the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Certificate Profile**—the certificate profile associated with the certificate.

NOTE: Issued certificates are displayed in blue.

2.2.8 The Certificates by CA chart

The **Certificates by CA** chart shown in the following illustration provides a breakdown of your certificates by signer, allowing you to determine the percentage of the publicly trusted certificates in your portfolio. This includes all certificates signed by CAs as well as self-signed certificates. This chart also highlights certificates issued by CAs other than Sectigo.



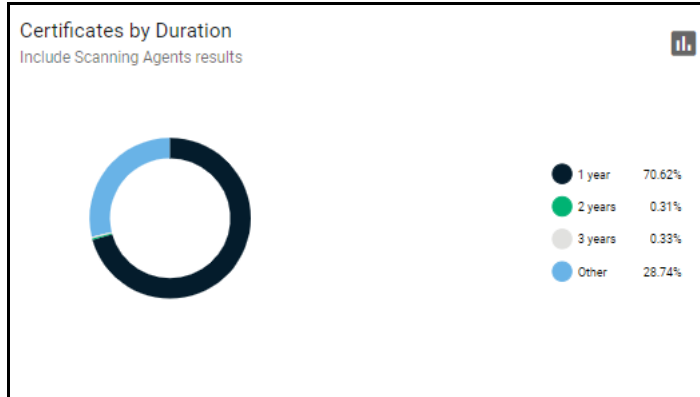
The following information is available:

- **Common Name**—the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Vendor**—the domain name of the vendor that issued the certificate.

NOTE: Issued certificates are displayed in blue.

2.2.9 The Certificates by Duration chart

The **Certificates by Duration** chart shown in the following illustration presents a breakdown of your certificates by the length of their term.



The following information is available:

- **Certificate Type**—the type of the issued or requested certificate.
- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Order Number**—the number assigned by the CA for the request.
- **Serial Number**—the unique identifier of the certificate.
- **Term**—the length of time for which the certificate is valid, starting from the time of issuance. For certificates that have not yet been approved, this is the certificate life time that was requested during the application process.
- **Status**—the current status of the certificate.
- **Requested**—the date when the certificate was requested by the end-user or administrator.
- **Collected**—the date when the certificate was collected by the end-user or administrator.
- **Expires**—the certificate expiry date.

2.2.10 The DCV Status chart

The **DCV Status Chart** chart shown in the following illustration shows a summary of the DCV status of registered domains. DCV is required for Sectigo to issue certificates for public domains and subdomains.

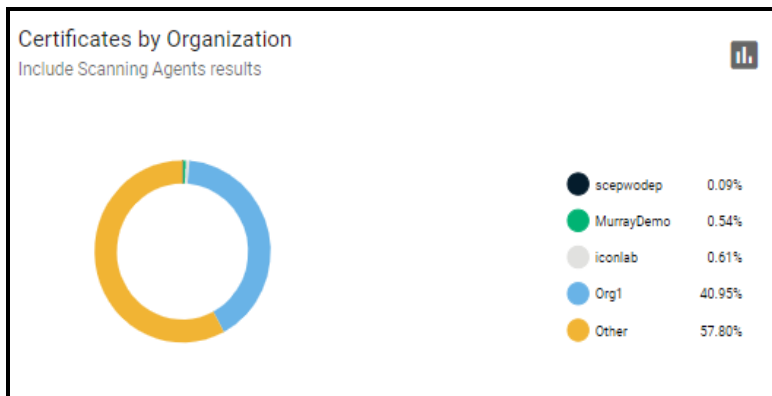


The following information is available:

- **Name**—the domain name.
- **Delegation Status**—the delegation status of the domain, such as approved, requested, and so on.
- **Date Requested**—the date on which the domain was requested.
- **DCV Status**—the validation status of the domain, such as validated, validated (revalidation), expired (revalidation), and awaiting submittal.

2.2.11 The Certificates by Organization chart

The **Certificates by Organization** chart shown in the following illustration displays how many certificates have been issued to each organization under your SCM account.

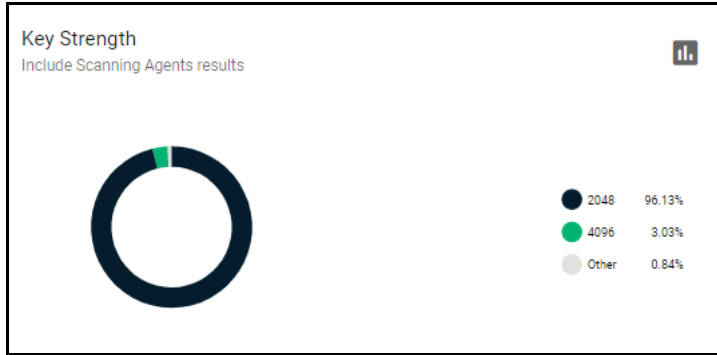


The following information is available:

- **Certificate Type**—the type of the issued or requested certificate.
- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Order Number**—the number assigned by the CA for the request.
- **Serial Number**—the unique identifier of the certificate.
- **Term**—the length of time for which the certificate is valid, starting from the time of issuance. For certificates that have not yet been approved, this is the certificate life time that was requested during the application process.
- **Status**—the current status of the certificate.
- **Requested**—the date when the certificate was requested by the end-user or administrator.
- **Collected**—the date when the certificate was collected by the end-user or administrator.
- **Expires**—the certificate expiry date.

2.2.12 The Key Strength chart

The **Key Strength** chart shown in the following illustration displays the composition of your certificate portfolio based on the size of the certificates' signatures. This can be useful for identifying certificates that need to be replaced to comply with National Institute of Standards (NIST) recommendations. NIST has stated that all certificates, using the RSA algorithm, issued after January 1, 2014 should be of at least 2048 bit in key length.



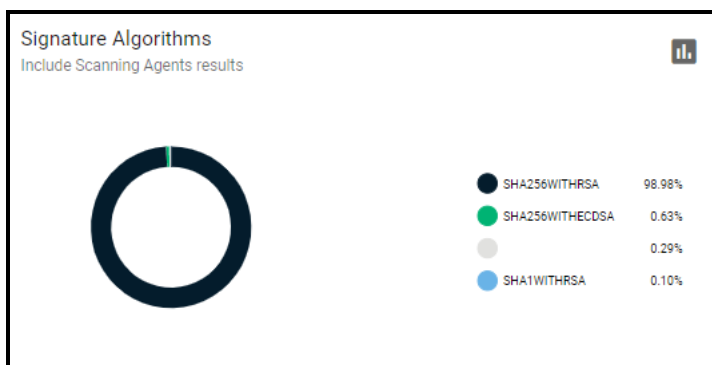
The following information is available:

- **Common Name**—the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Expires**—the date of the certificate expiry.
- **Key Algorithm**—the type of algorithm used, by the public and private keys, for encryption. For example, RSA, DSA, and EC.
- **Key Size**—the key size used, on the public and private keys, for encryption. For example, 1024, 2048, and 4096.

NOTE: Issued certificates are displayed in blue.

2.2.13 The Signature Algorithms chart

The **Signature Algorithms** chart shown in the following illustration provides an overview of the algorithms used by your certificates to hash and sign data. This chart helps with identifying certificates that are based on weaker algorithms which may need to be replaced before their expiry dates. Sectigo recommends SHA-256 and upwards, since MD5 has been proven insecure and Microsoft has stated that its products stopped trusting SHA-1 code signing and SSL certificates in 2016 and 2017 respectively.

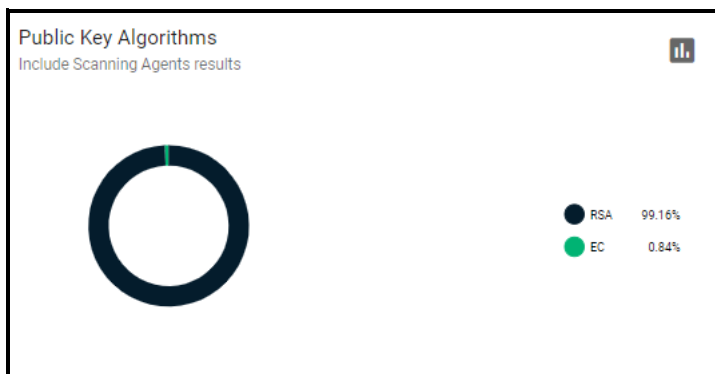


The following information is available:

- **Common Name**—the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Expires**—the date of the certificate expiry.
- **Signature Algorithm**—the type of signature algorithm used by the certificate. For example, SHA1 with RSA, SHA 256 with RSA, SHA384 with RSA, etc.

2.2.14 The Public Key Algorithms chart

The **Public Key Algorithms** chart shown in the following illustration provides an overview of the algorithms used to encrypt data by certificates on your network.



The following information is available:

- **Common Name**—the domain for which the certificate was issued. This domain name refers to the **Common Name** field in the SSL certificate itself.
- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Expires**—the date of the certificate expiry.
- **Signature Algorithm**—the type of signature algorithm used by the certificate. For example, SHA1 with RSA, SHA 256 with RSA, SHA384 with RSA, etc.
- **Key Algorithm**—the type of algorithm used, by the public and private keys, for encryption. For example, RSA, DSA, and EC.

Managing certificates

This chapter describes how to use SCM to request, collect, and manage certificates and explains the processes behind the administration and provisioning of various types of certificates.

This chapter describes the following topics:

- [Certificate management overview](#)
- [Managing SSL Certificates](#)
- [Managing Client Certificates](#)
- [Managing Code Signing Certificates](#)
- [Managing Device Certificates](#)

3.1 Certificate management overview

In SCM, certificate management is performed through the **Certificates** page which, depending on your privilege level, enables you to request, collect, revoke, and modify SSL, client, code signing, and device certificates.

The **Certificates** page shown in the following illustration is divided into the following four administrative areas:

- SSL Certificates
- Client Certificates
- Code Signing Certificates
- Device Certificates

ID	STATUS	COMMON NAME	COMMENTS	ORDER NUMBER
85216	ISSUED	*.ccmqa.com	Enrolled for SCM Extra Agent	3423871
85231	ISSUED	ccmqa.com		3440312
85236	ISSUED	multinst1.local	Enrolled for SCM Extra Agent	3620247
85237	ISSUED	multinst2.local	Enrolled for SCM Extra Agent	3620489
85754	ISSUED	ccmqa.com	Enrolled for SCM Extra Agent	3636111
85651	ISSUED	ccmqa.com	test	3625082
85215	ISSUED	apache38.ccmqa.com	Enrolled for SCM Extra Agent	3423676
86017	ISSUED	21.10.22.local	Enrolled for SCM by ms Agent	3643638
85740	ISSUED	16.02.2022.md.ov.ccmqa.com (renewed)	md.ov.azure.kv@ccmqa.com@10/16/2022	3635637
85758	ISSUED	ccmqa.com		

In addition to using the **Certificates** page, you can run a discovery scan on your servers to audit and monitor the entire network for all installed SSL certificates, including certificates issued by vendors other than Sectigo. Once completed, the discovered certificates are automatically imported into the **Certificates** page. For more information, see [“Performing certificate discovery tasks”](#) on page 132.

3.2 Managing SSL Certificates

The **SSL Certificates** page provides MRAOs, nominated RAO SSL, and nominated DRAO SSL administrators with the information and controls necessary to manage the life cycle of SSL certificates for an organization, as follows:

- MRAOs can request and manage SSL certificates for any organization and department. They can approve and decline certificate requests for any organization or department.
- RAO SSL administrators can request and manage certificates for their delegated organizations. They can approve and decline certificate requests for their organization.
- DRAO SSL administrators can request SSL certificates for domains belonging to their delegated departments. They can approve and decline certificate requests for their departments.

The screenshot shows the Sectigo Certificate Manager interface. The main area displays a table of SSL certificates with the following columns: ID, STATUS, COMMON NAME, COMMENTS, and ORDER NUMBER. The table contains 12 rows of certificate data. The left sidebar shows navigation options like Dashboard, Certificates, Client Certificates, Code Signing Certificates, Device Certificates, Discovery, Domains, Organizations, Persons, Reports, Enrollment, and Issuers. The top right corner shows the user 'admin mrao' and a search bar.

ID	STATUS	COMMON NAME	COMMENTS	ORDER NUMBER
85210	ISSUED	*.comqa.com	Enrolled for SCM Extra Agent	3423871
85231	ISSUED	comqa.com		3440312
85236	ISSUED	multinst.local	Enrolled for SCM Extra Agent	3620247
85237	ISSUED	multinst2.local	Enrolled for SCM Extra Agent	3620489
85754	ISSUED	comqa.com	Enrolled for SCM Extra Agent	3636111
85651	ISSUED	comqa.com	test	3625082
85215	ISSUED	#apache38.comqa.com	Enrolled for SCM Extra Agent	3423676
86017	ISSUED	21.10.22.local	Enrolled for SCM by ms Agent	3643638
85740	ISSUED	18.02.2022.mtl-ov.comqa.com (renewed)	mtl-ov.azure.kv@comqa.com@10/16/2022	3635637
85758	ISSUED	comqa.com		

The following control buttons may be displayed, depending on the status of a selected certificate:

- **Search**— Enables you to search certificates by ID, common name, or subject alternative name.
- **Import**— Enables you to import SSL certificates in .cer, .crt or .pem format. See [“How to import SSL certificates” on page 73](#).
- **Add** (the + icon in the upper-right corner of the screen)— Enables you to add a new certificate using the built-in enrollment wizard. See [“Using the SSL built-in enrollment wizard” on page 40](#).
- **Filter**— Enables you to sort the table information using custom filters.
- **Group**— Enables you to sort the table information using predefined groups.
- **Refresh**— Enables you to refresh the page.
- **Download CSV**— Enables you to export the currently displayed list to a spreadsheet in .csv format.
- **Manage Columns**— Enables you to select which parameters to display on the page.
- **Delete**— Delete the selected certificate.
- **Edit**— Enables you to modify SSL certificate parameters. This option is available only for certificates with a status of Requested, Rejected, Declined, or Invalid. See [“Approving, declining, viewing, and editing certificate requests” on page 70](#).
- **View**— Enables you to view information about the certificate. For more information, see [“How to view or modify SSL certificate details” on page 24](#).
- **Renew**— Opens the **Renew Certificate** dialog pre-populated with the company and domain details of the existing certificate. Clicking **OK** submits the certificate renewal request. This button is available only for the certificates with the status of Issued and Expired. See [“How to renew SSL certificates” on page 76](#).
- **Revoke**— Revokes the certificate. See [“How to revoke, replace, and delete SSL certificates” on page 79](#).
- **Replace**— Replaces the existing certificate with a new one, after prompting you to specify a new CSR. See [“How to revoke, replace, and delete SSL certificates” on page 79](#).
- **Install**— Activates the auto-installer tool to install the certificate on the target web server. For more information, see [“Generation of CSR with auto-installation” on page 55](#).
- **Approve**— Approves certificate requests and sends the request for the certificate to Sectigo, as the issuing CA. Once submitted, the certificate status changes to Applied. If the request is approved by Sectigo, the certificate's status changes to Issued. If the request was declined by Sectigo because of incorrect enrollment information (for example, a mistake in the CSR or

other form field), then the status would be listed as Invalid. If the request was declined by Sectigo for legal reasons, then the certificate would have a status of Rejected. Certificate requests can be approved by (1) a MRAO SSL administrator; (2) a RAO SSL administrator of the organization on whose behalf the request was made; (3) a DRAO SSL administrator of the department on whose behalf the request was made. See [“Approving, declining, viewing, and editing certificate requests” on page 70.](#)

- **Decline**—Declines the certificate request. This request is not sent to Sectigo for processing. See [“Approving, declining, viewing, and editing certificate requests” on page 70.](#)
- **Set Auto Renewal & Installation**—Creates a schedule for auto-renewing a certificate in advance of its expiry, and to configure auto-installation of the renewed certificate. For more information, see [“Automatic certificate renewal scheduling” on page 77.](#)
- **View Audit**—Enables you to view audit details for the certificate.

3.2.1 SSL certificate parameters

The following parameters exist for SSL certificates. You can choose which ones to display on the SSL Certificates page by selecting or deselecting them under **Manage Columns** in the top right.

Field	Description
Common Name	The domain name that was used during the SSL certificate request. This domain name refers to the common name in the SSL certificate itself.
General	
ID	ID number of the certificate.
Status	The status of the certificate.
Comments	Comments that don't fit under any other heading.
Order	
Order Number	The order number of the certificate request.
Certificate Profile	The brand name of the certificate.
Sub Type	The sub type of the certificate.
Term	The term of the certificate.
Requester	The email address of the end-user who requested this certificate through the self-enrollment form, or the name of the administrator who requested this certificate using auto-installation or the built-in wizard.
Requested Via	How the certificate was requested. For example, via Discovery, Web Form, Client Admin, ACME.
Approver	The name of the person who approved the certificate.
Certificate	
Subject	The Subject Distinguished Name (Subject DN) who was issued the certificate.

City	The name of the city entered when the organization or department was created.
State	The name of the state or province entered when the organization or department was created.
Country	The name of the country entered when the organization or department was created.
Subject Alt Name	The domain names for which the certificate is used.
Issuer	The details of the CA that issued the certificate, as well as the name of the certificate.
Expires	The date when the certificate expires.
Serial Number	The serial number of the certificate that is unique and can be used to identify the certificate.
Key Usage	The cryptographic purposes for which the certificate can be used. For example, key encipherment and signing.
Extended Key Usage	The higher level capabilities of the certificate. For example, web server authentication and client authentication.
Key Algorithm	The type of algorithm used for the encryption.
Key Size/Curve	The key size or curve used for the encryption.
Signature Algorithm	The signature algorithm of the certificate public key.
MD5 Hash	The MD5 hash (thumb print or fingerprint) for the certificate.
SHA1 Hash	The SHA1 hash (thumb print or fingerprint) for the certificate.
Ownership	
Organization	The name of the organization that requested or has been issued with the certificate.
Department	The department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
Timespan	
Requested	The date of the certificate request.
Approved	The date the certificate was approved.
Declined	The date the certificate was declined.
Issued	The date the certificate was issued.

Downloaded	The date the certificate was downloaded
Discovered	The date the certificate was discovered.
Revoked	The date the certificate was revoked.
Replaced	The date the certificate was replaced.
Management	
External Requester	The email address of the requester on behalf of which the administrator applied for this certificate through the built-in application form in SCM. Any email address(es) found in the Subject DN (Email field) and/or Subject Alternative Name (SAN) extension during a certificate discovery scan are included in the External Requester field.
Private Key	Indicates whether the certificate private key is managed by the PKS, and which PKS it is.
Install state	Indicates the current state of scheduled certificate installations, which can be one of the following: <ul style="list-style-type: none"> • Not Scheduled—The certificate is not scheduled for auto-installation. • Scheduled—The certificate is scheduled for auto-installation. • Started—Certificate installation on the remote server has started as scheduled. • Successful—The certificate was successfully installed on the remote server at the scheduled time. • Failed—Certificate installation on the remote server failed.
Renewal state	Indicates the current state of scheduled certificate auto-renewal, which can be one of the following: <ul style="list-style-type: none"> • Not Scheduled—The certificate is not scheduled for auto-renewal. • Scheduled—The schedule has been defined for auto-renewal of the certificate. • Started—The auto-renewal process has started as scheduled. • Successful—The certificate has been successfully auto-renewed and installed. • Failed—Auto-renewal of the certificate has failed.
Custom Fields	
name1	Use this field to give the certificate a custom name.

3.2.2 How to view or modify SSL certificate details

To view or modify the SSL certificate details, do the following:

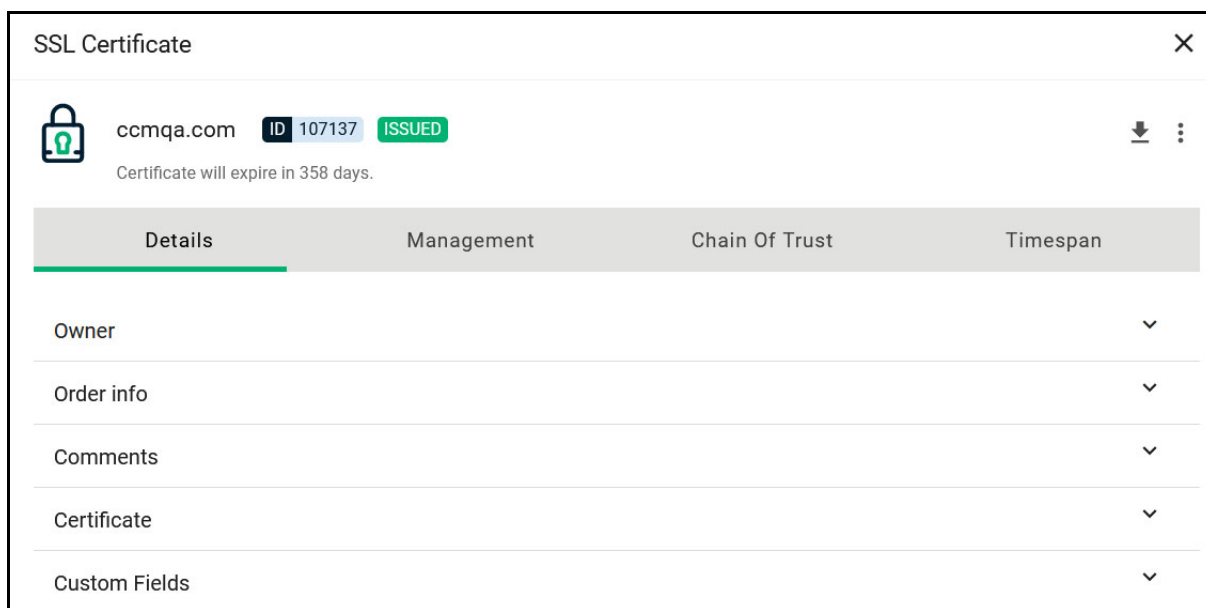
1. Navigate to **Certificates > SSL Certificates**.
2. Select a certificate in the list.
3. Click **View**.

This opens the **SSL Certificate** dialog that differs depending on the certificate's status. This screen enables you to do the following:

- View status and summary information

- Download the certificate in different formats
- View ownership and order information if certificate was requested using SCM
- Change ownership at any certificate status
- Configure notifications
- Configure auto-installation and auto-renewal
- View discover status
- View and manage private key if applicable
- View the full certificate chain

The **Certificate Summary** panel displays the number of days remaining before the certificate expires, along with SCM- and server-related information about the certificate and other controls. The contents of the **Certificate Summary** panel depends on the current status of the certificate.



The Certificate summary panel displays the following information:

- The **domain name** that was used during the SSL certificate request. This domain name refers to the common name in the SSL certificate itself.
- **ID number** of the certificate
- The certificate **status**
- The time until the certificate **expires**
- The **download** button which allows downloads in the following formats:
 - Certificate only, PEM encoded (.cer)
 - Certificate (w/ issuer after), PEM encoded (.pem)
 - Certificate (w/ chain), PEM encoded (.cer)
 - PKCS#7 (.p7b)
 - PKCS#7, PEM encoded (.crt)
 - Intermediate(s)/Root only, PEM encoded (.cer)
 - Root/Intermediate(s) only, PEM encoded (.cer)

- Certificate and Private key, PKCS#12 (.p12). The P12 format is only available if the PKS feature is enabled for your account, the PK agent is installed on your local network, and the certificate private key is being managed by the PKS.
- Additional information arranged in four tabs:
 - Details
 - Management
 - Chain of Trust
 - Timespan

3.2.2.1 Using the SSL Certificate Details tab

The Details tab contains information in some or all of the following fields, depending on the specific certificate:

- Ownership - the organization, department, and name of the requester and approver (as applicable) of the certificate. Certificate ownership can be moved between departments and their parent organization to ensure continuity of certificate management.
- Order information - the order number, certificate profile, sub type, term, and request type.
- Comments
- Certificate - the subject, issuer, serial number, key usage, extended key usage, validity dates, key type, vendor, MD5 hash, SHA1 hash
- Custom fields

SSL Certificate

sectigo.com ID 104295 ISSUED
Certificate will expire in 346 days.

Details Management Chain Of Trust Timespan

Ownership ^

Organization org3

Requester admin mrao

Approver admin mrao

Order info ^

Order Number 4450690

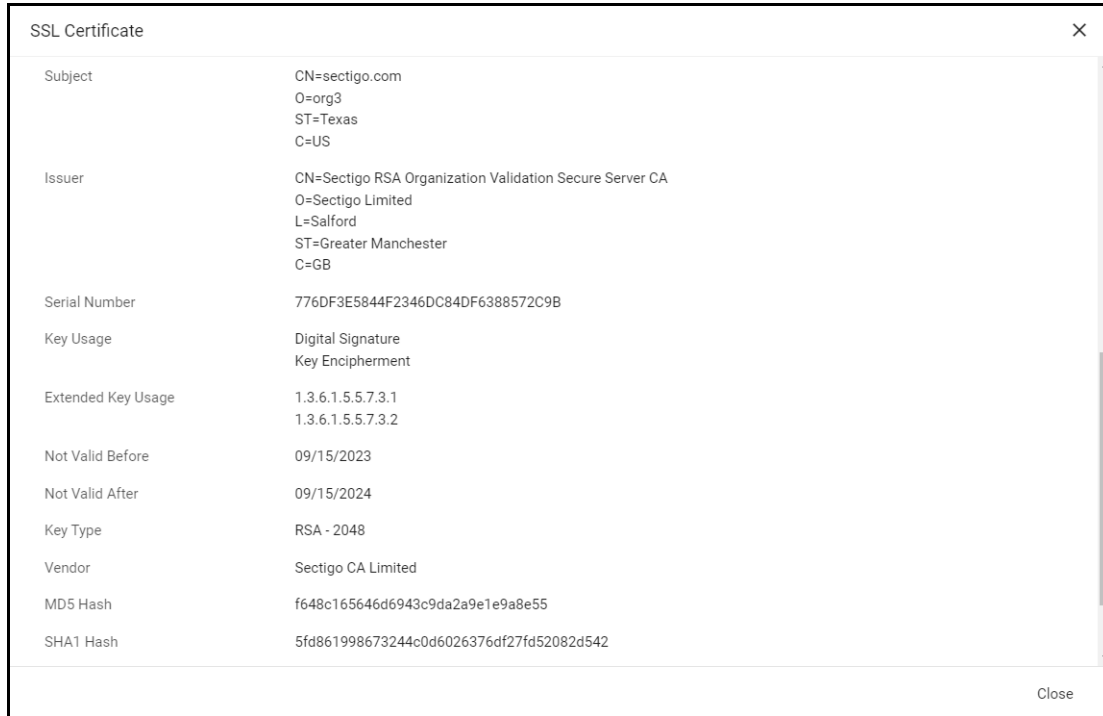
Certificate Profile Instant SSL

Sub Type OV

Term 365

Request Type Admin

Close

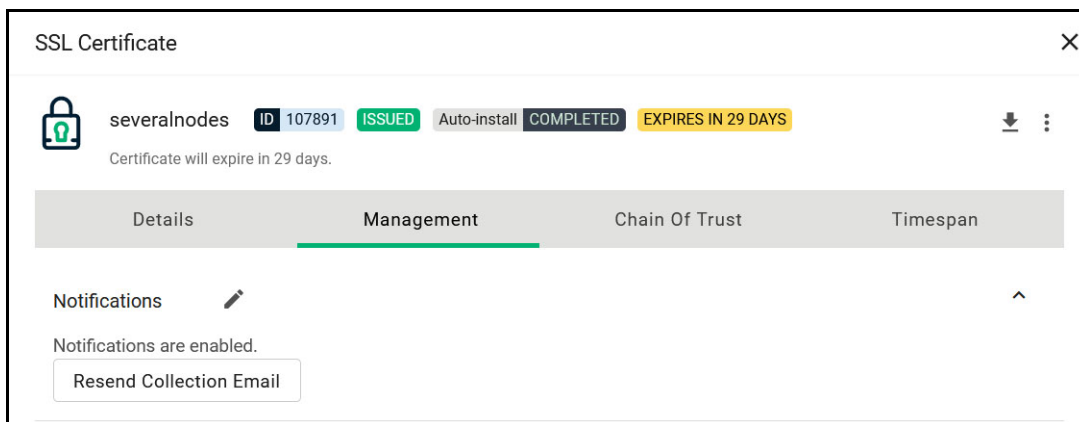


3.2.2.2 Using the Certificate Management tab

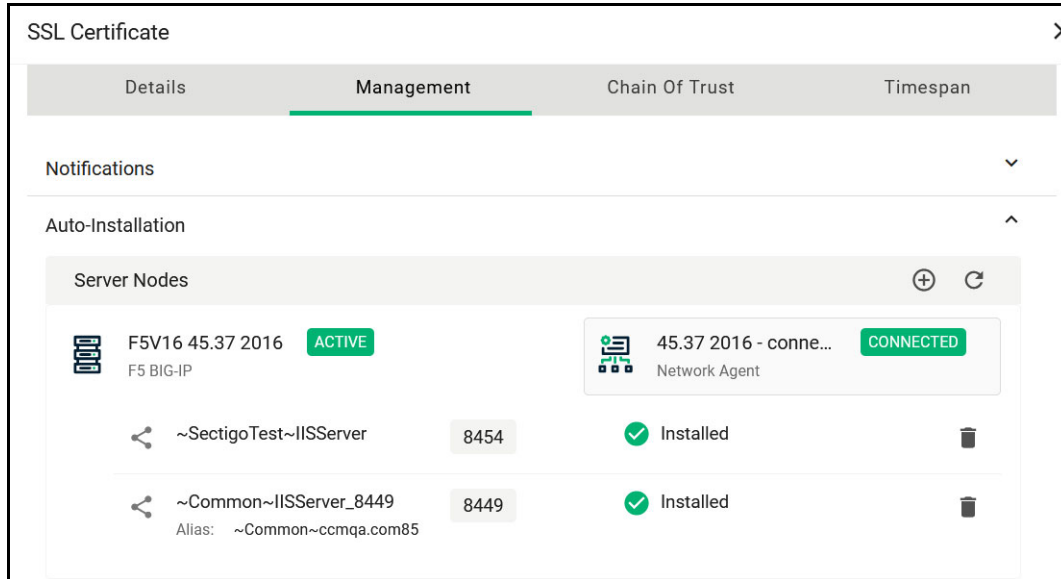
The **Certificate Management** tab displays the following management related features of certificates.

- Notifications
- Auto-installation
- Auto-renewal
- Locations
- Self Enrollment

In **Notifications**, you can view and modify notifications for the certificate.



In **Auto-installation**, you have information about server nodes associated with the certificate.



Locations describes where the certificate exists outside of SCM.

- Custom
 - Available for all certificate types
 - Created manually by the user
 - Fields: Name and Details
 - Multiple allowed, can be edited or deleted
- ACME Client
 - SSL Certificates only
- Network Host
 - SSL certificates only
 - created by network discovery scans
 - Fields: IP/port and Hostname (if known)
- Network Agent
 - SSL Certificates only
 - created by SCM during auto-install process
 - Fields: Alias (in local keystore), Agent ID, Agent Name
 - Also contains Private Key indicator
- Server Node/Port
 - SSL certificates only
 - Created by SCM during server discovery process or auto-install process
 - Fields: Agent ID, Agent Name, Server Name, Node, Port
- Private Key Agent
 - SSL certificates only
 - Created by SCM during auto-install process
 - Fields: Alias (in local keystore), Agent ID, Agent Name
 - Also contains Private Key indicator

- Azure Key Vault
 - SSL certificates only
 - Created by SCM during enroll with "Generation of CSR in Azure Key Vault"
 - Fields: Vault Name, URI, Certificate Name, Exportable Key flag
 - Also contains Private Key indicator
- Active Directory Entry
 - Available for all certificate types
 - Created by AD discovery scans
 - Fields: Object Type (User/Computer/Container), Name, DN, UPN

The screenshot shows a window titled "SSL Certificate" with a "Locations" section containing one entry: "Azure Key Vault" (Azure Key Vault Account 28.10). To the right, the details for this location are displayed in a table format:

Azure Key Vault	
URI	https://rustest-kv.vault.azure.net/certificates/ccmqa-com/pending
Name	Azure Key Vault Account 28.10
Certificate name	ccmqa-com
Private key exist	YES
Exportable Key	NO

3.2.2.3 Using the Certificate Chain Of Trust tab

The Certificate Chain Of Trust tab displays the details of the root and intermediate certificates linked to the SSL certificate chain.

The screenshot displays the 'SSL Certificate' management window. At the top, it shows the certificate's status: 'local', 'ID 88442', 'ISSUED', and 'Auto-renew NOT SCHEDULED'. Below this, there are tabs for 'Details', 'Management', 'Chain Of Trust' (which is selected), and 'Timespan'. The 'Chain Of Trust' tab shows a list of certificates in the chain:

- Sectigo Dev RSA Certification Authority**: Expires: 01/19/2038, Root Certificate.
- Sectigo Dev RSA Intermediate CA**: Expires: 01/01/2031, Intermediate Certificate.
- local**: Expires: 09/23/2023, End Entity.

On the right side of the 'Chain Of Trust' tab, there are expandable sections for 'Fields', 'Extensions', and 'Properties'. A 'Close' button is located at the bottom right of the window.

3.2.2.4 Using the Private Key Store to store and manage SSL certificate private keys

About private keys:

- For certificates enrolled by manually entering the CSR, you can upload the certificate's private key to the PKS. See detailed instructions [here](#).
- For certificates whose keys are managed by the PKS, you can download the certificate in .p12 format.
- This field is displayed only if the PKS feature is enabled for your account, and a Private Key Agent is installed on your local network.
- Private keys can only be uploaded and downloaded by administrators that have a valid client certificate selected under the **Certificate Auth** option in their administrator settings. See "[Managing administrators](#)".
- For certificates whose keys are managed by the private key store, there is a passphrase for the private key. The passphrase is displayed if **Show Passphrase** is enabled. This phrase is required to import the certificate on to any server, after downloading the certificate in .p12 format. This field is displayed only if the PKS feature is enabled for your account, a Private Key Agent is installed on your local network, and the certificate keys are managed by the private key store.

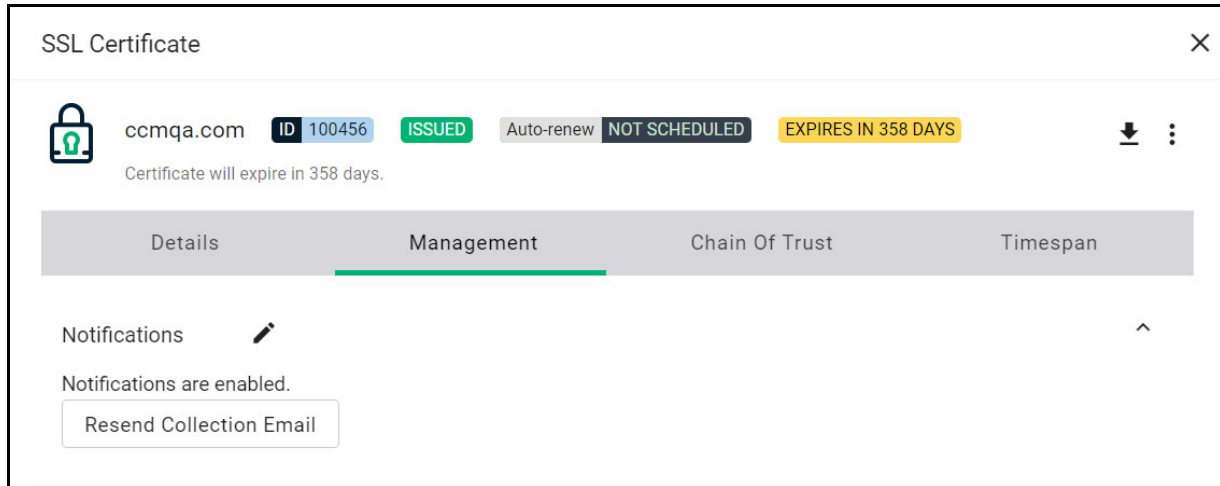
If the Private Key Store (PKS) is configured on your local network, you can upload the private key associated with this certificate for storage and management by the PKS. You can also download the private key of SSL certificates whose private keys are stored and managed by the PKS, and delete the key from the PKS.

To use this functionality, the PKS feature must be enabled for your account, and the PKS agent installed and configured on your local network. See detailed instructions [here](#).

To upload, download, or remove private keys, see instructions [here](#).

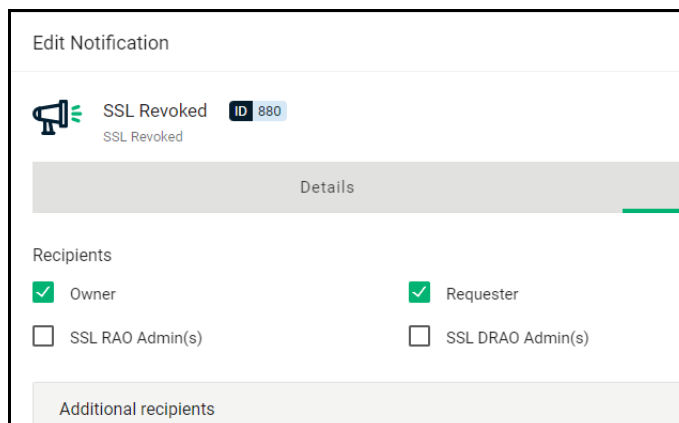
3.2.2.5 Editing notification email for issued SSL certificates

An automated notification email for certificate collection is sent to the domain administrator once SCM issues the certificate.



If the certificate is not downloaded by the domain administrator, you can resend the notification or edit it by going to the **Certificate Summary panel/Management** tab for issued SSL certificates.

You can resend the certificate collection email to the domain administrator, the applicant that applied for the certificate through the self-enrollment form, or the applicant on whose behalf the administrator has applied for the certificate through the built-in enrollment form.



3.2.2.6 Restarting Apache server after auto-installation of SSL certificates

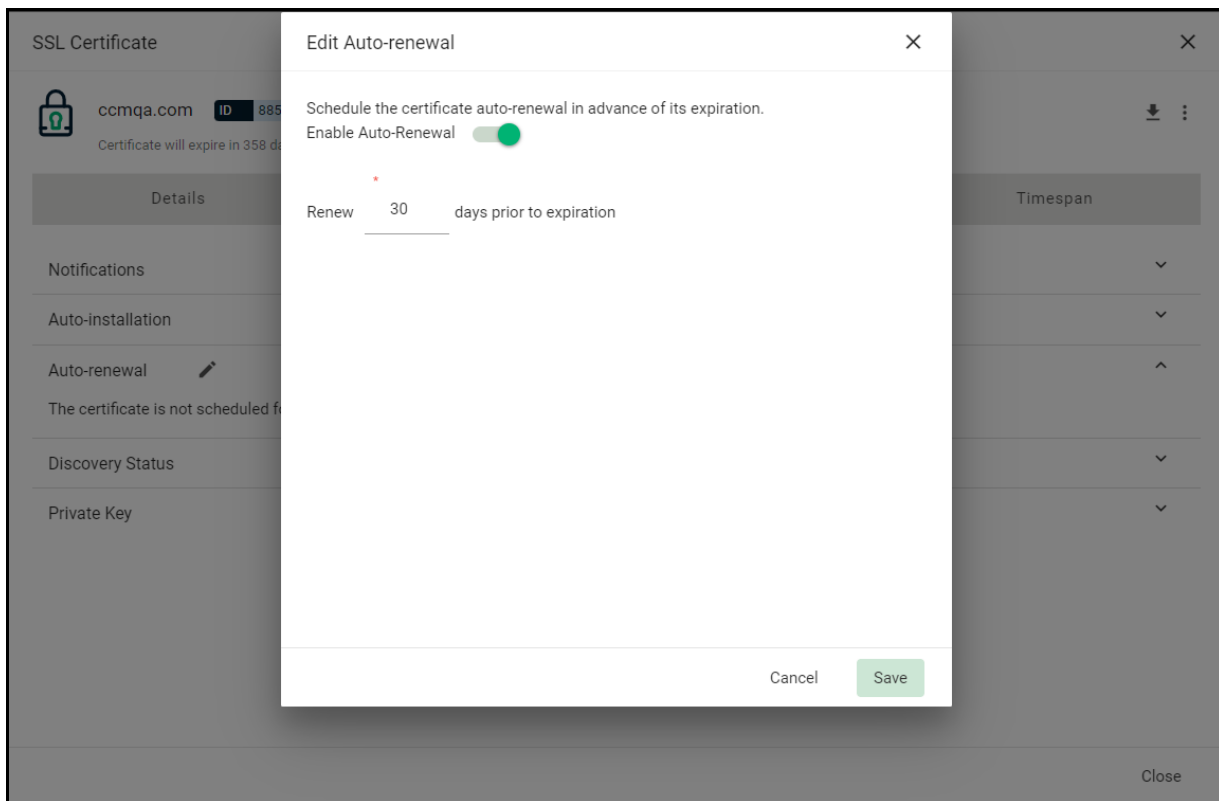
When installing SSL certificates on Apache servers, the server has to be restarted to finalize the installation. You can do this remotely from SCM by clicking **Restart** on the **Certificate Summary** panel. After rebooting, the **Server Software State** changes to Active.



3.2.2.7 Updating the auto-renewal status

You can use the **Certificate Summary** panel to update the auto-renewal status of a certificate as follows:

1. Navigate to **Certificates > SSL Certificates**, select a certificate, and then click **View**.
2. Select **Management**, expand the **Auto-renewal** field and click **Edit**.
3. Click **Enable Auto-Renewal**.
4. Choose the number of days prior to expiry when you want to start the auto-renewal process (default is 30 days). On the scheduled day, the agent will initiate a renewal request using the existing CSR and submit it to CA.
5. Click **Save**.



For more information, see [“Automatic certificate renewal scheduling”](#) on page 77.

3.2.3 How to request and issue SSL certificates to web servers and hosts

The following are the main methods that you can use to request and install SSL certificates:

- Self enrollment form—You or applicants authorized by you obtain certificates via the self enrollment form. Then you or your authorized representative have to install the certificate manually on the target web server. For more information, see [“Using the SSL certificate enrollment form” on page 35](#).
- Enrollment wizard with manual installation—You obtain certificates via the enrollment wizard, then you or your authorized representative have to install the certificate manually on the target web server. For more information, see [“Using the SSL built-in enrollment wizard” on page 40](#).
- Enrollment wizard with automatic CSR—You configure SCM and PKS to automatically create certificate requests for the domains and then manually install the certificate on a web server. For more information, see [“Generation of CSR” on page 49](#).
- Enrollment wizard with automatic installation—You configure SCM, PKS, and network agent to automatically create certificate requests for the domains and then automatically install the certificate on a web server. When a certificate is nearing expiry, a CSR is automatically generated and forwarded for the administrator's approval. Once issued by the CA, the certificate is collected and automatically installed on the web server. For more information, see [“Generation of CSR with auto-installation” on page 55](#).
- Bulk enrollment—You or applicants authorized by you submit multiple certificate requests using a CSV file. For more information, see [“How to import SSL certificates” on page 73](#).

The following requirements must be met prior to requesting or issuing certificates to web servers or hosts:

- The public domain for which the SSL certificate is intended has been enabled for SSL certificates, passed DCV, and has been activated for your account by your Sectigo account manager.
All certificate requests made on validated domains or subdomains thereof are issued without further validation. If you request a certificate for a brand new public domain, then this domain has to first undergo validation by Sectigo. Once validated, this new domain is added to your list of validated domains and future certificates are issued immediately.
Note that it is possible for one organization to have multiple certificates for different domain names. For more information, see [Delete an organization or department](#).
- You have created at least one organization or department to which that domain has been delegated (see [Managing organizations and departments](#)).
- If you want to enable external SSL applications, you configured an account for the SSL Web Form enrollment endpoint; the account must be for an organization or department to which that domain belongs, and the **Access Code** must be specified (see [“Managing bulk SSL requests” on page 163](#)).
- If you want certificates to expire on the same day of the year, you have selected **Sync Expiration Date** and specified the day of the month when the certificate is to expire in the **SSL Certificate** page of the **Add New** or **Edit Organization** dialog (see [Edit organization or department details](#)).
- For manual CSR and the self-enrollment form, the applicant has already created the CSR prior to beginning the application. A CSR is a message sent from an applicant to a CA when applying for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret.

The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key selected by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request.

The CSR may be accompanied by other credentials or proofs of identity required by the CA, and the CA may contact the applicant to obtain additional information.

The public key included in the CSR should be at least of a RSA 2048 key length or ECC p256 curve, and must match one of the key types allowed by the selected certificate profile.

The Subject typically includes the following Relative Distinguished Name (RDN) fields:

- CN—Common name, which in this case is the fully qualified domain name
- O—Organization
- OU—Organization unit, i.e., the department name
- L—Locality, i.e., town or city
- ST—State, province, region or county name
- C—Country (two-character country code as defined in ISO 3166)

If information is missing from the CSR, or differs from the organization details as specified in SCM, the SCM organization values are used.

Sectigo provides a range of documents about CSR generation designed to guide you and external applicants through the CSR creation process. For a list of these documents, contact Sectigo support.

Requesting and issuing of SSL certificates typically occurs as follows:

1. The applicant confirms completion of the prerequisites.
2. A certificate request is made via the certificate auto-installer, self-enrollment form, or wizard.
3. The certificate appears in the **SSL Certificates** table with the status of Requested. The MRAO, RAO SSL, or DRAO SSL administrator receives an email notification that a certificate request is awaiting approval.
4. The certificate request is checked, and then either approved or declined by appropriately privileged SSL administrator. If it is approved, the request is then forwarded to Sectigo for validation and issuance or rejection and the following takes place:
 - If the certificate application was submitted from SCM, the certificate is issued and the application status changes to Issued in the **SSL Certificates** table. You then can install the certificate remotely by clicking **Install**.
 - If the certificate application was submitted via the self-enrollment form or wizard, a collection mail is sent to the applicant. This mail contains a link to the certificate collection form (see [“Certificate collection and installation” on page 71](#)).
5. Once an administrator approves the request, that administrator becomes the owner of the request. At this stage, the administrator can also choose to view, edit, or decline the request (see [“Approving, declining, viewing, and editing certificate requests” on page 70](#)).
6. The applicant is designated as the requester of the certificate. If the applicant does not exist, then SCM adds them as a new end-user (viewable in the **Certificates > Client Certificates** table) when the certificate application form is successfully submitted.

3.2.3.1 Using the SSL certificate enrollment form

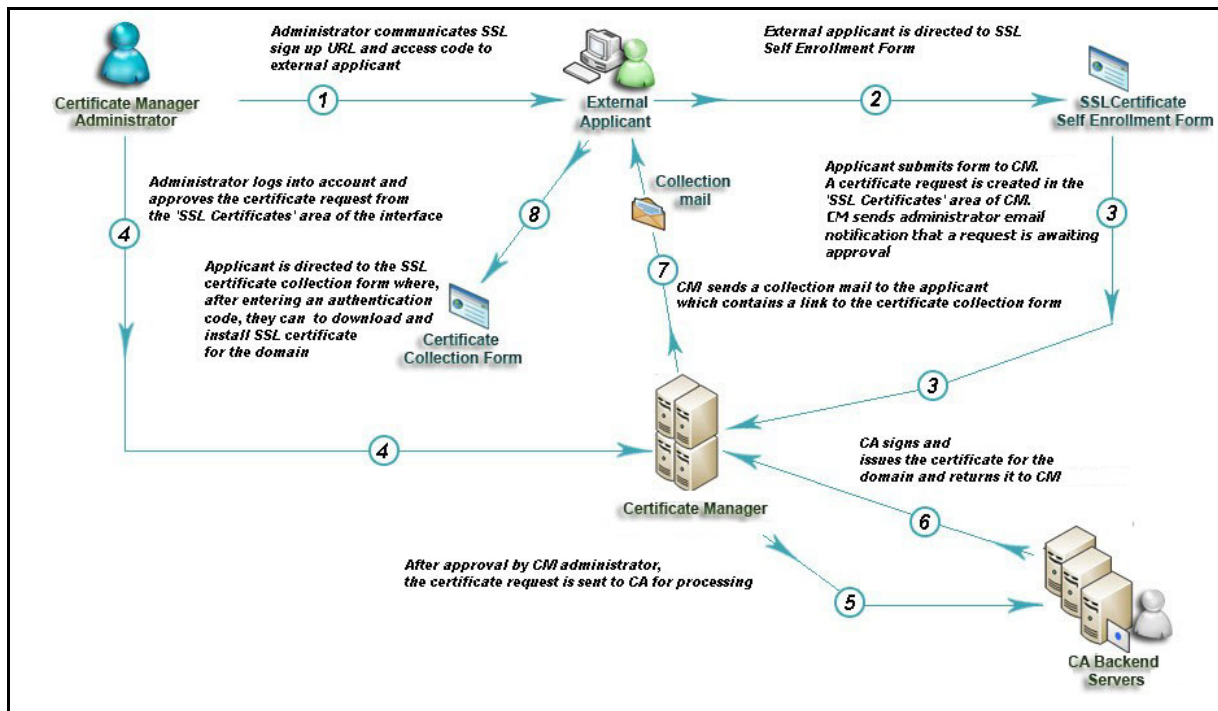
The self-enrollment form enables you or applicants that you direct to the request form to order SSL certificates. Applicants using this method must validate their application for the certificate as follows:

1. By entering the appropriate access code for an SSL Web Form enrollment endpoint account. The access code is a combination of alpha and numeric characters that the applicant needs to provide in order to authenticate the request to the certificate manager.
2. By entering an email address from the domain for which the certificate application is being made. This domain must have been delegated to the organization or department assigned to the SSL Web Form enrollment endpoint account.

After submitting the application form, the certificate is added to the **Certificates > SSL Certificates** table with a status of Requested. Then an SSL administrator with the required level of privileges should approve the request. Upon approval, SCM forwards the application to Sectigo for validation and further processing. See “[Approving, declining, viewing, and editing certificate requests](#)” on page 70.

After validating the application, Sectigo issues the certificate at which point the certificate's status changes to Issued, and a collection email is sent to the applicant who can now collect, download, and install the certificate on the web server. For more information on certificate collection and installation, see “[Certificate collection and installation](#)” on page 71.

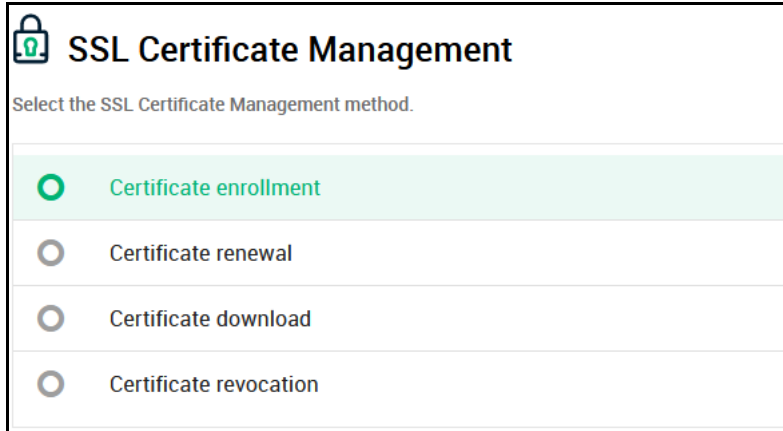
The following diagram illustrates the process of using the self-enrollment form.



Provide enrollment details to applicants using an out-of-band communication such as email. The communication must contain the following information:

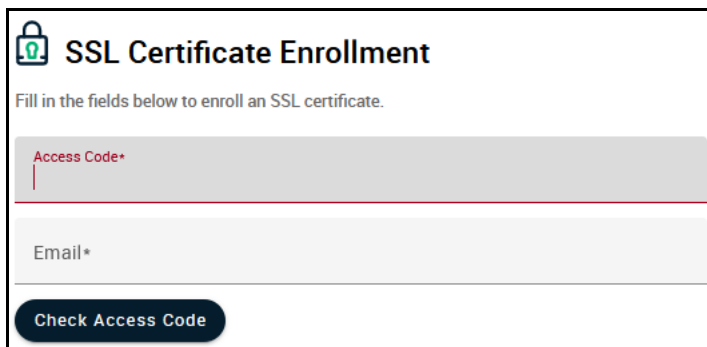
- A link to the **SSL Certificate Management** form, located at the address specified for the SSL Web Form enrollment endpoint. By default the address is similar to the following:
https://cert-manager.com/customer/<customer_uri>/ssl.
 To view the SSL Web Form URL, navigate to **Enrollment > Enrollment Forms**.
- The access code specified for the SSL Web Form enrollment endpoint account.

Accessing the link displays the form shown in the following illustration.



The screenshot shows a web interface titled "SSL Certificate Management" with a lock icon. Below the title is the instruction "Select the SSL Certificate Management method." There are four radio button options: "Certificate enrollment" (which is selected and highlighted in light green), "Certificate renewal", "Certificate download", and "Certificate revocation".

Clicking **Certificate enrollment** opens the **SSL Certificate Enrollment** form shown in the following illustration.



The screenshot shows a web interface titled "SSL Certificate Enrollment" with a lock icon. Below the title is the instruction "Fill in the fields below to enroll an SSL certificate." There are two input fields: "Access Code*" and "Email*". Below the fields is a button labeled "Check Access Code".

To access the full form, the applicant must enter the access code and an email address from a domain delegated to the organization or department of the enrollment endpoint account, and click **Check Access Code**. If both the access code and email address are successfully validated, the full certificate application form shown in the following illustration is displayed.

SSL Certificate Enrollment

Subject Alternative Names (Comma separated)

Fill in the fields below to enroll an SSL certificate.

Access Code*

●●●●

Email*

test@example.com

Certificate Info

Certificate Profile: *

Comodo EV Multi Domain SSL

Certificate Term: *

1 year

CSR: *

GET CN FROM CSR

UPLOAD CSR

Max CSR size is 32K

Common Name*

Renew

Auto renew ▼ days before expiration

i The Annual Renewal Passphrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. *Do not lose it.* You will need it when you want to revoke or renew your Digital ID.

Annual Renewal Passphrase

Confirm Annual Renewal Passphrase

External Requester

Acceptable format:

- email@domain.com
- email.1@domain.com, email.2@domain.com

Comments

Additional

[I have read and agree to the terms of EULA](#)

Enroll

The **Access Code** and **Email** address fields are pre-populated. The domain specified in the **Common Name** field must match the domain of the applicant's email address and that email account must be active so the applicant can receive emails.

NOTE: You can use your own custom form templates instead of the default form supplied by Sectigo. Contact your account manager for more information.

NOTE: In addition to the standard fields, MRAOs can add custom fields. See ["How to define custom fields"](#) on page 235.

The following table describes the self-enrollment form fields and elements. Mandatory fields are marked with a red asterisk on the form.

Field	Description
Access Code	The access code for the SSL Web Form enrollment endpoint account that you conveyed to the applicant.
Email	The email address of the applicant. The address must be for a domain that has been delegated to the organization or department of the enrollment endpoint account.

Field	Description
Certificate Profile	The certificate profile for the certificate. The certificate profiles included in the list (and available to the applicant) can be customized according to the needs of the organization.
Certificate Term	The validity period of the certificate. For example, 1 year, 2 years, 3 years. The available validity periods depend on the selected profile.
CSR	The CSR that Sectigo will use to process the application. The CSR must match one of the key types allowed by the selected certificate profile. Paste the CSR into this field or click Upload CSR to upload it as a .txt file. Once uploaded or pasted, the form automatically parses the CSR. For Multi-Domain Certificate (MDC) applications, the CSR only needs to be for a single common name (also known as the Primary Domain Name). Enter the additional domains in the Subject Alternative Names field on this form.
Get CN from CSR	Auto-populates the Common Name field with information from the CSR, ensuring the domain name in the application form matches the domain in the CSR. If the domain name entered in the Common Name field does not match the one in the CSR, Sectigo cannot issue the certificate. For MDC applications, the additional domains are entered in the Subject Alternative Names field. If the CSR contains these SANs, clicking Get CN from CSR also auto-populates the Subject Alternative Names field.
Common Name	The correct fully qualified domain name for the organization or department. The maximum allowed character length for this field is 64. For single domain certificates, the domain name in the format of <code>example.com</code> . For wildcard certificates, the domain name in the format of <code>*.example.com</code> . For MDC, the primary domain name in the format of <code>example.com</code> .
Renew	Specifies whether or not the certificate should be automatically renewed when it is nearing expiry. Applicants can also specify the number of days in advance of expiry when the renewal process should start. On the scheduled day, SCM automatically submits the renewal application to the CA with a CSR generated using the same parameters as the existing certificate.
Subject Alternative Names	If the Certificate Profile is for MDC, specifies the additional domains separated by commas. Mandatory for MDC certificates.
Annual Renewal Passphrase	The passphrase to be used to renew or revoke the certificate when using the external renewal or revocation page, located at the address specified for the SSL Web Form enrollment endpoint.
Confirm Passphrase	Confirmation of the passphrase.
External Requester	Email address of the end-user on behalf of whom the applicant is making the request. The address must be from the same domain for which the certificate is applied. The certificate collection email is sent to this email address.
Comments	Additional information for the administrator entered by the applicant. If there are no comments entered, the comment panel will not appear.

Field	Description
Certificate Requester	If Sectigo EV SSL or Sectigo EV Multi-Domain SSL certificate profile is selected, additional details about the requester. Typically, it would be the same information as provided in the EV Details page when adding a new organization (see Edit organization or department details).
Subscriber Agreement	Applicant must accept the terms and conditions before submitting the form by reading the agreement and clicking I have read and agree to the terms and clicking OK . The Subscriber Agreement differs depending on selected certificate profile. If Sectigo EV SSL or Sectigo EV Multi-Domain SSL certificate is selected, an additional agreement is shown and must be accepted.
Enroll	Submits the application and enrolls the new certificate request.

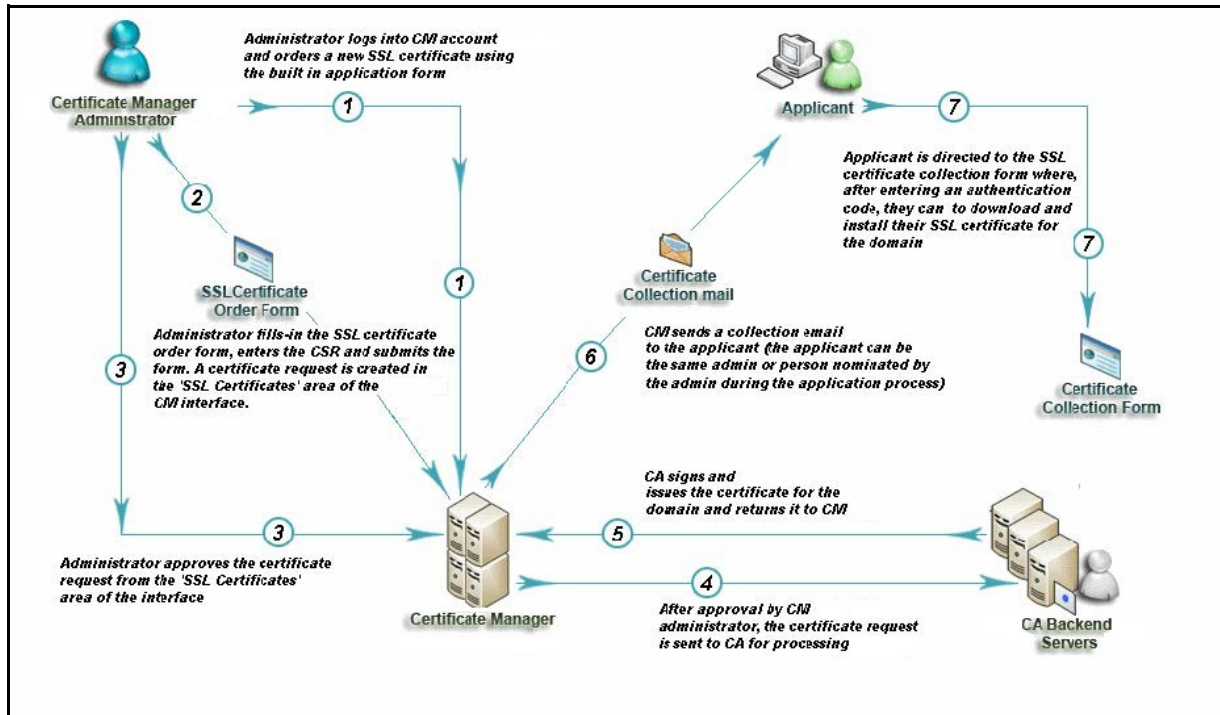
3.2.3.2 Using the SSL built-in enrollment wizard

The enrollment wizard enables you to enroll for SSL certificates in the following ways:

- **Using a Certificate Signing Request (CSR)**—you generate the CSR on a server on which the certificate needs to be installed, and then enter the CSR in the wizard. For more information, see [“Using a Certificate Signing Request” on page 41](#).
- **Generation of CSR** —the PKS installed on a server in your organization generates the CSR for the domain name and stores the private key. Once the certificate is issued, using SCM you can download it in .p12 format and install it on the server. For more information, see [“Generation of CSR” on page 49](#).
- **Generation of CSR with Auto-Installation**—the PKS installed on a server in your organization generates the CSR for the domain name and stores the private key, and the certificate is installed on the server by a network agent. For more information, see [“Generation of CSR with auto-installation” on page 55](#).
- **Generation of CSR in Azure Key Vault**—SCM generates the CSR and stores it in Azure Key Vault. Once the certificate is issued, you can download the certificate with the public-private key pair from SCM and install it on the server. For more information, see [“Generation of CSR in Azure Key Vault” on page 65](#).

3.2.3.2.1 Using a Certificate Signing Request

The following diagram illustrates the process of using the enrollment wizard for manual CSR generation.



You can manually apply for new certificates as follows:

1. Navigate to **Certificates > SSL Certificates** and then click the **Add** icon in the upper-right corner of the screen.
This opens the **Request SSL Certificate** wizard.
2. Select **Using a Certificate Signing Request (CSR)** and click **Next** to open the **Details** page.
3. Complete the **Details** fields, referring to the following table, and click **Next**. Mandatory settings are marked with a red asterisk.

Request SSL Certificate ×

Select The Enrollment Method

- Using a Certificate Signing Request (CSR)
With this method you'll need to provide a CSR.
- Generation of CSR
In order to be able to download the SSL certificate and the private key after issuance, you will need to have access to the Private Key Store.
- Generation of CSR with Auto-Installation
This method enables the configuration of certificate auto-installation.
It is only available to Organizations that have assigned Network Agents, and for certain web server types.
- Generation of CSR in Azure Key Vault
After issuance the certificate will be added to the Azure Key Vault.

Close Next

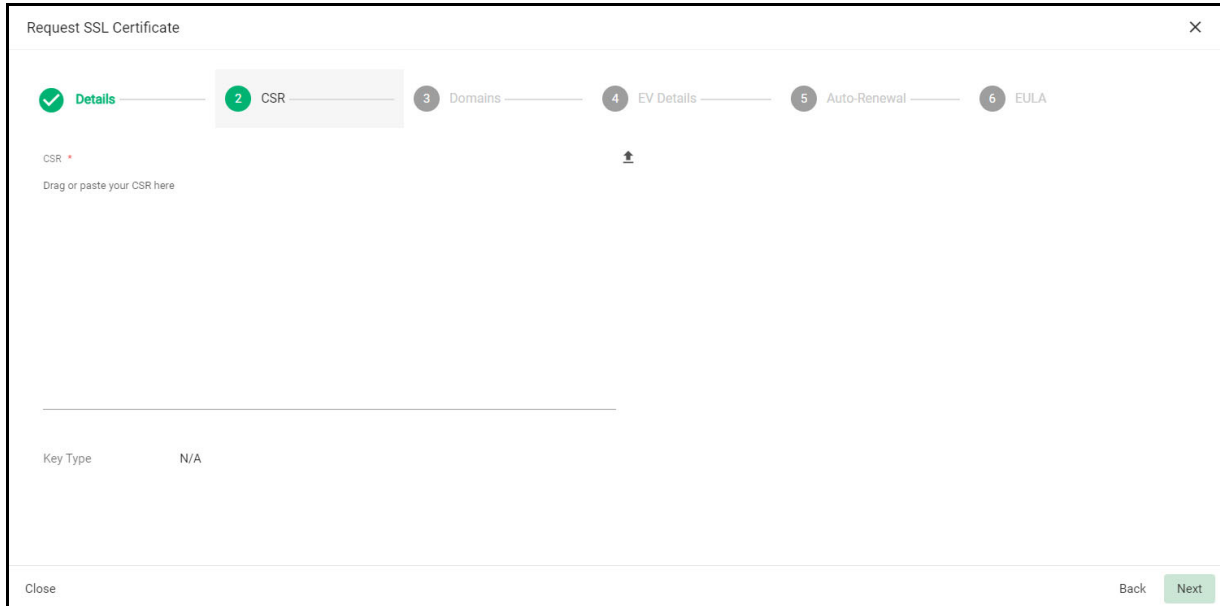
The screenshot shows a web form titled "Request SSL Certificate" with a progress indicator at the top showing four steps: 1. Details (active), 2. CSR, 3. Domains, and 4. Auto-Renewal. The "Details" section contains the following fields:

- Ownership:**
 - Organization: inwodep
 - Department: None
- Order info:**
 - Certificate Profile: SSL EV Certificate
 - Certificate Term: 1 year
- Requester:** admin.mrao

Buttons for "Close" and "Next" are visible at the bottom of the form.

Field	Description
Ownership	
Organization	The organization to which the SSL certificate will belong.
Department	The department to which the SSL certificate will belong. For the certificate to be applied to all departments, select Any .
Order info	
Certificate Profile	The certificate profile to be used for the certificate issuance. The profile description is also displayed (if provided).
Certificate Term	The validity period of the certificate. For example, 1 year, 2 years, 3 years. The available validity periods depend on the selected profile.
Common Name	The domain to which the certificate is to be issued. (Maximum 64 characters.)
Subject Alternative Names	Additional domain names, separated by commas. This field appears only if a multi domain or UCC certificate profile is selected.
Requester	Auto-populated with the name of the administrator making the application.
Comments	Comments pertaining to the certificate. If there are no comments entered, the comment panel will not appear.
Notifications	
External Requester	Email address of an external requester on whose behalf the application is made. The requester is still the administrator that is completing this form. The email address of the external requester is displayed as the External Requester in the Certificate Details of an issued certificate.

4. Paste your CSR into the **CSR** field or upload it as a `.txt` file by clicking **Get From File**. The CSR must match one of the key types allowed by the certificate profile specified on the **Details** page and Click **Next**.



The screenshot shows a web form titled "Request SSL Certificate" with a close button (X) in the top right corner. The form has a progress bar at the top with six steps: 1. Details (checked), 2. CSR (active), 3. Domains, 4. EV Details, 5. Auto-Renewal, and 6. EULA. Below the progress bar, there is a section for "CSR" with a red asterisk indicating it is required. The text "Drag or paste your CSR here" is displayed above a large empty text area. To the right of the text area is an upload icon (a square with a plus sign). Below the text area, there is a label "Key Type" followed by the value "N/A". At the bottom left of the form is a "Close" button, and at the bottom right are "Back" and "Next" buttons.

5. Check the Common Name for the domain and click **Next**.

Request SSL Certificate ✕

✓ Details ✓ CSR 3 Domains 4 Auto-renewal 5 EULA

Domains

Common Name
butest.com

Subject Alternative Names ⊕

↻

Close Back Next

6. Configure the **Auto renewal** options and click **Next**.

Request SSL Certificate

✓ Details — ✓ CSR — ✓ Domains — 4 Auto-renewal — 5 EULA

Schedule the certificate auto-renewal in advance of its expiration.

Enable Auto-Renewal

Close Back Next

7. Follow this procedure to configure the auto-renewal options:
 - a. Select **Enable Auto Renewal** to have SCM apply for a new certificate when the current one approaches expiry.
 - b. Use the **Auto-renewal Schedule** field to specify the number of days in advance of expiry that the renewal process should start. On the scheduled day, the agent will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.
8. If your account is configured for EV, click **Next** to open the **EV Details** page. The **EV Details** page differs. There can be a manual mode, EV RA and standard.

Request SSL Certificate ✕

✓ Details — ✓ CSR — ✓ Domains — **4** EV Details — 5 Auto-renewal 6 EULA

EV details listed below are copied from and can be edited only in 'EV Details' section of the selected organization's profile.
Incorporation / Registration Agency
As assigned by the incorporating Agency (for Private Organization Applicants Only).

Incorporating Agency	Jurisdiction of City or Town
Registration Number	State / Province
Date of Incorporation	Country
Phone Number	

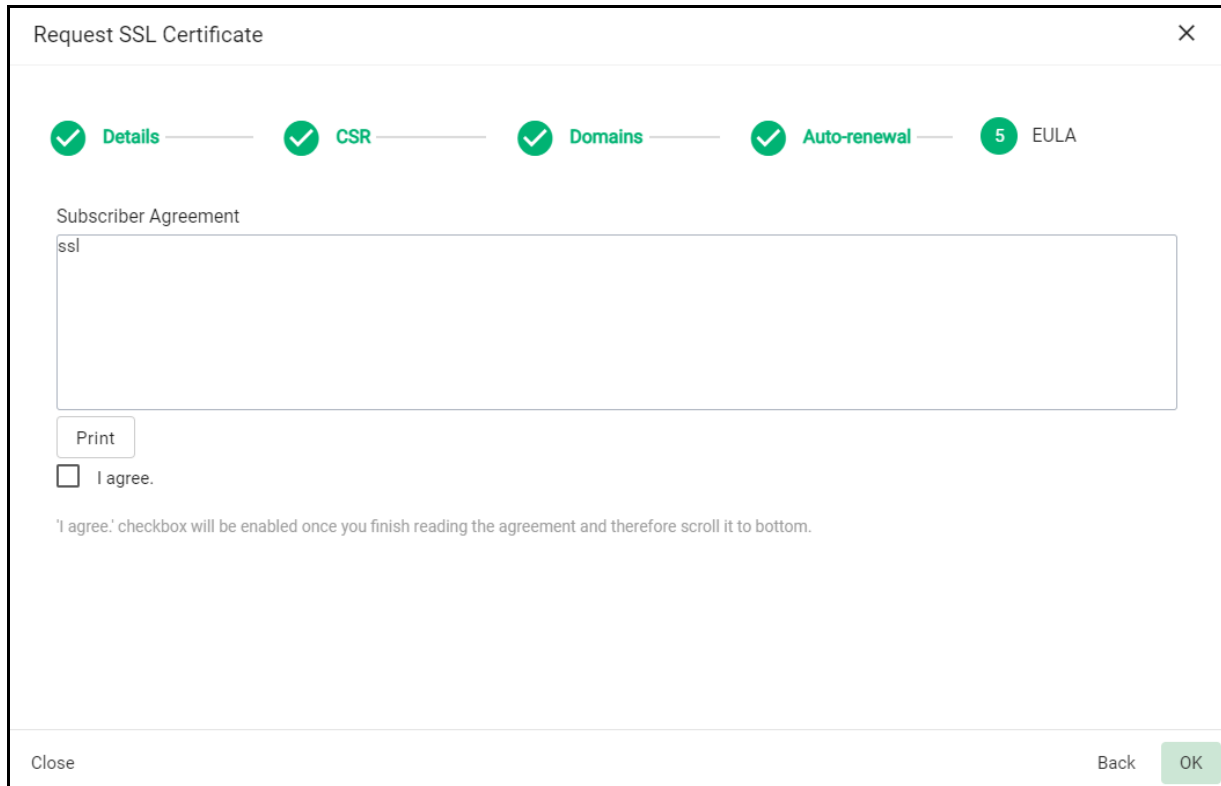
Contract Signer

Close Back Next

9. Complete the fields of the **EV Details** page.

The fields you need to complete depend on the EV mode activated for your account. Typically, it would be the same information as provided in the **EV Details** tab when adding a new organization (see [Edit organization or department details](#)). If the EV type for your account is RA, the fields in this page are auto-populated.

10. Click **Next** to open the **EULA** page.



The screenshot shows a window titled "Request SSL Certificate" with a close button (X) in the top right corner. At the top, there is a progress bar with five steps: "Details", "CSR", "Domains", "Auto-renewal", and "EULA". Each step has a green checkmark icon, and the "EULA" step is highlighted with a green circle containing the number "5". Below the progress bar, the text "Subscriber Agreement" is displayed above a large text area containing the word "ssl". To the left of the text area is a "Print" button. Below the text area is a checkbox labeled "I agree." with a note below it: "'I agree.' checkbox will be enabled once you finish reading the agreement and therefore scroll it to bottom." At the bottom left of the window is a "Close" button, and at the bottom right are "Back" and "OK" buttons.

11. Read the end user license agreement (EULA) and accept it by selecting **I Agree**, and then click **OK** to submit the application.

Upon completion of the wizard, the certificate is added to the **SSL Certificates** screen with a status of **Requested**. The next phase of the process is to have the requested certificate approved (see ["Approving, declining, viewing, and editing certificate requests"](#) on page 70).

3.2.3.2.2 Generation of CSR

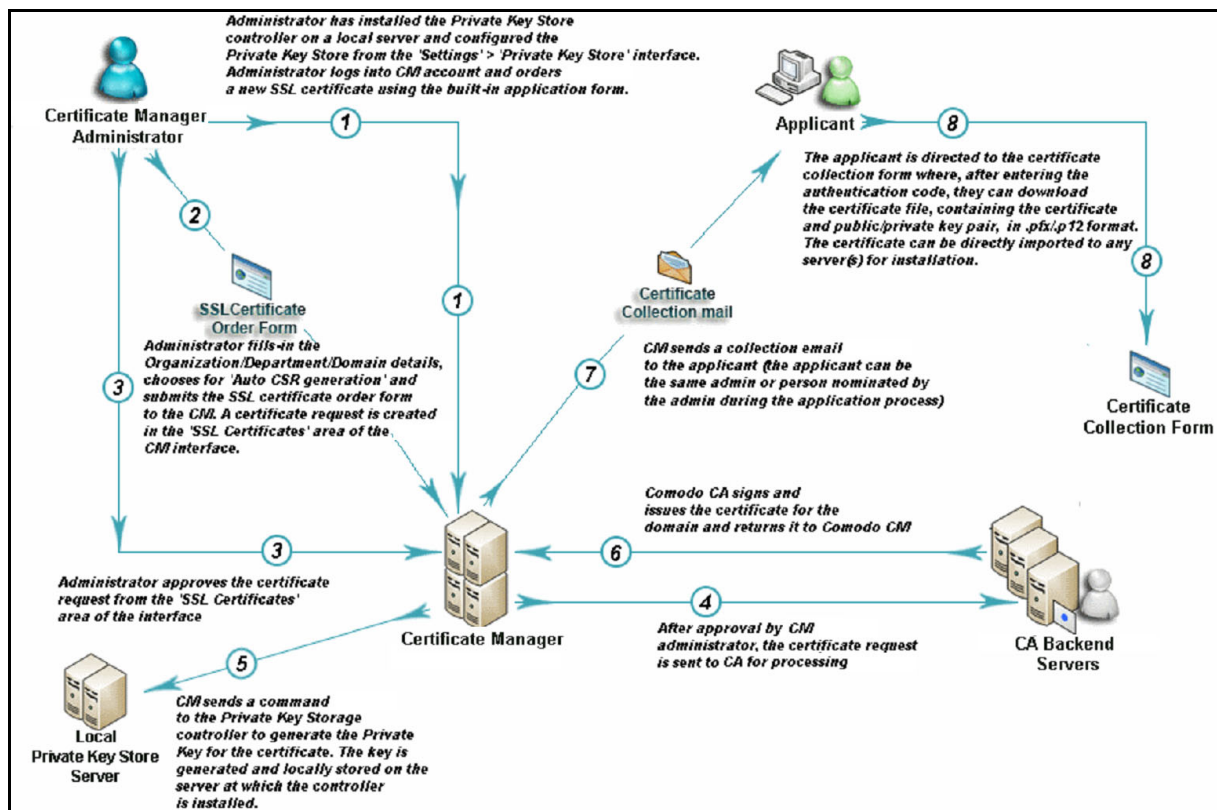
SCM can use the information entered for the organization, department, and common name to automatically generate a CSR at the start of the application process.

Prior to starting auto CSR generation, you need to install the PK agent on a local server. The agent should be connected to SCM to receive commands, and generate and store the private keys. Information about the PK agent can now be found [here](#).

During CSR generation, SCM issues a command to the PKS to create the private key for the certificate. The private key is stored in a database created by the agent on the local server and does not leave your network; the private key is not uploaded to SCM.

Upon approval and issuance, the certificate can be collected by you, the requester, or from the collection form. During collection, SCM retrieves the private key from the PKS over an encrypted channel and integrates it with the certificate. The certificate can then be downloaded in .p12 format. The certificate can be imported and installed on any server.

The following diagram illustrates the process of using the enrollment wizard to generate the CSR automatically.

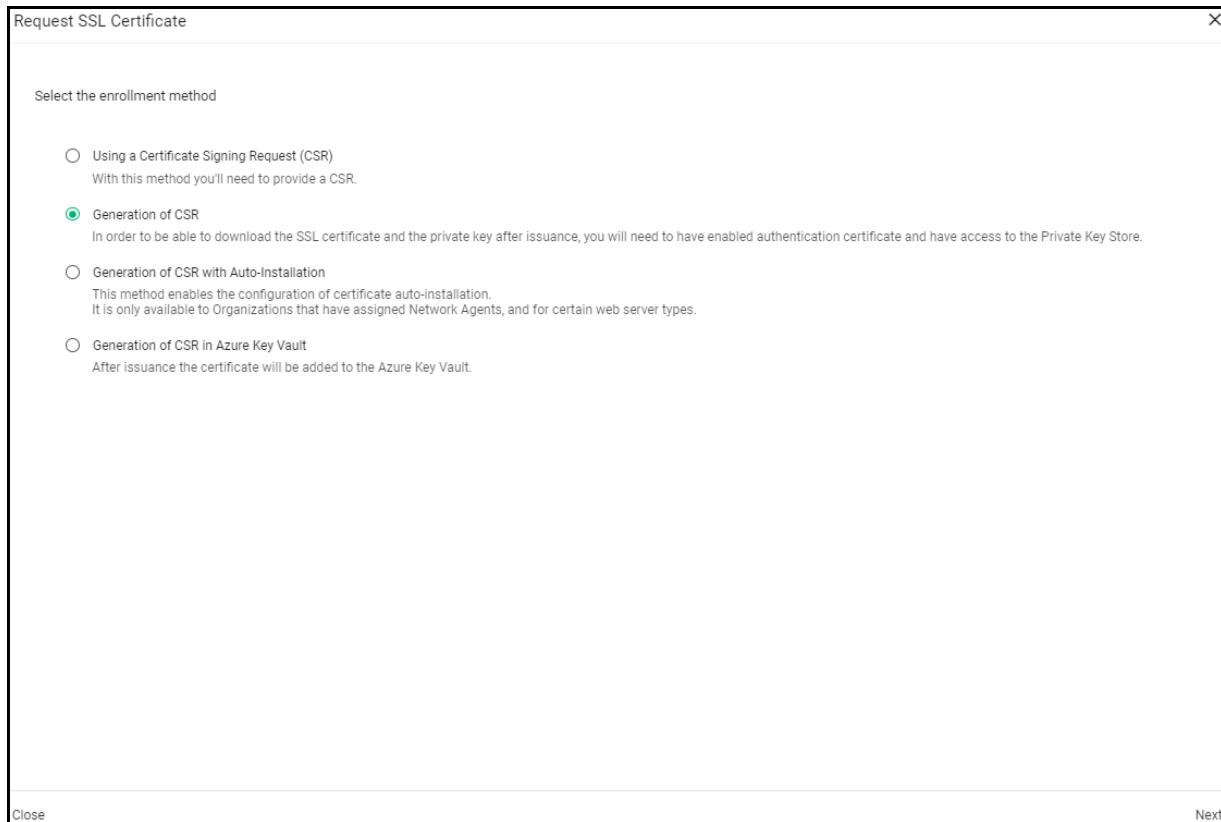


To apply for a new SSL certificate with auto-generated CSR, do the following:

1. Navigate to **Certificates > SSL Certificates** and then click the **Add** icon in the upper-right corner of the screen.

This opens the **Request SSL Certificate** wizard.

2. Select **Generation of CSR** and click **Next** to open the **CSR** page.



Request SSL Certificate

Select the enrollment method

- Using a Certificate Signing Request (CSR)
With this method you'll need to provide a CSR.
- Generation of CSR**
In order to be able to download the SSL certificate and the private key after issuance, you will need to have enabled authentication certificate and have access to the Private Key Store.
- Generation of CSR with Auto-Installation
This method enables the configuration of certificate auto-installation.
It is only available to Organizations that have assigned Network Agents, and for certain web server types.
- Generation of CSR in Azure Key Vault
After issuance the certificate will be added to the Azure Key Vault.

Close Next

- Fill in the **Details** page based on the table below and click **Next**. Mandatory settings are marked with a red asterisk.

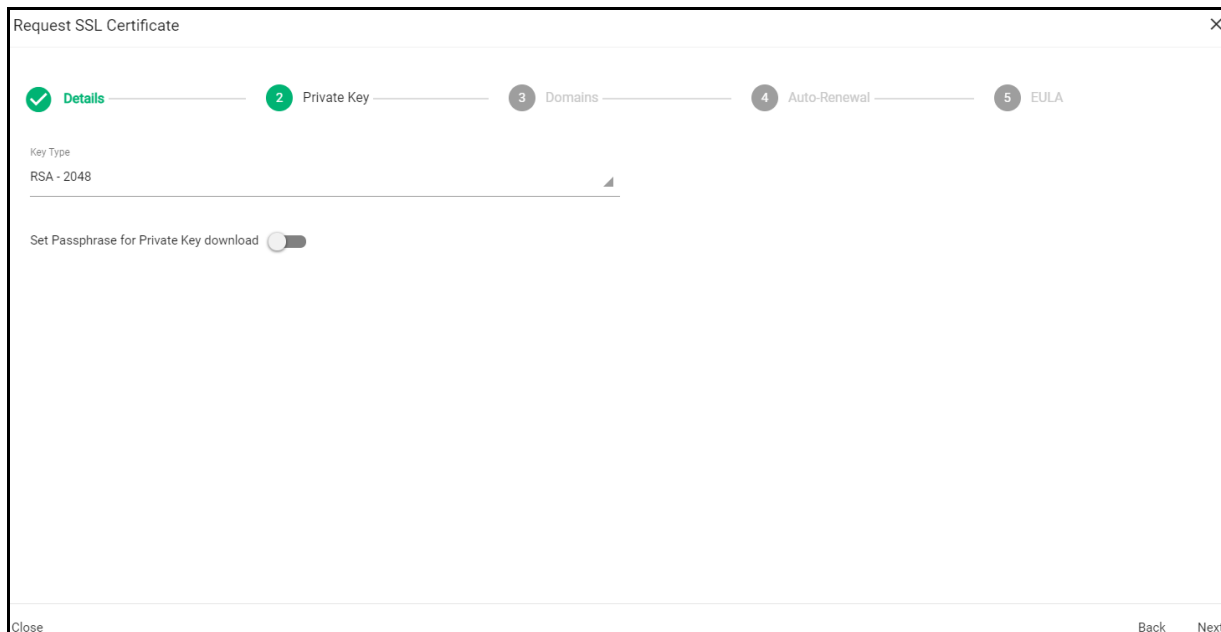
The screenshot shows a web form titled "Request SSL Certificate" with a progress indicator at the top showing four steps: 1. Details (active), 2. Private Key, 3. Domains, and 4. Auto-Renewal. The "Details" section contains the following fields:

- Owner**
 - Organization * (dropdown menu)
 - Department (dropdown menu)
- Order Info**
 - Certificate Profile * (dropdown menu with an information icon)
 - Certificate Term (dropdown menu)
- Requester**
 - admin mrap (text field)

Buttons for "Close" and "Next" are located at the bottom left and right of the form, respectively.

Field	Description
Organization	The organization to which the SSL certificate will belong.
Department	The department to which the SSL certificate will belong. For the certificate to be applied to all departments, select Any .
Certificate Profile	The certificate profile to be used for the certificate issuance. The profile description is also displayed (if provided).
Certificate Term	The validity period of the certificate. For example, 1 year, 2 years, 3 years. The available validity periods depend on the selected profile.
Common Name	The domain to which the certificate is to be issued. The maximum allowed character length for this field is 64.
Subject Alternative Names	Additional domain names, separated by commas. This field appears only if a multi domain or UCC certificate profile is selected.
Requester	Auto-populated with the name of the administrator making the application.
External Requester	Email address of an external requester on whose behalf the application is made. The requester is still the administrator that is completing this form. The email address of the external requester is displayed as the External Requester in the Certificate Details of an issued certificate.
Comments	Comments pertaining to the certificate. If there are no comments entered, the comment panel will not appear.

4. Specify the Private Key parameters, as follows:
 - a. In the **Key Type** list, select the key algorithm you want to use in the certificate.
 - b. For RSA, in the **Key Size** field, select either 2048 or 4096. The former is the recommended industry standard and provides very high security for public-facing and internal hosts. The latter is even more secure, but may lead to longer connection times due to the extra processing needed for exchanging keys during the SSL handshake.
For EC, in the **Key Curve** field, select the curve to use for encryption.
 - c. Enable **Set Passphrase for key download** to protect the certificate with a passphrase which can be manually entered or auto-generated. Store this information in a safe location. If entering the passphrase manually, type the passphrase and confirm it in the next field. To auto-generate the passphrase, click **Generate**. To view the passphrase, select **Show Passphrase**.



The screenshot shows a 'Request SSL Certificate' dialog box with a progress bar at the top. The progress bar has five steps: 1. Details (checked), 2. Private Key (active), 3. Domains, 4. Auto-Renewal, and 5. EULA. Below the progress bar, the 'Key Type' is set to 'RSA - 2048'. There is a 'Set Passphrase for Private Key download' toggle switch that is currently turned on. At the bottom left, there is a 'Close' button, and at the bottom right, there are 'Back' and 'Next' buttons.

5. Click **Next** to open the **Domains** page and enter the domain name.
6. Click **Next**.

The screenshot shows a 'Request SSL Certificate' dialog box with a progress bar at the top. The progress bar has five steps: 1. Details (checked), 2. Private Key (checked), 3. Domains (active), 4. Auto-Renewal, and 5. EULA. Below the progress bar, the 'Domains' section is visible. It includes a 'Common Name' field with a red asterisk, containing the text 'DocdomainSCM.local'. Below this is a 'Subject Alternative Names' field with a plus sign icon to its right. At the bottom left of the dialog is a 'Close' button, and at the bottom right are 'Back' and 'Next' buttons.

7. If your account is configured for EV, click **Next** to open the **EV Details** page.
8. Complete the fields of the **EV Details** page.

The fields you need to complete depend on the EV mode activated for your account. Typically, it would be the same information as provided in the **EV Details** page when adding a new organization (see).
9. Click **Next** to open the **Auto-Renewal** page.
10. Follow this procedure to configure the auto-renewal options:
 - a. Select **Enable auto renewal of this certificate** to have SCM apply for a new certificate when the current one approaches expiry.
 - b. Use the **Number of days before expiration to start auto renewal** field to specify the number of days in advance of expiry that the renewal process should start. On the scheduled day, the agent will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.

Request SSL Certificate

Details
 Private Key
 Domains
 4 Auto-Renewal
 5 EULA

Schedule the certificate auto-renewal in advance of its expiration.

Enable Auto-Renewal

Close Back Next

11. Click **Next** to open the **EULA** page.
12. Read the EULA and accept it by selecting **I Agree**, and then click **OK** to submit the application.

Request SSL Certificate

Details
 Private Key
 Domains
 Auto-Renewal
 5 EULA

Subscriber Agreement

SSL EULA! IMPORTANT – PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING AN AusCERT CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING AN AusCERT CERTIFICATE OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT AND THAT YOU AGREE TO AND ACCEPT THE TERMS AS PRESENTED HEREIN. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE AN AusCERT CERTIFICATE AND CLICK "I DECLINE" BELOW. The terms and conditions set forth below constitute a binding agreement between you (the "Subscriber" or "you") and The University of Queensland trading as AusCERT, which has its principal place of business at The University of Queensland, Queensland 4072, Australia ("AusCERT"), with respect to your use of the AusCERT digital certificate services (the "Agreement"). 1. You, the Subscriber, hereby agree that: 1.1. you will comply with the "Subscriber" obligations as set out in the CPS and fill your role as, and follow the procedures set out for, a Subscriber under the CPS in respect of your use of Certificates and the Subscription Services and that all obligations placed on a Subscriber and all representations and warranties made by a Subscriber under the CPS shall be incorporated into this agreement by reference; 1.2. you will ensure that your staff and representatives involved with the Subscription Services read and understand the terms and conditions in the CPS and associated policies that are published in the Repository; 1.3. you will use

Print

I agree.

"I agree" checkbox will be enabled once you finish reading the agreement and therefore scroll it to bottom.

Close Back OK

Upon completion of the wizard, the certificate is added to the **SSL Certificates** page with a status of **Requested**. The next phase of the process is to have the requested certificate approved (see [“Approving, declining, viewing, and editing certificate requests” on page 70](#)).

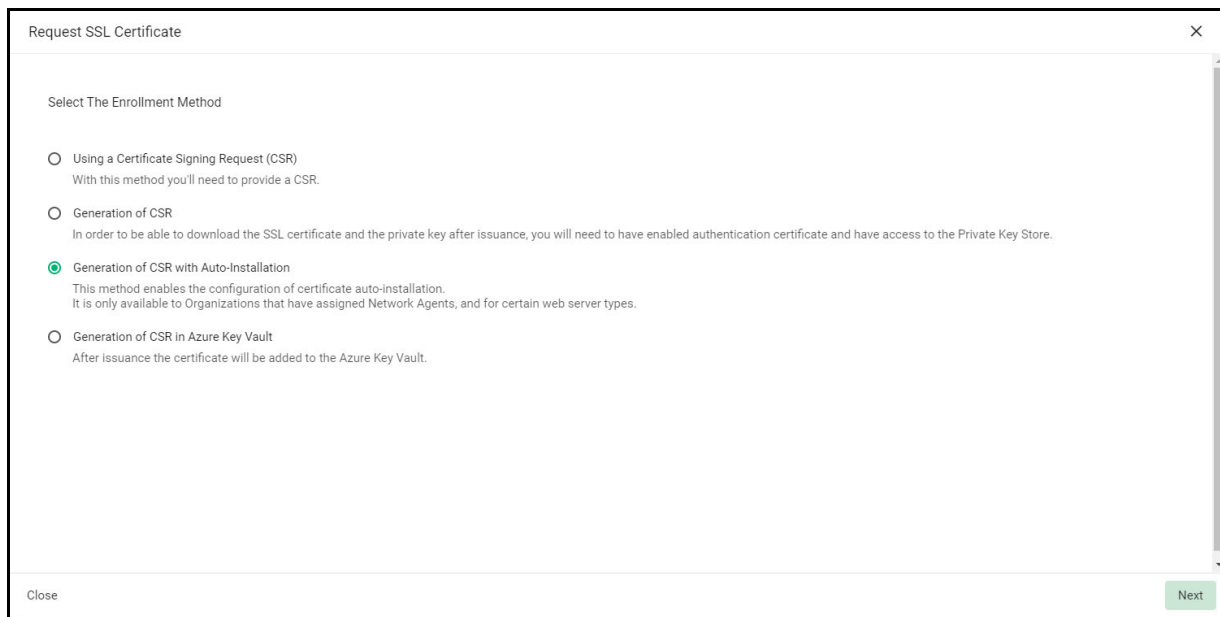
3.2.3.2.3 Generation of CSR with auto-installation

Prior to starting auto CSR generation, you need to install the PKS agent on a local server. The agent should be connected to SCM to receive commands, and generate and store the private keys. Information about the PKS agent can now be found [here](#).

Before managing the automatic installation and renewal of SSL certificates, you must have a network agent configured appropriately. Information about the Network agents can now be found [here](#).

To enroll a certificate for auto-installation, follow this procedure:

1. Navigate to **Certificates > SSL Certificates** and click the **Add** icon in the upper-right corner. This opens the **Request SSL Certificate** wizard.



The screenshot shows a window titled "Request SSL Certificate" with a close button (X) in the top right corner. The main content area is titled "Select The Enrollment Method" and contains four radio button options:

- Using a Certificate Signing Request (CSR)
With this method you'll need to provide a CSR.
- Generation of CSR
In order to be able to download the SSL certificate and the private key after issuance, you will need to have enabled authentication certificate and have access to the Private Key Store.
- Generation of CSR with Auto-Installation
This method enables the configuration of certificate auto-installation. It is only available to Organizations that have assigned Network Agents, and for certain web server types.
- Generation of CSR in Azure Key Vault
After issuance the certificate will be added to the Azure Key Vault.

At the bottom left of the window is a "Close" button, and at the bottom right is a "Next" button.

2. Select **Generation of CSR with Auto Installation** and click **Next**.
3. Fill in the **Details** page fields based on the information provided in the following table below. Mandatory settings are marked by a red asterisk.

The screenshot shows a web form titled "Request SSL Certificate" with a progress bar at the top indicating six steps: 1. Details (active), 2. Private Key, 3. Domains, 4. Nodes & Ports, 5. Auto-Installation, and 6. Auto-Renewal. The "Details" section contains the following fields:

- Ownership**
 - Organization: inwodep
 - Department: None
- Order info**
 - Certificate Profile: 99994 sec name OV
 - Certificate Term: 365
 - Requester: admin mrao

At the bottom right, there is a "Next" button and a "Close" button at the bottom left.

Field	Description
Ownership	
Organization	The organization to which the SSL certificate will belong.
Department	The department to which the SSL certificate will belong. For the certificate to be applied to all departments, select Any .
Order info	
Certificate Profile	The certificate profile to be used for the certificate issuance. The profile description is also displayed (if provided).
Certificate Term	The validity period of the certificate. For example, 1 year, 2 years, 3 years. The available validity periods depend on the selected profile.
Requester	Auto-populated with the name of the administrator making the application.
Comments	Comments pertaining to the certificate. If there are no comments entered, the comment panel will not appear.
Notifications	
External Requesters	Email address of an external requester on whose behalf the application is made. The requester is still the administrator that is completing this form. The email address of the external requester is displayed as the External Requester in the Certificate Details of an issued certificate.

4. Click **Next** to open the **Private Key** page.

Request SSL Certificate

1 Details — 2 Private Key — 3 Domains — 4 EV Details — 5 Nodes & Ports — 6 Auto-Installation — 7 Auto-Renewal — 8 EULA

Key Type
RSA - 4096

Close Back Next

5. Specify the Private Key parameters, as follows:

- a. In the **Key Algorithm** field, select the key algorithm you want to use in the certificate.
- b. For RSA, in the **Key Type** field, select either 2048 or 4096.

2048 is the recommended industry standard and provides very high security for public-facing and internal hosts.

4096 is even more secure, but may lead to longer connection times due to the extra processing needed for exchanging keys during the SSL handshake.

- c. For EC, in the **Key Curve** field, select the curve to use for encryption.

6. Click **Next** to open the **Domains** page.

Request SSL Certificate

1 Details — 2 Private Key — 3 Domains — 4 EV Details — 5 Nodes & Ports — 6 Auto-Installation — 7 Auto-Renewal — 8 EULA

Domains

Common Name *

Subject Alternative Names ⓘ Use commas or spaces to separate multiple values for bulk input.

Close Back Next

7. Fill in the **Domains** page fields based on the information provided in the following table below. Mandatory settings are marked by a red asterisk.

Field	Description
Common Name	The domain to which the certificate is to be issued.
Subject Alternative Names	Additional domain names, separated by commas. This field appears only if a multi domain or UCC certificate profile is selected.

8. Click **Next**.
9. If your account is configured for EV, click **Next** to open the **EV Details** page.
10. Complete the fields of the **EV Details** page.

The fields you need to complete depend on the EV mode activated for your account. Typically, it would be the same information as provided in the **EV Details** page when adding a new organization (see [Edit organization or department details](#)).

If the EV type is RA for your account, this information is auto-populated.

11. Click **Next** to open the **Nodes & Ports** page.

Request SSL Certificate

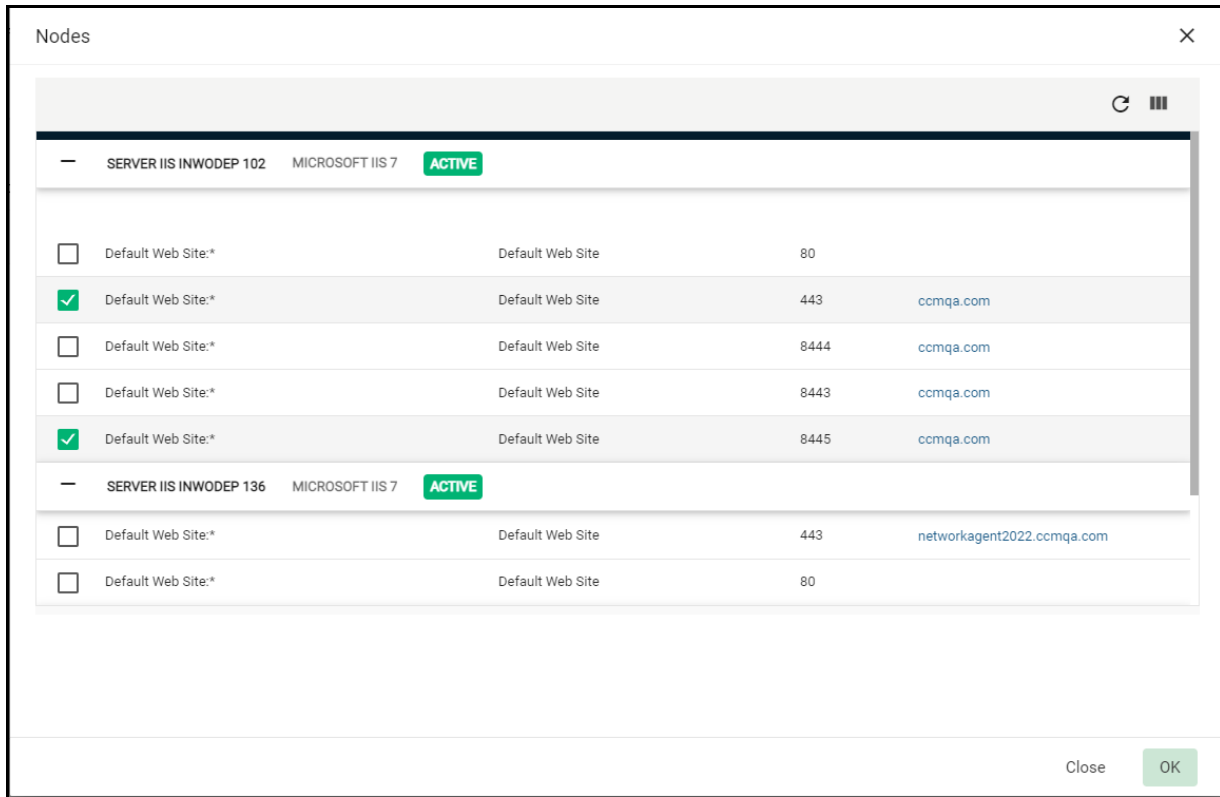
Details —
 Private Key —
 Domains —
 EV Details —
 5 Nodes & Ports —
 6 Auto-Installation —
 7 Auto-Renewal —
 8 EULA

Set the nodes and ports where **ccmqa.com** is to be installed.

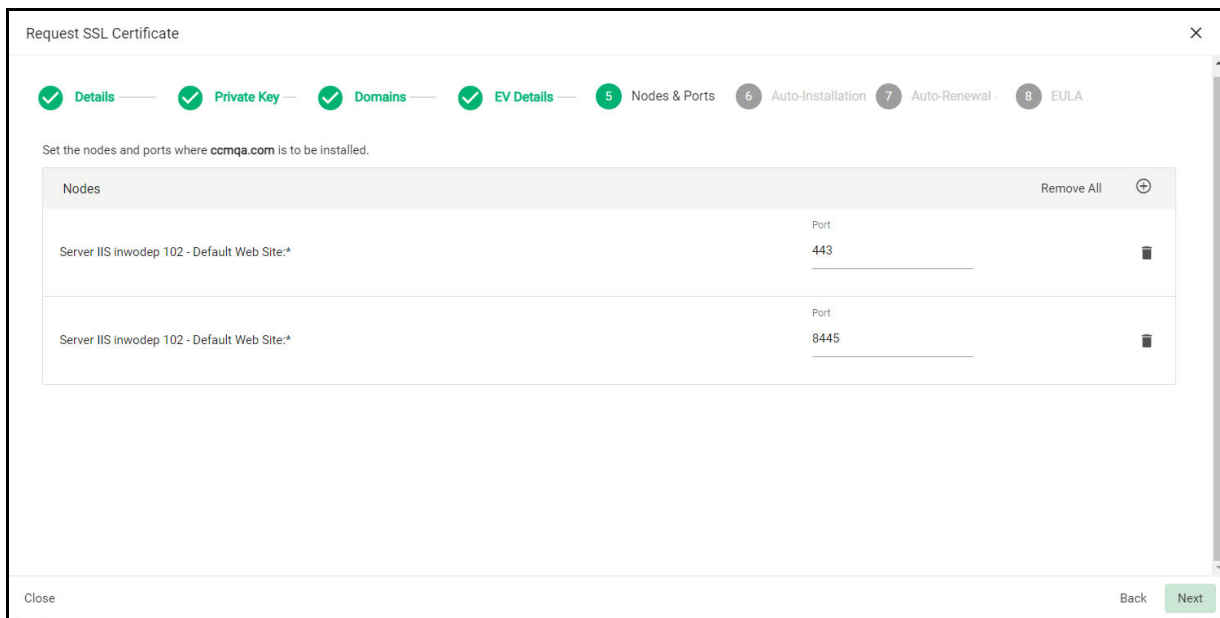
Nodes Remove All +

Close Back Next

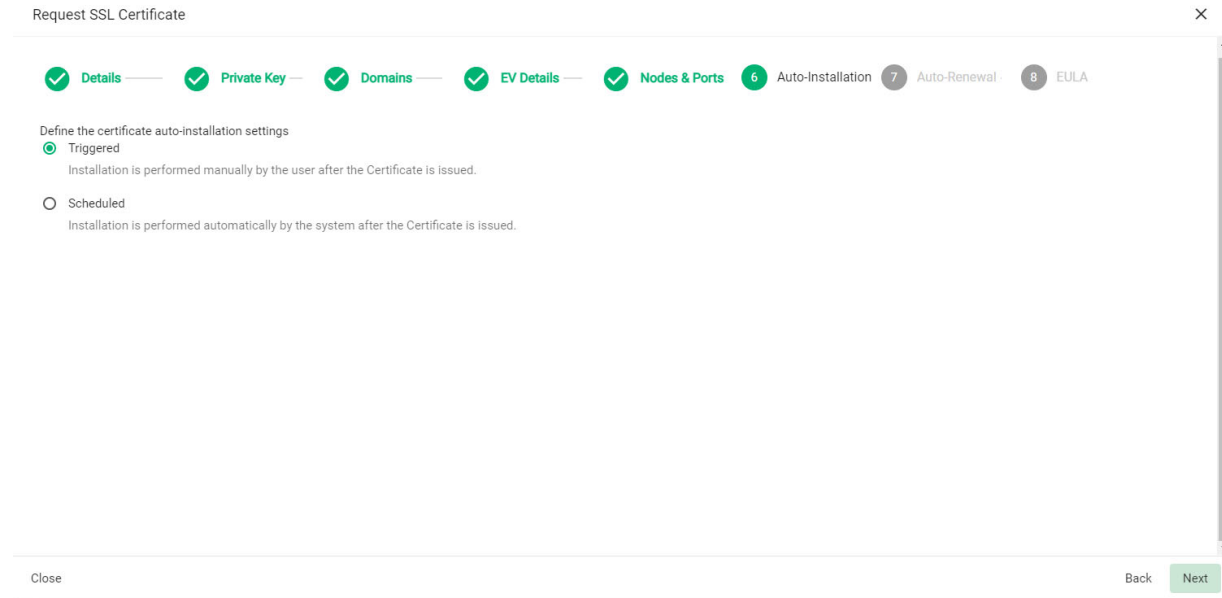
12. Click **Add**.



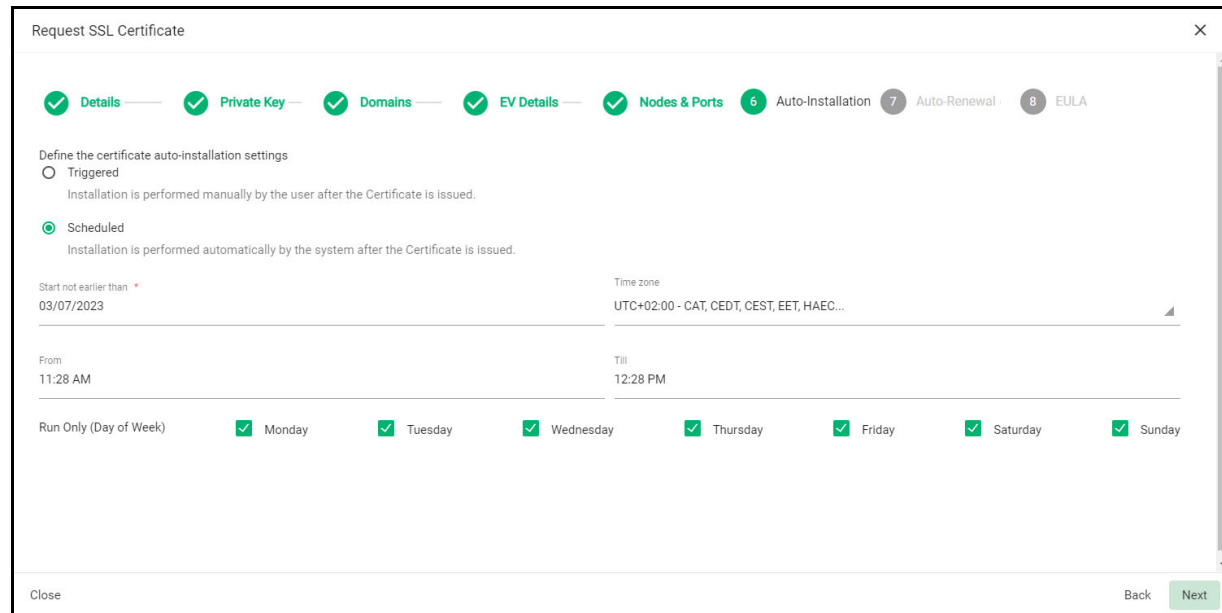
13. Select one or more servers hosting one or more of your target domains and click **OK**.
14. Select one or more domains on which to install the certificate on, and then supply a value for the **Bind To** column that corresponds to the port number to which the SSL certificate should be bound after issuance. This value is editable for a protocol with HTTP status.



15. Click **Next** to open the **Auto-Installation** page.



16. Use the **Auto-Installation** page to choose whether you want to start auto-installation manually or schedule it for a later time:
 - Select **Triggered** to start the auto-installation manually after completing the wizard. To do this, navigate to **Certificates > SSL Certificates**, select the certificate, and then click **Install**.
 - Select **Scheduled** to specify a date and time to run the auto-installer. The agent will generate the CSR and submit it to Sectigo the next time it polls SCM after the scheduled time.



17. If you selected **Scheduled auto-installation**, populate the **Schedule** fields based on the information provided in the following table.

Field	Description
Time zone	The time zone from which installation times are calculated and scheduled. The time zones available are grouped using Coordinated Universal Time (UTC). If you cannot find your local or preferred time zone, you can determine your UTC grouping online.
Start not earlier than	Specifies the earliest date that the automatic installation can be run.
Run Between (Time of Day)	The range of time, during a 24-hour period, in which an automatic installation can be run.
Run Only (Day of Week)	The days of the week on which automatic installation can be run.

18. Click **Next** to open the **Auto-Renewal** page.

Request SSL Certificate

Details —
 Private Key —
 Domains —
 EV Details —
 Nodes & Ports —
 Auto-Installation 7 —
 Auto-Renewal 8 —
 EULA

Schedule the certificate auto-renewal in advance of its expiration.

Enable Auto-Renewal

Create new key pair while renewing

Renew days prior to expiration

Close Back Next

19. Follow this procedure to configure the auto-renewal options:
- Select **Enable auto renewal of this certificate** to have SCM apply for a new certificate when the current one approaches expiry.
 - Select **Create new key pair while renewing** to specify that you want to generate a new key pair for the renewed certificate. Leaving this option disabled means SCM is to reuse the key pair of the old certificate.
 - Use the **Number of days before expiration to start auto renewal** field to specify the number of days before the expiration date when the renewal process should begin. On the scheduled day, the agent will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.

If auto-renewal is enabled, certificates requested using the **Auto generation of CSR with auto installation** setting are installed automatically at the time of renewal.

20. Click **Next** to open the EULA page.

Request SSL Certificate

Details Private Key Domains EV Details Nodes & Ports Auto-Installation Auto-Renewal **8 EULA**

Subscriber Agreement

IMPORTANT—PLEASE READ THIS SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE OR BEFORE CLICKING ON "I ACCEPT". YOU AGREE THAT BY APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO ITS TERMS. IF YOU ARE APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU ARE AN AUTHORIZED REPRESENTATIVE OF SUCH ENTITY AND HAVE THE AUTHORITY TO ACCEPT THIS AGREEMENT ON SUCH ENTITY'S BEHALF. IF YOU DO NOT HAVE SUCH AUTHORITY OR IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A SECTIGO CERTIFICATE AND DO NOT CLICK "I ACCEPT". SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT This Sectigo Certificate Subscriber Agreement (this "Agreement") is between the individual or legal entity identified on the issued Certificate(s) resulting from this Agreement ("Subscriber") and Sectigo Limited, a limited company formed under the laws of England and Wales with registered offices at 26 Office Village, 3rd Floor, Exchange Quay, Trafford Road, Salford, Manchester M5 3EQ, United Kingdom and registered number 04058690 ("Sectigo"). This Agreement governs Subscriber's application for and use of a Certificate issued from Sectigo. Subscriber and Sectigo agree as follows: 1. Definitions. 1.1. "Application Software

Print

I agree.

I agree. checkbox will be enabled once you finish reading the agreement and therefore scroll it to bottom.

Certification:

IMPORTANT—PLEASE READ THIS SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE OR BEFORE CLICKING ON "I ACCEPT". YOU AGREE THAT BY APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO ITS TERMS. IF YOU ARE APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU ARE AN AUTHORIZED REPRESENTATIVE OF SUCH ENTITY AND HAVE THE AUTHORITY TO ACCEPT THIS AGREEMENT ON SUCH ENTITY'S BEHALF. IF YOU DO NOT HAVE SUCH AUTHORITY OR IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A SECTIGO CERTIFICATE AND DO NOT CLICK "I ACCEPT". SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT This Sectigo Certificate Subscriber Agreement (this "Agreement") is between the individual or legal entity identified on the issued Certificate(s) resulting from this Agreement ("Subscriber") and Sectigo Limited, a limited company formed under the laws of England and Wales with registered offices at 26 Office Village, 3rd Floor, Exchange Quay, Trafford Road, Salford, Manchester M5 3EQ, United Kingdom and registered number 04058690 ("Sectigo"). This Agreement governs Subscriber's application for and use of a Certificate issued from Sectigo. Subscriber and Sectigo agree as follows: 1. Definitions. 1.1. "Application Software

Close Back OK

21. Read the EULA and accept it by selecting **I Agree**, and then click **OK** to submit the application.

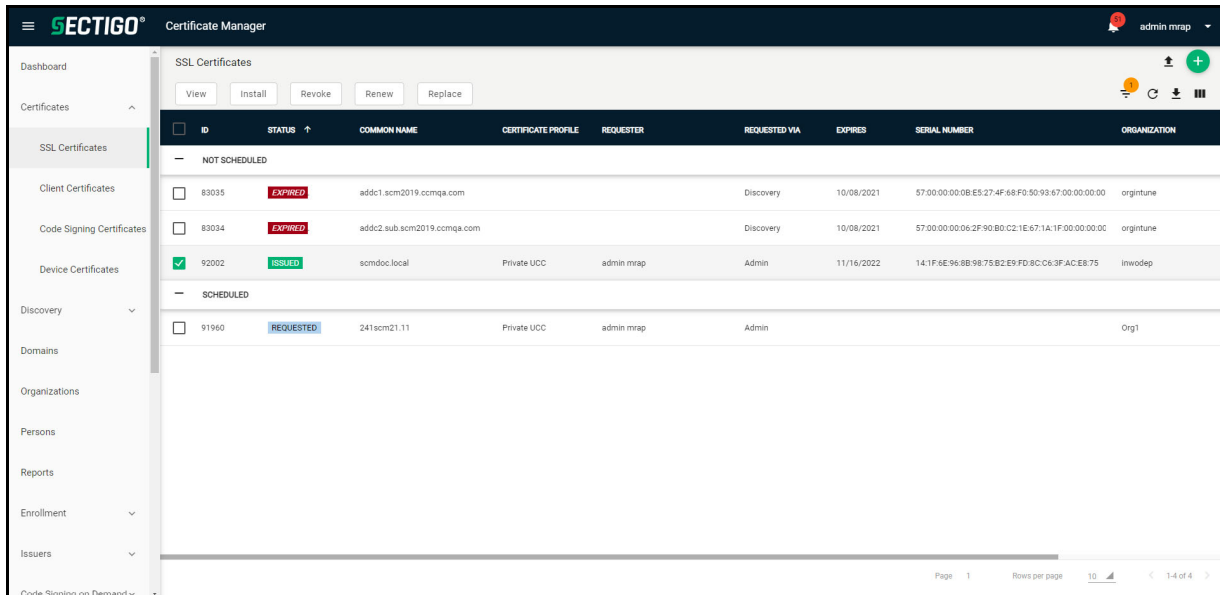
Upon completion of the wizard, the certificate is added to the **SSL Certificates** page with a status of **Requested**. The next phase of the process is to have the requested certificate approved (see [“Approving, declining, viewing, and editing certificate requests” on page 70](#)).

Once approved, the CSR is submitted to Sectigo to apply for the certificate. The certificate status changes to **Applied**.

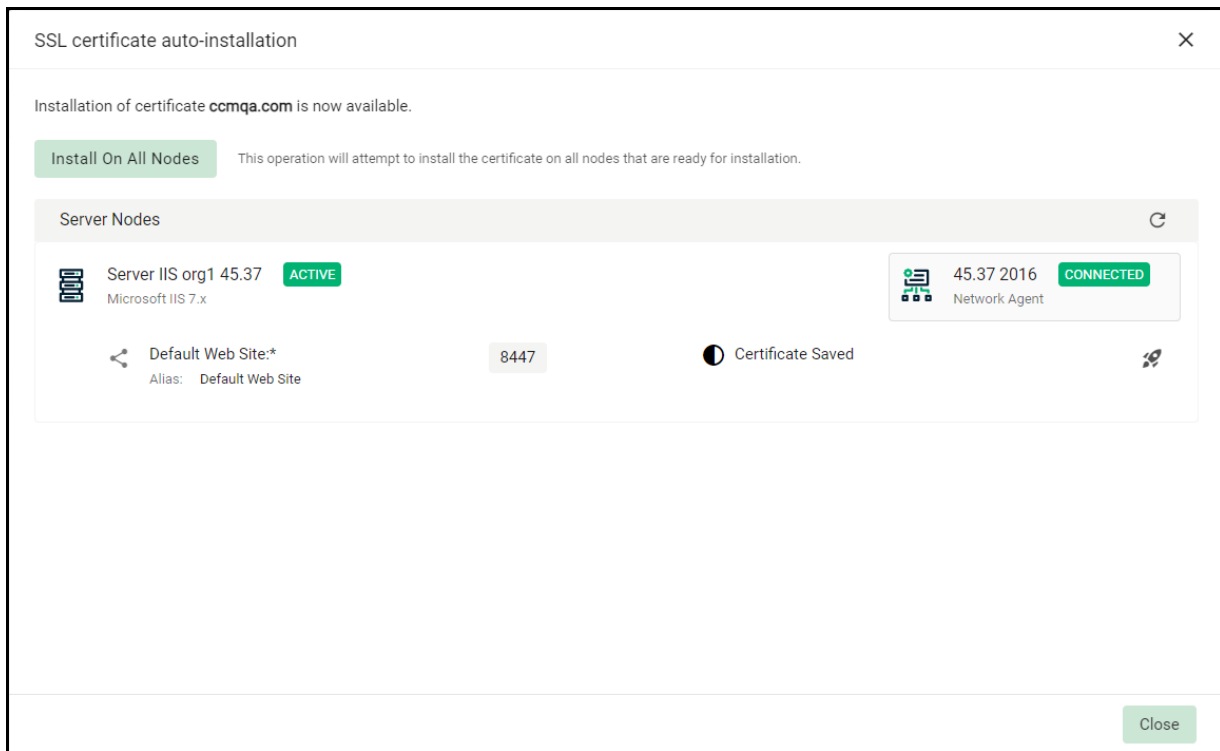
The agent tracks the order number and downloads the certificate once it is issued. The certificate is then stored and its status changes to **Issued**.

To manually initiate auto-installation of an issued certificate, follow this procedure:

1. Navigate to **Certificates > SSL Certificates**, select the certificate, and click **Install**.



This displays the **SSL certificate auto-installation dialog**.



During the auto-installation process, an item can have one of the following statuses:

- **Not Started** - no operations started or applied for this item
- **Private Key Saved** - a private key is saved on this item agent, no active operations
- **Certificate Saved** - a certificate chain is saved on this item agent, no active operations
- **Certificate Deployed** - a certificate is deployed to this item node, but the server requires restart

- **Installed** - an installation has been completed on this item
- **Failed** - the current operation is failed
- **Invalid** - this item can't take part in the installation process any more, since it lost it's link to the node, server or agent

2. Click **Install Certificate**.

The certificate installation begins and the state of the certificate changes to **Installing Certificate**.

When the installation completes, various servers process the certificates in the following ways:

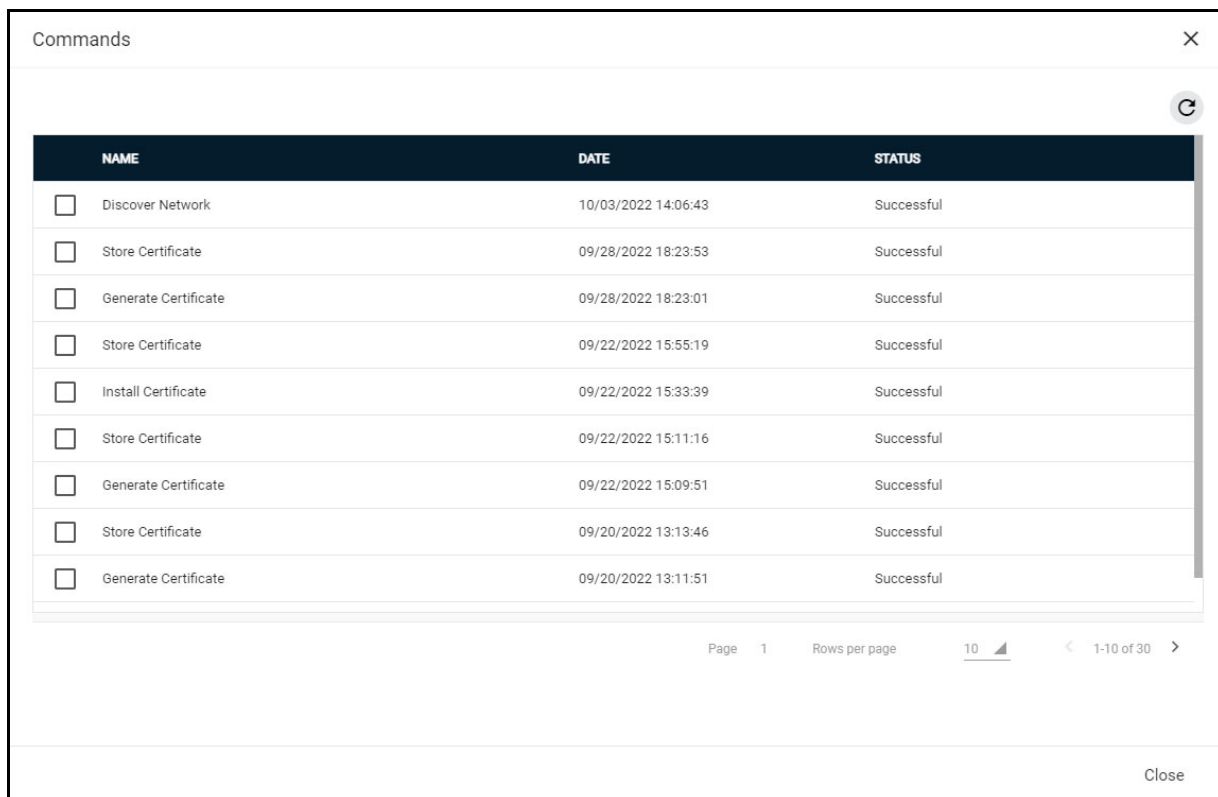
- On IIS servers, Tomcat, and F5 BIG-IP, the certificate is activated immediately and the install state changes to **Successful**.
- On Apache, the certificate becomes active after the server is restarted. The install state changes to **Restart Required**. The server can be restarted from SCM through the **Certificate Details** dialog. See ["Restarting Apache server after auto-installation of SSL certificates"](#) on page 32 for more information.

After restarting the server, the certificate is activated and the install state changes to **Completed**.

You can check whether or not the agent has stored the certificate as follows:

1. Navigate to **Integrations > Network Agents**.
2. Select the agent and click **Commands**.

The **Store Certificate** command should show a status of successful.

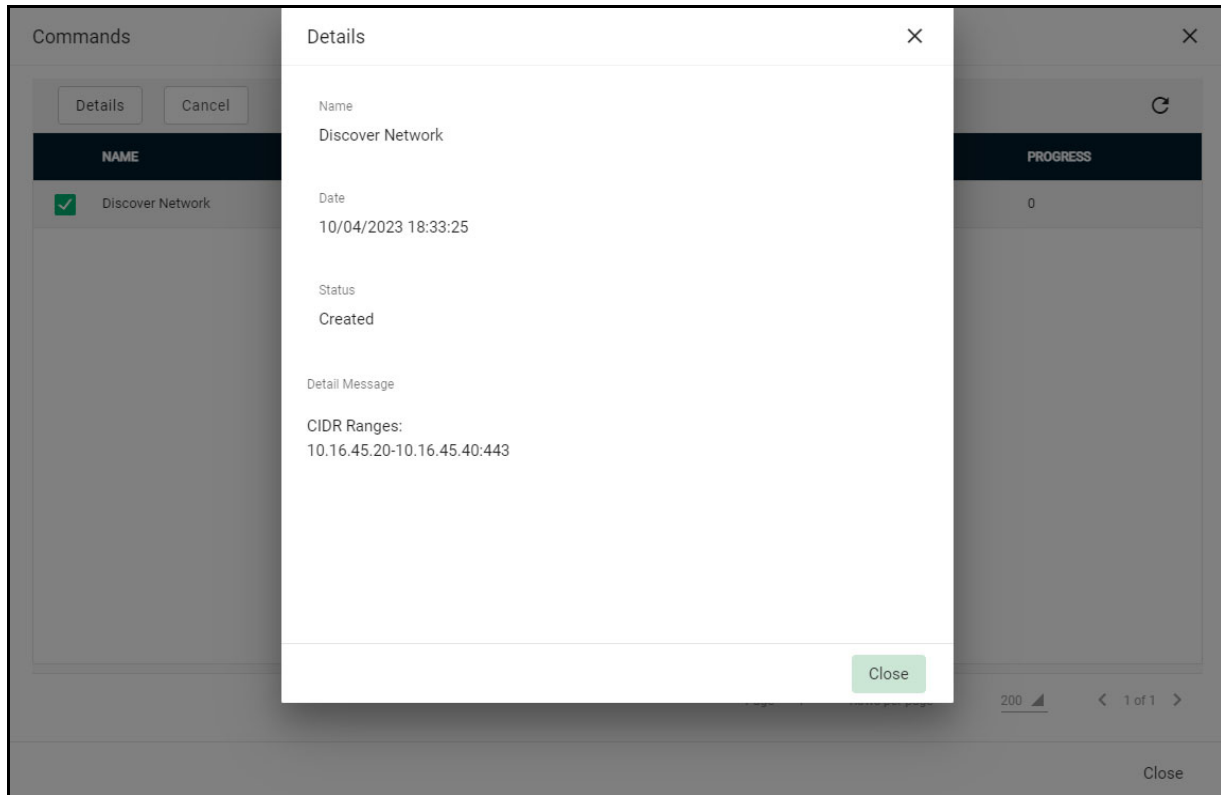


NAME	DATE	STATUS
<input type="checkbox"/> Discover Network	10/03/2022 14:06:43	Successful
<input type="checkbox"/> Store Certificate	09/28/2022 18:23:53	Successful
<input type="checkbox"/> Generate Certificate	09/28/2022 18:23:01	Successful
<input type="checkbox"/> Store Certificate	09/22/2022 15:55:19	Successful
<input type="checkbox"/> Install Certificate	09/22/2022 15:33:39	Successful
<input type="checkbox"/> Store Certificate	09/22/2022 15:11:16	Successful
<input type="checkbox"/> Generate Certificate	09/22/2022 15:09:51	Successful
<input type="checkbox"/> Store Certificate	09/20/2022 13:13:46	Successful
<input type="checkbox"/> Generate Certificate	09/20/2022 13:11:51	Successful

Page 1 Rows per page 10 1-10 of 30

Close

3. To view the command details, select the command and click **Details**.



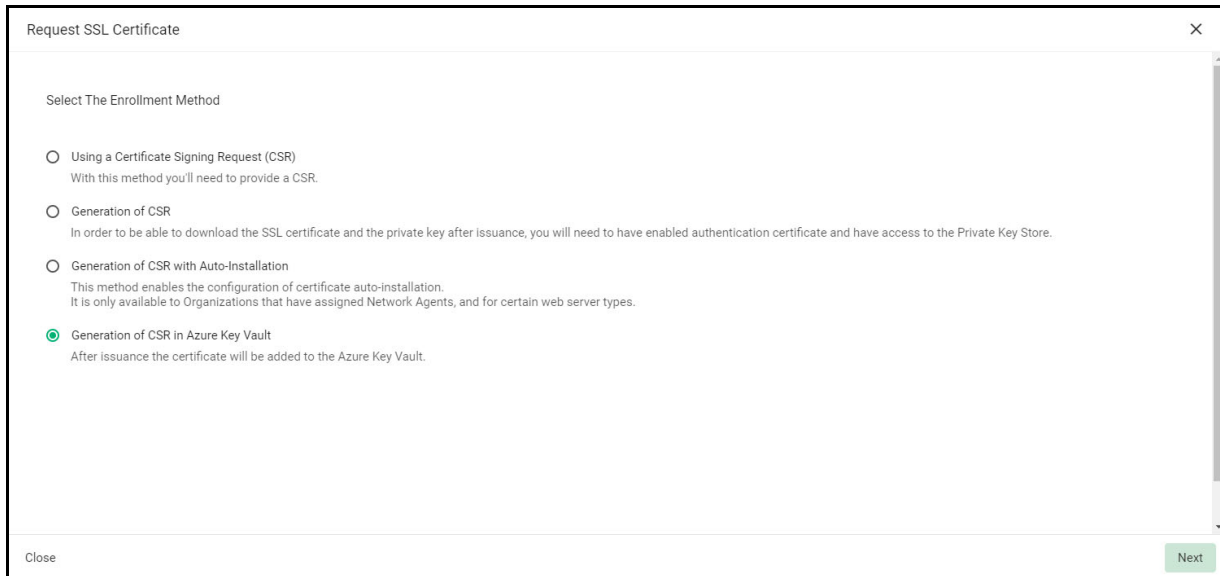
3.2.3.2.4 Generation of CSR in Azure Key Vault

Before enrolling SSL certificates with Azure Key Vault, you must have Azure Key Vault enabled for your account and an SCM Azure Account configured. For more information, see [“Microsoft Azure configuration overview” on page 203](#).

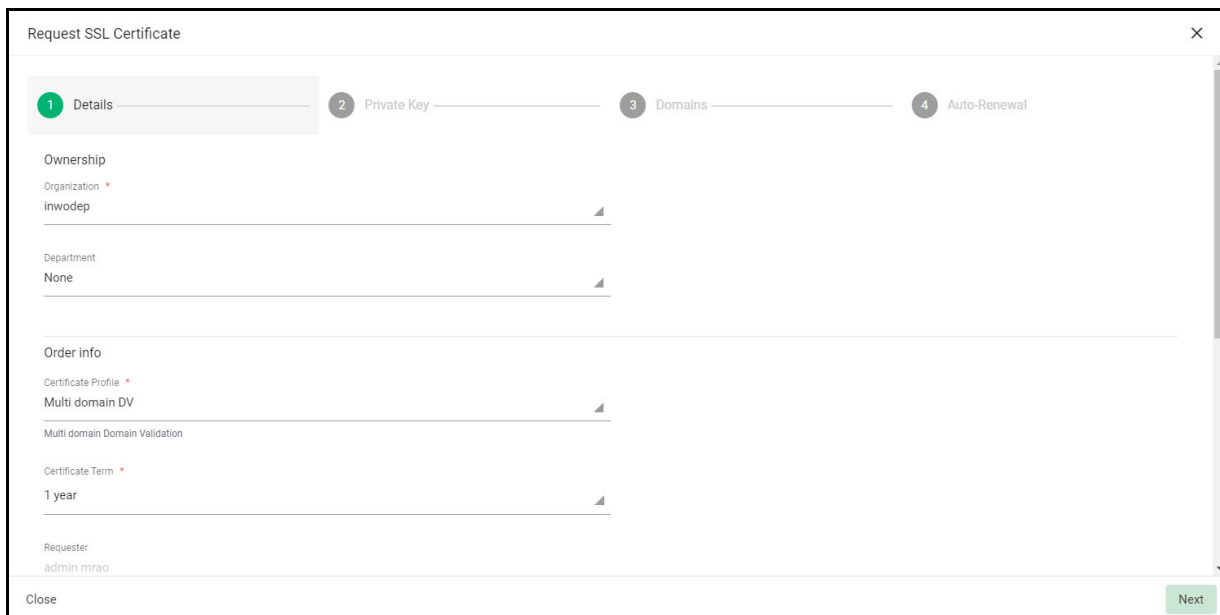
You can trigger an auto-generation of new certificates in Azure Key Vault as follows:

1. Navigate to **Certificates > SSL Certificates** and then click the **Add** icon.

This opens the **Request SSL Certificate** wizard shown in the following illustration.



2. Select **Generation of CSR in Azure Key Vault** and click **Next** to open the Details page shown in the following illustration.

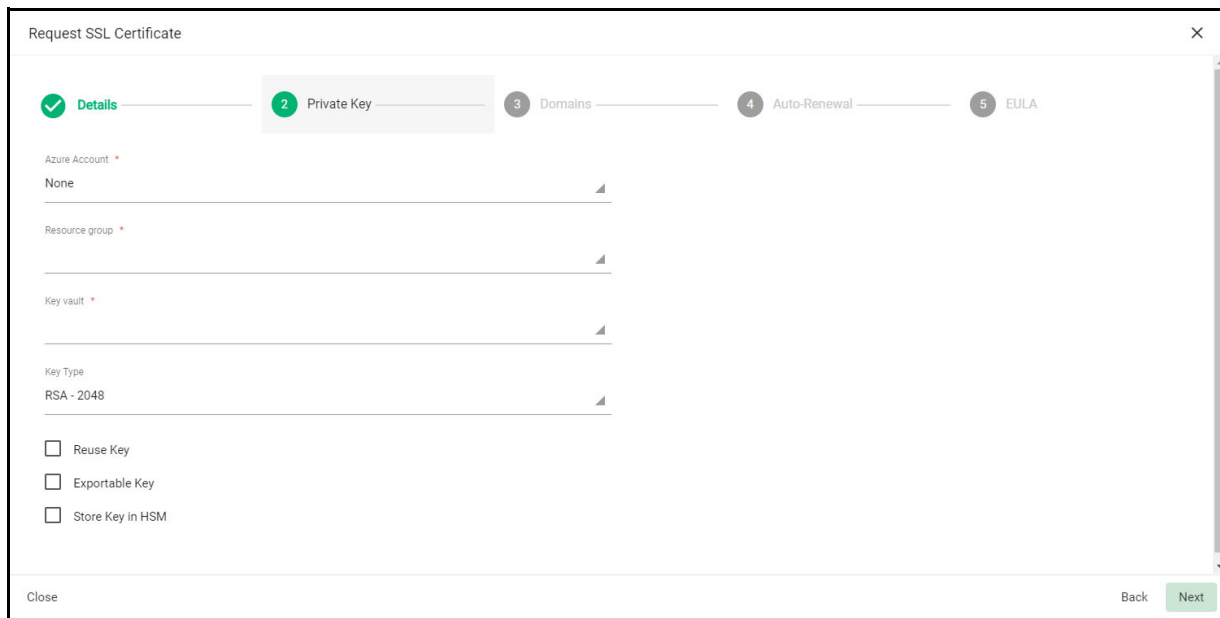


3. Complete the **Details** fields based on the information provided in the following table.

Field	Description
Ownership	
Organization	The organization to which the SSL certificate will belong.
Department	The department to which the SSL certificate will belong. For the certificate to be applied to all departments, select Any .

Field	Description
Order info	
Certificate Profile	The certificate profile to be used for the certificate issuance. The profile description is also displayed (if provided).
Certificate Term	The validity period of the certificate. For example, 1 year, 2 years, 3 years. The available validity periods depend on the selected profile.
Requester	Auto-populated with the name of the administrator making the application.
Comments (optional)	Comments pertaining to the certificate. If there are no comments entered, the comment panel will not appear.
Notifications	
External Requesters	Email address of an external requester on whose behalf the application is made. The requester is still the administrator that is completing this form. The email address of the external requester is displayed as the External Requester in the Certificate Details of an issued certificate.

4. Click **Next** to open the **Private Key** page.



5. Specify the Private Key parameters based on the information provided in the following table.

Field	Description
Azure Account	Select the SCM Azure Account configured for the Azure Key Vault to which you want to connect.

Field	Description
Resource group	Select the resource group containing the appropriate Azure Key Vault.
Key vault	Select the Azure Key Vault in which the CSR is to be generated.
Key Algorithm	The key algorithm to be used for the certificate's key pair (RSA or EC). (EC is only available if enabled for the certificate template; contact your Sectigo account manager).
Key Type	Select the key size or curve to use for the encryption.
Reuse Key ^a	Indicates whether the existing key will be used when renewing the certificate.
Exportable Key ^a	Indicates whether the private key for the certificate can be exported.
Store Key in HSM	Indicates whether the key will be stored in the HSM (if available).

a. If the reuse and exportable key policies are subsequently changed in Azure, the Azure policies will be used during renewal or replacement.

6. If your account is configured for EV, click **Next** to open the **EV Details** page.

7. Complete the fields of the **EV Details** page.

The fields you need to complete depend on the EV mode activated for your account. Typically, it would be the same information as provided in the **EV Details** page when adding a new organization (see [Edit organization or department details](#)).

8. Click **Next** to open the **Domains** page and complete the domains information based on the following table.

Field	Description
Common Name ^a	The domain to which the certificate is to be issued. The maximum allowed character length for this field is 64.
Subject Alternative Names	Additional domain names, separated by commas. This field appears only if a multi domain or UCC certificate profile is selected.

a. The certificate name in Azure Key Vault cannot contain asterisks or periods. For example, if you specify a common name of *.cmqa.com, the certificate name in Azure Key Vault is -cmqa-com.

The screenshot shows the 'Request SSL Certificate' form at the 'Domains' step. The progress bar at the top indicates that 'Details' and 'Private Key' are completed (green checkmarks), 'Domains' is the current step (green circle with '3'), 'Auto-Renewal' is next (grey circle with '4'), and 'EULA' is the final step (grey circle with '5'). The form contains a 'Domains' section with a 'Common Name *' text input field and a 'Subject Alternative Names' text input field with a plus icon. A blue tooltip box is positioned over the plus icon, containing the text: 'Use commas or spaces to separate multiple values for bulk input.' At the bottom of the form, there are 'Close', 'Back', and 'Next' buttons.

9. Click **Next** to open the **Auto-renewal** page shown in the following illustration.

The screenshot shows the 'Request SSL Certificate' form at the 'Auto-Renewal' step. The progress bar at the top indicates that 'Details', 'Private Key', and 'Domains' are completed (green checkmarks), 'Auto-Renewal' is the current step (green circle with '4'), and 'EULA' is the final step (grey circle with '5'). The form contains the text 'Schedule the certificate auto-renewal in advance of its expiration.' and a toggle switch labeled 'Enable Auto-Renewal' which is currently turned off. At the bottom of the form, there are 'Close', 'Back', and 'Next' buttons.

10. Follow this procedure to configure the auto-renewal options:
 - a. Select **Enable auto renewal of this certificate** to have SCM apply for a new certificate when the current one approaches expiry.
 - b. Use the **Number of days before expiration to start auto renewal** field to specify the number of days in advance of expiry that the renewal process should start. On the scheduled day, the agent will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.
11. Click **Next** to open the **EULA** page shown in the following illustration.

Request SSL Certificate

Details
 Private Key
 Domains
 Auto-Renewal
 5 EULA

Subscriber Agreement

SSL EULA! IMPORTANT – PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING AN AusCERT CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING AN AusCERT CERTIFICATE OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT AND THAT YOU AGREE TO AND ACCEPT THE TERMS AS PRESENTED HEREIN. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE AN AusCERT CERTIFICATE AND CLICK "I DECLINE" BELOW. The terms and conditions set forth below constitute a binding agreement between you (the "Subscriber" or "you") and The University of Queensland trading as AusCERT, which has its principal place of business at The University of Queensland, Queensland 4072, Australia ("AusCERT"), with respect to your use of the AusCERT digital certificate services (the "Agreement"). 1. You, the Subscriber, hereby agree that: 1.1. you will comply with the "Subscriber" obligations as set out in the CPS and fill your role as, and follow the procedures set out for, a Subscriber under the CPS in respect of your use of Certificates and the Subscription Services and that all obligations placed on a Subscriber and all representations and warranties made by a Subscriber under the CPS shall be incorporated into this agreement by reference; 1.2. you will ensure that your staff and representatives involved with the Subscription Services read and understand the terms and conditions in the CPS and associated policies that are published in the Repository; 1.3. you will use

Print

I agree.

"I agree" checkbox will be enabled once you finish reading the agreement and therefore scroll it to bottom.

Close Back OK

12. Read the EULA and accept it by selecting **I Agree**, and then click **OK** to submit the application.

Upon completion of the wizard, the certificate is added to the **SSL Certificates** page with a status of **Requested**. The next phase of the process is to have the requested certificate approved (see [“Approving, declining, viewing, and editing certificate requests”](#) on page 70).

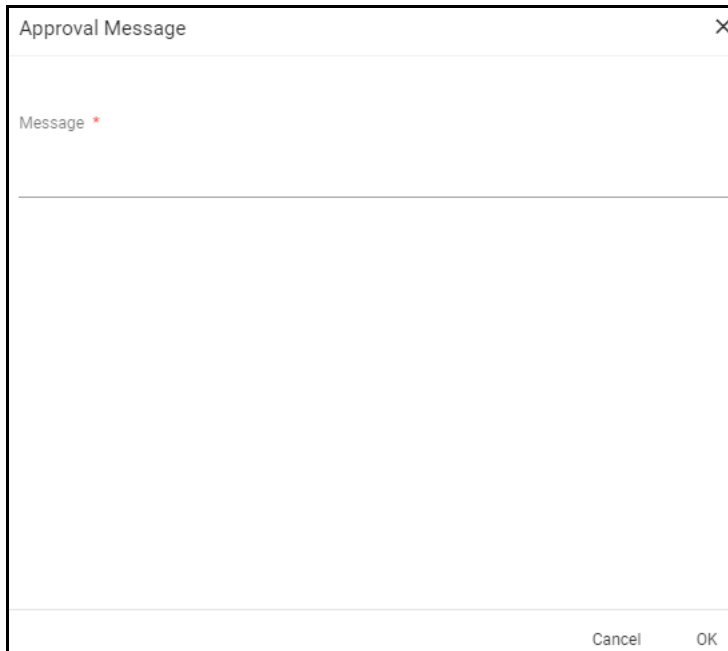
3.2.3.3 Approving, declining, viewing, and editing certificate requests

After a successful application via either the auto-installer, SSL certificate enrollment form, or enrollment wizard, a certificate request appears under **Certificates > SSL Certificates**.

To perform one of the actions related to the certificate request, you use filters to view all certificates with a status of **Requested**, and then select the certificate that you want to approve, decline, view, or edit. Note that at this point, the certificate request has not been submitted to Sectigo and is pending approval by an administrator, unless the application was made by an administrator who can approve their own request.

To modify the application before submitting it to Sectigo for processing, click **Edit**. The **Edit SSL Certificate** wizard is displayed. Complete the wizard by following instructions provided in [“Using a Certificate Signing Request”](#) on page 41.

To submit the application to Sectigo for processing, click **Approve** to display the **Approval Message** dialog shown in the following illustration, type in a message to be included with the approval notification email, and click **OK**.



NOTE: The SSL Approved Notification should have been enabled for the requester to receive an email notification.

Once the request has been submitted to Sectigo, the certificate status changes to Approved, and then changes to Applied if accepted by Sectigo. When the certificate is issued, Sectigo sends a certificate collection email to the applicant, at which point the certificate's status changes to Issued in SCM.

To reject a request, click **Decline**, which changes the certificate status to Declined. If an SSL Declined notification has been enabled, then an email is sent to the applicant informing them that the request has been rejected. Declined requests can still be approved at any time by a MRAO, RAO SSL, or DRAO SSL administrator.

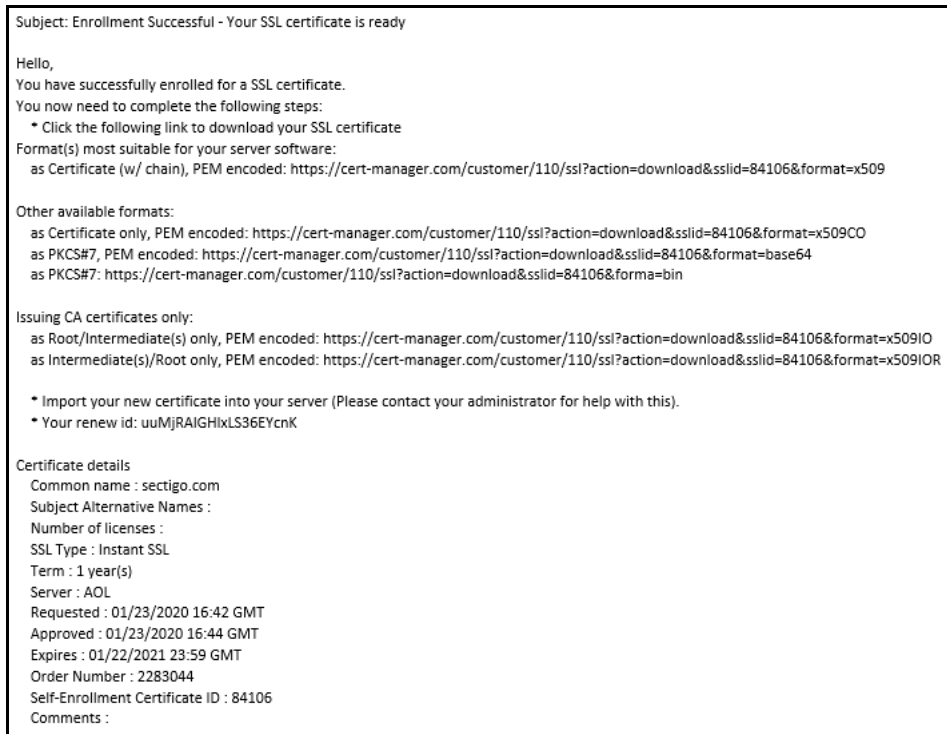
For more information, see [“Managing SSL Certificates”](#) on page 20.

3.2.3.4 Certificate collection and installation

Once the application process has been successfully completed, the requester downloads the certificate, saves it in a secure location on their computer, and then installs it on their server.

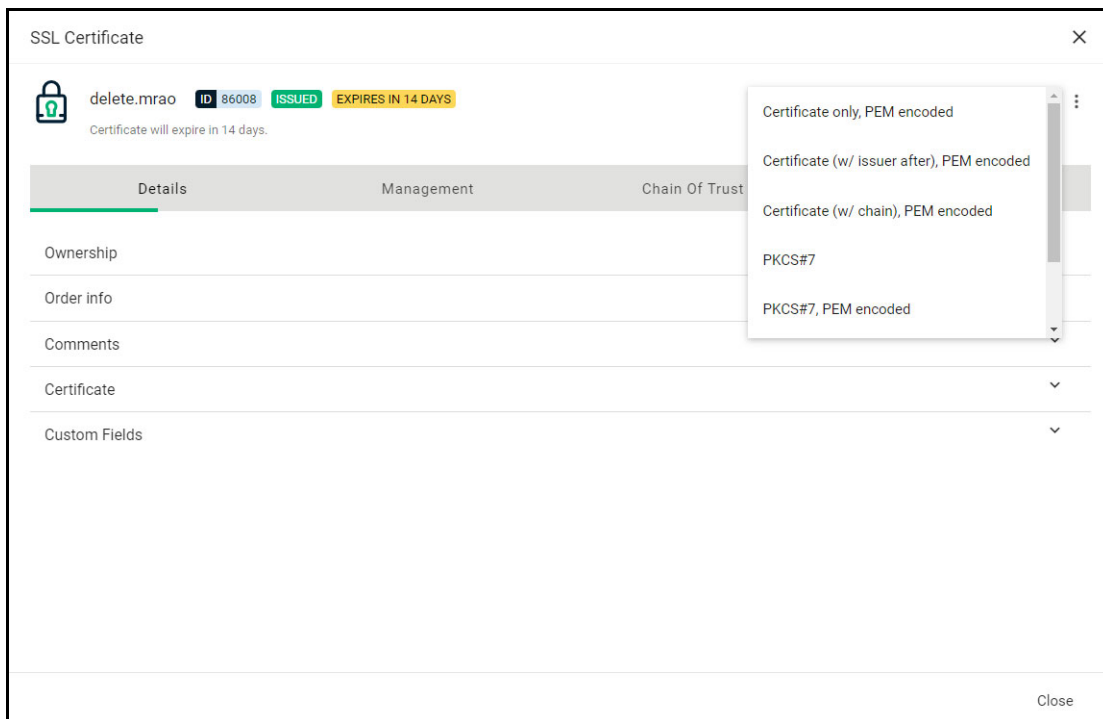
After Sectigo has issued the certificate for which an application was made via the SSL certificate enrollment wizard or the self-enrollment form, SCM sends a collection email to the requester.

The certificate collection email contains a summary of the certificate details, a link to the certificate collection form, and a unique certificate ID that is used for validation.



Note: You can modify the contents of these emails by navigating to **Settings > Notification Templates**.

To download the certificate, the applicant clicks **Download** and chooses the format.



The installation process depends on the web server type. For more information and instructions, select the appropriate installation guide available at the Sectigo support site at sectigo.com/support.

Alternatively, MRAO, RAO SSL, and DRAO SSL administrators can download the certificate and provide it to the requester. To do this, navigate to **Certificates > SSL Certificates**, select the certificate, and click **Details**. See “Using the SSL Certificate Details tab” on page 27.

If the private key is managed by the PKS, you have the option to download the certificate along with the private key in .p12 format. Doing so can make it easier to export the certificate to another web server. However, you must ensure that the file is stored in a highly secure location.

You can only download certificates in .p12 format after you have authenticated yourself with a certificate on the computer from which you are accessing SCM. See “Using the Private Key Store to store and manage SSL certificate private keys” on page 31.

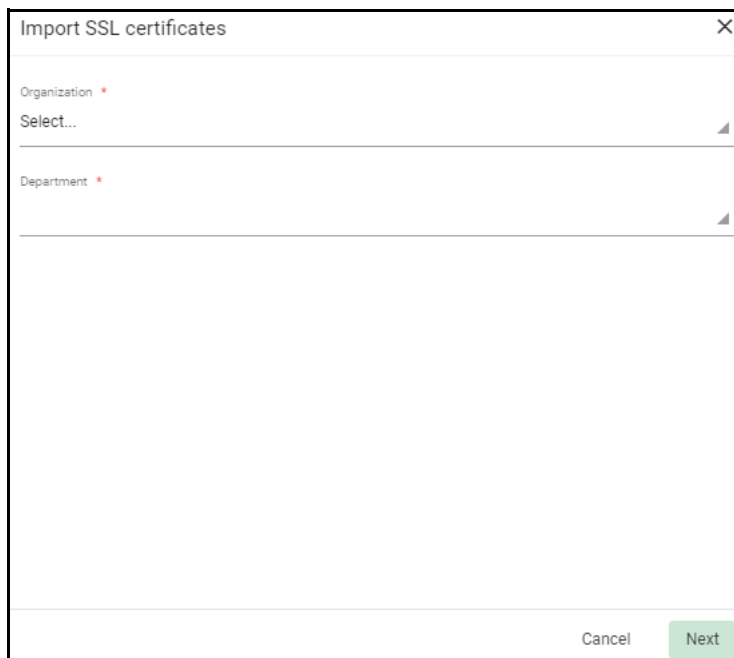
3.2.4 How to import SSL certificates

You can import SSL certificates in a ZIP file containing certificates in .cer, .crt or .pem format.

Imported certificates are classified as externally managed, and treated the same as external certificates discovered via a discovery scan that have been assigned to an organization.

To import SSL certificates, do the following:

1. Navigate to **Certificates > SSL Certificates**.
2. In the upper-right corner, click **Import** to open the **Import SSL certificates** dialog.



The screenshot shows a dialog box titled "Import SSL certificates" with a close button (X) in the top right corner. The dialog contains two dropdown menus. The first is labeled "Organization" with a red asterisk and "Select..." below it. The second is labeled "Department" with a red asterisk. At the bottom of the dialog, there are two buttons: "Cancel" and "Next".

3. Select the organization and department to which the certificates belong.
4. Click **Next**, choose the archive to be imported and click **Open**.

The progress of the import is displayed.

5. When the import is finished, click **Close**.

3.2.4.1 SSL certificate CSV file format and importing guidelines

The data for SSL certificate bulk enrollment requests must be structured correctly and submitted in a CSV format. Parameters specified for each separate certificate included in the request must be written on one line and separated by commas, except the last parameter in the line. All parameters are mandatory, except for Subject Alternative Names (SAN); if the certificate has no SANs, the parameter is left blank. If a parameter contains one or more commas within its string, this parameter must be placed in quotes.

The following parameters must be present in each line of the CSV file in the order listed:

1. Common Name—string.
2. SAN—the whole value must be in quotes, domains inside, comma separated.
3. Certificate Type—string, must be the same as the certificate profile **Name**.
4. Certificate Term—string, must be the same as it appears in the certificate profile.
5. Server Software—string. It is currently suggested that you populate this space with "OTHER".

For example, to request enrollment for an EliteSSL Certificate profile for 1 year with a common name of scmqa.com without SANs, the following line would be included in the CVS file:

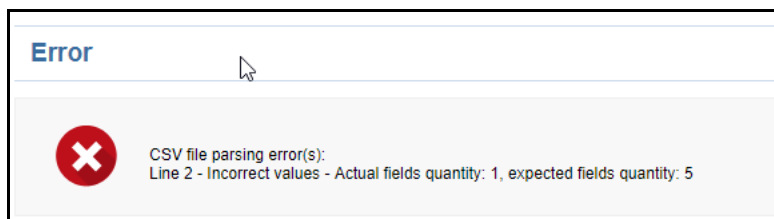
```
scmqa.com, , EliteSSL Certificate, 1 year, OTHER
```

The following example requests enrollment for an AMT Multi-Domain SSL Certificate for 2 years with a common name of scmqa.com, and with SANs fly.com and new.com:

```
scmqa.com, "fly.com, new.com", AMT Multi-Domain SSL Certificate, 2 years, OTHER
```

3.2.4.2 Bulk SSL certificate CSV file errors

When submitting a bulk enrollment request accompanied by a CSV file that contains errors, an error message similar to the one shown in the following illustration might appear.



The following table lists errors that may arise during parsing of an SSL Certificate CSV file.

Error ID	Error message	Reason
1	CSV file parsing error(s): Line <line ID> - Required field 'commonName' is not specified. (Displayed in red bold above every field.)	The CSV file contains a line without a common name.
2	CSV file parsing error(s): Line <line ID> - Required field 'certType' is not specified. (Displayed in red bold above every field.)	The CSV file contains a line without a certificate type.
3	CSV file parsing error(s): Line <line ID> - Required field 'certTerm' is not specified.	The CSV file contains a line without a certificate validity period (term).
4	CSV file parsing error(s): Line <line ID> - Required field 'serverSoftware' is not specified	The CSV file contains a line without a server software.
5	CSV file parsing error(s): Line <line ID> - Please use commas only to delimit domain alternative names (for example - domain_one.com, domain_two.com, etc.)	The CSV file contains a line in which not all parameters are separated by commas.
6	CSV file parsing error(s): Line <line ID> - field 'certType' contains disallowed value: <value>	The specified certificate type is not found among certificate profiles allowed for the organization for which this request is being submitted. Or this certificate type does not exist.
7	CSV file parsing error(s): Line <line ID> - field 'certTerm' contains disallowed value: <value>	The specified certificate term is not permitted for the certificate type specified in the same line.
8	CSV file parsing error(s): Line <line ID> - field 'serverSoftware' contains disallowed value: <value>	The specified server software is not found among the server software allowed for the organization for which the request is being submitted.
9	CSV file parsing error(s): Line <line ID> - Incorrect values - Actual fields quantity: <value>, expected fields quantity: <value>	The number of commas in a line of the CSV file is other than four.
10	CSV file parsing error(s): Line <line ID> - Field 'san' contains non-empty value: '<0>'. Subject alternative names are not allowed for '<specified certType>' certificate type.	A line in the CSV file contains Subject Alternative Names, whereas the certificate type specified in the same line is not multi-domain.

3.2.5 How to renew SSL certificates

You can either renew certificates manually or enable automatic renewal. External applicants can renew the certificates manually via the self-renewal form.

3.2.5.1 Certificate renewal by administrators

The **SSL Certificates** page enables you to renew both managed and external (also known as unmanaged) certificates, with the renewal process being different for each:

- Managed certificates are issued via SCM based on a specific combination of domain and organization. A CSR is submitted the first time an application for a certificate for any such combination is made. SCM assigns a status of issued, applied, or requested to managed certificates. Typically, you do not need to submit a CSR to renew managed certificates, as SCM can reuse the existing CSR.
- External certificates are those certificates which are found during a discovery scan but were not issued via SCM. To renew external certificates, a new CSR is required because SCM does not have it on record. After issuance, this certificate becomes managed.

If you moved a domain from one organization to another, then you are effectively creating a new certificate application instead of renewing a certificate. If this is the case, you have to submit a new CSR.

To renew a managed certificate using a new key pair, do the following:

1. Navigate to **Certificates > SSL Certificates**.
2. Select a certificate of any status and click **Renew**.
3. Select **Using new Key Pair**.
4. Click **Next**.
5. Complete the wizard by following instructions provided in [“Using a Certificate Signing Request” on page 41](#).

To renew a managed certificate using an existing key pair, do the following:

1. Navigate to **Certificates > SSL Certificates**.
2. Select a certificate of any status and click **Renew**.
3. Select **Using existing Key Pair and details**.
4. Click **Confirm**.

If the selected certificate is unmanaged, the **Renew SSL Certificate** wizard is displayed. Complete the wizard by following instructions provided in [“Using a Certificate Signing Request” on page 41](#).

Once issued, the renewed certificate becomes available for collection and installation. For more information, see [“Certificate collection and installation” on page 71](#).

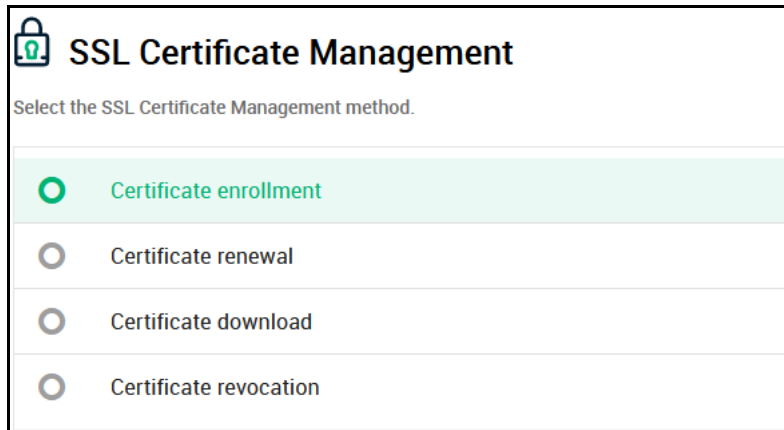
3.2.5.2 Certificate renewal by end-users

Applicants can renew their SSL certificates using the self-renewal application form located at the address specified for the SSL Web Form enrollment endpoint. By default the address is similar to the following:

`https://cert-manager.com/customer/<customer_uri>/ssl.`

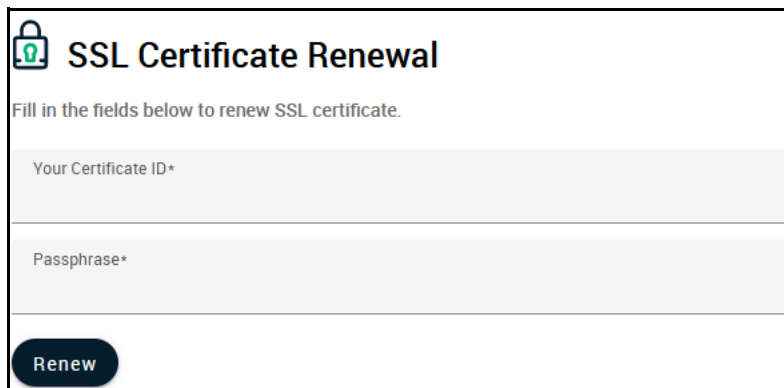
To view the SSL Web Form URL, navigate to **Settings > Enrollment Endpoints**.

Accessing the link displays the **SSL Certificate Management** form shown in the following illustration.



The screenshot shows the 'SSL Certificate Management' form. At the top left is a lock icon. The title is 'SSL Certificate Management'. Below the title is the instruction 'Select the SSL Certificate Management method.' There are four radio button options: 'Certificate enrollment' (selected), 'Certificate renewal', 'Certificate download', and 'Certificate revocation'.

Clicking **Certificate renewal** opens the **SSL Certificate Renewal** form shown in the following illustration.



The screenshot shows the 'SSL Certificate Renewal' form. At the top left is a lock icon. The title is 'SSL Certificate Renewal'. Below the title is the instruction 'Fill in the fields below to renew SSL certificate.' There are two input fields: 'Your Certificate ID*' and 'Passphrase*'. At the bottom left is a dark blue 'Renew' button.

Before proceeding, the end-user has to authenticate the request by entering the following:

- The certificate ID provided in the certificate collection email. You can view the certificate ID by navigating to **Certificates > SSL Certificates**. You may need to communicate the certificate ID to the external applicant.
- The certificate renewal or certificate revocation passphrase which was created during enrollment for the original certificate.

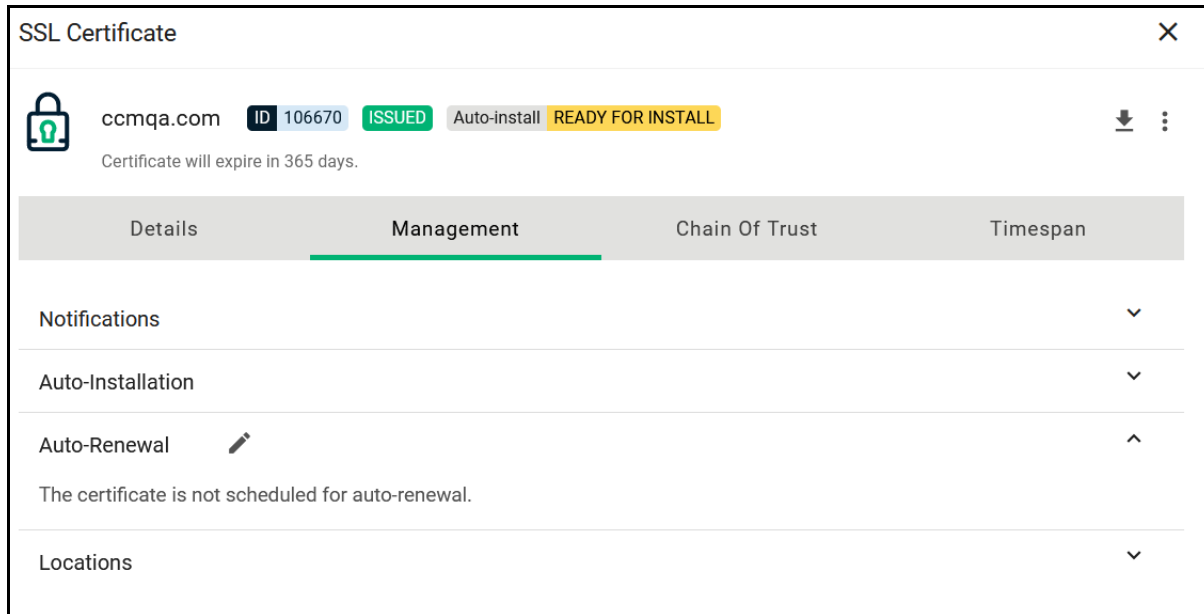
Clicking **Renew** renews the certificate with the same information as in the existing certificate.

Once issued, the renewed certificate becomes available for collection and installation. For more information, see [“Certificate collection and installation” on page 71](#).

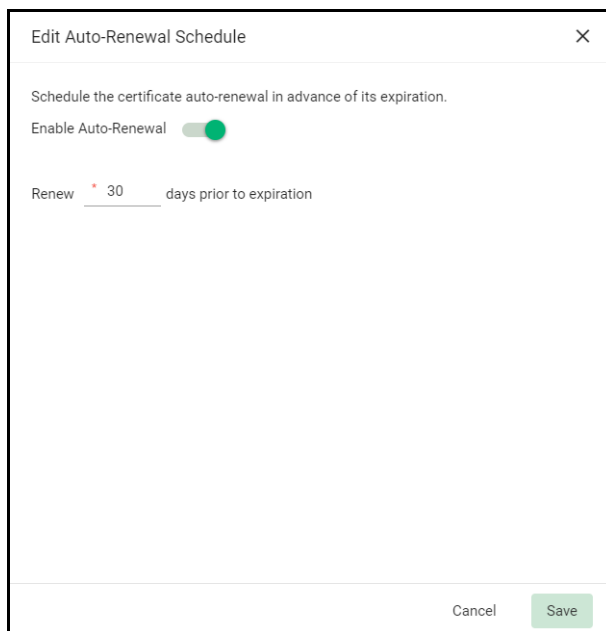
3.2.5.3 Automatic certificate renewal scheduling

To schedule or configure an automatic renewal of SSL certificates, do the following:

1. Navigate to **Certificates > SSL Certificates**, select a certificate, and then click **View**.
2. Click **Management** and expand **Auto-Renewal**.
3. Click **Edit**



This displays the **Auto-renewal settings for SSL Certificate** dialog.



4. Select **Enable Auto-Renewal** to have SCM apply for a new certificate when the current one approaches expiry.
5. Specify the number of days in advance of expiry that the renewal process should start.
6. Click **Save**.

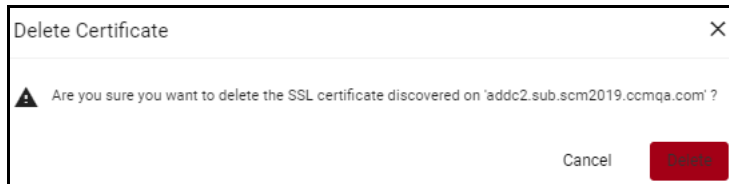
On the scheduled day, the agent will automatically generate a new CSR using the same certificate parameters as the existing certificate and submit it to the CA.

For information on other options available in the **Certificate Summary** panel, see [“How to view or modify SSL certificate details”](#) on page 24.

3.2.6 How to revoke, replace, and delete SSL certificates

Administrators can revoke, replace, and delete certificates. External applicants can revoke SSL certificates using the self-enrollment form.

To delete a certificate, navigate to **Certificates > SSL Certificates**, select a certificate, click **Delete**, and click Delete to confirm.

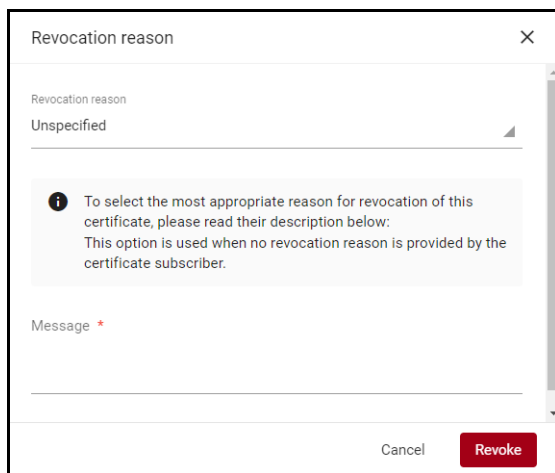


NOTE: You can only delete external certificates.

3.2.6.1 Certificate revocation by administrators

To revoke an SSL certificate, follow this procedure:

1. Navigate to **Certificates > SSL Certificates**, select a certificate, and click **Revoke**.
2. Select one of the options from the **Revocation reason** list shown in the following illustration and provide an explanation to be submitted together with the revocation notification email.



3. Click **Revoke**.

NOTE: Before revoking certificates, you may want to add an SSL Revoked notification so that the owner and/or requester are notified. Notifications are configured in the **Settings > Notifications** page. For more information, see [“Configuring notifications”](#) on page 235.

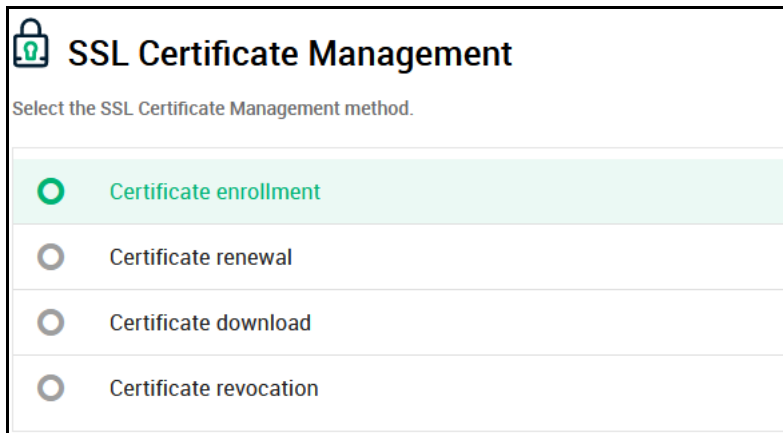
3.2.6.2 Certificate revocation by end-users

Applicants can revoke their SSL certificates using the self-renewal application form located at the address specified for the SSL Web Form enrollment endpoint. By default the address is similar to the following:

```
https://cert-manager.com/customer/<customer_uri>/ssl.
```

To view the SSL Web Form URL, navigate to **Enrollment > Enrollment Endpoints**.

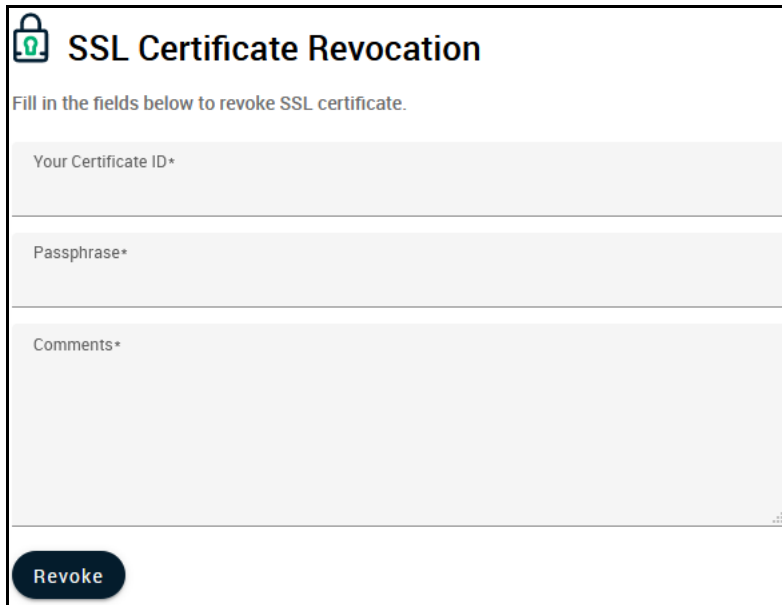
Accessing the link displays the **SSL Certificate Management** form shown in the following illustration.



The screenshot shows a web form titled "SSL Certificate Management" with a lock icon. Below the title is the instruction "Select the SSL Certificate Management method." There are four radio button options: "Certificate enrollment" (selected), "Certificate renewal", "Certificate download", and "Certificate revocation".

SSL Certificate Management	
Select the SSL Certificate Management method.	
<input checked="" type="radio"/>	Certificate enrollment
<input type="radio"/>	Certificate renewal
<input type="radio"/>	Certificate download
<input type="radio"/>	Certificate revocation

Clicking **Certificate revocation** opens the **SSL Certificate Revocation** form shown in the following illustration.



The screenshot shows a web form titled "SSL Certificate Revocation" with a lock icon. Below the title is the instruction: "Fill in the fields below to revoke SSL certificate." The form contains three input fields: "Your Certificate ID*", "Passphrase*", and "Comments*". At the bottom left of the form is a dark blue button labeled "Revoke".

Before proceeding, the end-user has to authenticate the request by entering the following:

- The certificate ID provided in the certificate collection email. You can view the certificate ID by navigating to **Certificates > SSL Certificates**. You may need to communicate the certificate ID to the external applicant.
- The certificate renewal or certificate revocation passphrase which was created during enrollment for the original certificate.
- A reason for the revocation.

Clicking **Revoke** revokes the certificate.

3.2.6.3 Replacing certificates

You cannot replace certificates if they were issued with auto-installation or if your organization does not have **Validated** status.

To replace an existing SSL certificate, follow this procedure:

1. Navigate to **Certificates > SSL Certificates**, select a certificate, and click **Replace** to open the **Replace existing SSL for domain** dialog.

If the PKS is installed and connected, you have the option of specifying whether you want to create a new CSR manually or automatically. Otherwise, you must replace the CSR manually.

2. To replace the CSR manually, select **Provide Manual CSR** and paste the new CSR in the **CSR** field. Provide a reason for replacement.
3. Click **Save**.
4. Depending on your selection, follow the instructions provided in [“Using a Certificate Signing Request”](#) on page 41 or [“Generation of CSR”](#) on page 49.

3.3 Managing Client Certificates

Depending on your security role, the **Client Certificates** page shown in the following illustration enables you to manage end-users and their client certificates.

MRAO administrators can view client certificates and archived private keys for end-users of any organization or department.

RAO Client Certificate administrators can view the client certificates as well as end-users of organizations and any subordinate departments that have been delegated to them.

DRAO Client Certificate administrators can view the client certificates and end-users of departments that have been delegated to them.

ID	STATUS	ORDER NUMBER	CERTIFICATE PROFILE	TERM	REQUESTED VIA	SUBJECT	SUBJECT ALT NAME	EXPIRES	SERIAL NUMBER	NAME
<input type="checkbox"/>	ISSUED	3635556	GEANT Personal S/MIME	365	Enrollment Fo...	CN=16.10.2022.0+or...	upn=2022,rfc822na...	10/17/2023	2D:85:1B:AA:A2...	16.10.2022
<input type="checkbox"/>	ISSUED	3635302	client_intune_99994	365	Enrollment Fo...	E=12@ccmqa.com,C...	rfc822name+12@cc...	10/15/2023	97:42:27:7D:43:6...	12.12
<input type="checkbox"/>	ISSUED	3626017	client_intune_99994	365	Enrollment Fo...	E=kmcert@ccmqa.c...	upn=number362599...	10/13/2023	04:AA:C6:55:1E:3...	kmtest austest
<input type="checkbox"/>	ISSUED	3626014	client_intune	365	Enrollment Fo...	E=kmcert@ccmqa.c...	upn=number362599...	10/13/2023	67:E0:CA:5C:80:4...	kmtest austest
<input type="checkbox"/>	ISSUED	3626013	client_intune	365	Enrollment Fo...	E=kmcert@ccmqa.c...	upn=number362599...	10/13/2023	D5:88:49:2C:08:8...	kmtest austest
<input type="checkbox"/>	ISSUED	3440663	client_intune_99994	365	Enrollment Fo...	E=org3@ccmqa.com...	rfc822name+org31...	09/13/2023	CD:ED:29:54:2A:3...	org3 person
<input type="checkbox"/>	ISSUED	3440558	GEANT IOTF Personal	365	Enrollment Fo...	CN=Robot - Name2 ...	upn=name2@ccmqa...	09/13/2023	37:79:18:0E:A9:A...	Name2 LastNa...
<input type="checkbox"/>	ISSUED	3440325	GEANT IOTF Personal Robot	365	Web API	CN=Robot - Name2 ...	upn=name2@ccmqa...	09/13/2023	DC:FA:1A:7B:10:F...	Name2 LastNa...
<input type="checkbox"/>	ISSUED	3424328	High Persona Validated Cert	365	Enrollment Fo...	E=smime@localhost...	upn=localhost.ccmq...	09/10/2023	0F:7B:ED:A3:EE:E...	client enrollment
<input type="checkbox"/>	ISSUED	3400802	client_intune	365	Enrollment Fo...	E=1@ccmqa.com,C...	upn=pppnm,rfc822...	08/09/2023	A4:16:17:8D:CC:E...	person w secre...

Before end-users can be issued a client certificate, they must be added to SCM as a Person under an organization or department. The **Persons** page lists the end-users who have been added to SCM. The following parameters are available:

- **Name**—the end-user name.
- **Common Name**—the end-user common name.
- **Organization**—the name of the organization to which the end-user belongs.
- **Department**—the name of the department to which the end-user belongs (if applicable).
- **Email**—the end-user email address.
- **Alternative Emails**—the end-user alternative email address.
- **UPN**—the end-user principal name.
- **Contact Phone**—the end-user phone number.
- **Created**—the date when the end-user was created.
- **Modified**—the date when the end-user was modified.

Depending on the status of the selected end-user's certificates, you can perform the following actions on end-users:

- **Import**—Enables you to import client certificates in `.cer`, `.crt` or `.pem` format.
- **Add**—Enables you to add a new end-user and configure a client certificate for them.
- **Filter**—Enables you to sort the table information using custom filters.
- **Group**—Enables you to sort the table information using predefined groups.
- **Refresh**—Enables you to refresh the page.**Download CSV**—Enables you to export the currently displayed list to a spreadsheet in `.csv` format.
- **Manage Columns**—Helps to manage columns for the Client certificates.**Delete**—Enables you to delete the selected end-user.
- **Edit**—Enables you to modify the selected end-user's details.
- **Certificates**—Enables you to view and manage the selected end-user's certificates.

NOTE: Client certificates are downloaded in `.p12` format, and these files can optionally be protected with a password (also referred to as a

PIN). Although end-users can bypass setting a password when enrolling the certificate, setting a password is recommended as not all applications support non-password protected certificates.

- **View Audit**—Displays the certificate audit details.

NAME	COMMON NAME	ORGANIZATION	DEPARTMENT	EMAIL	ALTERNATIVE EMAILS	UPN	EPPN	CONTACT PHONE	CREATED	MODIFIED
<input type="checkbox"/> pdc2016 admin241	pdcc2016 admin241	Org1		win2016admin@ccmqa.com		Administrator@PDC2016.ccmqa.co			12/10/2020	12/10/2020
<input checked="" type="checkbox"/> pdc2411111 ywy2016	pdcc2411111 ywy2016	Org1		pdcc2016@ccmqa.com		Administrator@pdcc2016.ccmqa.co			07/17/2020	07/17/2020

3.3.1 How to view end-user Client Certificates

You can view all certificates that belong to a specific end-user as follows:

1. Navigate to **Persons**, and select an end-user in the list.
2. Click **Certificates** to open the **Certificates for** dialog shown in the following illustration.

The certificates for the selected end-user are listed in chronological order, with the newest certificate listed first. If a certificate has been revoked, the date of revocation is displayed in the **Revoked** column.

ID	STATUS	ORDER NUMBER	CERTIFICATE PROFILE	SUB TYPE	TERM
<input type="checkbox"/> 4791	ISSUED	4487810	client_intune_99994	Private	365
<input type="checkbox"/> 4719	ISSUED	4459914	Public S/MIME Organization Vali...	Public Organizatio...	365
<input type="checkbox"/> 4718	ISSUED	4459907	Public S/MIME Organization Vali...	Public Organizatio...	365
<input type="checkbox"/> 4715	ISSUED	4459180	Public S/MIME Organization Vali...	Public Organizatio...	365
<input type="checkbox"/> 4714	ISSUED	4458879	Public S/MIME Organization Vali...	Public Organizatio...	365
<input type="checkbox"/> 4713	ISSUED	4458817	Public S/MIME Organization Vali...	Public Organizatio...	365
<input type="checkbox"/> 4712	ISSUED	4458757	Public S/MIME Mailbox Validate...	Public Mailbox Vali...	365
<input type="checkbox"/> 4711	ISSUED	4458734	Public S/MIME Mailbox Validate...	Public Mailbox Vali...	365
<input type="checkbox"/> 4710	ISSUED	4458640	Public S/MIME Organization Vali...	Public Organizatio...	365
<input type="checkbox"/> 4709	ISSUED	4458509	Public S/MIME Mailbox Validate...	Public Mailbox Vali...	365

The following table lists fields and controls available in the **Certificates for** dialog.

Field	Description
General	
ID	ID number of the certificate

Field	Description
Status	The current status of the certificate, as follows: <ul style="list-style-type: none"> • Invited—The end-user has been sent an invitation email by you. • Requested—The request has been sent to the CA for approval. • Applied—The end-user has validated the email and applied for the certificate. • Issued—The certificate was issued by the CA and collected by SCM. Blue text indicates that the certificate was issued by the CA but has not been installed. • Revoked—The certificate is invalid because it was revoked. • Expired—The certificate is invalid because its validity period has expired. • Rejected—The CA rejected the request after the validation check.
Order	
Order Number	The order number of the certificate request made to CA
Certificate Profile	The certificate profile used during certificate issuance
Sub Type	The sub type of the certificate
Term	The number of days that the certificate is valid
Ownership	
Organization	The name of the organization that requested or has been issued with the certificate
Department	The department of the organization that is associated with the certificate
Requested Via	How the certificate was requested. For example, via Discovery, Web Form, Client Admin, ACME
Name	Common name
Email	Email address
Certificate	
Subject Alt Name	The domain names for which the certificate is used
Issuer	The details of the CA that issued the certificate, as well as the name of the certificate
Expires	The expiry date of the certificate
Serial Number	The serial number of the certificate.
Key Usage	The cryptographic purposes for which the certificate can be used. For example, key digital signing, encryption, and so on.
Extended Key Usage	Higher level capabilities of the certificate
Key Algorithm	The type of algorithm used for the encryption

Field	Description
Key Size/Curve	The key size or curve used for the encryption
Signature Algorithm	The signature algorithm of the certificate public key
MD5 Hash	The MD5 hash (thumb print or fingerprint) for the certificate
SHA1 Hash	The SHA1 hash (thumb print or fingerprint) for the certificate
Timespan	
Requested	The date of the request made by SCM to the CA
Issued	The date the certificate was issued
Downloaded	The date the certificate was downloaded
Revoked	The date the certificate was revoked
Enroll type	The method used to enroll the certificate
Replaced	The date the certificate was replaced
Deleted	The date the certificate was deleted
Management	
Key Vault	The type of the certificate key.

Depending on your security role and the status of the selected certificate, you can perform the following actions on end-user client certificates:

- **View**— Enables you to view end-user client certificate details. See [“How to view end-user Client Certificates” on page 84](#).
- **Revoke**— Enables you to revoke an end-user's certificate. Once revoked, the date and time of revocation is displayed in the **Revoke** column. See [“How to revoke Client Certificates” on page 109](#).
- **Export to Intune**— Enables you to export client certificates and private keys from SCM to Intune for use with mobile device management. Only available if Intune is configured. See [“Configuring Azure for Intune Exporter” on page 218](#).
- **View Audit**— Enables you to view audit details for the certificate.
- **Download**— Enables you to download the client certificate from key escrow. If you download a certificate via this method, this certificate will be revoked. See [“How to recover an end-user's private key from Escrow” on page 241](#). This option is only available if key escrow has been configured for the organization or department. See [“Configuring Key Escrow and encryption” on page 236](#).
- **Filter**— Enables you to sort the table information using custom filters.
- **Group**— Enables you to sort the table information using predefined groups.
- **Refresh**— Enables you to refresh the page.

- **Download CSV**—Enables you to export the currently displayed list to a spreadsheet in `.csv` format.
- **Manage Columns**—Helps to manage columns for the Client certificates.

3.3.2 How to view or modify Client certificate details

To view or modify a Client certificate's details, do the following:

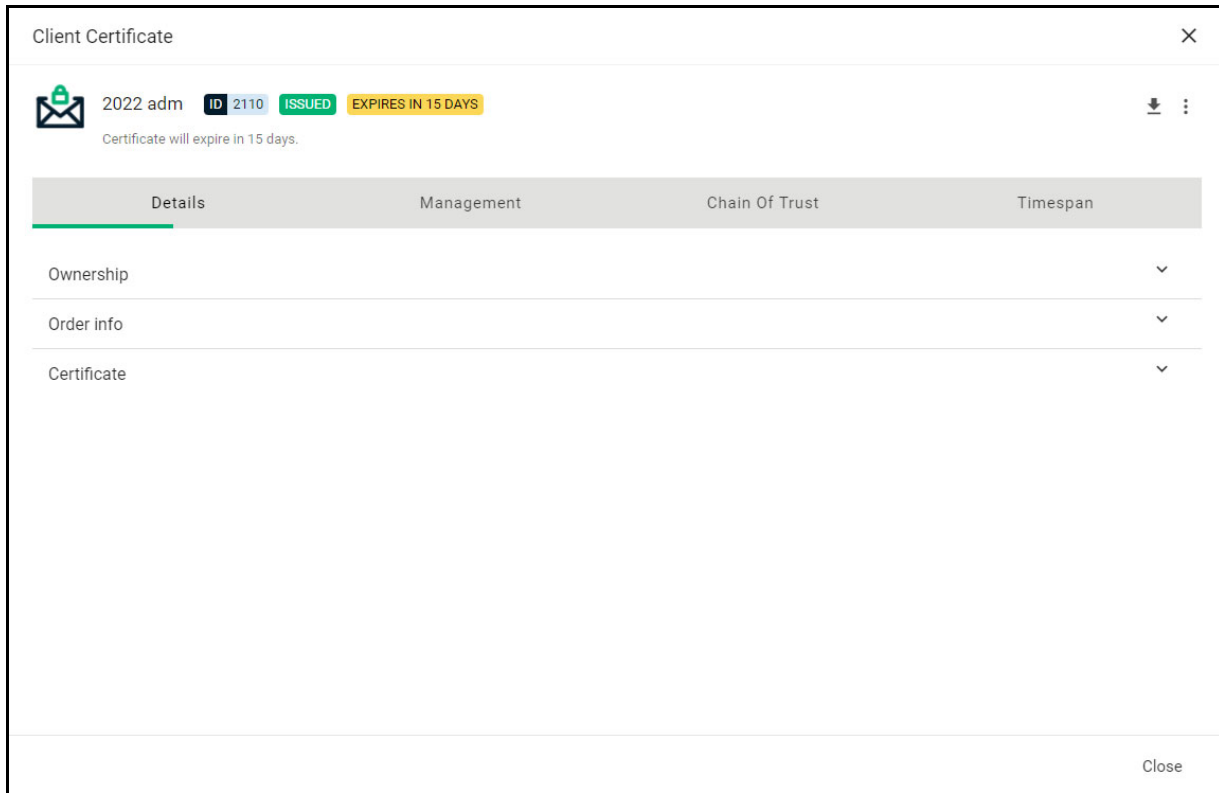
1. Navigate to **Certificates > Client Certificates**.
2. Select a certificate in the list.
3. Click **View**.

This opens the **Client Certificate** dialog that enables you to do the following:

- View status and summary information
- Download the certificate in different formats
- View ownership and order information if certificate was requested using SCM
- Configure notifications
- View and manage private key if applicable
- View the full certificate chain

Alternatively, you can view a certificate by navigating to **Persons**, and selecting a certificate for a specific end-user.

The **Client Certificate** Summary panel displays the number of days remaining before the certificate expires, along with SCM and server-related information about the certificate and other controls.



The following table lists fields available in the **Client Certificate** summary.

Field	Description
Status	<p>The current status of the certificate, as follows:</p> <ul style="list-style-type: none"> • Invited – The end-user has been sent an invitation email by you. • Requested – The request has been sent to the CA for approval. • Applied – The end-user has validated the invitation email. • Issued – The certificate was issued by the CA and collected by SCM. Blue text indicates that the certificate was issued by the CA but has not been installed. • Revoked – The certificate is invalid because it was revoked. • Expired – The certificate is invalid because its validity period has expired. • Rejected – The CA rejected the request after the validation check.
Ordered	The date of the request made by SCM to the CA
Certificate Profile	The certificate profile used during certificate issuance
Term	The validity period of the certificate
Subject	The name and email address of the end-user
Principal Name	The principal name included in the certificate

Field	Description
Address 1 Address 2 Address 3 City State or Province Postal Code	The address details of the organization
Collected	The date of the collection of certificate by SCM from CA
Revoked	The date of the revocation of the certificate
Expires	The expiry date of the certificate
Order Number	The order number of the certificate request made to CA
Serial Number	The serial number of the certificate
Key Escrow	Indicates whether or not the key escrow is available for the certificate recovery
Key Usage	The cryptographic purposes for which the certificate can be used. For example, key digital signing, encryption, and so on.
Extended Key Usage	Higher level capabilities of the certificate
Suspend Notifications	Disables all notifications for events such as certificate download, expiry, and revocation from SCM to the administrator and the end-user, for this certificate.
Locations	<p>Locations describes where the certificate exists outside of SCM.</p> <ul style="list-style-type: none"> • Custom <ul style="list-style-type: none"> - Available for all certificate types - Created manually by the user - Fields: Name and Details - Multiple allowed, can be edited or deleted • Sectigo Key Vault <ul style="list-style-type: none"> - Client certificates only - Created by SCM if storing private key - Also contains Private Key indicator • Legacy Key Vault <ul style="list-style-type: none"> - Client certificates only - Created by SCM if storing private key - Fields: Escrow Level (CUSTOMER/RAO/DRAO) - Also contains Private Key indicator • Active Directory Entry <ul style="list-style-type: none"> - Available for all certificate types - Created by AD discovery scans - Fields: Object Type (User/Computer/Container), Name, DN, UPN

3.3.3 How to manage end-users

Before an applicant can be issued a client certificate, they must be added to SCM as a Person assigned to an organization and optionally to a department.

You can add end-users to organizations in SCM in one of the following ways:

- Manually (see “Adding end-users manually” on page 90).
- By loading multiple end-users from a .csv file (see “Complete the fields based on the information provided in the following table, then click Save.” on page 91).
- Automatically when end-users enroll via the certificate self-enrollment form (see “Enabling the end-user self-enrollment by access code” on page 98).

A new end-user is also created and added to SCM when an SSL certificate application is made through the SSL self-enrollment form. If the applicant does not already exist as an end-user when the form is submitted, then a new end-user is created with the name `requesterSSL` <domain_name> where domain name is the domain for which the application was made. This end-user is automatically assigned membership of the organization for which the SSL certificate was ordered. This end-user, however, does not own a client certificate.

End-users can also be modified and deleted, either of which causes their certificate to be revoked.

3.3.3.1 Adding end-users manually

You add end-users as follows:

1. Navigate to **Persons**.
2. In the upper-right corner, click the **Add** icon to open the **Add New Person** dialog shown in the following illustration.

The screenshot shows a dialog box titled "Add New Person" with a close button (X) in the top right corner. The dialog is divided into two main sections: "Ownership" and "Personal Information".

Ownership Section:

- Organization:** A dropdown menu with "inwodep" selected.
- Department:** A dropdown menu with "None" selected.
- Domain:** A dropdown menu with "*.ccmqa.com" selected.

Personal Information Section:

- First Name ***: A text input field with a red asterisk indicating it is required.
- Middle Name**: A text input field.

At the bottom of the dialog, there are two buttons: "Cancel" and "Next".

3. Complete the fields based on the information provided in the following table, then click **Save**.

Field	Description
Ownership	
Organization	The organization to which the new end-user belongs.
Department	The department to which the new end-user belongs.
Domain	The domain with which the end-user is associated. Only domains delegated to the selected organization and department are available.
Personal Information	
Email Address	The end-user's email address. The email is restricted to the selected domain.
Common Name	The common name to be included in the certificate. For client certificates, you typically specify the end-user's full name.
First Name	The end-user first name. The combined length of First Name and Last Name cannot exceed 64 characters.
Middle Name	The end-user middle name.
Last Name	The end-user last name. The combined length of First Name and Last Name cannot exceed 64 characters.
Phone Number	The contact phone number for the end-user.
Alternative emails	The alternative email addresses for the end-user. Enter email addresses separated by commas.
Secret ID	An identifier for the details of an existing end-user in SCM. Assigning SIDs to end-users simplifies the client certificate enrollment process for those end-users and reduces errors. This is because, as the details of the end-user are already stored, the end-user needs only specify the email address. To enable enrollment by SID, you must fill out this field.

Field	Description
Validation Type ^a	<p>The type of client certificate that is issued to an applicant. The valid values are Standard and High, and is based on the degree of end-user authentication that is carried out prior to issuance.</p> <p>Standard certificates can be issued quickly and take advantage of the end-user authentication mechanisms that are built into SCM. A end-user applying for a Standard certificate is authenticated using the following criteria:</p> <ul style="list-style-type: none"> • The end-user must apply for a certificate from an email address at a domain that has been delegated to the issuing organization. • The organization has been validated as the owner of that domain. • The end-user must know either a unique access code or secret ID that is entered on the certificate enrollment form. You communicate these values to the end-user via out-of-band communication. The end-user must be able to receive an automated confirmation email sent to the email address of the certificate that they are applying for. The email contains a validation code that the end-user needs to enter at the certificate collection web page. <p>High personal validation certificates require that the end-user undergo the preceding validation steps and face-to-face meeting with the issuing organization. The additional validation steps must be completed prior to you selecting a High personal validation type.</p>
Principal Name ^b	<p>The email address that should appear as principal name in the certificate to be issued.</p> <p>Client certificates issued to the end-users of the organizations or departments with the Allow Principal Name option selected (it is off by default) include the Principal Name, in addition to the RFC822 name, in the SAN field.</p> <p>If included, the principal name becomes the primary email address of the end-user to whom the certificate is issued. This can be customized at a later time by editing the end-user if the Allow Principal Name Customization option is selected for the organization or department.</p> <p>These options are set when adding or editing organizations or departments. For more information, see "Using Certificate Settings for Client Certificates" on page 165.</p> <p>If principal name support is enabled for an organization but not for a department, this field is auto-populated with the email address entered in the Email Address field.</p>
EPPN ^c	<p>The eduPersonPrincipalName. This is a scoped NetID of the person for the purposes of inter-institutional authentication. Should be stored in the form of user@univ.edu, where univ.edu is the name of the local security domain.</p>

a. Appears only if enabled for your account. Contact your Sectigo account manager.

b. Appears only if Allow Principal Name is enabled for the organization or department.

c. Appears only if EPPN is enabled for your account. Contact your Sectigo account manager.

3.3.3.2 End-user CSV file format and importing guidelines

The following table lists fields, with their possible values and formats, that can be imported from the CSV file for each end-user.

The fields in the CSV file differ depending on whether or not principal name support is enabled for the organization. For organizations for which the principal name support is not enabled (the default), the **Principal Name** field is not included. Principal name support is configured when adding or editing organizations or departments.

Department is mandatory only if multiple end-users are being imported by a DRAO Client Certificate; MRAO, RAO Client Certificate, as well as DRAO Client Certificate administrators that are also MRAO or RAO Client Certificate administrators, can leave this field blank.

Optional fields without values must be included but left blank. If **Common Name** is left blank, it is automatically filled using **First Name** and **Last Name**.

The **Secret ID** field can be used to add a layer of authentication to the process. If specified, the end-user has to enter the identifier in the certificate enrollment form. For more information, see [“Enabling the end-user enrollment by invitation” on page 106](#).

With the exception of the **Secret ID** and **Phone** fields, ensure that the fields are imported using characters as per the following table, including commas and quotation marks.

Field	Required	Minimum Characters	Maximum Characters	Format	Supported Characters
First Name	Yes	1	128		A-Z a-z 0-9 . - space
Middle Name	No	0	128		A-Z a-z 0-9 . - space
Last Name	Yes	1	128		A-Z a-z 0-9 . - space
Email (Primary)	Yes	3	128	Valid email address	A-Z a-z 0-9 . - _ @

Field	Required	Minimum Characters	Maximum Characters	Format	Supported Characters
Email (Alternative)	Yes	3	128	Valid email addresses separated by a space	A-Z a-z 0-9 . - _ @ space
Validation Type	No				high standard
Organization	Yes	1	128		Any
Department	No	0	128		Any
Secret ID	No	0	128		Any

The following example pertains to organizations for which principal name support is enabled:

```
First1,Middle1,Last1,User1-al@abc.com,User1-sec-al@abc.com,
standard,sysorg,sysdep,Secret1,380487000001,UA,User1-al@abc.com,User@System,
"First1 Last1"
```

NOTE: If an organization has principal name support enabled and a department belonging to that organization does not, when loading end-users of the department, the Principal Name field must be included but should be left blank.

The following example pertains to organizations for which principal name support is not enabled:

```
First1,Middle1,Last1,User1-al@abc.com,User1-sec-al@abc.com,
standard,sysorg,sysdep,Secret1,380487000001,UA,User@System,
"First1 Last1"
```

The following would result in failure to import end-users:

- Lines do not have the correct number of fields.
- Any mandatory field is not completed.
- The organization does not exist.
- The department, if present, does not exist.
- The department, if present, does not exist for the specified organization.
- The value provided in the Primary Email Address field is not in a valid format or the email domain cannot be determined.
- The domain of the primary email address is not delegated to the organization or is not active.

- The domain of the primary email address is not delegated to the department (if department is supplied).
- The value provided in the Secondary Email Address field (if supplied) is not in a valid format or the email domain cannot be determined.
- The domain of the secondary email address is not delegated to the organization or is not active.
- The domain of the secondary email address is not delegated to the department (if department is supplied).
- The administrator attempting the import does not have the correct permissions for the organization or department:
 - MRAO administrators have permission to import for any valid organization or department. MRAOs may leave the Department field blank.
 - RAO Client Certificate administrators have permission to import for organizations and any subordinate departments that have been delegated to them. RAO Client Certificate administrators may leave the Department field blank.
 - DRAO Client Certificate administrators have permission to import for departments that have been delegated to them. DRAO Client Certificate administrators cannot leave the Department field blank unless they are also a RAO Client Certificate for the same organization.

3.3.3.3 Loading multiple end-users from a CSV file

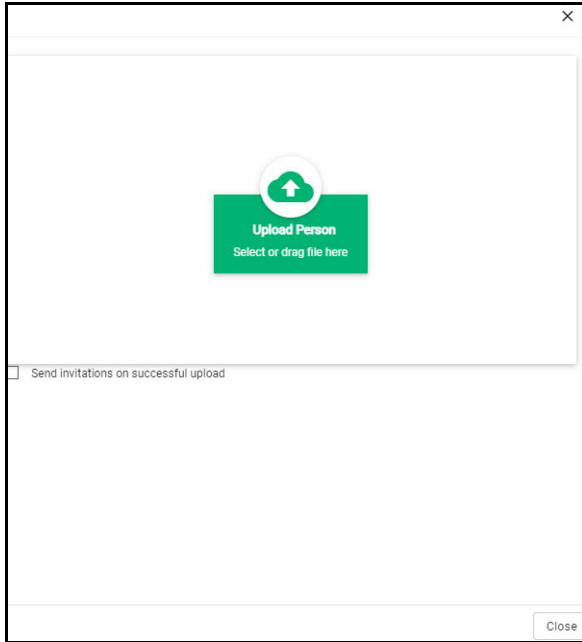
MRAO, RAO Client Certificate, and DRAO Client Certificate administrators can import a list of end-users into SCM in comma separated values (`.csv`) format. After importing the list, your employees then only need to perform self-enrollment using their secret ID.

To load multiple end-users, do the following:

1. Use a software application such as Microsoft Excel or LibreOffice Calc to generate a `.csv` file containing a list of end-users.

For information on how to structure `.csv` files for importing multiple end-users, see [Appendix A: CSV import format requirements](#).

2. In SCM, navigate to **Persons** and in the upper-right corner, click **Import from CSV** to display the **Import persons from CSV** dialog.



3. Browse to your `.csv` file and click **Submit** to start the import.

NOTE: Only end-users included in lines without errors are imported.

4. When the import completes, click **Close**.

The end users are now listed in the **Client Certificates** table.

Email invitations are automatically sent to users for whom a secret ID was provided (see [“Enabling the end-user self-enrollment by secret identifier” on page 103](#)).

To issue certificates for end-users without a secret ID, send invitations manually (see [“Enabling the end-user enrollment by invitation” on page 106](#)).

3.3.3.4 Modifying and deleting end-users

You can modify the end-user details at any time by navigating to **Persons**, and then clicking **Edit** to open the **Edit Person Details** dialog.

If any information in this dialog is changed, with the exception of the secret ID, any previously issued client certificates for this email address are automatically revoked.

Except as described below, the fields are the same as those for the **Add New Person** dialog. For more information, see [“Adding end-users manually” on page 90](#).

The **Secret ID** field is not displayed for security reasons. To modify the secret ID, click **Reset Secret ID** to display the **Secret ID** field, where you to specify a new secret ID, as shown in the following illustration. To retain the existing secret ID, click **Don't Reset Secret ID**.

If enabled for the organization, you can customize the principal name for the end-user. Enter the new principal name as it should appear in the **Subject Alternative Name (SAN)** field of the certificate in the **Principal Name** field. You can revert the principal name changes to the email address of the end-user by clicking **Copy E-Mail**.

Renaming an end-user does not affect the search and filtering actions in the **Client Certificates** page. SCM enables you to search for a particular end-user or client certificates using both the old name and the new name (if a name has been changed).

You can delete any end-user by selecting their name, clicking **Delete**, and then clicking **OK** on the **Person deletion** dialog to confirm. Once the end-user is deleted, their certificate is revoked.

3.3.4 How to request and issue Client Certificates to end-users

End-users can be enrolled for client certificates (that is, email certificates, end-user authentication certificates, and dual-use certificates) in one of the following ways:

- **Self-enrollment by access code**—End-users apply for their own client certificate by accessing the self-enrollment form. You inform the end-user of the URL at which the self-enrollment form is hosted and the access code of the enrollment endpoint account. See [“Enabling the end-user self-enrollment by access code” on page 98](#) for more information.
- **Self-enrollment by secret identifier**—End-users previously added to SCM apply for their own client certificate by accessing the self-enrollment form. You inform the end-user of the URL at which the self-enrollment form is hosted and the secret ID you assigned them. See [“Enabling the end-user self-enrollment by secret identifier” on page 103](#) for more information.
- **Enrollment by administrator’s invitation**—Involves sending invitation notifications to end-users previously added to SCM. The invitation contains a validation link and instructions for the end-users to download and install their certificates. See [“Enabling the end-user enrollment by invitation” on page 106](#) for more information.

3.3.4.1 Enabling the end-user self-enrollment by access code

You can direct the end-user to self-enroll using the access code specified for the enrollment endpoint, and the end-user can apply for, collect, download, and install their certificate.

The following requirements must be met for end-user self-enrollment by access code to succeed:

- You configured an account for the Client Certificate Web Form enrollment endpoint, the organization or department specified for the account is one to which the end-user belongs, and the **Access Code** is specified (see [“Managing bulk SSL requests” on page 163](#)).
- The domain from which the client certificate is to be issued must have been enabled for client certificates, prevalidated by Sectigo, and activated by your Sectigo account manager (for example, if you want to issue client certificates to end-user@mycompany.com, then mycompany.com must have been prevalidated by Sectigo).
If you request a certificate for a brand new domain, then this domain will first have to undergo validation by Sectigo. Once validated, the new domain is added to your list of prevalidated domains and future certificates are issued immediately.
- The domain from which the client certificates are to be issued has been delegated to the organization or department of the enrollment endpoint account (see [Delete an organization or department](#)).
- A RAO Client Certificate or DRAO Client Certificate administrator has been delegated control of this organization or department.

Upon fulfillment of the preceding requirements, the following needs to occur:

1. You direct the personal certificate applicant to the access code-based client self-enrollment form, ensuring that the application is done from the end-user's computer.
2. The applicant completes and then submits the self-enrollment form, specifying the correct access code for the Client Certificate Web Form enrollment endpoint account and providing an email from a domain that has been delegated to the account’s organization or department.
3. SCM sends a validation notification to the applicant containing a link to the **Account Validation** form and a request code.

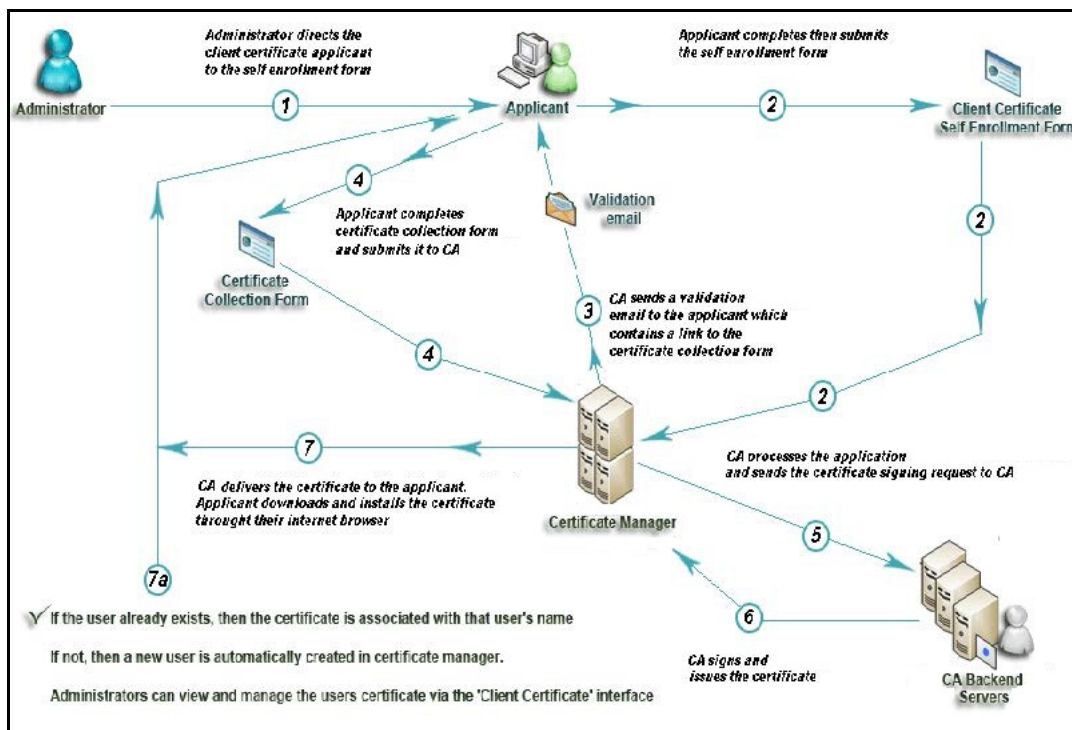
- The applicant completes the **Account Validation** form and the certificate request is sent to Sectigo servers. If the application is successful, the applicant can download and install their personal certificate (see *"Certificate collection and installation"* on page 71).

If the applicant already exists as an end-user (viewable by navigating to **Certificates > Client Certificates**), then the certificate is added to their account.

If the applicant does not exist as an end-user, then SCM automatically adds this applicant as a new end-user when the certificate is issued.

If the applicant already exists as an administrator (visible via the **Admins** page), but not as an end-user of the client certificate, then SCM automatically adds this applicant as a new end-user.


The following diagram illustrates the process of using the self-enrollment form.



Provide enrollment details to applicants using an out-of-band communication such as email. The communication must contain the following information:

- A link to the access code-based **Client Certificate Enroll** form, located at the address specified for the Client Certificate Web Form enrollment endpoint. By default the address is similar to the following
https://cert-manager.com/customer/<customer_uri>/smime
- The access code specified for the Client Certificate Web Form enrollment endpoint account.

Accessing the link displays the form shown in the following illustration.




Client Certificate Management

Select the Client Certificate Management method.

- Certificate enrollment by AccessCode
- Certificate renewal by AccessCode
- Certificate enrollment by SecretID
- Certificate renewal by SecretID
- Certificate revocation

Clicking **Certificate Enrollment by Access Code** displays the **Client Certificate Enrollment** form as shown in the following illustration.



Client Certificate Enrollment

Fill in the fields below to enroll a Client certificate.

ⓘ This passphrase will be necessary to revoke or renew this certificate

[I have read and agree to the terms of the Sectigo Client Certificate EULA](#)

Cancel
Enroll

The following table describes the form fields and elements. Mandatory fields are marked with an asterisk on the form.

Field	Description
Access Code	The access code for the Client Certificate Web Form enrollment endpoint account that you conveyed to the applicant.
First Name	The applicant's first name.
Middle Name	The applicant's middle name.
Last Name	The applicant's last name.
Email Address	The applicant's email address. The email address must be for a domain that has been delegated to the organization or department of the enrollment endpoint account.
Certificate Profile ^a	The certificate profile to be used for the certificate issuance. The profile description (if provided) is also displayed.
Certificate Term ^b	The validity period of the certificate.
Key Type ^b	The key algorithm and size/curve to be used in the certificate. RSA or EC is supported, depending on the selected certificate profile.
Passphrase	A phrase to be used to renew or revoke the certificate when using the external renewal or revocation page. The passphrase should be entered in the first field and reentered in the second field for confirmation.
EULA acceptance	Acceptance of the terms and conditions before submitting the form.
Enroll	Submits the application and enrolls the applicant for the client certificate.

- a. Displays only if the access code and email address are successfully validated, and if more than one certificate profile has been assigned to the enrollment endpoint account.
- b. Displays only if the access code and email address are successfully validated.

NOTE: In addition to the standard fields, MRAOs can add custom fields. See ["How to define custom fields"](#) on page 235.

After completing the form and clicking **Enroll**, a **Confirmation** message is displayed as shown in the following illustration.

You have requested a Client Certificate with the follow details:

Email: **autotest@ccmqa.com**,
Name: **option option**.

We have sent you an email containing an enrollment link in order to complete the rest of the enrollment process.

[Back](#)

SCM sends the applicant an email similar to that shown in the following illustration. This email contains a URL to validate the application, a request validation code, and instructions to download the certificate.

Subject: Validation Email - You have requested email certificate validation.


Dear enrollment,

You now need to complete the following steps:

- * Click the following link to validate your email <https://cert-manager.com/customer/110/smime?action=validate&requestCode=pLq2GouBUI8KqT8OYl8qEnE14&email=autotest%40ccmqa%2ecom> (if the link doesn't work please copy request code pLq2GouBUI8KqT8OYl8qEnE14 and paste it into proper field in the validation form).
- Your request code: pLq2GouBUI8KqT8OYl8qEnE14
- * Type in a PIN to protect your email certificate
- * Click 'Download' to collect your certificate. You should save this file to a safe place on your hard drive.
- * Import your new certificate into your email client and/or internet browser. (Please contact your administrator for help with this/Please click the following link for instructions)


NOTE: You can modify the contents of these emails by navigating to **Settings > Notification Template**.

Upon clicking the link, the end-user is redirected to the **Account Validation** form shown in the following illustration. The **Code** and **Email** fields of the form are populated automatically.

 **Account Validation**

Code+
pLq2GouBUI8KqT8OYl8qEnE14

Email
autotest@ccmqa.com

 If specified, this Password will be used to protect the PKCS#12 file with your certificate and private key. You will need to specify it during installation.

Password

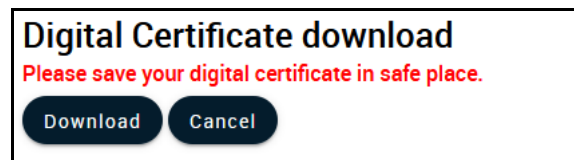
Re-type Password

Validate **Cancel**

The following table describes the fields in the form. Mandatory fields are marked with an asterisk.

Field	Description
Code	The validation request code. This field is auto-populated when the applicant clicks the validation link in the email.
Email	The email address of the applicant. This field is auto-populated.
Password	A password (PIN) to protect the certificate. This is needed for accessing the certificate (for example, while exporting the certificate for backup and while importing the certificate to restore the certificate from the backup). The password should be at least eight characters long.
Re-type Password	Confirmation of the password.

After completing the validation process, a certificate collection form appears, as shown in the following illustration.



This form enables the end-user to download and save the certificate on their computer.

SCM delivers the certificate to the end-user in PKCS#12 file format (.p12 file). The password (PIN) specified in the **Password** field of the **Account Validation** form is used to protect access to this .p12 file. The end-user is asked for this password when they import the certificate into the certificate store of their computer.

If an end-user does not exist in SCM, then they are automatically created and added as a new end-user belonging to the organization to which the certificate was issued. This new end-user is viewable in the **Certificates > Client Certificates** page with the following parameters:

- **Name**—The name that the end-user specified in the **Client Certificate Enrollment** form.
- **Email**—The email address that the certificate was issued to, as specified in the **Client Certificate Enrollment** form.
- **Organization**—The name of the organization to which this end-user belongs, matching the domain of the end-user's email address.

If the end-user already exists, then the certificate is associated with their end-user name.

3.3.4.2 Enabling the end-user self-enrollment by secret identifier

You can direct the end-user to self-enroll using the secret ID specified for them, and the end-user can apply for, collect, download, and install their certificate.

The following requirements must be met for end-user self-enrollment by secret ID to succeed:

- The domain from which the client certificate is to be issued must have been enabled for client certificates, prevalidated by Sectigo, and activated by your Sectigo account manager (for example, if you want to issue client certificates to end-user@mycompany.com, then mycompany.com must have been prevalidated by Sectigo).

If you request a certificate for a brand new domain, then this domain first has to undergo validation by Sectigo. Once validated, the new domain is added to your list of prevalidated domains and future certificates are issued immediately.

- The domain from which the client certificates are to be issued has been delegated to an organization or department (see [Delete an organization or department](#)).
- A RAO Client Certificate or DRAO Client Certificate administrator has been delegated control of this organization or department.
- You added the end-user and specified a secret ID for the end-user through either the **Add New Person** or **Edit Person** dialog (see [“Adding end-users manually” on page 90](#)). The secret ID should be a combination of alpha and numeric characters.


Upon fulfillment of the preceding requirements, the following needs to occur:

1. You direct the client certificate applicant to the access secret ID-based self-enrollment form, ensuring that the application is done from the end-user's computer.
2. The applicant completes and then submits the self-enrollment form, specifying the secret ID assigned to them and providing an email from a domain that has been delegated to that organization or department.
3. The certificate request is sent to Sectigo servers. If the application is successful, the applicant can download and install their personal certificate.

To communicate the enrollment details to end-users to whom you want to issue client certificates, use an out-of-band communication method such as email. The communication must contain the following information:

- A link to the secret ID-based self-enrollment form available at
`https://cert-manager.com/customer/<customer_uri>/smime?action=enroll&swt=sid.`
- The secret ID specified for the end-user.

When the end-user accesses the link, the **Digital Certificate Download** form is displayed as shown in the following illustration.



Digital Certificate Download

Fill in the fields below to enroll a Client certificate

Email Address*

Secret identifier*

Password:

Confirm Password:

i The Annual Renewal Passphrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. *Do not lose it.* You will need it when you want to revoke or renew your Digital ID.

Annual Renewal Passphrase*

Confirm Annual Renewal Passphrase*

[I have read and agree to the terms of the Sectigo Client Certificate EULA](#)

Enroll

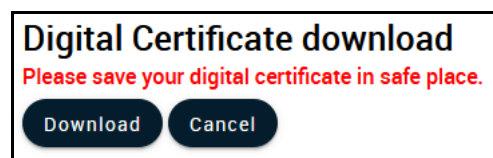
The following table describes the form fields and elements. Mandatory fields are marked with an asterisk.

Field	Description
Email Address	The applicant's email address. The address must match the email address entered in the person profile.
Secret identifier	The secret ID you assigned and communicated to the applicant.
Certificate Profile ^a	The certificate profile to be used for the certificate issuance. The profile description (if provided) is also displayed.
Certificate Term ^a	The validity period of the certificate.
Key Type ^a	The key algorithm and size/curve to be used in the certificate. RSA or EC is supported, depending on the selected certificate profile.

Field	Description
Password	The password (PIN) for the certificate. The password should be entered in the first field and reentered in the second field for confirmation. This is needed for accessing the certificate (for example, while exporting the certificate for backup and while importing the certificate to restore the certificate from the backup). The password should be at least eight characters long.
Annual Renewal Passphrase	A phrase to be used to renew or revoke the certificate when using the external renewal or revocation page. The passphrase should be entered in the first field and reentered in the second field for confirmation.
EULA Acceptance	The applicant must accept the terms and conditions before submitting the form.
Enroll	Submits the application and enrolls the applicant for the client certificate.

- a. Displays only if the email address and secret identifier are successfully validated.

After completing the form and clicking **Enroll**, a certificate collection form appears, as shown in the following illustration.



This form enables the end-user to download and save the certificate on their computer.

SCM delivers the certificate to the end-user in a PKCS#12 file format (.p12 file). The password (PIN) specified in the **Password** field of the **Digital Certificate Download** form is used to protect access to this .p12 file. The end-user is asked for this password when they import the certificate into the certificate store of their computer.

3.3.4.3 Enabling the end-user enrollment by invitation

You can send invitations to end-users who have already been added to SCM. For this process to succeed, the following requirements must be met:

- The domain from which the client certificate is to be issued must have been enabled for client certificates, prevalidated by Sectigo, and activated by your Sectigo account manager (for example, if you want to issue client certificates to end-user@mycompany.com, then mycompany.com must have been prevalidated by Sectigo).
If you request a certificate for a brand new domain, then this domain first has to undergo validation by Sectigo. Once validated, the new domain is added to your list of prevalidated domains and future certificates are issued immediately.
- The domain from which the client certificates are to be issued has been delegated to an organization or department (see [Delete an organization or department](#)).
- A RAO Client Certificate or DRAO Client Certificate administrator has been delegated control of this organization or department.
- You added the end-user via the **Certificates > Client Certificates** page.

To send an enrollment invitation containing a link to the registration form to the end-user, do the following:

1. Navigate to **Persons**.
2. Select the end-user and click **Edit**.
3. In the **Edit Person Details** dialog, select **Enrollment Invitation**.
4. Click the **Add** icon to open the **Send Invitation to** dialog. This displays the details of the end-user and enables you to specify the enrollment endpoint and account for the client certificate profile.

5. Select the enrollment endpoint to be used to enroll the certificate.
6. Select the account.
7. Click **Send**.

An invitation email is sent to the end-user, providing a link to the **User Registration** form and a request code that the end-user needs in order to validate that they are the correct applicant.

Subject: Invitation | Email - You have requested email certificate validation.

Dear enrollment,

You now need to complete the following steps:

- * Click the following link to validate your email <https://cert-manager.com/customer/110/smime?action=validate&requestCode=pLq2GouBUI8KqT8OYl8qEnE14&email=autotest%40ccmq%2ecom> (if the link doesn't work please copy request code pLq2GouBUI8KqT8OYl8qEnE14 and paste it into proper field in the validation form).
Your request code: pLq2GouBUI8KqT8OYl8qEnE14
- * Type in a PIN to protect your email certificate
- * Click 'Download' to collect your certificate. You should save this file to a safe place on your hard drive.
- * Import your new certificate into your email client and/or internet browser. (Please contact your administrator for help with this/Please click the following link for instructions)

NOTE: You can modify the contents of these emails by navigating to the **Settings > Notification Template** page.

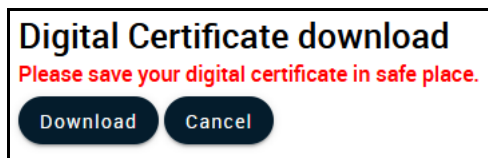
Clicking the link in the email opens the **User Registration** form and populates the request **Code** and **Email** fields.

The following table describes the form fields and elements. Mandatory fields are marked with an asterisk on the form.

Field / Element	Description
Code	The validation request code. Auto-populated when the applicant clicks the validation link contained in the email.
Email	Email address of the applicant. This field is auto-populated.

Field / Element	Description
Password	A password (PIN) to protect the certificate. The password should be entered in the first field and reentered in the second field for confirmation. This is needed for accessing the certificate (for example, while exporting the certificate for backup and while importing the certificate to restore the certificate from the backup). The password should be at least eight characters long.
Passphrase	A phrase to be used to renew or revoke the certificate when using the external renewal or revocation page. The passphrase should be entered in the first field and reentered in the second field for confirmation.
EULA Acceptance	Acceptance of the terms and conditions before submitting the form.
Submit	Submits the application.

After completing the validation process, a certificate collection form appears, as shown in the following illustration.



This form enables the end-user to download and save the certificate on their computer.

SCM delivers the certificate to the end-user in PKCS#12 file format (.p12 file). The password (PIN) specified in the **Password** field of the **User Registration** form is used to protect access to this .p12 file. The end-user is asked for this password when they import the certificate into the certificate store of their computer.

3.3.5 How to download private keys from Sectigo Key Vault and Key Escrow

If Sectigo Key Vault is enabled for your account, MRAO administrators with the **Allow download keys from Key Vault** privilege enabled can download client certificate private keys stored in the vault. See [“How to download an end-user's Private Key from Sectigo Key Vault” on page 242.](#)

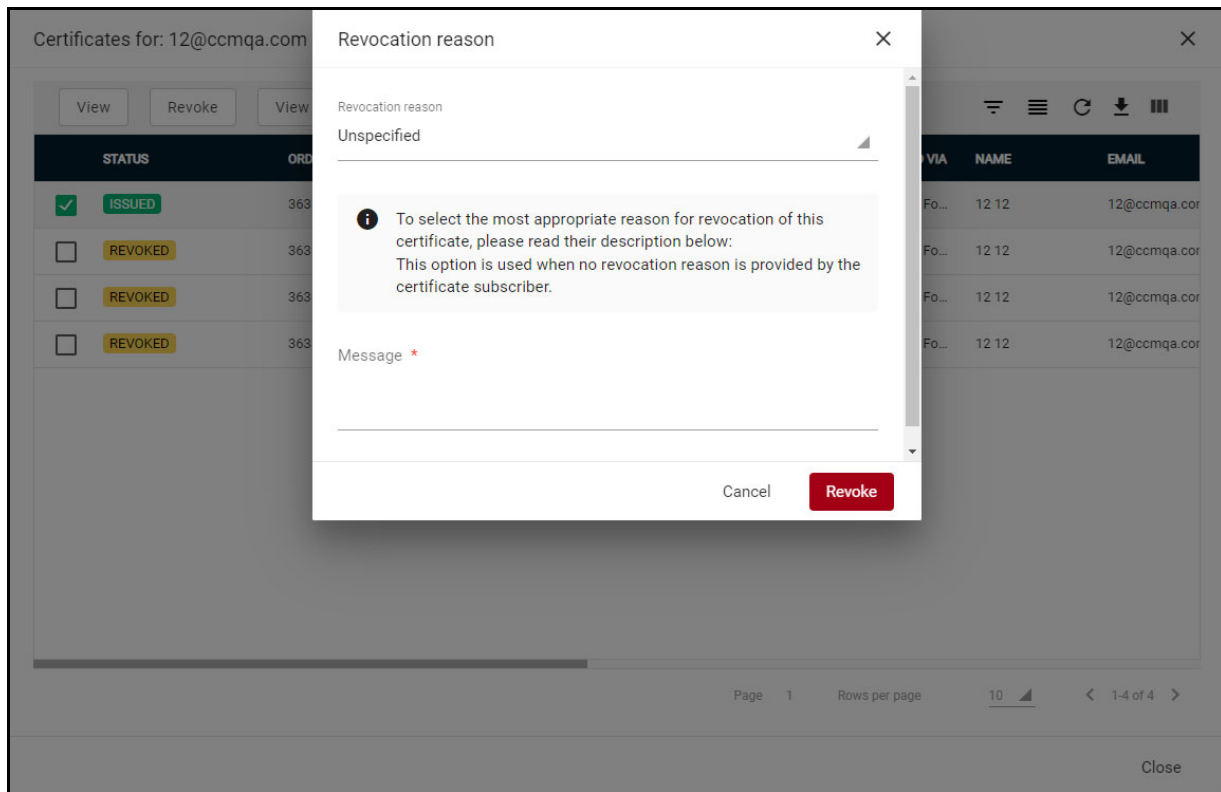
If Key Escrow is enabled for your account, encryption has been configured, and key recovery is enabled for the organization, you can download client certificate private keys from key escrow. Downloading a client certificate from escrow revokes the certificate. See [“How to recover an end-user's private key from Escrow” on page 241.](#)

3.3.6 How to revoke Client Certificates

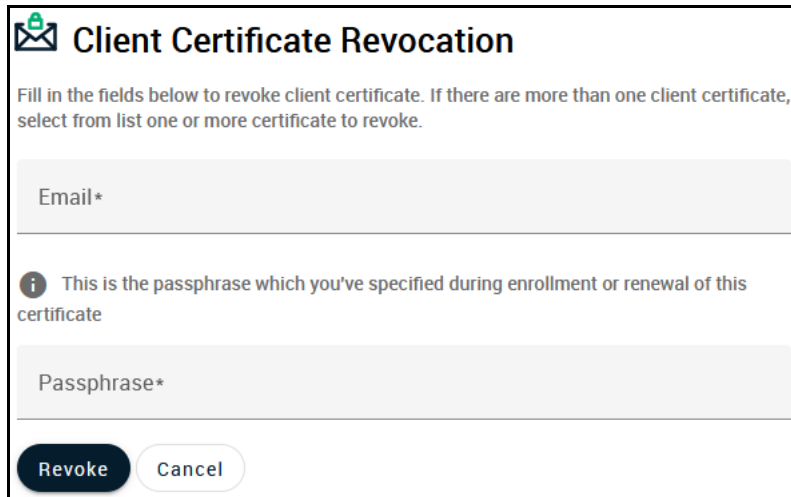
The client certificates that belong to any end-user can be revoked by either you or the end-user themselves.

To revoke a client certificate, do the following:

1. Navigate to **Persons**.
2. Select the end-user and click **Certificates** to open the **Certificates for** dialog.
3. Select the client certificate and click **Revoke**.
4. Select the revocation reason from the list and add a message.
5. Click **Revoke** to confirm.



The end-user can revoke their client certificate using the **Client Certificate Revocation** form shown in the following illustration.



Client Certificate Revocation

Fill in the fields below to revoke client certificate. If there are more than one client certificate, select from list one or more certificate to revoke.

Email*

i This is the passphrase which you've specified during enrollment or renewal of this certificate

Passphrase*

Revoke Cancel

To revoke a client certificate using this form, do the following:

1. Send the end-user a link to the form, available at
https://cert-manager.com/customer/<customer_uri>/smime?action=revoke
2. The end-user accesses the form and enters the email address and the passphrase that they set during self-enrollment or registration, and submits the form.

3.4 Managing Code Signing Certificates

Depending on your security role, the **Code Signing Certificates** page shown in the following illustration provides MRAOs, nominated RAO Code Signing, and nominated DRAO Code Signing administrators with the information and controls necessary to issue and manage the lifecycle of the code signing certificates for their organization or department.

MRAOs can request and manage code signing certificates for any organization or department.

RAO Code Signing administrators can request and manage certificates for their delegated organizations and departments.

DRAO Code Signing administrators can request code signing certificates for departments that have been delegated to them.

ID	STATUS	MANAGED	ORDER NUMBER	CERTIFICATE ...	TERM	REQUESTED VIA	SUBJECT	SUBJECT ALT NAME	ISSUER	EXPIRES	SERIAL NUMBER
<input type="checkbox"/>	ISSUED	Yes	3646907	CS ES	365	Web form	CN=orig1,O=orig1,ST=...	rfc822name=admin...	CN=Sectigo De...	10/28/2023	13:0C:3B:2C:68:34
<input type="checkbox"/>	ISSUED	Yes	3646943	CS ES	365	Web form	CN=orig1,O=orig1,ST=...	rfc822name=admin...	CN=Sectigo De...	10/28/2023	1D:5A:63:41:51:87
<input type="checkbox"/>	APPLIED	Yes	3647569	CS ES	365	Web form					
<input type="checkbox"/>	DOWNLOADED	Yes	Fx9y1lwtkJcS0joA...	CS pca	30	Web form	CN=orig1,O=orig1,ST=...	rfc822name=cs19@...	CN=testscep70...	11/18/2022	53:C7:5C:92:82:48
<input type="checkbox"/>	APPLIED	Yes	3628569	Elena's test (bl...	365	Web form					
<input type="checkbox"/>	DOWNLOADED	Yes	FyQ3ZiNk6mhlEg...	CS pca	30	Web form	CN=orig1,O=orig1,ST=...	rfc822name=janedo...	CN=testscep70...	12/04/2022	2F:EB:5F:69:88:2F
<input type="checkbox"/>	ISSUED	Yes	3625999	SECTIGO Publ...	365	Web form	CN=orig1,O=orig1,ST=...	rfc822name=stanisl...	CN=Sectigo De...	10/13/2023	4C:A5:58:64:9F:86
<input type="checkbox"/>	ISSUED	No			365	Discovery	CN=CN=Administra...	rfc822name=scm20...	CN=testscep70...	07/14/2023	6B:97:4C:09:CS:8A

This table lists fields available for the code signing certificates.

Field	Description
ID	The identification number of the certificate request made to the CA.
Status	The status of the certificate. Can be one of the following: <ul style="list-style-type: none"> Invited – The applicant has been sent an invitation email by an administrator. Requested – A request for the certificate has been sent to the CA for approval. Applied – The applicant has validated the email and applied for the certificate. Issued – The certificate was issued by the CA and collected by SCM, but has not yet been downloaded by the applicant. Revoked – The certificate is invalid because it was revoked. Expired – The certificate is invalid because its validity period has expired. Rejected – The CA rejected the request after validation check.
Order Number	The order number of the certificate request made to the CA.
Certificate Profile	The certificate profile to which the certificate belongs.
Term	The number of days that the certificate is valid.
Requested Via	How the certificate was requested. For example, via Web Form, Discovery, REST API.
Subject	The subject of the issued certificate. For example, o = OrgName2, cn = CommonName, etc.
Subject Alternative Name	The names of domains for which the certificate is used.
Issuer	Details of the CA that issued the certificate and the name of the certificate.
Expires	The expiry date of the certificate.
Serial Number	The certificate's serial number.

Field	Description
Key Usage	The cryptographic purposes for which the certificate can be used. For example, key digital signing, encryption, and so on.
Extended Key Usage	Higher level capabilities of the certificate.
Key Algorithm	The type of algorithm used for encryption.
Key Size / Curve	The key size used by the certificate for encryption.
Signature Algorithm	The type of algorithm used for the signing of the certificate.
MD5 Hash	The MD5 hash (thumb print or fingerprint) for the certificate.
SHA1 Hash	The SHA1 hash (thumb print or fingerprint) for the certificate.
Organization	The name of the organization to which the applicant belongs.
Department	The name of the department to which the applicant belongs.
Name	The requester's name.
Email	The email address of the requester.
HSM Type	The HSM type that is used for ordering a certificate.
Shipping Type	The shipping type for the certificate. It can be STANDARD, EXPEDITED, INTERNATIONAL.
Subject Alternative Name Email	The requester email. If specified, this email will be added to the Subject Alternative Name.
Requested	The date that the certificate was requested.
Issued	The date when the certificate was issued.
Revoked	The date when the certificate was revoked.
Control Buttons	
Search	Enables you to search certificates by ID, or subject alternative name.
Invitations	Sends an invitation to external users.
Filter	Enables you to sort the table information using custom filters.
Group	Enables you to sort the table information using predefined groups.
Refresh	Enables you to refresh the page.

Field	Description
Download CSV	Downloads a list of code signing certificates in CSV format.
Manage Columns	Helps to manage columns for the Code Signing certificates.
Certificate Control Buttons ^a	
Delete	Removes the certificate.
View	Displays the certificate details.
Revoke	Revokes the certificate.
View Audit	Displays the certificate audit details.

a. Depend on the status of the selected certificate.

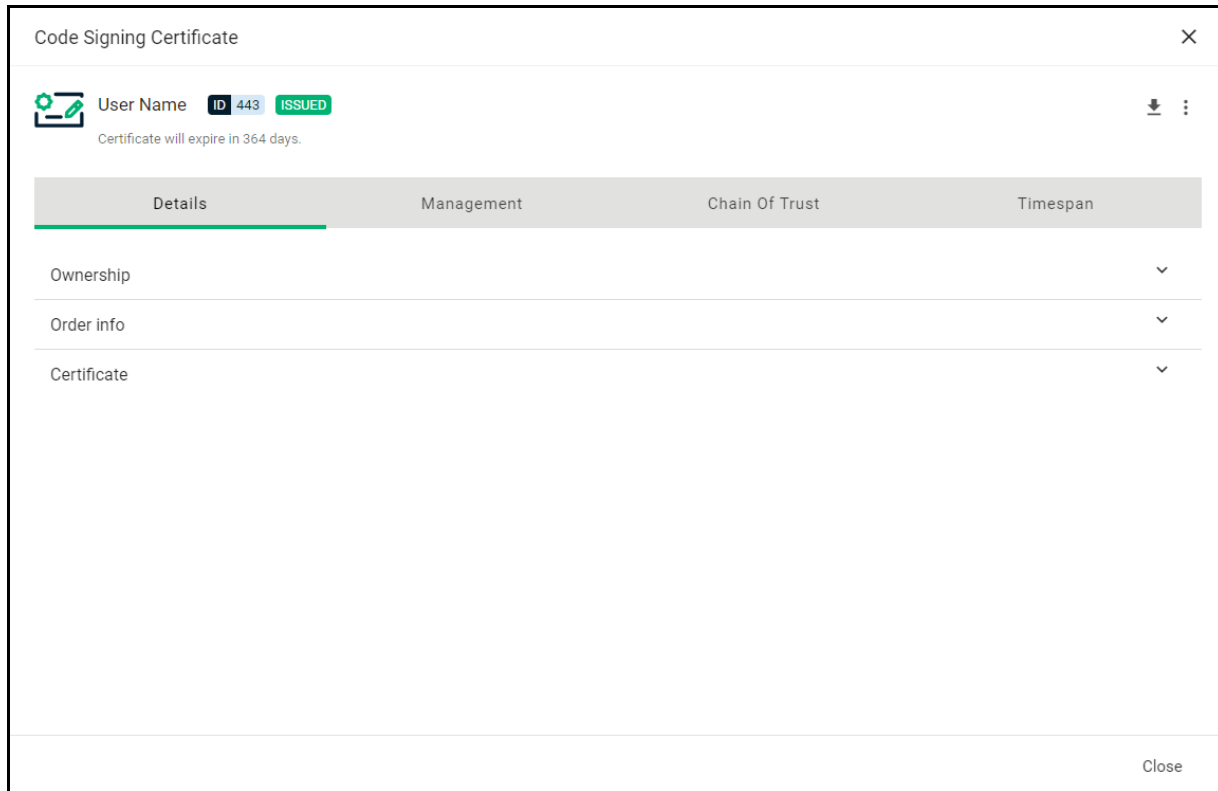
3.4.1 Modify code signing certificate

To view or modify a code signing certificate's details, do the following:

1. Navigate to **Certificates > Code Signing Certificates**.
2. Select a certificate in the list.
3. Click **View**.

This opens the **Code Signing Certificate** dialog that enables you to do the following:

- View status and summary information
- Download the certificate in different formats
- View ownership and order information if certificate was requested using SCM
- Change ownership at any certificate status
- Configure notifications
- View and manage private key if applicable
- View the full certificate chain



3.4.2 How to request and issue code signing certificates

The following requirements must be met for the process to succeed:

- If you request a publicly trusted code signing certificate, the organization must be validated.
- If you request a publicly trusted code signing certificate with an email address in the subject alternative name (SAN), the domain of that email address must be validated.
- If you request a code signing certificate with an email address in the subject alternative name, that domain must be delegated to the organization or department for code signing purposes.
- The RAO Code Signing or DRAO Code Signing administrator has been delegated control of this organization or department.
- The MRAO or delegated RAO administrator has enabled code signing certificates for the organization or department by selecting **Enabled** in the **Code Signing Certificate** page of the **Add New** or **Edit Organization** dialog (see [Edit certificate settings](#)).

Upon fulfillment of the preceding requirements, the following needs to occur in order for the code signing certificates to be enrolled to end-users:

1. An invitation email is sent from SCM to the end-user.
2. Upon receiving the invitation email, the end user clicks the included link to be directed to the self-enrollment form.
3. The end-user must complete the form and submit the request to SCM.
No approvals are required in SCM since the request has been preapproved by sending the invitation.

- Depending on the CSR generation method of the selected account, the end-user may be redirected to the endpoint list of their certificates or they may be requested to download the PKCS#12 file on the page. An email notification with links to download the certificate is sent by SCM.

3.4.2.1 Sending code signing certificate invitations

You can send code signing certificates invitations as follows:

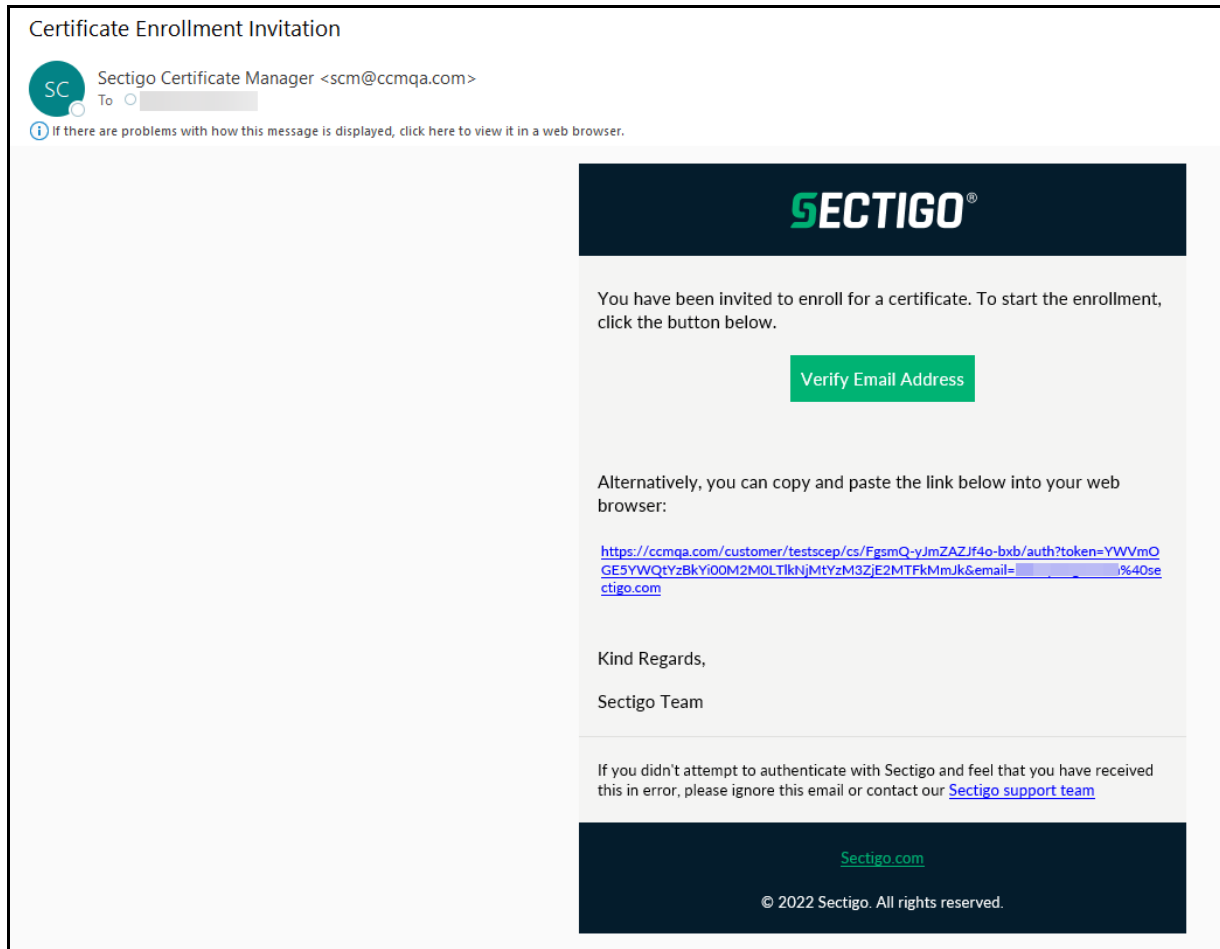
- Navigate to **Certificates > Code Signing Certificates**.
- In the upper-right corner, click **Invitations** and then click the **Add** icon to open the **Send Invitation** dialog.

- Complete the fields based on the information provided in the following table and click **Send**.

Field/Element	Description
Email	The email address to send the invitation to.
Details	
Enrollment Endpoint	The certificate enrollment endpoint
Account	The account of the enrollment endpoint
Profile	The certificate profiles available for the selected account. If multiple profiles are possible, the end-user will be allowed to select from them.

3.4.3 Completing the code signing certificate request

- Verify the email address specified in the email you receive.



- Complete the **Code Signing Certificate Enrollment** form based on the information provided in the following table. Mandatory fields are marked with an asterisk.

Field/Element	Description
Certificate Term	The validity period of the certificate. For example, 1 year, 2 years, 3 years. The available validity periods depend on the selected profile.
Certificate Email (SAN)	The email address to include the certificates subject alternative name (SAN) extension. Optional for publicly trusted code signing certificates.
Title	Your official or preferred title (e.g., Mr., Mrs.)
First Name	Your first name
Last Name	Your last name
Key Type	The type of algorithm used for generating the key pair. It is not applicable to the Provided by User CSR generation method.

Field/Element	Description
PKCS#12 Password	A password used to encrypt PKCS#12 download file (if marked mandatory in endpoint account). It is not applicable to the Provided by User CSR generation method.

3. Accept EULA and click **Submit**.

Depending on the CSR generation method of the account, the end-user may immediately be able to download the issued certificate or a PKCS#12 file containing the private key and certificate. In addition to the end-user downloading the certificate themselves, you can download the certificate in a variety of formats from SCM. To do this, navigate to **Certificates > Code Signing Certificates**, select the certificate, and click **Download**.

3.4.3.1 Code signing certificate CSV file format and importing guidelines

The following table lists fields, with their possible values and formats, that can be imported from the CSV file for each certificate.

Field	Required	Minimum Characters	Maximum Characters	Format	Supported Characters
Organization	Yes	1	128		Any
Department	No ^a	0	128		Any
Term	Yes	1	1	Integer	01/05/13
Email Address	Yes	3	128	Valid email address	A-Z a-z 0-9 . - _ @
Full Name	Yes	1	64	Valid name	A-Z a-z 0-9 . - ,
Contact Email	No	3	128	Valid email address	A-Z a-z 0-9 . - _ @

a. Department can be excluded but the comma following it must be kept.

The following example pertains to organizations that include a department:

```
"Test Organization", "Test Department", "1", "jsmith@example.org", "JOHN SMITH", "jsmith@alternativeemail.com"
```

The following example pertains to organizations that do not include a department:

```
"Test Organization", , "1", "jsmith@example.org", "JOHN SMITH", "jsmith@alternativeemail.com"
```

3.5 Managing Device Certificates

Depending on your security role, the **Device Certificates** page shown in the following illustration enables you to manage certificates issued to devices that have been added to SCM via active directory or self-enrollment. Device certificates can be issued from a private CA or via AD. To add a private CA to your account, contact your Sectigo account manager.

MRAO administrators can view, approve, and decline the device certificates and end-users of any organization or department.

RAO Device Certificate administrators can view, approve, and decline the device certificates of organizations and any subordinate departments that have been delegated to these administrators.

DRAO Device Certificate administrators can view, approve, and decline the device certificates of departments that have been delegated to these administrators.

ID	STATUS	COMMON NAME	ORDER NUMBER	CERTIFICATE PROFILE	TERM	REQUESTED VIA	SUBJECT	SUBJECT ALT NAME
288	ISSUED	comqa.com	3396215	default	730	Enrollment Form	CN=fccmqa.com,C=U...	
634	ISSUED	org1	3643641	device_intune_new	365	MS Agent	CN=org1,O=org1	dNSName=Win-202
637	ISSUED	local.orgname.local	3643900	device_intune_new	365	Enrollment Form	CN=local.orgname.l...	
587	ISSUED	comqa.com	Fx7ombdHTreLdr...	ap.pca.device	365	Enrollment Form	CN=fccmqa.com,O=f...	
607	ISSUED				0	Discovery		dNSName=Win-202
291	ISSUED	comqa.com	3400372	device_intune	365	Enrollment Form	CN=fccmqa.com	
604	ISSUED				0	Discovery		dNSName=Win-202
611	ISSUED	WIN-2022-PDC			0	Discovery	CN=WIN-2022-PDC...	dNSName=Win-202
1843	ISSUED	8192.device.local	3740102	device_intune_99994	365	Enrollment Form	CN=8192.device.loc...	
603	ISSUED	WIN-2022-DJ.scm2022.comqa.c...			0	Discovery	CN=WIN-2022-DJ.sc...	dNSName=Win-203

The following table describes the settings that are available for device certificates:

Column	Description
ID	ID number of the certificate

Column	Description
Status	<p>The current status of the certificate, which can be one of the following:</p> <ul style="list-style-type: none"> • Requested—A request has been made by either (1) the MS Agent installed on the AD server to which the device is enrolled; (2) the device through SCEP; (3) an API call by the Mobile Device Manager (MDM) software used by the organization; (4) the self-enrollment form. You can view, edit, approve, decline, or revoke the request. • Declined—A request that was made using the self-enrollment form has been rejected by an appropriately privileged administrator. • Applied—The request has been approved and sent to Sectigo. • Issued—The certificate has been issued by Sectigo or MS CA and collected by SCM. • Expired—The certificate is invalid because its validity period has expired. • Revoked—The certificate is invalid because it was revoked. • Rejected—The CA rejected the request after a validation check.
Order	
Order Number	The order number of the certificate request made to CA
Certificate Profile	The certificate profile used during certificate issuance
Sub Type	The sub type of the certificate
Term	The number of days that the certificate is valid
Requested Via	How the certificate was requested. For example, via Discovery, Web Form, Client Admin, ACME
Common Name	The name of the device for which the certificate was issued. The device name is used as a common name in the device certificate itself.
Order Number	The order number of the certificate.
Ownership	
Organization	The name of the organization to which the certificate belongs.
Department	The name of the department to which the certificate belongs, if applicable).
Requester	The email address of the end-user who requested this certificate through the self-enrollment form, or the name of the administrator who requested this certificate using auto-installation or the built-in wizard.
Expires	The expiration date of the certificate.
Key Usage	The cryptographic purposes for which the certificate can be used. For example, signing, non repudiation, authentication and encryption.
Extended Key Usage	Higher level capabilities of the certificate.
Serial Number	A unique number which identifies the certificate.

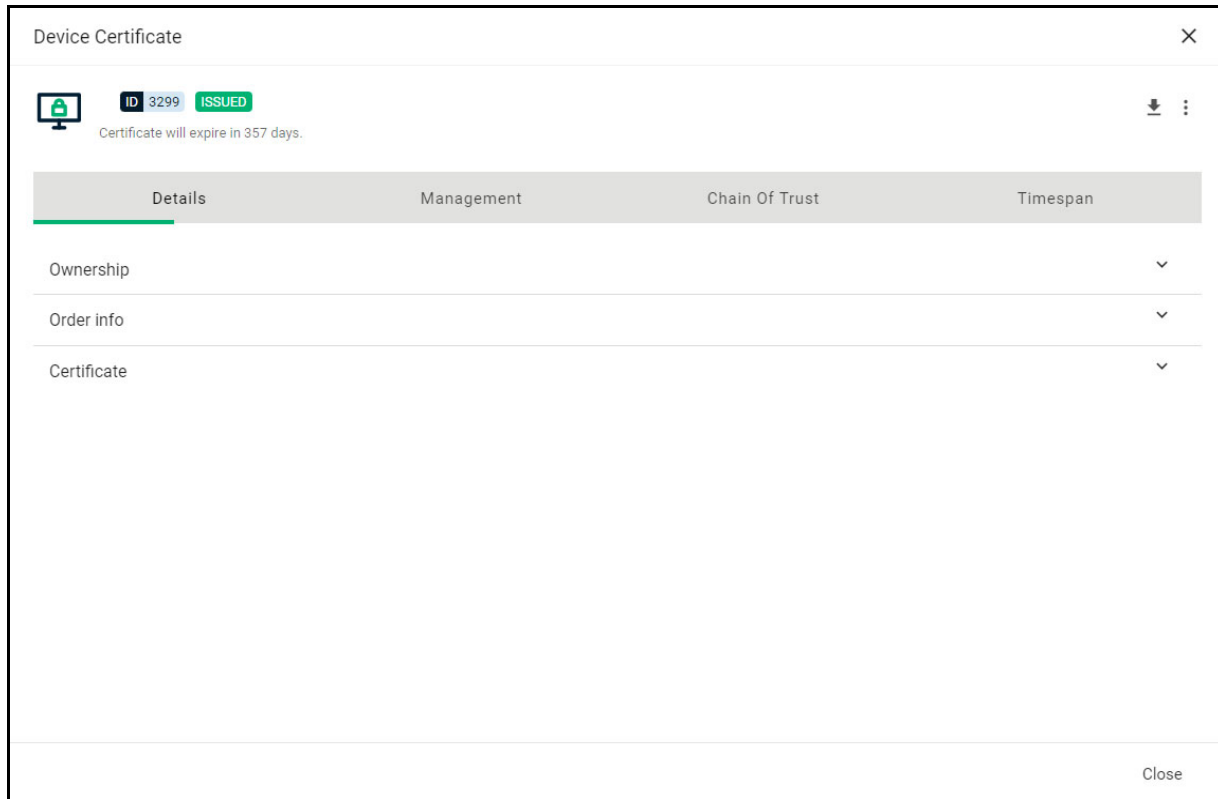
Column	Description
Certificate Profile	The certificate profile of the device certificate.
Signature Algorithm	The signature algorithm of the public key of the certificate.
Key Algorithm	The type of algorithm used for encryption.
Key Size/Curve	The key size or curve used for encryption.
Control Buttons	
Search	Enables you to search certificates by ID, common name, or subject alternative name.
Add	Applies for a new code signing certificate.
Filter	Enables you to sort the table information using custom filters.
Group	Enables you to sort the table information using predefined groups.
Refresh	Enables you to refresh the page.
Download CSV	Saves the list of device certificates in CSV format.
Enroll with MS CA	Generates a certificate using MS CA.
Certificate Control Buttons ^a	
View	Displays a summary of details about the selected certificate.
Approve	Enables you to approve the certificate request via self-enrollment.
Decline	Enables you to decline the certificate request via self-enrollment.
Revoke	Enables you to revoke the certificate.
Resend Collection Link	Enables you to resend the device certificate Collection Mail.
Download	Download an issued certificate. This applies to certificates from MS CA.

a. The certificate control buttons that are displayed depend on the status of the selected certificate.

3.5.1 How to view device certificate details

You can view a device certificate details as follows:

1. Navigate to **Certificates > Device Certificates**.
2. Select a certificate and click **View** to open the **Device Certificate** dialog shown in the following illustration.



The following table lists the fields and their values available in the **Device Certificate** dialog.

Field	Description
Email	The email of the end-user.
Status	The status of the certificate, as follows: <ul style="list-style-type: none"> • Requested – A request has been received for the certificate. Requests need to be approved by the administrator. • Declined – A request that was made using the self-enrollment form has been rejected by an administrator. • Applied – The request has been approved and sent to Sectigo. • Issued – The certificate has been issued by the CA and collected by SCM. • Expired – The certificate is invalid because its term has expired. • Revoked – The certificate is invalid because it was revoked. • Rejected – The CA rejected the request after a validation check.
Order Number	Order number of the certificate. Does not apply to certificates enrolled via MS CA.
Organization	The name of the organization to which the device certificate belongs.
Department	The name of the department to which the device certificate belongs.
Requested	The date the certificate request was sent to Sectigo from SCM or date of certificate request from MS CA by the administrator.

Field	Description
Collected	The date the certificate was collected by SCM from Sectigo.
Expires	The expiry date of the certificate.
Serial Number	The serial number of the certificate as assigned by the CA.
Key Usage	The cryptographic purposes for which the certificate can be used.
Extended Key Usage	Higher level capabilities of the certificate.
Download The Certificate	Enables the download of the certificate in the following formats: <ul style="list-style-type: none"> • Certificate only, PEM encoded (.cer) • Certificate (w/ issuer after), PEM encoded (.pem) • Certificate (w/ chain), PEM encoded (.cer) • PKCS#7 (.p7b) • PKCS#7, PEM encoded (.crt) • Intermediate(s)/Root only, PEM encoded (.cer) • Root/Intermediate(s) only, PEM encoded (.cer)
Optional fields	Available for certificates applied for manually or using the self-enrollment form. Displays details from the CSR subject such as organization name, common name, and so on.
Suspend Notifications	Disables all notifications for events such as certificate download, expiry, and revocation from SCM to the administrator and the end-user, for this certificate.

3.5.2 How to request and issue device certificates

Device certificates can be issued to devices in one of the following ways:

- **Active Directory**—Enroll device certificates from SCM CA proxy or MS CA using AD.
 - SCM CA proxy: Certificates can be requested for devices added to AD servers that have been integrated with SCM. See [“Issuing device certificates through SCEP” on page 124](#).
- **SCEP**—Using the built-in SCEP server, certificates can be requested and issued for devices that have been configured with a suitable configuration profile. See [“Issuing device certificates through SCEP” on page 124](#) for details.
- **API Integration**—Mobile Device Management (MDM) solutions can be integrated into SCM through an API. You can apply configuration profiles to managed devices to enroll for certificates to SCM. For details on API integration, see https://support.sectigo.com/Com_KnowledgeProductPage?c=API_Documentation&k=&lang=.
- **Self Enrollment**—Device certificates can be requested by applicants using the self-enrollment form available by accessing a link provided by an administrator. See [“Issuing device certificates through self-enrollment” on page 124](#) for details.
- **Manually**—Administrators can add device certificates directly in SCM.

Issuing device certificates via SCEP, API integration, self-enrollment, or manually requires that you have a private CA configured and at least one device certificate profile that uses the private CA as its enrolling backend. See [“CA Backends” on page 196](#) and [“How to manage certificate profiles” on page 160](#).

3.5.2.1 Issuing device certificates through SCEP

Using a configuration profile that has been pushed to target devices, devices can request certificates from SCM via SCEP. The configuration profile can be created using software such as the iOS configuration utility.

The following requirements must be met for the process to succeed:

- Your account must have SCEP enabled for device certificates. Contact your Sectigo account manager for details.
- You must have at least one certificate profile configured for use with device certificates. For more information on certificate profiles, see [“How to manage certificate profiles” on page 160](#).
- You created a Device certificate SCEP enrollment endpoint and configured an account for the endpoint, including an access code. The Device certificate SCEP enrollment endpoint URL will be included in the configuration profile for over-the-air (OTA) enrollment. See [“Managing SCEP RA certificates” on page 176](#).

Typically, the process involves the following:

1. You generate a configuration profile for OTA enrollment using a configuration software, then apply the profile to target devices. The SCEP enrollment access code specified for the SCEP endpoint account is included in the profile. This means the certificate request generated by the device contains the access code as the `challengePassword` parameter.
2. Once applied, the device generates the certificate request and forwards it to SCM.
3. The certificate requests are added to the **Device Certificates** page for approval, with a status of Requested.
4. A RAO or DRAO with appropriate privileges approves the request, then SCM forwards the request to Sectigo. The status of the certificate changes to Applied.
5. Upon issuance of the certificate, SCM collects the certificates. The status of the certificate changes to Issued.
6. The SCEP server pushes the certificates to the target devices for installation.

For details on values of parameters to be specified in the configuration profile, contact your Sectigo account manager.

3.5.2.2 Issuing device certificates through self-enrollment

Self-enrollment enables external applicants to request device certificates using the self enrollment form, accessed at the URL of the device certificate enrollment endpoint.

The following requirements must be met for the process to succeed:

- The issuance of device certificates is enabled for your account.
- You have at least one certificate profile configured for use with device certificates. For more information on certificate profiles, see [“How to manage certificate profiles” on page 160](#).
- You added a device certificate enrollment endpoint (see [“How to map MS AD certificate templates to SCM” on page 166](#)).
- The RAO Device Certificate or DRAO Device Certificate administrator has been delegated control of this Organization or Department.

- The applicant has already created the CSR prior to beginning the application. The public key included in the CSR should be at least of a RSA 2048 key length or ECC p256 curve and must match one of the key types allowed by the selected certificate profile.

The subject typically includes the following RDN fields:

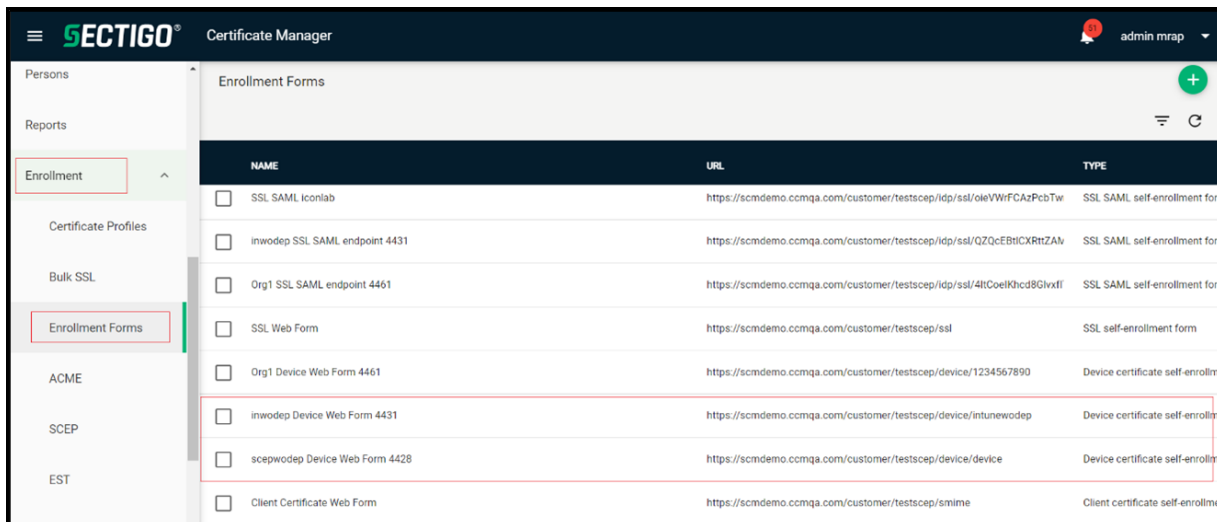
- CN—Common name, e.g., host name, DNS name
- O—Organization
- OU—Organization unit, i.e., the department name
- L—Locality, i.e., town or city
- ST—State, province, region or county name
- C—Country (two-character country code as defined in ISO 3166)

Additional DNS names can be specified using the SAN field. If information is missing from the CSR, or differs from the organization details as specified in SCM, the SCM organization values are used.

Upon fulfillment of the preceding requirements, the following needs to occur in order for the device certificates to be provisioned to end-users via a self-enrollment process:

1. You send the link to the **Device Certificate Enroll** form, located at the address specified for the device enrollment endpoint.

To view the Device certificate self-enrollment form URL, navigate to **Enrollment > Enrollment Forms**.



NAME	URL	TYPE
<input type="checkbox"/> SSL SAML Iconlab	https://scmdemo.cmqa.com/customer/testscope/idp/ssl/oleVWfCAzPcbTw	SSL SAML self-enrollment form
<input type="checkbox"/> inwodep SSL SAML endpoint 4431	https://scmdemo.cmqa.com/customer/testscope/idp/ssl/QZQcEBtCXrtZAN	SSL SAML self-enrollment form
<input type="checkbox"/> Org1 SSL SAML endpoint 4461	https://scmdemo.cmqa.com/customer/testscope/idp/ssl/4ItCoelKhcd8GivxII	SSL SAML self-enrollment form
<input type="checkbox"/> SSL Web Form	https://scmdemo.cmqa.com/customer/testscope/ssl	SSL self-enrollment form
<input type="checkbox"/> Org1 Device Web Form 4461	https://scmdemo.cmqa.com/customer/testscope/device/1234567890	Device certificate self-enrollment form
<input type="checkbox"/> inwodep Device Web Form 4431	https://scmdemo.cmqa.com/customer/testscope/device/intunewodep	Device certificate self-enrollment form
<input type="checkbox"/> scepwodep Device Web Form 4428	https://scmdemo.cmqa.com/customer/testscope/device/device	Device certificate self-enrollment form
<input type="checkbox"/> Client Certificate Web Form	https://scmdemo.cmqa.com/customer/testscope/smime	Client certificate self-enrollment form

2. The applicant completes and then submits the self-enrollment form.
3. The certificate request is approved by appropriate administrators.
4. If the application is successful, the applicant can download and install their device certificate (see [“About device certificate collection”](#) on page 129).

Provide enrollment details to applicants using an out-of-band communication such as email.

When the end-user accesses the Device certificate self-enrollment form URL, the **Device Certificate Enrollment** form is displayed as shown in the following illustration.

Device Certificate Enrollment

Fill in the fields below to enroll a certificate

Certificate Profile:*
ad99994

Certificate Term:*
1y

Email*

CSR*

device

device**

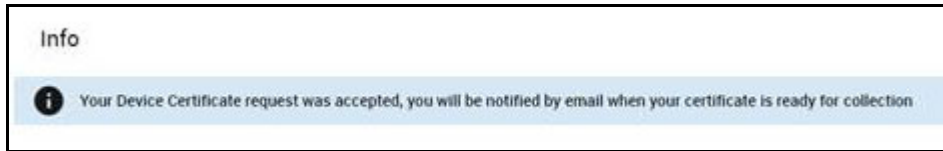
Submit

The following table describes the form fields and elements. Mandatory fields are marked with asterisks.

Field ^a	Description
Certificate Profile	The device certificate profile.
Certificate Term	The term for the device certificate.
Email Address	The applicant's full email address. The device certificate collection notification is sent to this email address.
CSR	The CSR that Sectigo will use to process the application. The CSR can be pasted into this field. The CSR must match one of the key types allowed by the selected certificate profile.
Submit	Submits the application and enrolls the applicant for the device certificate.

a. The fields in the form are the default fields. There may be more fields if custom fields have been defined for the form.

After submitting the form, a confirmation as shown in the following illustration is displayed.



3.5.2.3 Issuing device certificates manually

You can request device certificates directly from SCM.

The following requirements must be met for the process to succeed:

- The issuance of device certificates is enabled for your account.
- You have at least one certificate profile configured for use with device certificates. For more information on certificate profiles, see [“How to manage certificate profiles” on page 160](#).
- The RAO Device Certificate or DRAO Device Certificate administrator has been delegated control of this Organization or Department.
- You have already created the CSR prior to beginning the application. The public key included in the CSR should be at least of a RSA 2048 key length or ECC p256 curve, and must match one of the key types allowed by the selected certificate profile.

The Subject field typically includes the following RDN fields:

- CN—Common name, e.g., host name, DNS name
- O—Organization
- OU—Organization unit, i.e., the department name
- L—Locality, i.e., town or city
- ST—State, province, region or county name
- C—Country (two-character country code as defined in ISO 3166)

Additional DNS names can be specified using the SAN field. If information is missing from the CSR, or differs from the organization details as specified in SCM, the SCM organization values are used.

Upon fulfillment of the preceding requirements, add a device certificate by doing the following:

1. Navigate to **Certificates > Device Certificates**.
2. In the upper-right corner, click the **Add** icon. This displays the **Request Device Certificate** dialog.

The screenshot shows a 'Request Device Certificate' dialog box. It has a title bar with a close button (X). The form contains the following fields:

- Organization ***: inwodep
- Department**: None
- Certificate Profile ***: ap.pca.device
- Term**: 365
- CSR ***: Drag or paste your CSR here
- deviceCustomField ***: (empty)

At the bottom right, there are 'Cancel' and 'Save' buttons.

3. Fill out the fields as described in the following table and click **OK**.

Field ^a	Description
Organization	The name of the organization to which the device certificate belongs.
Department	The name of the department to which the device certificate belongs.
Certificate Profile	The certificate profile to be used for the certificate issuance. The profile description is also displayed (if provided).
Term	The term for the device certificate.
CSR	The CSR that Sectigo will use to process the application. The CSR can be pasted into this field. The CSR must match one of the key types allowed by the selected certificate profile.

a. The fields in the form are the default fields. There may be more fields if custom fields have been defined for the form.

The certificate is added to the **Device Certificates** page with a status of Applied. Once Sectigo issues the certificate, its status is set to Issued and a collection email is sent to the administrator who submitted the request. See [“About device certificate collection” on page 129](#).

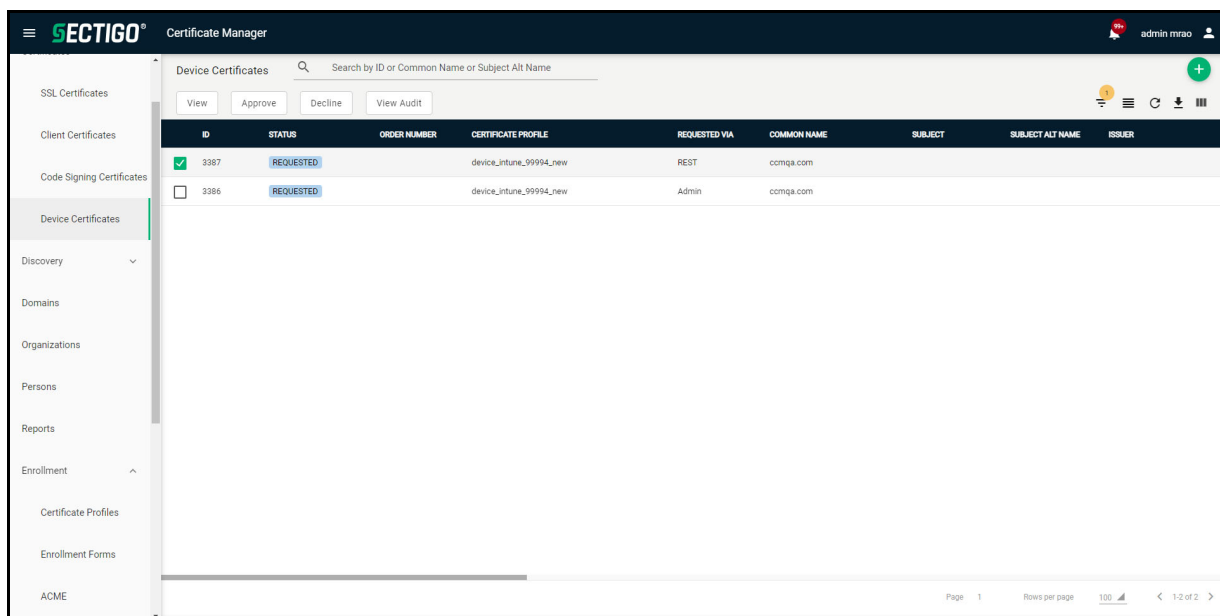
3.5.2.4 Approving and declining device certificate requests

Device certificates that have been requested via SCEP are listed in the **Device Certificates** page with a status of Requested, and device certificates that have been requested using the self enrollment form are listed in the **Device Certificates** page with a status of **Requested**.

Before SCM can forward the request to Sectigo, an administrator with appropriate privileges must approve the request.

To approve or decline a device certificate request, do the following:

1. Navigate to **Certificates > Device Certificates**.
2. Select a device certificate with a status of **Requested**.
3. Click **Approve** or **Decline**.

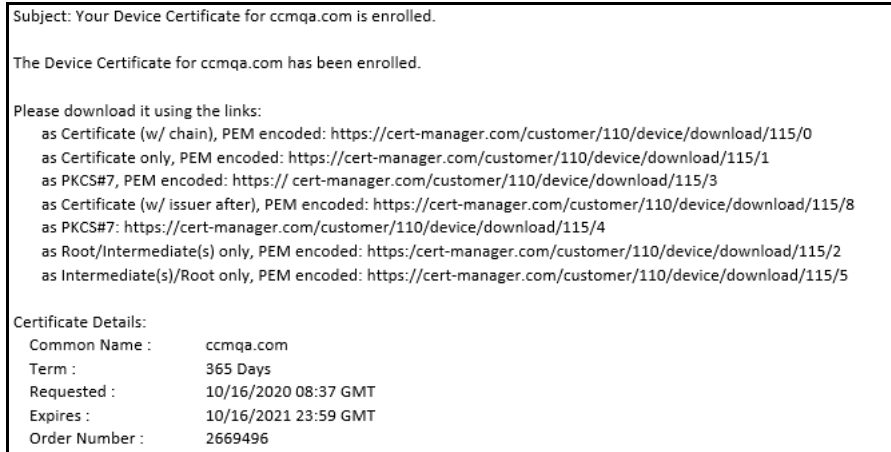


The status of the approved certificate is displayed as **Applied**. Once the certificate is issued, a collection form is sent via email, enabling the user to download and save the certificate.

3.5.2.5 About device certificate collection

When a certificate is issued, a device certificate collection mail similar to that shown in the following illustration is sent to the email address provided in the enrollment form, or to the administrator who requested the certificate.

SCM delivers the certificate to the applicant in the formats shown in the following illustration.



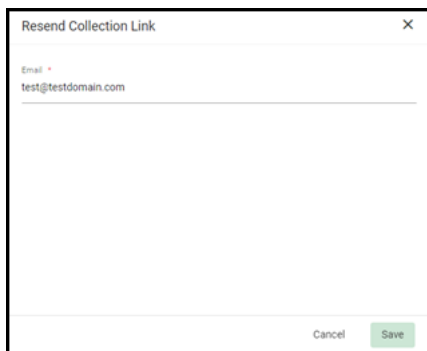
Alternatively, you can download the certificate and provide it to the requester. To do this, navigate to **Certificates > Device Certificates**, select the certificate, and click **View**. See [“How to view device certificate details” on page 121](#).

3.5.2.6 Resending the device certificate collection email

SCM automatically sends a collection email to applicants once a device certificate has been issued. However, if the certificate is not downloaded for some time, you may want to resend the mail.

You can resend the certificate collection email as follows:

1. Navigate to **Certificates > Device Certificates** and select the certificate with a status of Issued for which you want to resend the collection mail.
2. Click **Resend Collection Link** to open the **Resend Collection Link** dialog.



The recipient email address defaults to the address entered during certificate enrollment.

3. To send the mail to a different email address, enter the new address in the **Email** field.
4. Click **Save**.

The collection mail is sent to the specified address.

3.5.2.7 Revoking device certificates

Device certificates issued to or downloaded by end-users can be revoked by appropriate administrators any time before the certificate expiry date.

To revoke a device certificate, do the following:

1. Navigate to **Certificates > Device Certificates**.
2. Select the certificate from the list and click **Revoke** to open the **Revocation reason** dialog.

Revocation reason

Revocation reason
Unspecified

i To select the most appropriate reason for revocation of this certificate, please read their description below:
This option is used when no revocation reason is provided by the certificate subscriber.

Message *

Cancel Revoke

3. Select a reason for revocation from the list, add the message and click **Revoke**.
Upon completion, the certificate is displayed with a status of Revoked.

Performing certificate discovery tasks

This chapter describes how to use SCM for scanning networks and integrated AD servers to identify various certificates.

This chapter describes the following topics:

- [Certificate discovery tasks overview](#)
- [Performing network discovery tasks](#)
- [Performing AD discovery tasks](#)
- [Managing assignment rules](#)
- [Managing certificate buckets](#)

4.1 Certificate discovery tasks overview

SCM enables scanning of networks and integrated AD servers to identify the following certificates:

- SSL certificates installed on your network servers. This includes certificates issued to domains and network devices, and external certificates (that is, not managed by SCM), including certificates issued by third party vendors, and self-signed certificates.
- Certificates (typically client) installed on servers, devices, and endpoints on AD domains. AD scans discover the network and object structure, and locate all types of certificates, including SSL, client, code signing, and device.

The **Discovery** page lets you configure and run network discovery scans, AD scans, and to view certificates and network objects identified by the scans. The **Discovery** page contains the following sub-areas:

- **Network Discovery Tasks** enables you to add, schedule, and run discovery tasks on networks. For more information, see [“Performing network discovery tasks” on page 133](#).
- **MS AD Discovery Tasks** enables MRAOs with the MS AD Discovery privilege to add, schedule, and run discovery tasks on AD Servers. For more information, see [“Performing AD discovery tasks” on page 142](#).
- **Assignment Rules** enables MRAOs to define rules for automatically assigning external certificates identified by discovery scans to organizations and departments, as well as apply the rules while configuring discovery scans. For more information, see [“To view certificate details, select a certificate and click Details.” on page 150](#).
- **Certificate Buckets** allows you to view the results from scans and to configure automatic assignment using rules or manual assignment to organizations/departments. For more information, see [“Managing certificate buckets” on page 153](#).

Scans are performed using the following two types of agents:

Network Agents—Network agents are installed on network servers to facilitate the discovery of SSL certificates in networks. In addition, the agents are used for automatic installation of SSL certificates on Apache HTTP, Apache Tomcat, IIS 7, 7.5, 8, and F5 BIG IP servers. Information about the Network agents can now be found [here](#).

- **MS Agents**—MS Agents are installed on AD servers to facilitate the discovery process in AD domains. In addition, these agents perform the following:
 - Act as a CA proxy and can be used to provision authentication certificates for devices added via NDES.
 - Allow certificate templates on AD servers to be mapped to SCM certificate types and certificate profiles. This enables SCM to act as a private CA for an organization or department. Domain administrators can create custom certificate templates on their server as required and request that SCM administrators map these templates to private certificate profiles. Domain administrators can enroll for certificates from the AD server by selecting the respective template.
 - Provide authentication certificates to devices.

See [“MS agents” on page 230](#) for more information.

Assignment rules are used during discovery tasks to assign external certificates to organizations and departments based on the criteria you specify. For more information, see [“To view certificate details, select a certificate and click Details.” on page 150](#).

4.2 Performing network discovery tasks

The **Network Discovery Tasks** page shown in the following illustration enables you to scan and monitor a network for all installed SSL certificates, both managed and external, including Sectigo certificates that may or may not have been issued using SCM, any third party vendor certificates, and any self-signed certificates. You can add and configure discovery tasks for different networks to be scanned and can optionally set a schedule for them for periodical scanning.

Using assignment rules, external certificates discovered during a scan can be automatically assigned to a specific organization or department.

Typically, the process includes the following:

- Scanning a network in order to find the deployed certificates.
- Discovered items are shown in SCM as follows:
 - All discovered managed SSL certificates and external SSL certificates assigned to organizations and departments via an assignment rule, are added to the **SSL Certificates** page.
 - All certificates discovered on the network are shown in the **Certificate Buckets** page, as described in [“How to view certificates via certificate buckets” on page 153](#).
- SCM updates the status of existing certificates that were issued using SCM, if required.
- External certificates can become managed via renewal of a particular certificate.

Using the Auto agent you can run scans of publicly accessible servers or, using a Network Agent, servers in your internal network. Internal scans require that a Network Agent has been installed and configured, as described in [Network Agents](#).

It is recommended that you do the following:

- Schedule regular discovery scans.
- Run a manual scan after every change to an SSL certificate configuration. Otherwise, it is possible that the **SSL Certificates** page shows inaccurate information (for example, you may have uploaded a certificate to your website but in SCM the certificate has a status of Issued and a discovery status of Not deployed if you have not run the scan again).
- Run a manual scan after any change to the network in general.

A MRAO can add, modify, and run scans for tasks using any installed network agent and any assignment rule.

A RAO SSL can add, modify, and run scans for tasks using network agents and assignment rules pertaining to organizations and their departments that have been delegated to this administrator.

A DRAO SSL can add, modify, and run scans for tasks using network agents and assignment rules pertaining to departments that have been delegated to this administrator.

ID	NAME	AGENT	CERTIFICATE BUCKET	RANGES TO SCAN	STATUS	SCHEDULE	LAST SC
<input type="checkbox"/> 787	ap.test	Cloud	bucket1	google.com	Successful	Manual	04/14/2
<input type="checkbox"/> 783	Task SCM-7430	Cloud	Bucket SCM-7430	151.101.66.150-151.101.66.160	Successful	Manual	04/18/2
<input type="checkbox"/> 635	ProxyTestingV2.29	Cloud	ProxyTestingV2.29	192.168.23.151	Scan in Progress	Manual	04/18/2
<input checked="" type="checkbox"/> 627	1000	Cloud	google.com	10.1.1.0/24	Manual	Manual	04/18/2
<input type="checkbox"/> 612	Task1	67winCustomizedBroken	google.com	google.com	Scan in Progress	Manual	04/06/2
<input type="checkbox"/> 609	t3	Net28	google.com	google.com	Scan in Progress	Manual	04/14/2
<input type="checkbox"/> 600	devYPF5A	devYPAgent	devYIP	10.16.45.62	Scan in Progress	Manual	04/14/2
<input type="checkbox"/> 999	Uploaded_task	Net28	166	10.101.66.0/24	Canceled	Run Once	04/15/2
<input type="checkbox"/> 590	00001	Agent acme 164	166	2.10.0.0/24	Canceled	Manual	04/14/2
<input type="checkbox"/> 585	Tes888	Cloud	drao3	2321.edu	Successful	Manual	04/10/2

The following table lists settings available in the **Network Discovery Tasks** page.

Field / Element	Description
ID	ID number of the certificate discovery task.
Name	The name of the certificate discovery task.
Agent	The name of the agent that is to be used.
Certificate Bucket	The name of the certificate bucket.
Ranges to Scan	The IP ranges that are to be scanned during this task.

Field / Element	Description
Status	The status of the scan: successful, failed, in progress, or canceled. Clicking the status displays the respective result. For example, clicking Successful displays the number of certificates discovered.
Schedule	Indicates whether the scan is to be run manually or scheduled.
Last Scanned	The date and time of the last scan performed.
Controls	
Add	Enables you to add a new task
Filter	Enables you to sort the table information using custom filters
Group	Enables you to sort the table information into predefined groups
Refresh	Enables you to refresh the page
Upload	Enables you to upload a file
Download	Enables you to download a file
Columns	Enables you to modify which columns of information appear the table
Discovery Task Controls	
Delete	Enables you to delete the selected discovery task.
Edit	Enables you to edit the selected discovery task.
Scan	Enables you to start a new scan for the selected discovery task.
Cancel	Cancel the selected discovery scan (visible only while scan is in progress).
History	Displays the details of past scans performed for the selected discovery task and enables you to download scan reports.
View Audit	Allows you to see audit events to the selected discovery task.

You can generate reports on discovered certificates and network discovery tasks for specific organizations and departments in the **Reports** page. See [“Generating reports” on page 159](#).

4.2.1 How to add and modify network discovery tasks

To add or modify a network discovery scan task, do the following:

1. Navigate to **Discovery > Network Discovery Tasks**.
2. Click **Add** or select a task and click **Edit**.

The **Common** settings are used to configure scan settings.

Add Network Discovery Task

Common Schedule

Name *

Agent
Cloud

Certificate Buckets *
07.03.23 AD Rules

Ranges to Scan

Cancel Save

3. Enter a name to describe the task.
4. Select the agent for the task to use. Use the **Auto** option to have SCM choose the most suitable agent or to perform a scan of publicly accessible servers; SCM chooses the agent based on the ranges to scan set for the task.
5. Select the assignment rule.
6. To add or modify the ranges, click **Add** or select a range and click **Edit**.

Edit Scan Range

CIDR
e.g. 10.10.10.10/32

IP or IP range
e.g. 10.10.10.10 or 10.11.6.9-10.11.12.13

Host name
e.g. host1.domain.com
test.com

Port
443

Cancel Save

7. Choose **CIDR** to add the range in CIDR format, **IP or IP range** to enter IP addresses, or **Host name** to enter a host name.
8. Enter the port number to use.
9. Click **Save** to add the scan range.

You can add multiple ranges. To remove a scan range, select it and click **Remove**. Complete the **Schedule** settings to set the scan day, date and start time, and the frequency of the task.

Edit Network Discovery Task
✕

Common
Schedule

Frequency
Weekly ▾

Day of Week
Sunday ▾

Time zone
UTC+02:00 - CAT, CEDT, CEST, EET, HAEC... ▾

Time
02:27 AM

Next 5 scans

03/12/2023 02:27:09 UTC+2
03/19/2023 02:27:09 UTC+2
03/26/2023 02:27:09 UTC+2

Cancel
Save

Available scan frequencies are Manual (on demand), Run Once, Daily, Weekly, Monthly, Quarterly, Semi-Annually and Annually.

10. Click **Save**.

Newly created discovery tasks are displayed in the **Network Discovery Tasks** page.

4.2.2 How to import multiple network discovery tasks from a CSV file

To add multiple network discovery tasks using a .csv file, do the following:

1. Navigate to **Discovery > Network Discovery Tasks**.
2. Click **Import**.
3. Click **Import Network Discovery Task** from CSV or drag and drop your .csv file.
4. Once the upload is complete, click **OK** and then **Close**.

4.2.2.1 Network discovery task CSV file format

When creating a .csv file for the bulk import of network discovery tasks, the columns must be populated using the information and order outlined in the following table.

Column	Field	Description
A	Task Name	The name to be displayed for this network discovery task in SCM.

Column	Field	Description
B	Agent Name	The name of the agent that is to be used. For Cloud agent, leave it blank. You must have at least one agent configured to interact with your required scan ranges. For more information on configuring a network agent, see here .
C	Scan Ranges	The IP or IP range to be scanned. Ranges can be specified using a hyphen and can include a host name. CIDR format is supported.
D	Ports	The ports to be scanned. Multiple ports can be included using a comma-separated list enclosed in quotations ("233, 235, 255"). Port ranges can also be specified using a hyphen.
E	Schedule	The times when this network discovery task is to be run. Supported values are: Manual, Once, Daily, Weekly, Monthly, Quarterly, SemiAnnually, Annually. Tasks are scheduled for one minute following the upload of the CSV file and all tasks other than Manual and Daily are run on Sundays. You can also indicate a time zone by adding / followed by your UTC time zone.
F	Bucket ID	The bucket ID to be displayed for this network discovery task in SCM.

The following is an example of a simple .csv file for the creation of two network discovery tasks.

	A	B	C	D	E	F
1	Example Task Name	01win38	10.101.66.1/24	443	Manual	397b80e0-4d08-4048-a070-055e85031919
2	Example Task Name 2	Cloud	sectigo.com	443	Run Once	397b80e0-4d08-4048-a070-055e85031919
3						

4.2.3 How to delete a discovery task

To delete a discovery task, do the following:

1. Navigate to **Discovery > Network Discovery Tasks**.
2. Select the task in the list and click the trash icon to delete.
3. Click **Delete** to confirm.

4.2.4 How to run network discovery scans

Scans run according to the schedule set for the task, or you can run scans manually. You can run multiple discovery tasks at the same time.

To run a scan, select the discovery task in the list and click **Scan**.

The progress of the scan is displayed in the **Status** column.

Assuming the **Discovery Scan Summary** notification has been configured, once the scan is complete, SCM sends a notification email.

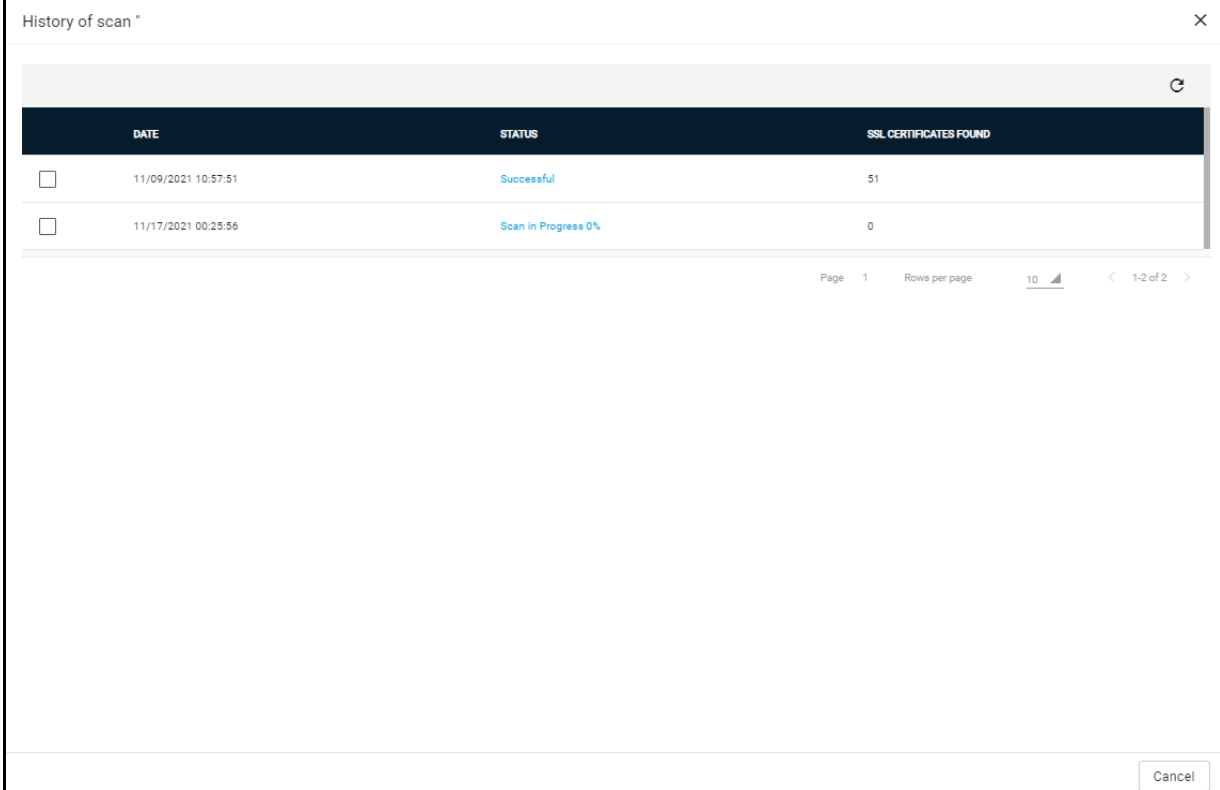
Subject: Discovery Scan Summary 03/26/2020 10:20 GMT		
Started: 03/26/2020 10:20 GMT		
Ended: 03/26/2020 10:22 GMT		
Scan Type: Manual		
Started By: John Smith		
IPs Scanned: 12		
Completion Status: SUCCESSFUL		
	Total	New
SSL Certificates:	5	5
SCM:	4	4
Other:	1	1
Self-Signed:	0	0

NOTE: You can modify the contents of these emails by navigating to **Settings > Notification Template**.

4.2.5 How to view a history of network discovery tasks

You can view the previous five scan results of each discovery task. You can also download a report on each task and assign external, discovered certificates to an organization or department.

1. Navigate to **Discovery > Network Discovery Tasks**.
2. Select the task and click **History** to open the **History of scan** dialog.



The screenshot shows a dialog box titled "History of scan" with a close button (X) in the top right corner. Below the title bar is a refresh icon. The main content is a table with three columns: "DATE", "STATUS", and "SSL CERTIFICATES FOUND". There are two rows of data, each with a checkbox in the left margin. The first row shows a scan on 11/09/2021 at 10:57:51 with a status of "Successful" and 51 certificates found. The second row shows a scan on 11/17/2021 at 00:25:56 with a status of "Scan in Progress 0%" and 0 certificates found. At the bottom right of the dialog, there is a "Cancel" button. Below the table, there is a pagination control showing "Page 1", "Rows per page 10", and "1-2 of 2".

DATE	STATUS	SSL CERTIFICATES FOUND
<input type="checkbox"/> 11/09/2021 10:57:51	Successful	51
<input type="checkbox"/> 11/17/2021 00:25:56	Scan in Progress 0%	0

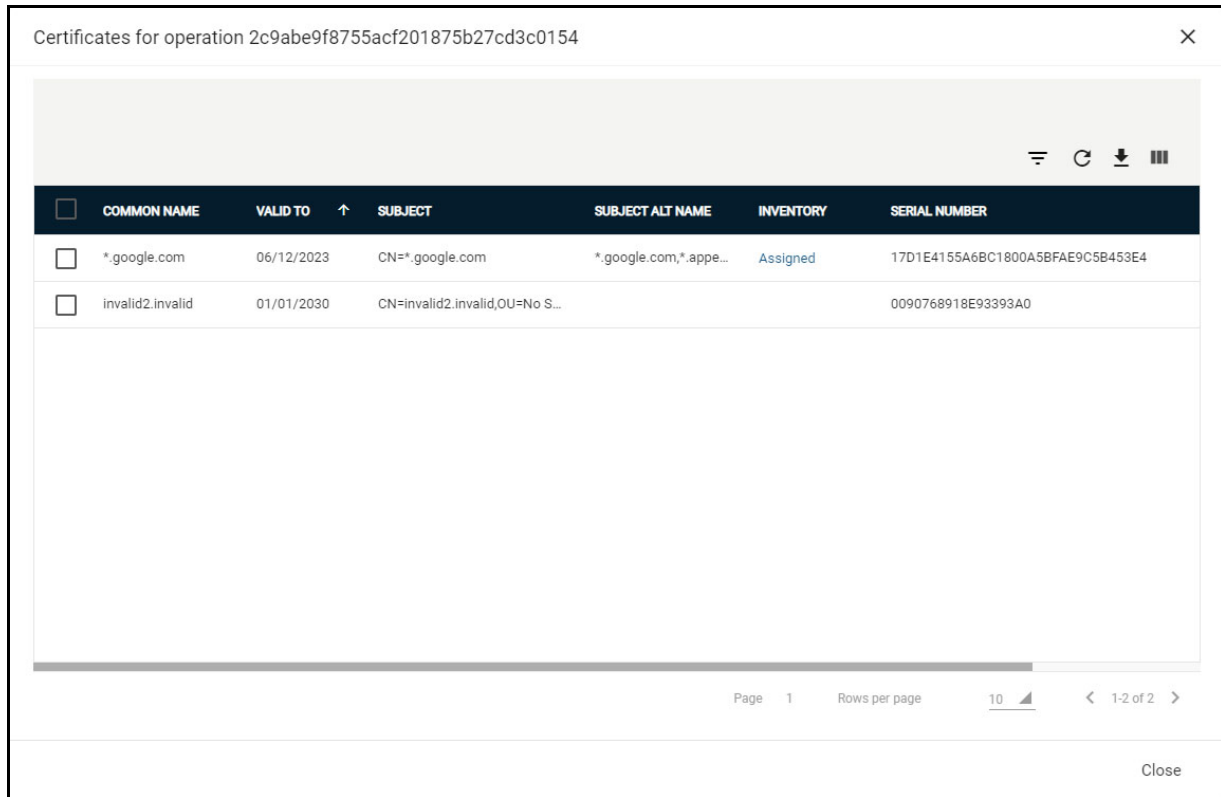
3. Select a network discovery task from the list and click **Details**.
4. Click **Download CSV** to download a report on all scans run for the discovery scan in .csv file format.

The following table describes the information included in the report.

Column	Description
IP Address	The IP address of the server on which the certificate was discovered.
Port	The port on the server on which the certificate was discovered.
Host Name	The name of the server on which the certificate was discovered.
Common Name	The registered domain name for website or domain.
Valid to	The expiry date of the certificate.
Valid from	The issuance date of the certificate.
Key Algorithm	The type of algorithm used for encryption.
Key Size	The key size used by the certificate for encryption.
Signature Algorithm	The type of algorithm used for the signing of the certificate.
Inventory	Indicates whether the certificate is managed, assigned, or external. Clicking Managed or Assigned opens the Certificate Details . Clicking External displays the Assign to Organization/Department dialog.
Found date	Date the certificate was discovered.

To view the list of certificates discovered during a scan, select the scan and click **History** to open the **History of scan** dialog.

To view details of the latest certificates discovered: in the **History of scan** dialog, select the task and click **Details**.



<input type="checkbox"/>	COMMON NAME	VALID TO	SUBJECT	SUBJECT ALT NAME	INVENTORY	SERIAL NUMBER
<input type="checkbox"/>	*.google.com	06/12/2023	CN=*.google.com	*.google.com,*.appe...	Assigned	17D1E4155A6BC1800A5BFAE9C5B453E4
<input type="checkbox"/>	invalid2.invalid	01/01/2030	CN=invalid2.invalid,OU=No S...			0090768918E93393A0

To view the details of scan information in a spreadsheet: click the **Download CSV** icon to download the table in .CSV format.

To view certificate details: select a certificate and click **Details**. For more information, see [“How to view or modify SSL certificate details”](#) on page 24.

To manually assign external certificates to an organization or department: select one or more certificates and click **Assign to**. For more information, see [“Manually assigning certificates to organizations and departments”](#) on page 156.

4.3 Performing AD discovery tasks

The **MS AD Discovery Tasks** page shown in the following illustration enables MRAOs with the MS AD Discovery privilege to configure scans on AD servers which have been integrated with SCM. AD scans locate all certificates installed on servers, devices, and endpoints on active directory domains. Each scan identifies the network or object structure and locates all types of certificates, typically client certificates.

You can add assignment rules to scans to automatically assign external certificates to a specific organization or department.

Typically, the process includes the following:

- Scanning an AD domain in order to find the network object structure, endpoints, user accounts, and all deployed certificates.

- Discovered items are shown in SCM as follows:
 - All discovered managed certificates and external certificates assigned to organizations and departments via an assignment rule are listed under the respective certificate types in the **Certificates** page.
 - All items discovered on the AD domain are shown in the **Certificate Buckets** page, as described in [“How to view certificates via certificate buckets”](#) on page 153, including certificates and artifacts such as devices, user accounts, and endpoints.
- SCM updates the status of existing certificates that were issued using SCM, if required.
- External certificates can become managed via renewal of a particular certificate.

Before attempting to run a scan on an AD domain, ensure that the MS Agent has been installed on the required AD server and the server has been integrated with SCM. See [“MS agents”](#) on page 230 for more information.

It is recommended that you do the following:

- Schedule regular discovery scans.
- Run a manual scan after every change to a certificate configuration. Otherwise, it is possible that the **Certificates** page shows inaccurate information (for example, you may have uploaded a certificate to your website but in SCM the certificate has a state of Issued and a discovery status of Not deployed if you have not run the scan again).
- Run a manual scan after any change to the network in general.

ID	NAME	AGENT	CERTIFICATE BUCKET	STATUS	SCHEDULE	LAST SCANNED
633	admin 21-19-24.2023-04..	Agent60	google.com	Scan in Progress	Semi-Annually	05/29/2023 14:24:00
612	admin 21-04-49.2023-04..	Agent60	google.com		Manual	
611	admin 21-00-58.2023-04..	Agent60	google.com	Scan in Progress	Weekly	06/10/2023 05:06:00
545	Agent92	7.03.23	Agent92		Manual	12/19/2022 10:49:55
544	MS SCAN19	10.16.45.40 pdc 2019	MS SCAN19		Run Once	
543	MS SCAN19	10.16.45.40 pdc 2019	MS SCAN19		Run Once	12/19/2022 15:40:40
542	MS SCAN19	10.16.45.40 pdc 2019	MS SCAN19		Run Once	12/19/2022 15:38:40

The following table lists settings and elements of the **MS AD Discovery Tasks** page.

Field / Element	Description
ID	ID number of the certificate discovery task.
Name	The name of the certificate discovery task.
Agent	The name of the agent that is to be used.
Certificate Bucket	The name of the certificate bucket.
Status	The status of the scan: successful, failed, in progress, or canceled. Clicking the status displays the respective result. For example, clicking Successful displays the number of certificates discovered.

Field / Element	Description
Schedule	Indicates whether the scan is to be run manually or scheduled.
Last Scanned	The date and time of the last scan performed.
Controls	
Add	Enables you to add a new task
Filter	Enables you to sort the table information using custom filters
Group	Enables you to sort the table information into predefined groups
Refresh	Enables you to refresh the page
Download	Enables you to download a file
Columns	Enables you to modify which columns of information appear the table
Discovery Task Controls	
Delete	Enables you to delete the selected discovery task.
Edit	Enables you to edit the selected discovery task.
Scan	Enables you to start a new scan for the selected discovery task.
Cancel	Cancels the selected discovery scan (appears only while scan is in progress).
History	Displays the details of past scans performed for the selected discovery task and enables you to download scan reports.
View Audit	Allows you to see audit events to the selected discovery task.

4.3.1 How to add and modify MS AD discovery tasks

To add or modify a MS AD discovery scan task, do the following:

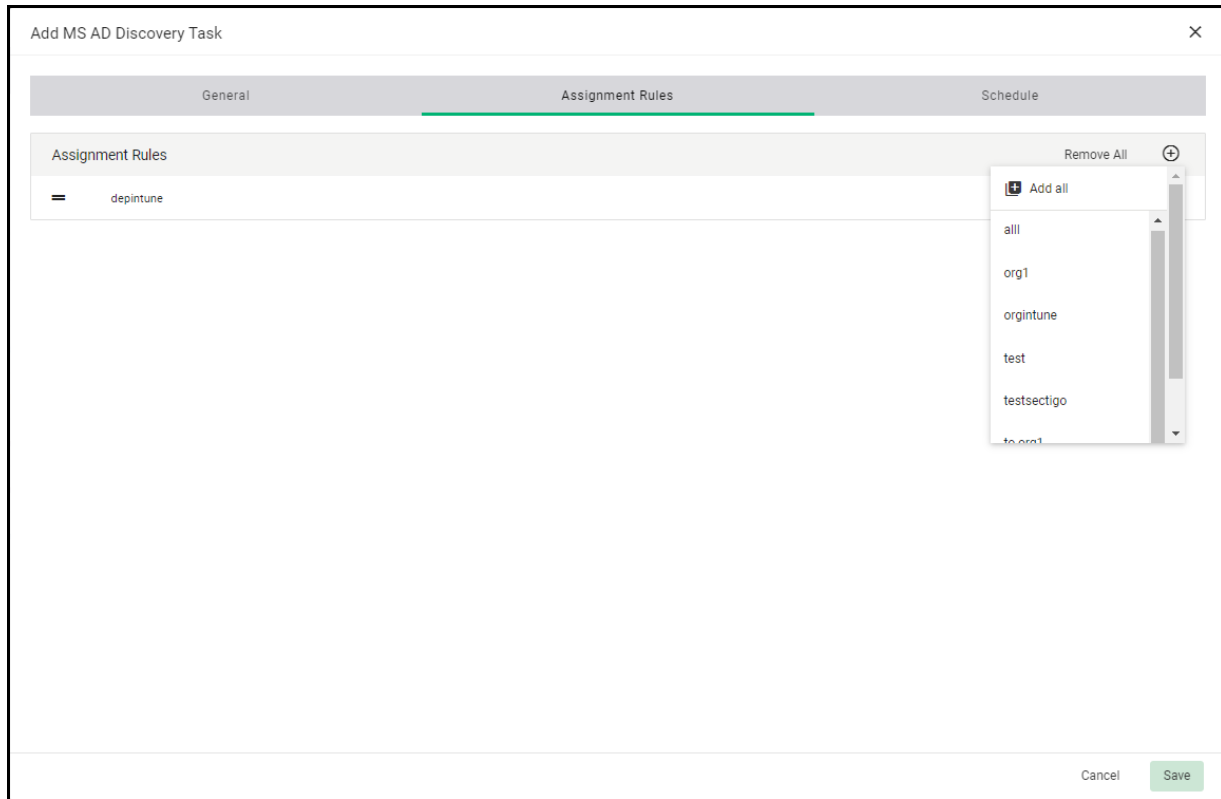
1. Navigate to **Discovery > MS AD Discovery Tasks**.

2. Click **Add** or select a task and click **Edit**.

3. Complete the **Common** settings based on descriptions provided in the following table.

Field	Description
Name	The name to describe the AD discovery task.
Agent	The MS Agent or AD agent cluster to be used for scanning.
Domains to Scan	The names of the AD domains to scan, separated by commas. If nothing is entered, all domains in AD will be scanned.
Max Depth of the Scan	The number of network hierarchy levels to be scanned. The depth of the scan should cover all required endpoints, users, and other AD objects in the network. 0 = Unlimited

4. Complete the **Assignment Rules** settings to add rules which assign external certificates identified by the scan to an organization or department.



- To add a rule to the task, click the Add icon on the right and select the rule from the **Available rules** in the drop-down list.
 - To add all available rules, click **Add > Add all**. To remove all rules, click **Remove All**.
 - To create a new rule, select **Add > New Assignment Rule**. (Rules can also be configured in the **Assignment Rules** page; see [“To view certificate details, select a certificate and click Details.”](#) on page 150.)
5. Complete the **Schedule** settings shown in the following illustration to set the scan day, date and start time, and the frequency of the task.
 Available scan frequencies are Manual (on demand), Run Once, Daily, Weekly, Monthly, Quarterly, Semi-Annually and Annually.
 6. Click **Save**.

Newly created AD discovery tasks are displayed in the **MS AD Discovery Tasks** page.

The screenshot shows a dialog box titled "Add MS AD Discovery Task" with a close button (X) in the top right corner. The dialog has three tabs: "General", "Assignment Rules", and "Schedule". The "Schedule" tab is selected and highlighted with a green underline. The "Schedule" tab contains the following fields:

- Frequency: Weekly
- Day of Week: Sunday
- Time zone: UTC-03:00 - ADT, ROTT, ART, BRT, CLST...
- Time: 04:44 PM
- Next 5 scans:
 - 11/14/2021 21:44:37 UTC+2
 - 11/21/2021 21:44:37 UTC+2
 - 11/28/2021 21:44:37 UTC+2

At the bottom right of the dialog, there are "Cancel" and "Save" buttons.

4.3.2 How to delete AD discovery tasks

To delete an AD discovery task, do the following:

1. Navigate to **Discovery > MS AD Discovery Tasks**.
2. Select the task in the list and click **Delete**.
3. Click **Yes** to confirm.

4.3.3 How to run AD discovery scans

Scans run according to the schedule set for the task, or you can run scans manually. You can run multiple discovery tasks at the same time.

To run a scan, select the discovery task from the list and click **Scan**.

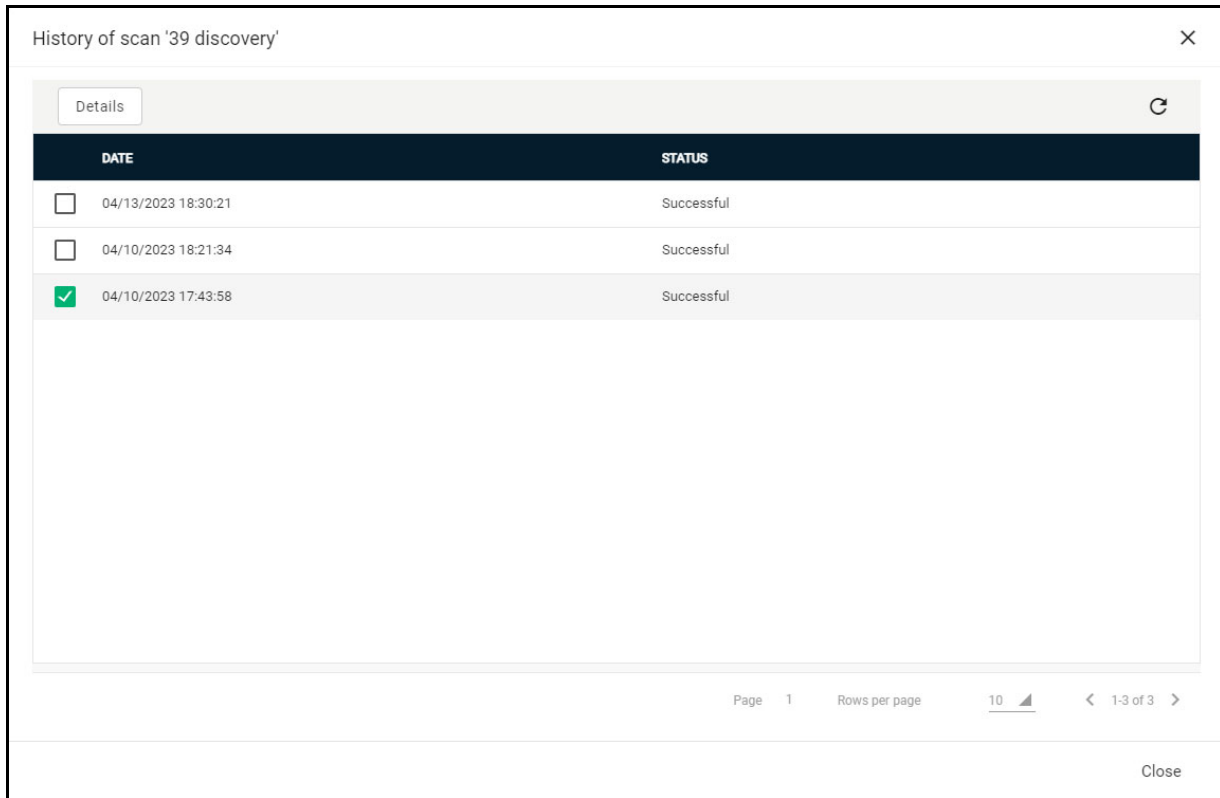
To cancel the scanning process, click **Cancel**, specify the reason in the **Reason** field, and click **Save**.

When a scan is canceled, the system reverts to the state that existed before the scan started (any data collected during scanning cannot be applied until the scanning process is completed).

4.3.4 How to view a history of AD discovery tasks

You can view the results previous scans of each AD discovery task. You can also view details of certificates identified by each scan and assign external discovered certificates to an organization or department.

To view the history of a discovery task, navigate to **Discovery > MS AD Discovery Tasks**, select the task, and click **History** to open the **History of scan** dialog.

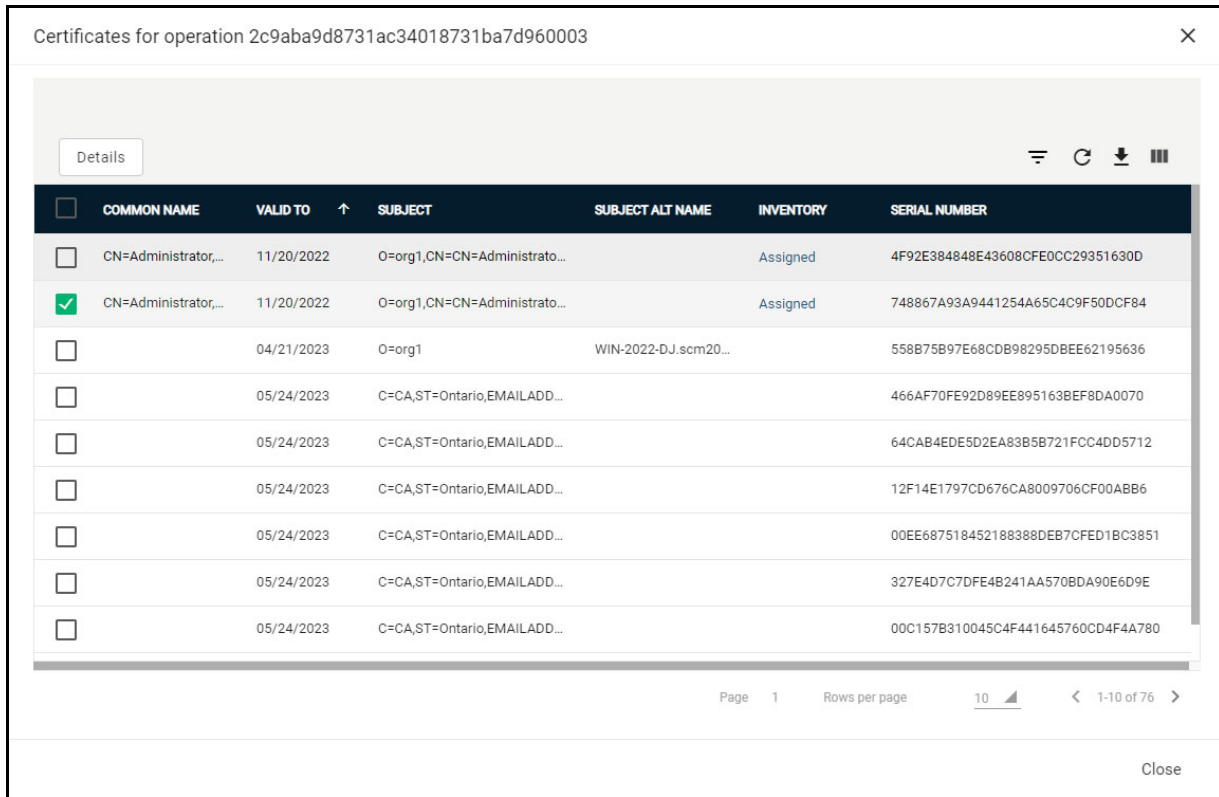


DATE	STATUS
<input type="checkbox"/> 04/13/2023 18:30:21	Successful
<input type="checkbox"/> 04/10/2023 18:21:34	Successful
<input checked="" type="checkbox"/> 04/10/2023 17:43:58	Successful

Page 1 Rows per page 10 1-3 of 3

Close

To view all certificates discovered during the scan, select a scan and click **Details** to open the **Certificates for operation** dialog.



The following table lists settings available in the **Certificates for operation** dialog.

Field/Element	Description
Common Name	The value in the Common Name field of the certificate. This varies according to the certificate type. SSL certificates usually display a domain name. Client certificates may display an email address or host name, and device certificates usually display the host name of the device.
Valid To	The expiry date of the certificate.
Type	The type of certificate, such as SSL, client, code signing, or device.
Status	The current status of the certificate.
Inventory	Indicates whether the certificate is managed or external. Clicking Managed or Assigned opens the Certificate Details . Clicking External displays the Assign to Organization/Department dialog.
Serial Number	The serial number of the certificate, which can be used to identify the certificate.
Key Usage	The cryptographic purposes for which the certificate can be used. For example, key encipherment and signing.
Extended Key Usage	Higher level capabilities of the certificate. For example, web server authentication and client authentication.

Field/Element	Description
Details	Displays details for the selected certificate.
Assign To	Assigns the selected certificate(s) to an organization and department.

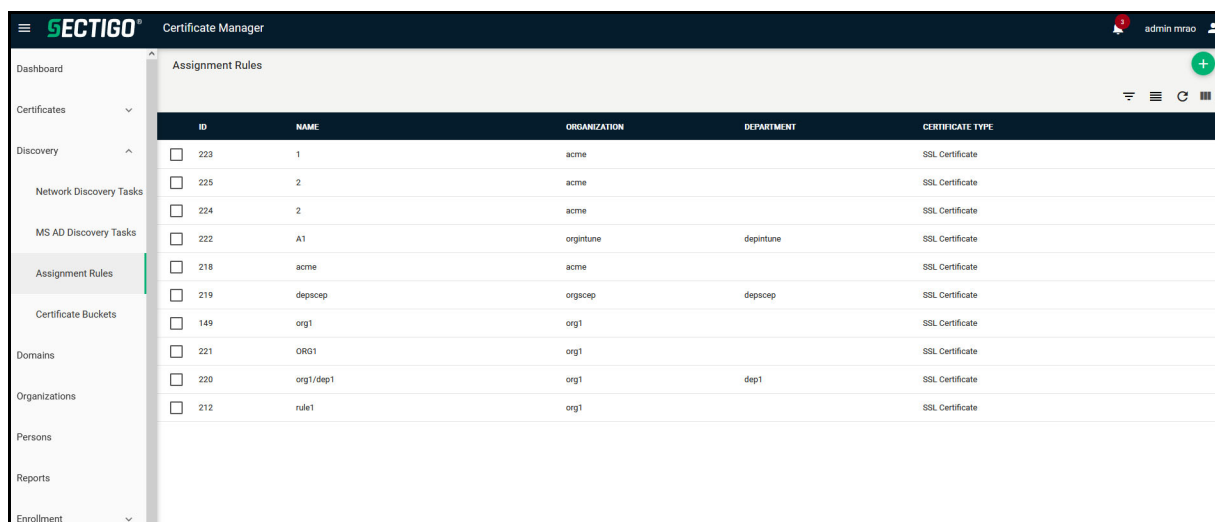
To view the details of scan information in a spreadsheet, click the **Download CSV** icon to download the table in .CSV format.

To view certificate details, select a certificate and click **Details**.

4.4 Managing assignment rules

The **Assignment Rules** page shown in the following illustration enables you to create rules for use in discovery scans. These rules are used to automatically assign external (also known as unmanaged) certificates found after a discovery scan to a specific organization or department. These rules assign certificates to a particular entity based on one or more conditions; the certificates must match all the conditions in the rule in order to be considered a match.

The rules can be applied while configuring network discovery tasks and MS AD discovery tasks, so that each external certificate found by a discovery scan and satisfying conditions in all of the assignment rules is automatically assigned to the respective organizations and departments. For more information, see [“Certificate discovery tasks overview” on page 132](#).



ID	NAME	ORGANIZATION	DEPARTMENT	CERTIFICATE TYPE
<input type="checkbox"/> 223	1	acme		SSL Certificate
<input type="checkbox"/> 225	2	acme		SSL Certificate
<input type="checkbox"/> 224	2	acme		SSL Certificate
<input type="checkbox"/> 222	A1	orgintune	depintune	SSL Certificate
<input type="checkbox"/> 218	acme	acme		SSL Certificate
<input type="checkbox"/> 219	depscep	orgscep	depscep	SSL Certificate
<input type="checkbox"/> 149	org1	org1		SSL Certificate
<input type="checkbox"/> 221	ORG1	org1		SSL Certificate
<input type="checkbox"/> 220	org1/dep1	org1	dep1	SSL Certificate
<input type="checkbox"/> 212	rule1	org1		SSL Certificate

The rules you can set depend on your security role, as follows:

- MRAOs can create and manage rules to assign discovered certificates on any network to any organization and department.
- RAOs SSL can create and manage rules to assign certificates discovered on their networks to organizations and sub-departments which have been delegated to them.

- DRAOs SSL can create and manage rules to assign certificates discovered on their networks to departments which have been delegated to them.

The following table lists settings available in the **Assignment Rules** page.

Column	Description
ID	ID number of the certificate discovery task.
Name	The name of the external certificate assignment rule.
Organization	The name of the organization to which the certificates matching the criteria specified in the rule is to be auto-assigned.
Department	The name of the department to which the certificates matching the criteria specified in the rule is to be auto-assigned.
Certificate Type	The type of certificate
Controls	
Add	Enables you to add a new task
Filter	Enables you to sort the table information using custom filters
Group	Enables you to sort the table information into predefined groups
Refresh	Enables you to refresh the page
Download	Enables you to download a file
Columns	Enables you to modify which columns of information appear the table
Edit	Edits the selected assignment rule.
Delete	Deletes the selected assignment rule.

To create or modify a rule, do the following:

1. Navigate to **Discovery > Assignment Rules**.
2. To create a rule, click **Add**. To modify a rule, select the rule and click **Edit**.

Create New Assignment Rule

Assignment Rule Name *

If certificate discovered meets all conditions below

Conditions Remove All +

Assign to ...

Organization
exporter

Department
None

Cancel Save

3. Enter a description of the rule in the **Assignment Rule Name** field.
4. Set the condition for identifying the certificates to be auto-assigned as per the rule:
 - a. Select the field of the certificate to be searched from the first list.
 - b. Select the relationship between the field value and the condition value from the second list. The relationship can be Matches, Starts With, Ends With, Contains, or Match Regex. Use Match Regex to enter a condition value using regular expressions.
 - c. Enter the condition value in the text field.

For example, to auto-assign certificates with common name dithers.com, select Common Name from the first list, select Matches from the second list, and enter dithers.com in the text field.

To add or remove conditions, use the Plus and Minus buttons.

NOTE: Conditions are added on an AND basis; that is, for a certificate to match, it must satisfy *all* the conditions in the assignment rule.

5. Choose the organization and optional department to which the certificates meeting all the conditions are to be auto-assigned using the respective **Assign to** lists.
6. Click **Save**.

The rule is added to the list and is available for selection while configuring a discovery task. To remove a rule, select the rule, click **Delete**, and confirm by clicking **Delete** in the opened confirmation dialog.

4.5 Managing certificate buckets

The **Certificate Buckets** page allows you to view a summary of the found certificates installed on every scanned network. You can also configure automatic assignment using rules, or manual assignment to organizations/departments.

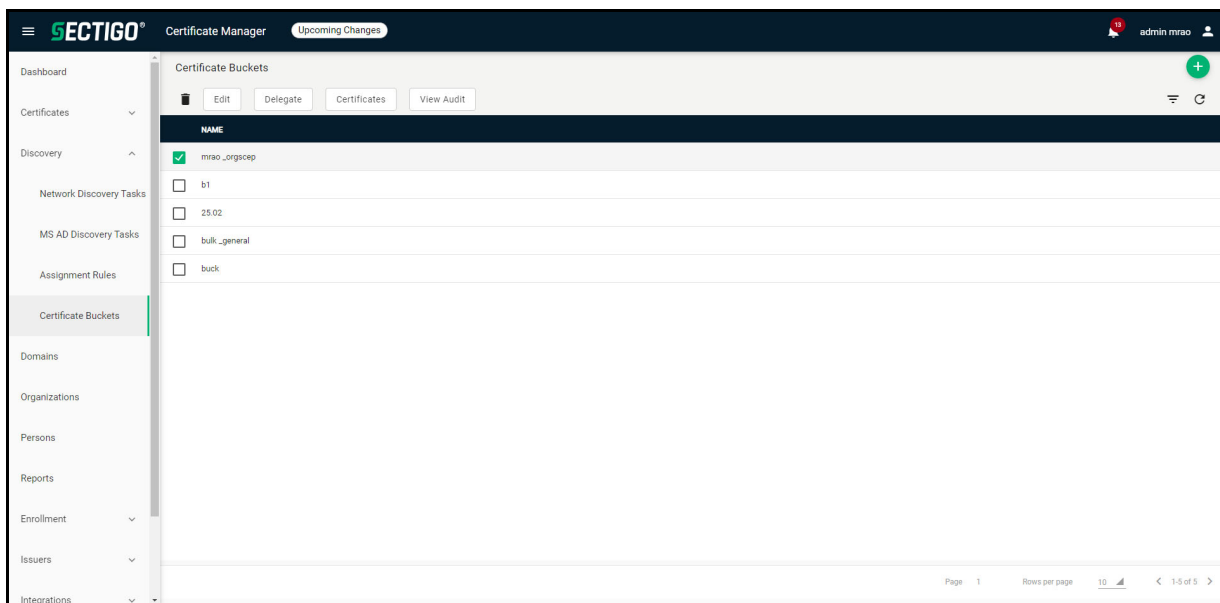
MRAOs can view certificates installed on all networks on which the network discovery scans were run.

RAO SSL can view certificates installed on networks of organizations and their departments that have been delegated to these administrators.

DRAO SSL can view the certificates installed on networks of departments that have been delegated to these administrators.

4.5.1 How to view certificates via certificate buckets

To view a summary of the certificates installed on all scanned networks, navigate to **Discovery > Certificate Buckets > Certificates**.



The following table lists settings and elements of the **Certificate Buckets** page.

Field / Element	Description
ID	The bucket ID number
Name	The name of the certificate bucket
Delegation Mode	How the bucket is delegated
Controls	

Field / Element	Description
Add	Adds a new certificate bucket
Filter	Enables you to sort the table information using custom filters
Refresh	Enables you to refresh the page
Certificate Buckets Controls	
Delete	Enables you to delete the selected certificate bucket
Edit	Enables you to edit the selected certificate bucket
Delegate	Enables you to delegate existing certificate buckets to organizations and departments
Certificates	Enables you to assign the selected certificates to the certificate bucket organizations and departments
View Audit	Allows you to see audit events to the selected certificate buckets

4.5.2 How to add and modify certificate buckets

To add or modify a certificate bucket, do the following:

1. Navigate to **Discovery > Certificate Buckets**.
2. Click **Add** or select a task and click **Edit**.

The screenshot shows a modal dialog box titled "Add Certificate Bucket". It contains a text input field for "Name *". Below this is a section titled "General" with a dropdown arrow. Underneath the "General" section, there is a note: "This certificate bucket will be available for all existing organizations." At the bottom right of the dialog, there are two buttons: "Cancel" and "Next".

3. Enter a name to describe the bucket.
4. Select the **General** or **Customized** type.

5. Select the organizations and domains from the list and click **Next**.

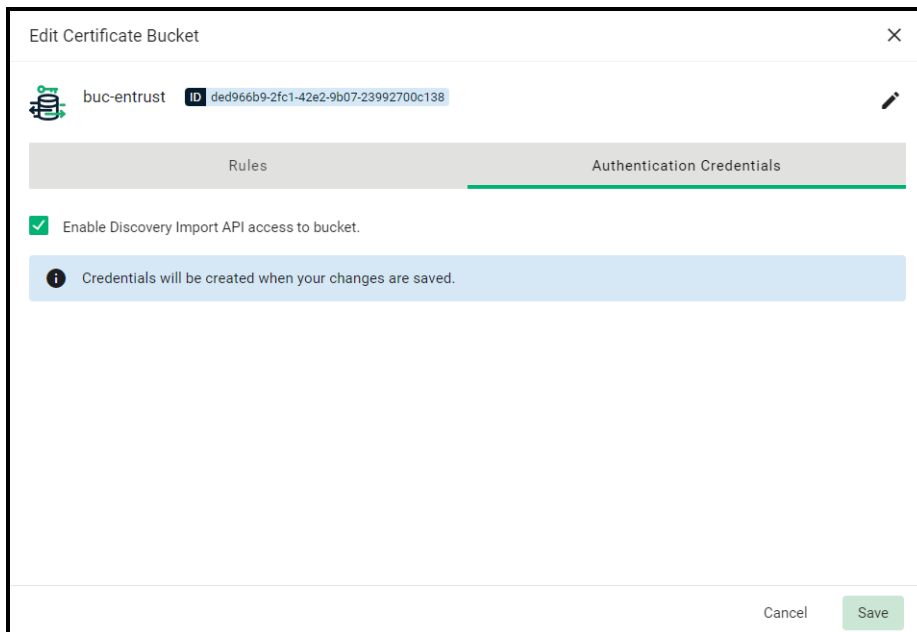
To add a rule to the certificate bucket, click the **Add** icon and select it from the list or create a new rule. For more information, see ["To view certificate details, select a certificate and click Details."](#) on page 150.

6. Click **Save**.

4.5.2.1 How to manage authentication credentials in certificate buckets

To enable the authentication credentials:

1. Navigate to **Discovery > Certificate Buckets**.
2. Select the bucket and click **Edit**.
3. Navigate to the **Authentication Credentials** tab.
4. Select the **Enable Discovery Import API access to bucket** checkbox.
5. Click **Save**.



6. Copy and save the **Client Secret** and **Client ID**.
7. Click **Close**.

4.5.2.1.1 How to manage Client Secret

To reset the client secret:

1. Navigate to **Discovery > Certificate Buckets**.
2. Select the bucket and click **Edit**.
3. Navigate to **Client Secret** on the **Authentication Credentials** tab and click **Edit**.
4. In the **Reset Secret** dialog click **OK**.

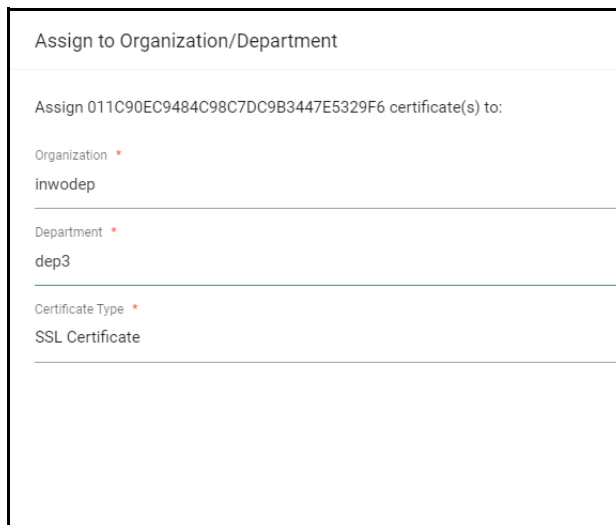
4.5.2.2 Manually assigning certificates to organizations and departments

Discovered managed certificates (issued via SCM) are preassigned to their respective organizations or departments specified during their enrollment setup process. External certificates that are found installed on the network by network discovery scans are assigned to organizations and department according to the assignment rules added to the task. See [“How to add and modify network discovery tasks” on page 135](#).

Certificates that fail to match the assignment rules are not assigned to an organization or department, and will not appear in the **Certificates > SSL Certificates** page. You can manually assign these certificates to organizations and departments.

To manually assign certificates to organizations and departments, do the following:

1. Navigate to **Discovery > Certificate Buckets**.
2. Select a certificate bucket and click **Certificates** to access a list of certificates installed on the network.
3. Select one or more external certificates from the list and click **Assign To** to open the **Assign to Organization/Department** dialog.



Assign to Organization/Department

Assign 011C90EC9484C98C7DC9B3447E5329F6 certificate(s) to:

Organization *
inwodep

Department *
dep3

Certificate Type *
SSL Certificate

4. Use the **Assign To** field to specify the organization and, optionally, department to which the certificate(s) should be assigned.
5. Click **Save**.

Once assigned, the certificates appear in the **Certificates > SSL Certificates** page.

4.5.2.3 How to export MS AD discovery tasks and certificates to CSV from the certificate buckets

To download the table in .csv format, do the following:

1. Navigate to **Discovery > Certificate Buckets**.
2. Select a certificate bucket and click **Certificates**.
3. Select one or more certificates and click the **Download CSV** icon.

Certificates for bucket 10.04.01 X

Run Rules

☰ ↻ ⬇️ ☰

<input type="checkbox"/>	COMMON NAME	VALID TO	SUBJECT	SUBJECT ALT NAME	INVENTORY	SERIAL NUMBER
<input checked="" type="checkbox"/>	WIN-2019-PDC	11/26/2022	CN=WIN-2019-PDC,DC=com,...			5200000003CD3CF25D99E7DC8700000000003
<input type="checkbox"/>	WIN-2019-PDC	11/26/2022	CN=WIN-2019-PDC,DC=com,...			520000000564E14A21DF5F520E00000000005
<input type="checkbox"/>	WIN-2019-PDC	11/26/2022	CN=WIN-2019-PDC,DC=com,...			5200000007A6EE48C97E63442700000000007
<input type="checkbox"/>	WIN-2019-PDC	11/26/2022	CN=WIN-2019-PDC,DC=com,...			520000000A9D0950BACA02F3CA0000000000A
<input checked="" type="checkbox"/>	Users,Administrator	12/02/2022	CN=Users,CN=Administrator,...		Assigned	5200000009340AF07ED6B3761C00000000009
<input type="checkbox"/>	Users,Administrator	12/08/2022	CN=Users,CN=Administrator,...			520000000D9335FE4848895D745000000000D
<input type="checkbox"/>	Users,Administrator	12/08/2022	CN=Users,CN=Administrator,...		Assigned	520000000E5575766ECAF30730000000000E
<input type="checkbox"/>	Users,Administrator	12/09/2022	CN=Users,CN=Administrator,...		Assigned	52000000196AECB12B50B74AD0000000000019
<input type="checkbox"/>	WIN-2019-PDC	12/09/2022	CN=WIN-2019-PDC,DC=com,...			5200000032C68B55545C54F40300000000032

Page 1 Rows per page 10 1-10 of 603

Close

Configuring organizations and domains

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the organizations and domains can now be found in the following locations:

- [Understanding organizations and departments](#)
- [Understanding domains](#)

Generating reports

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the reports can now be found in the following location:

- [Reports](#)

Managing enrollments

The **Enrollment** section allows you to configure all things required to enroll for a certificate, whether that is a manual enrollment or using an enrollment endpoint.

This chapter describes the following topics:

- Certificate Profiles
- Bulk SSL
- Enrollment Forms
- ACME
- SCEP
- EST
- REST
- MS AD Certificate Template Mapping

7.1 How to manage certificate profiles

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the certificate profiles can now be found in the following location:

- [Certificate profiles](#)

7.2 Bulk enrollment of SSL certificates

The bulk enrollment form enables you or applicants that you direct to the request form to order SSL certificates in bulk. Applicants using this method must validate their application for the certificate as follows:

1. By entering the appropriate access code for a **Bulk Enrollment Web Form** enrollment endpoint account. The access code is a combination of alpha and numeric characters that the applicant needs to provide in order to authenticate the request to SCM.
2. By entering an email address from the domain for which the certificate application is being made. This domain must have been delegated to the organization or department assigned to the **Bulk Enrollment Web Form** enrollment endpoint account.

Bulk enrollment must be authorized for your account by your Sectigo account manager.

7.2.1 Submitting bulk SSL requests

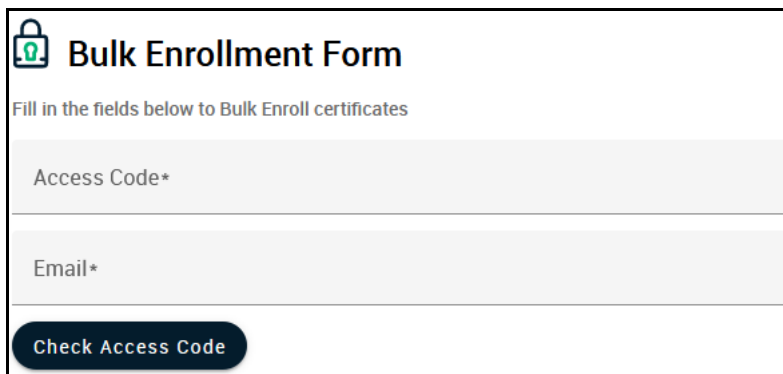
To submit bulk enrollment requests (BER), the following conditions must be met:

- The data for the BER is structured correctly in CSV format. Use a software application such as Microsoft Excel or LibreOffice Calc to generate a `.csv` file containing a list of certificates. For information on how to structure `.csv` files for importing multiple SSL certificates, see [Appendix A: CSV import format requirements](#).
- The requester must be authorized under a domain that can submit SSL requests under the organization or department of the Bulk Enrollment Web Form enrollment endpoint account whose access code was specified on the **Bulk Enrollment Form**. See .
- The organization or department must have at least one domain delegated to it, with the SSL certificate type permitted. You can verify this by navigating to **Organizations**, selecting the organization to which the bulk enrollment requester belongs, and clicking **Domains**. See .
- The organization or department under which bulk requests are to be submitted cannot have the **Make External Requester Mandatory** option selected. See .
- A PKS agent must be installed on your local network and connected to SCM. You can verify this by navigating to **Settings > Private Key Store**; if the connection has been established, the **Agent Status** is **Connected**. Information about the PKS agent can now be found [here](#).
- There must be no active custom fields made mandatory for the enrollment form.

After completing initial steps, you have to provide the enrollment details to the requester using an out-of-band communication, such as email. The communication must contain the following information:

- A link to the bulk enrollment form in the default format of `https://cert-manager.com/customer/<customer_uri>/bulkenroll`.
- The access code specified for the Bulk Enrollment Web Form enrollment endpoint account.

Accessing the link displays the **Bulk Enrollment Form** shown in the following illustration.



The screenshot shows a web form titled "Bulk Enrollment Form" with a lock icon. Below the title is the instruction "Fill in the fields below to Bulk Enroll certificates". There are two input fields: "Access Code*" and "Email*". At the bottom of the form is a dark blue button labeled "Check Access Code".

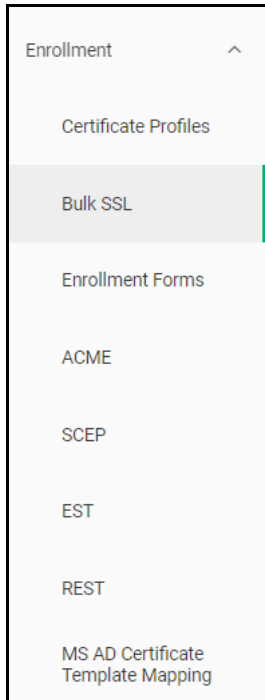
To access the full form, the applicant must enter the access code and an email address from a domain delegated to the organization or department of the enrollment endpoint account, and click **Check Access Code**. If both the access code and email address are successfully validated, the full enrollment form shown in the following illustration is displayed.

The following table describes the bulk self-enrollment form fields and elements. Mandatory fields are marked with an asterisk on the form.

Field	Description
Access Code	The access code for the SSL Web Form enrollment endpoint account that you conveyed to the applicant.
Email	The email address of the applicant. The address must be for a domain that has been assigned to the organization or department of the enrollment endpoint account.
p12 passphrase	A password to protect the certificates enrolled by auto-generation of CSR by SCM and whose keys are managed by PKS. This password is required to import the certificates onto the server after downloading the certificate in .p12 format.
Key size	The key size to use for the private keys of the certificates (default is 2048 bit).
CSV File	The CSV file containing the data for the BER.
Submit	Submits the application and enrolls the new bulk certificate request.

7.2.2 Managing bulk SSL requests

Once the form is submitted, the request is displayed in the **Bulk SSL** page accessible by navigating to **Enrollment > Bulk SSL**.



The following table describes the elements of the **Bulk SSL** page.

Field	Description
Organization	The organization for which the certificates are being requested
Department	The department for which the certificates are being requested
Status	The Status of the bulk request. Can be one of the following: <ul style="list-style-type: none"> • Awaiting Approval • Approving—One or more certificate requests in the BER have been approved • Approved—The BER has been approved • Declined—The BER has been declined • Failed—The BER has failed • Successful—All certificate requests in the BER have been finalized.
Edit	Enables you to modify the algorithm and key size to use for generating certificate keys of the selected BER. Only available for requests with a status of Awaiting Approval.
Approve	Enables you to approve the selected BER. Only available for requests with a status of Awaiting Approval.
Decline	Enables you to decline the selected BER. Only available for requests with a status of Awaiting Approval.

Field	Description
Details	Opens the Bulk Certificate Requests dialog where you can view the certificate requests and, for certificate requests that have a status of Awaiting Approval, approve or decline individual requests.
Resend Notification	Resends the notification to the requester that the bulk request has been approved. Only available for BERs with a status of Successful.

Before taking effect, the request has to be verified. That is, each of its Single Certificate Requests (SCRs) have to be either approved or declined in whole or in part by a MRAO, RAO, or DRAO of the organization or department under which the request has been submitted.

Each BER, as well as its SCRs and the individual certificate requests (ICR) corresponding to these SCRs, has a set of applicable statuses that succeed one another throughout the bulk enrollment processing which consists of the following stages:

1. **Post-submission:** a request is submitted and appears in the **Bulk SSL** page. A BER can be modified at this stage.
2. **Approval:** bulk enrollment is either approved or declined in whole or in part by a MRAO, RAO, or DRAO.
3. **Consideration:** for each approved SCR, an ICR is created with a status of Requested and is accessible via **Certificates > SSL Certificates**. These requests do not have to be approved.

The status of each SCR does not change until the status of its corresponding ICR is finalized (becomes Issued, Invalid, or Rejected). Once finalized, the corresponding SCR status is finalized.

Since SCRs of a BER can be approved separately, the Approval and Consideration stages may overlap. Typically, a request can reach the Consideration stage only if it has not been declined by the MRAO, RAO, or DRAO during the Approval stage, as long as at least one SCR for the request has been approved. Therefore, although some SCRs in a BER may have already been issued certificates or have been deemed invalid (after having been considered by the MRAO, RAO, or DRAO and had their status finalized), others may be newly-approved or still awaiting approval, placing them just before the Consideration stage. If an SCR is declined at the Approval stage, it cannot pass from Approval to Consideration.

4. **Conclusion:** once all SCRs in a bulk enrollment request are finalized, the request is finalized and the issued certificates are available for download.

To monitor the status of a BER, navigate to **Enrollment > Bulk SSL**, select the request, and click **Details**.

The following table describes how the status of the BER, the SCRs, and their corresponding ICRs change at each stage of the process.

BER Stage	Status of BER	Status of SCR Within the Request	Status of ICR of Approved SCR	Interdependency Between BER Status, its SCRs, and Corresponding ICRs
Post-submission	Interim status: Awaiting Approval	Interim status: Awaiting Approval	N/A	BER and all of its SCRs have Awaiting Approval status.
Approval	Interim status one of: Awaiting Approval, Approving, Approved Final status one of: Declined, Failed	Interim status one of: Awaiting Approval, Approved Final status one of: Declined ^a , Failed	N/A	<ul style="list-style-type: none"> At least one SCR in this BER is Awaiting Approval: the status of the entire BER is Awaiting Approval. The entire BER has been approved in one action (even if some of its SCRs have been declined) and it takes time to execute the related updates: status of the BER becomes Approved. All SCRs in the BER have been approved or declined (i.e., they have status of Approved or Declined), and at least one SCR has status of Approved, and the related updates have been completed: the status of the BER becomes Approved. All SCRs of the BER in whole or in part have status of Declined: the status of BER becomes Declined; the BER cannot proceed any further. All SCRs in the BER have Failed status (did not pass validation): the status of the BER is Failed; the BER cannot proceed any further.
Consideration	Interim status one of: Awaiting Approval, Approving, Approved	Interim status: Approved Final status one of: Failed, Issued, Declined	Interim status one of: Requested, Applied Final status one of: Issued, Invalid, Rejected	<p>Changes in status of SCRs and ICRs at this stage have no influence over the status of the BER.</p> <ul style="list-style-type: none"> The SCR is Approved so a corresponding ICR is created with initial status of Requested: the status of its SCR remains Approved. The status of ICR is changed from Requested to Applied: the status of its SCR remains Approved. The status of ICR is changed from Requested or Applied to Invalid or Rejected: the status of its SCR becomes Failed. The status of ICR is changed from Applied to Issued: the status of its SCR becomes Issued.

- a. Declined is a final status of an SCR designated at the Approval stage and no ICR is created for these SCRs. These SCRs do not pass to the Consideration stage and remain in the Declined status until the end of the BER process.

The rest of the validation steps are the same as performed during the creation of a new SSL request. Once all the SCRs included in the BER have been processed, an email with links is sent to the requester allowing them to download certificates issued as part of this bulk enrollment. The links expire after two days. If the certificates are not downloaded within this time frame, navigate to **Enrollment > Bulk SSL**, select the request, and click **Resend Notification**.

Notifications are sent to the bulk enrollment requester using email templates as described in the following table.

Email Template Name	Timeline	Method
SSL Bulk Awaiting Approval	Bulk enrollment submitted.	Emailed to the MRAO, owner, or requester, if configured.
SSL Bulk Enroll Completed	Bulk enrollment has attained final status other than Declined.	Automatically emailed to the address specified by the requester during bulk enrollment submission.

The notification emails include details for each SCR in the request. Notifications can be customized by navigating to **Settings > Notifications**. See [“Configuring notifications” on page 235](#).

The body and title of the notification emails can be customized by the MRAO by navigating to **Settings > Notification Templates**. See [“Configuring notification templates” on page 235](#).

7.3 How to map MS AD certificate templates to SCM

As part of our ongoing efforts to improve our documentation, the content about mapping MS AD certificate templates previously covered in this chapter has been moved online.

Information about mapping MS AD certificate templates can now be found in the following location:

- [Mapping MS AD certificate templates](#)

7.4 Configuring enrollment endpoints

The **Enrollment** pages enable you to configure the endpoints used by external users and services to enroll certificates.

Endpoints can be the following types:

- Self-enrollment form endpoints:
 - **Client** certificate self-enrollment form—connects to the shared self-enrollment form for enrolling client certificates.
 - **Code Signing** self-enrollment form—connects to the shared self-enrollment form for enrolling SSL certificates.
 - **SSL** self-enrollment form—connects to the shared self-enrollment form for enrolling SSL certificates.

- **Device** certificate self-enrollment form—connect to self-enrollment forms for enrolling device certificates.
- Bulk enrollment form endpoint—connects to the shared bulk SSL enrollment form.
- SCEP endpoints:
 - Client certificate SCEP—for enrolling client certificates using SCEP.
 - Device certificate SCEP—for enrolling device certificates using SCEP.
 - Client certificate Intune SCEP—for enrolling client certificates using SCEP via Intune.
 - Device certificate Intune SCEP—for enrolling device certificates using SCEP via Intune.

For information on configuring Intune SCEP endpoints, see .

- ACME endpoints:
 - Sectigo Public ACME—connects to the public ACME service to enroll and manage SSL certificates.
 - Universal ACME—connects to the private ACME service that is connected to a Private CA and uses private trust level certificate profiles for enrolling and managing SSL certificates.

For information on configuring ACME server endpoints, see .

- EST endpoints:
 - Client certificate EST—for enrolling client certificates using EST.
 - Device certificate EST—for enrolling device certificates using EST.
 - SSL EST—for enrolling SSL certificates using EST.
- REST endpoints:
 - Client certificate REST—for enrolling client certificates using REST API.
 - Code Signing certificate REST—for enrolling code signing certificates using REST API.
 - Device certificate REST—for enrolling device certificates using REST API.
 - SSL certificate REST—for enrolling SSL certificates using REST API.

NOTE: All types of the listed endpoints available depend on the features that have been enabled for your account.

NAME	URL	TYPE
<input type="checkbox"/> IDP_DEVICE_NEW	https://comqa.com/customer/testscep/device/zPLR-dvKtJ3CcQvMawvF	Device certificate self-enrollment form
<input type="checkbox"/> scepwdep Device Web Form 4428	https://comqa.com/customer/testscep/device/device	Device certificate self-enrollment form
<input type="checkbox"/> ldp_device	https://comqa.com/customer/testscep/device/Au4B9kYq9f0Mgns8MMo	Device certificate self-enrollment form
<input type="checkbox"/> depintune Device Web Form 4430	https://comqa.com/customer/testscep/device/intunedep	Device certificate self-enrollment form
<input type="checkbox"/> orgintune Device Web Form 4429	https://comqa.com/customer/testscep/device/intune	Device certificate self-enrollment form
<input type="checkbox"/> NewName	https://comqa.com/customer/testscep/smime/CS5pW4sRD9gCHUKIV6c	Client certificate self-enrollment form
<input type="checkbox"/> Client Certificate Web Form	https://comqa.com/customer/testscep/smime	Client certificate self-enrollment form
<input type="checkbox"/> IDP	https://comqa.com/customer/testscep/smime/s1z-CLRDLJ4Dcyx78e1	Client certificate self-enrollment form
<input checked="" type="checkbox"/> Client	https://comqa.com/customer/testscep/smime/UWA50lvIC1gmkiH9j60A	Client certificate self-enrollment form
<input type="checkbox"/> EnrollmentTest1	https://comqa.com/customer/testscep/ssl/mLj6439LLBckX1YkDQzF	SSL self-enrollment form

The following table lists settings available in the **Enrollment** pages.

Column	Description
Name	The name of the endpoint.
URL	The URL where the endpoint can be accessed.
Type	The type of endpoint. May be one of the following: <ul style="list-style-type: none"> • Client certificate Intune SCEP • Client certificate SCEP • Client certificate self-enrollment form • Client certificate EST • Client certificate REST • Code Signing certificate REST • Device certificate Intune SCEP • Device certificate SCEP • Device certificate self-enrollment form • Device certificate EST • Device certificate REST • Universal ACME • Sectigo Public ACME • SSL certificate Bulk enrollment • SSL certificate self-enrollment form • SSL certificate EST • SSL certificate REST
Add	Enables you to add SSL, Client, Device, and Code Signing certificate self-enrollment form endpoints.
Edit	Enables you to modify settings for the selected endpoint.
Delete	Deletes the selected type of the certificate self-enrollment form endpoint.
Accounts	Opens the account configuration for the selected shared endpoint.
View Audit	Allows you to see audit events to the selected enrollment endpoint.

7.4.1 Creating and modifying enrollment form endpoints

To create and manage enrollment form endpoint accounts, navigate to **Enrollment > Enrollment Forms**.

The following table lists settings available in the enrollment forms page:

Field / Element	Description
Name	A descriptive name for the endpoint.
Type	The type of endpoint to add. Options include the Device certificate self-enrollment form. This option is only available when adding an endpoint.
Edit	Allows you to edit the name of the endpoint
Details	
URI Extension	The URI extension of the form. The URI extension is appended to the URL to create a unique URL for the endpoint. The URL of the enrollment form is automatically shown below the URI extension field. This URL should be passed to applicants so they can access the form.
Generate	Generates a unique URI extension for the endpoints
Configuration	
Authentication Types	Authentication methods available for the certificate enrollment: <ul style="list-style-type: none"> • Email Confirmation • Identity Provider (IdP)^a • Secret ID^b
Enrollment Form Help	The text that is displayed on the self-enrollment page to provide additional information or direction to users. Maximum 2048 characters.
URL Address	The URL to which the text links.
URL Link Text	The link text to be displayed on the self-enrollment page. When an end-user clicks the link, they are redirected to the URL specified in the Help Link Target field.

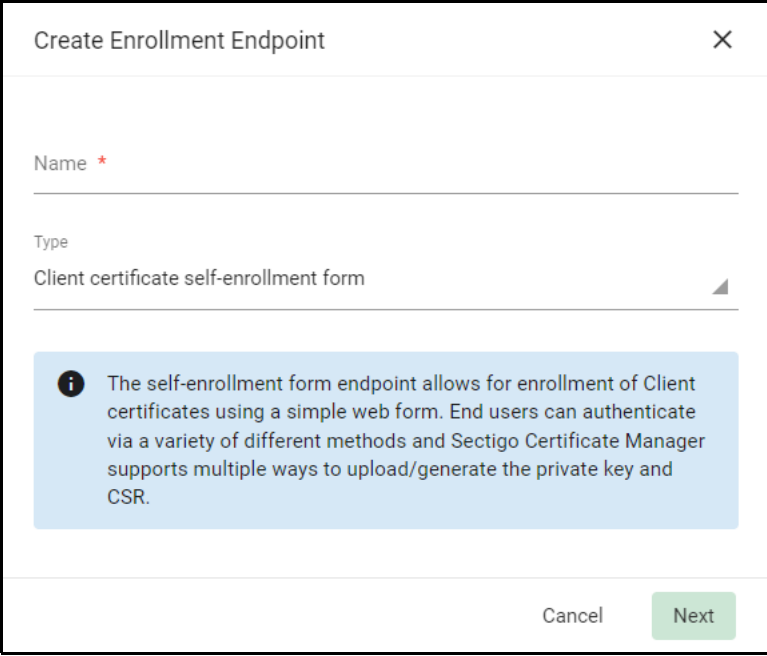
a. Available only for SSL, Client, Device Certificates.

b. Available only for Client Certificates.

To add or modify an Enrollment form endpoints for **SSL, Client, Device, and Code Signing Certificates**, do the following:

1. Navigate to **Enrollment > Enrollment Forms** and click **Add (+)**.
2. In the **Create Enrollment Endpoint** window, enter a name for the **New Enrollment Endpoint**.

3. Select the appropriate self-enrollment form.



Create Enrollment Endpoint

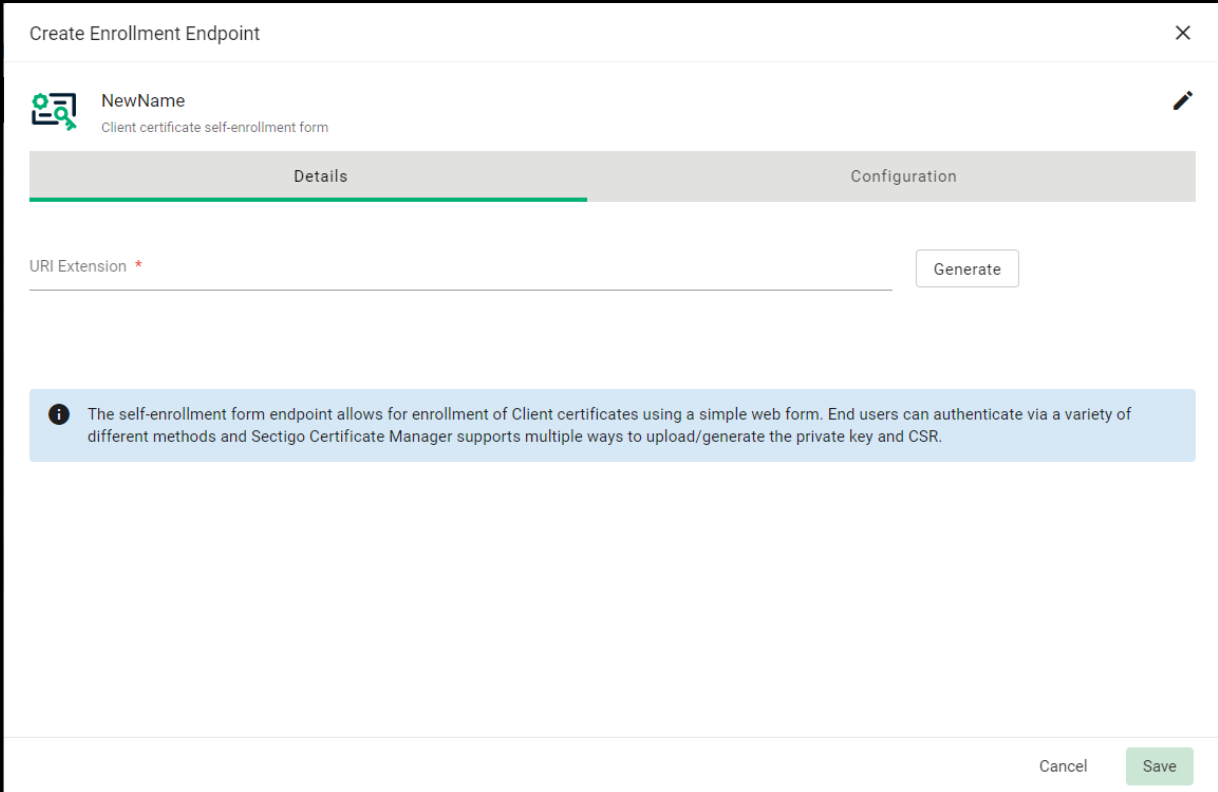
Name *

Type
Client certificate self-enrollment form

i The self-enrollment form endpoint allows for enrollment of Client certificates using a simple web form. End users can authenticate via a variety of different methods and Sectigo Certificate Manager supports multiple ways to upload/generate the private key and CSR.

Cancel Next

4. Click **Next**.
5. In the **Details** tab, click **Generate** to generate the URI extension.



Create Enrollment Endpoint

NewName
Client certificate self-enrollment form

Details Configuration

URI Extension * Generate

i The self-enrollment form endpoint allows for enrollment of Client certificates using a simple web form. End users can authenticate via a variety of different methods and Sectigo Certificate Manager supports multiple ways to upload/generate the private key and CSR.

Cancel Save

NOTE: The value generated for the URI extension can be distributed to the end users via group policy or through automated scripts that load it

in the browser on the end user's system to invoke the certificate creation flow.

6. In the **Configuration** tab, select the appropriate Authentication Type(s) for your requirements/setup.

The screenshot shows a 'Create Enrollment Endpoint' dialog box with a 'Configuration' tab selected. The dialog has a title bar with a close button (X) and a 'New test' icon. Below the title bar, there are two tabs: 'Details' and 'Configuration'. The 'Configuration' tab is active and shows the following options:

- Authentication Types:**
 - Email Confirmation
 - Identity provider
 - Secret ID
- Enrollment Form Help:**

This instructions will be displayed to the user in the web form during enrollment.

Help Instructions

- Link to external website for additional instructions:**

URL Link Text

URL Address

At the bottom right of the dialog, there are 'Cancel' and 'Save' buttons.

7. Click **Save**.
8. Create an account. For information on configuring web form accounts, see .
9. Select an existing client certificate enrollment form and copy the URL for the endpoint.
10. Open a browser and paste the client enrollment endpoint URL.

Depending on the authentication type(s) selected during the account creation, an authentication page will appear with selected options.
11. Complete the authentication and download the certificate.

7.4.2 Certificate enrollment authentication types

The Sectigo self-enrollment supports the following authentication types for the certificate enrollment:

- SSL certificate
 - Email
 - Identity Provider (IdP)
- Client certificate
 - Email
 - Identity Provider (IdP)

- Secret ID
- Device certificate
 - Email
 - Identity Provider (IdP)
- Code Signing certificate
 - Email

NOTE: IdP authentication is done via SAML. Customer is expected to configure the IdP assertion details with Sectigo backend for service access upon successful authentication.

7.4.3 Adding and modifying web form accounts

To create and manage enrollment form endpoint accounts, navigate to **Enrollment > Enrollment Forms**, select the appropriate enrollment form, and click **Accounts**.

This displays the **SSL, Device, Client, or Code Signing Certificate Web Form Accounts** dialog, which lists the accounts that have been configured for the selected endpoint. The **Client Certificate Web Form Accounts** dialog is shown in the following illustration.

RAO and **DRAO** administrators can only create and modify Web Form accounts for organizations and departments that are delegated to them.

Client Certificate Web Form Accounts

✕

+

🗑️ Edit View Audit ⌵ ↻

	NAME	ORGANIZATION	DEPARTMENT
<input type="checkbox"/>	Client	inwodep	
<input checked="" type="checkbox"/>	Client	org1	

Page 1 Rows per page 10 1-2 of 2

Close

The following table lists settings available in the certificate web form accounts dialog.

Column	Description
Name	The name of the web form account
Organization	The organization for which the web form account serves as endpoint
Department	The department for which the web form account serves as endpoint
Add	Adds a new account
Edit	Edits the selected account
Delete	Deletes the selected account
View Audit	Allows you to see audit events to the selected web form account

To add or modify a Web Form account, do the following:

1. Navigate to **Enrollment > Enrollment Forms**, select the Enrollment Form endpoint.
2. Click **Accounts**.
3. To add an account, click **Add** on the Web Form Accounts dialog.

The **Create Client Certificate Web Form Account** dialog is shown in the following illustration.

To edit an account, select the account and click **Edit**.

4. Complete the fields based on the information in the following table, and then click **Save**.

Field / Element	Description
Name	A descriptive name for the account.
Organization	The organization associated with the account. End-users enrolling certificates using this account must have an email from a domain delegated to this organization. Once an account is created, the organization cannot be changed.
Department	The department associated with the account. End-users enrolling certificates using this account must have an email from a domain delegated to this organization. Once an account is created, the department cannot be changed.
Profiles	The certificate profiles available when enrolling certificates using this account. Use the arrow buttons or drag the certificate profiles from the Available Certificate Profiles list to the Assigned Certificate Profiles list.
Allow Empty PKCS12 Password ^a	When enabled, end-users can bypass setting a password when enrolling the certificate. Setting a password is recommended as not all applications support non-password protected certificates.

Field / Element	Description
Automatically Approve Requests ^b	When enabled, SSL certificate requests submitted through the self-enrollment form are automatically approved. Departments do not inherit this setting from their parent organization. As EV certificates require additional approval, this setting is not applied.
CSR Generation method	
Browser	A CSR generated in the browser.
Server	A CSR generated on a server.
Provided by user	A CSR generated and provided by a user.
Sectigo Security app	A CSR generated through the Sectigo Security application.
Authorization methods	
Access Code	Used to authenticate certificate requests made using the self-enrollment form. This code should be conveyed to the applicant along with the URL of the endpoint. Applicants using the enrollment form need to enter this code. Choose a complex code containing a combination of alpha and numeric characters.
IdP assertions mapping	A mapping rule that defines which assertion attribute gets mapped to which value.
None	By selecting this, no method will be assigned.

a. Client Certificate Web Form accounts only.

b. SSL Web Form accounts only.

If you are adding an account, the account is added to the list of accounts in the accounts dialog.

Device endpoints are added as required for organizations and departments.

NOTE: Client endpoints are only available if IdP is configured for your account. Contact your Sectigo account manager.

7.4.4 How to configure SCEP endpoints

SCM supports the SCEP protocol to automate client and device certificate enrollment for mobile devices. Mobile Device Management (MDM) systems such as Sectigo MDM and Microsoft Intune use SCEP for PKI certificate enrollment on mobile devices. These services connect to SCM via SCEP endpoints, which define the URL the external services will use to connect to the SCM SCEP server.

For more information on SCEP, see [What is SCEP?](https://sectigo.com/what-is-scep/) at sectigo.com.

NOTE: SCEP endpoints are only available if SCEP is configured for your account, and an RA certificate is configured. Contact your Sectigo account manager.

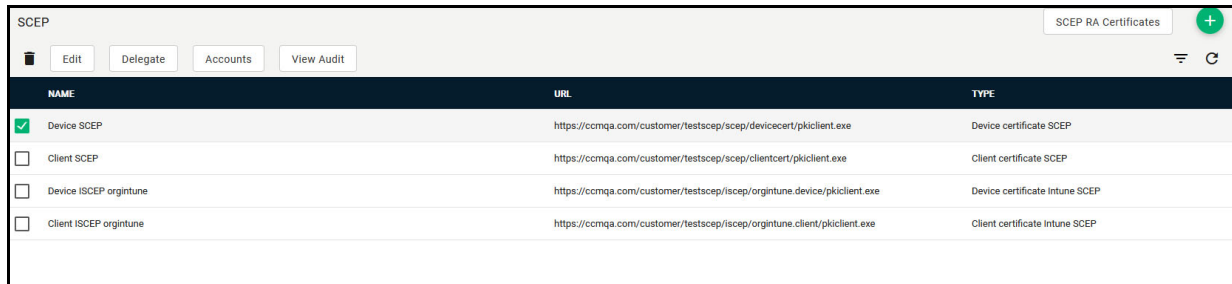
NOTE: For information on adding Intune SCEP endpoints, see .

Configuring SCEP endpoints is a two-stage process:

1. Add the SCEP endpoint.

Typically you will add an endpoint for device and/or client certificates, as appropriate. This provides the endpoint URL that the EST client will use to connect to the SCM EST server.

2. Create EST endpoint accounts to manage access to the endpoint.



The following table lists settings and elements of the **Enrollment > SCEP** page.

Field / Element	Description
Name	The name of the endpoint
URL	The URL of the endpoint
Type	The type of endpoint. The available types are: Device certificate, Client certificate, Device Intune certificate, and Client Intune certificate.
Delete	Delete the certificate
Edit	Edit the endpoint details
Delegate	View/change delegates to the endpoint
Accounts	View/change accounts
View Audit	View audit
SCEP RA Certificates	View/download the RA certificates for the endpoint

7.4.4.1 Managing SCEP RA certificates

The **Enrollment > SCEP** page shown in the following illustration enables MRAO administrators to view and download RA certificates for SCEP that have been configured for your account.

An RA certificate is required to configure a SCEP endpoint. RA certificates are anchored by the same root that you use to issue certificates, as follows:

- To issue device certificates via SCEP, you need an RA certificate issued from your private CA backend.

- To issue public client (SMIME) certificates via SCEP, you need an RA certificate issued from your public CA backend.

RA certificates are configured for your account by Sectigo, and are only available if SCEP is enabled for your account. Contact your Sectigo account manager.

For information on configuring SCEP endpoints, see . To download and install certificates, select a certificate and click **Download**. Certificates are downloaded in `.cer` format for installation in your trust store.

The following table lists settings and elements of the **Enrollment > SCEP > SCEP RA Certificates** page.

Field / Element	Description
Name	The name of the RA certificate.
Backend Name	The name of the certificate back end.
View	Enables you to view the selected certificate.
Download	Downloads the selected RA certificate for installation on your trust store. Certificates are downloaded in <code>.cer</code> format.

The screenshot shows a web interface titled "SCEP RA Certificates". It features a table with two columns: "NAME" and "BACKEND NAME". The table contains one row with the following data:

NAME	BACKEND NAME
<input type="checkbox"/> QARA sasp	SECTIGO Public CA

At the bottom of the table, there is a pagination control showing "Page 1", "Rows per page 10", and "1 of 1".

7.4.4.2 Adding SCEP endpoints

To add or modify SCEP enrollment endpoints, do the following:

- Navigate to **Enrollment > SCEP**.
- To create a SCEP enrollment endpoint, click **Add** to display the **Create Enrollment Endpoint** dialog, create a name, and select a SCEP endpoint type from the **Type** list.

To modify a SCEP endpoint, select the endpoint and click **Edit**.

Create Enrollment Endpoint
✕

Name *

Type

Client certificate SCEP

i The SCEP enrollment endpoint allows for enrollment of Client certificates using the Simple Certificate Enrollment Protocol as described in RFC 8894. Sectigo Certificate Manager supports multiple challengePasswords per endpoint by creating multiple accounts.

Cancel
Next

3. Click **Next**.
4. Complete the fields based on the information in the following table, and then click **Save**.

Field / Element	Description
Details	
URI Extension	The URI extension used to create a unique URL for the endpoint that SCEP clients will use to connect to the SCM SCEP server. This URL should be used in the SCEP client configuration so the client can access the SCEP server.
Configuration	
SCEP RA Certificate	The RA certificate associated with the endpoint. The RA certificate should be issued from the same backend that will be used to issue the certificates. For information about viewing your RA certificates, see .
GetCACert Response Format	The format of the CA certificate that is provided to SCEP.
GetCert Response Format	The format of the certificate that is provided to SCEP.

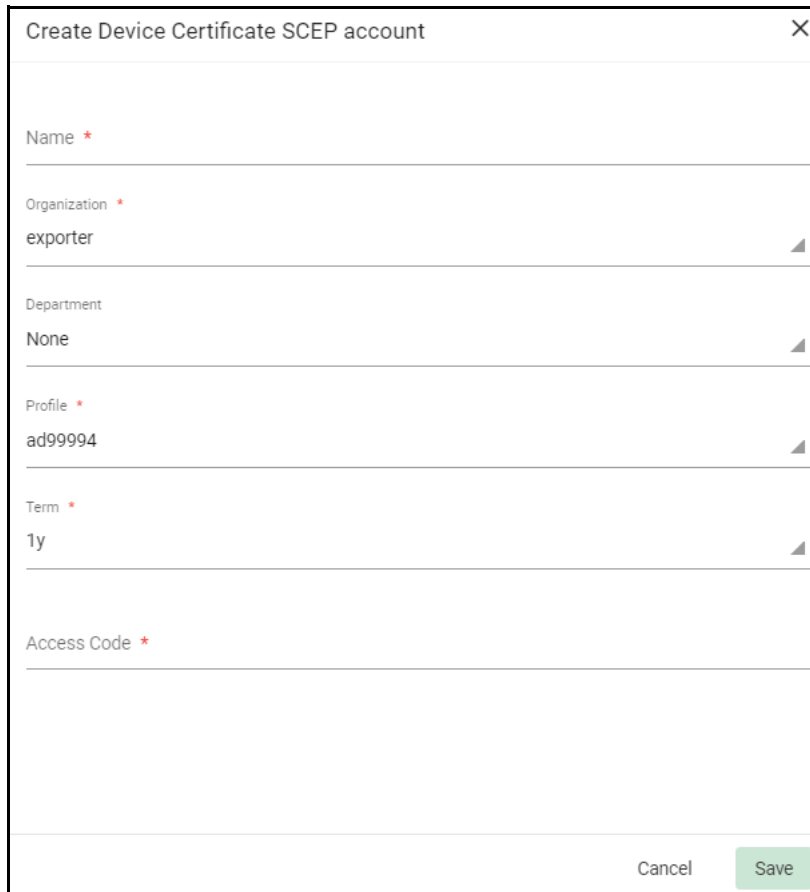
7.4.4.3 How to add and modify accounts for SCEP endpoints

RAO and DRAO administrators can only create and modify endpoint accounts for organizations and departments that are delegated to them.

To add or modify a SCEP account, do the following:

1. Navigate to **Enrollment > SCEP**, select a SCEP endpoint, and click **Accounts**.
2. To add an account, click **Add** on the **SCEP Accounts** dialog to open the **Create SCEP Account** dialog shown in the following illustration.

To edit an account, select the account and click **Edit** to open the **Edit SCEP Account** dialog.



Create Device Certificate SCEP account

Name *

Organization *

exporter

Department

None

Profile *

ad99994

Term *

1y

Access Code *

Cancel Save

3. Provide a descriptive name for the account.
4. If you are adding an account, select the organization and, optionally, the department for which the SCEP account will serve as endpoint.
Once the account is created, the organization and department cannot be changed.
5. Select the device or client certificate profile to be used for certificates that are issued via this account. Only profiles delegated to the selected organization and department are available.
6. Set the term for certificates that are issued via this account.
7. Enter an access code. The access code is used to authenticate certificate requests that are made using SCEP. This code must consist of a combination of alpha and numeric characters. The access code should be entered as the `challengePassword` SCEP parameter.
8. Click **Save**.

If you are adding an account, the account is added to the list of accounts in the **SCEP Accounts** dialog.

7.4.5 How to configure EST endpoints

SCM supports the EST protocol to automate SSL, client and device certificate enrollment.

For more information on EST, see [What is EST?](https://sectigo.com/what-is-est/) at sectigo.com.

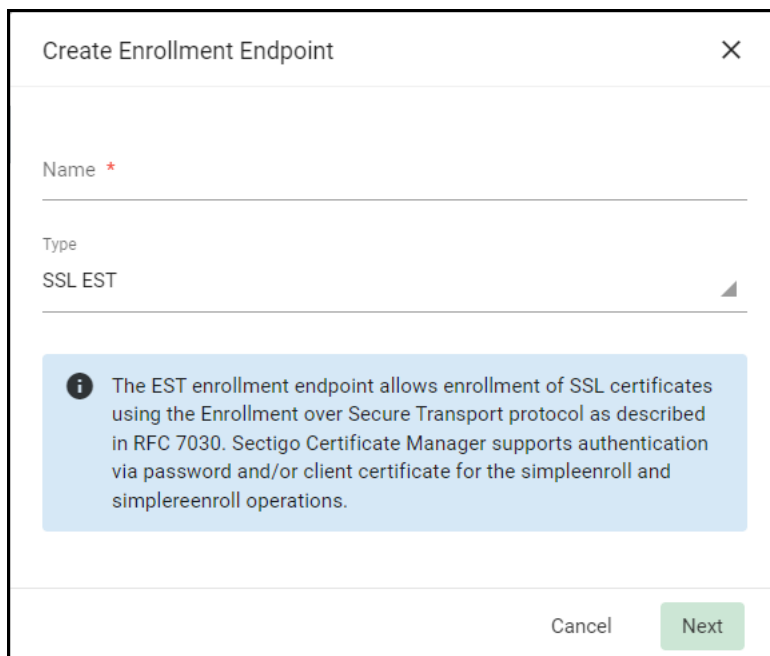
NOTE: EST endpoints are only available if EST is configured for your account, and Private CA is configured. Contact your Sectigo account manager.

Configuring EST endpoints is a one-stage process: add the EST endpoint. This provides the endpoint URL that the EST client will use to connect to the SCM EST server.

7.4.5.1 Adding EST endpoints

To add or modify EST enrollment endpoints, do the following:

1. Navigate to **Enrollment > EST**.
2. To create an EST enrollment endpoint, click **Add** to display the **Create Enrollment Endpoint** dialog.
 - To modify an EST endpoint, select the endpoint and click **Edit**.
3. Enter a descriptive name for the endpoint.
4. Select an EST endpoint type from the **Type** list.
5. Click **Next**.



Create Enrollment Endpoint

Name *

Type

SSL EST

i The EST enrollment endpoint allows enrollment of SSL certificates using the Enrollment over Secure Transport protocol as described in RFC 7030. Sectigo Certificate Manager supports authentication via password and/or client certificate for the `simpleenroll` and `simplereenroll` operations.

Cancel Next

6. In the **Create Enrollment Endpoint** form, complete the fields, referring to this table, and then click **Save**.

Field / Element	Description
Details	
URI Extension	The URI extension used to create a unique URL for the endpoint that EST clients will use to connect to the SCM EST server. The URL is automatically shown below the URI Extension field. This URL should be used in the EST client configuration so the client can access the EST server.
Organization	The organization associated with the endpoint. Once an endpoint is created, the organization cannot be changed.
Department	The department associated with the endpoint. Once an endpoint is created, the department cannot be changed.
Profile	A certificate profile for which EST enrollments use.
CAs	A list with CA certificates. Available only for public backends.
Authentication	
Username	The username used for authentication to the EST endpoint.
Password	The password used for authentication to the EST endpoint. The password is mandatory if certificate authentication is not being used.
Authentication Certificate Issuer	An authentication certificate issuer to validate the client certificate during authentication. The issuer certificate must be provided in the PEM format. Multiple entries are allowed. This option can be performed only if Certificate Authentication is enabled.
Certificate Revocation Check	The revocation check for confirming the certificate is not revoked. This option can be performed only if Certificate Authentication is enabled.

7.4.6 How to add and modify accounts for REST endpoints

RAO and DRAO administrators can only create and modify endpoint accounts for organizations and departments that are delegated to them.

To add a REST account, do the following:

1. Navigate to **Enrollment > REST**, select a REST endpoint, and click **Accounts**.
2. Click **Add** to open the **Create REST Account** dialog.

Create Device Certificates REST Account

REST enrollment accounts control the authentication to the endpoint and the issuing of certificate options.

Account Name *

Owner

Organization * 445t Department None

Certificate

Profile * ap.pca.device Term * 365

Cancel Create

3. Provide a descriptive name for the account.
4. Select the organization and, optionally, the department for which the REST account will serve as endpoint.
Once the account is created, the organization and department cannot be changed.
5. Select the device or client certificate profile to be used for certificates that are issued via this account. Only profiles delegated to the selected organization and department are available.
6. Set the term for certificates that are issued via this account.
7. Click **Create**.

The account is added to the list of accounts in the **REST Accounts** dialog.

To modify a REST account, do the following:

1. Navigate to **Enrollment > REST**, select a REST endpoint, and click **Accounts**.
2. Select the account and click **Edit**.
3. Make changes as necessary. You may modify the **Account Name**, **Profile**, **Term**, and **Client Secret** fields.
4. Click **Save**.

Using the Sectigo ACME Service

SCM supports the Automatic Certificate Management Environment (ACME) protocol, which automates interactions between a CA and its customers' web servers, including certificate installation, renewal, and domain validation. Using a third-party ACME client (for example, Certbot), customers can connect to Sectigo ACME servers (the endpoints) via an appropriately configured ACME endpoint account. The ACME endpoint can then be used by the ACME client to enroll and manage SSL certificates.

For more information on ACME, see [ACME Explained](#) at sectigo.com.

This chapter describes the Sectigo ACME service and provides information on configuring ACME endpoints in SCM and using the Certbot ACME client with the service.

This chapter describes the following topics:

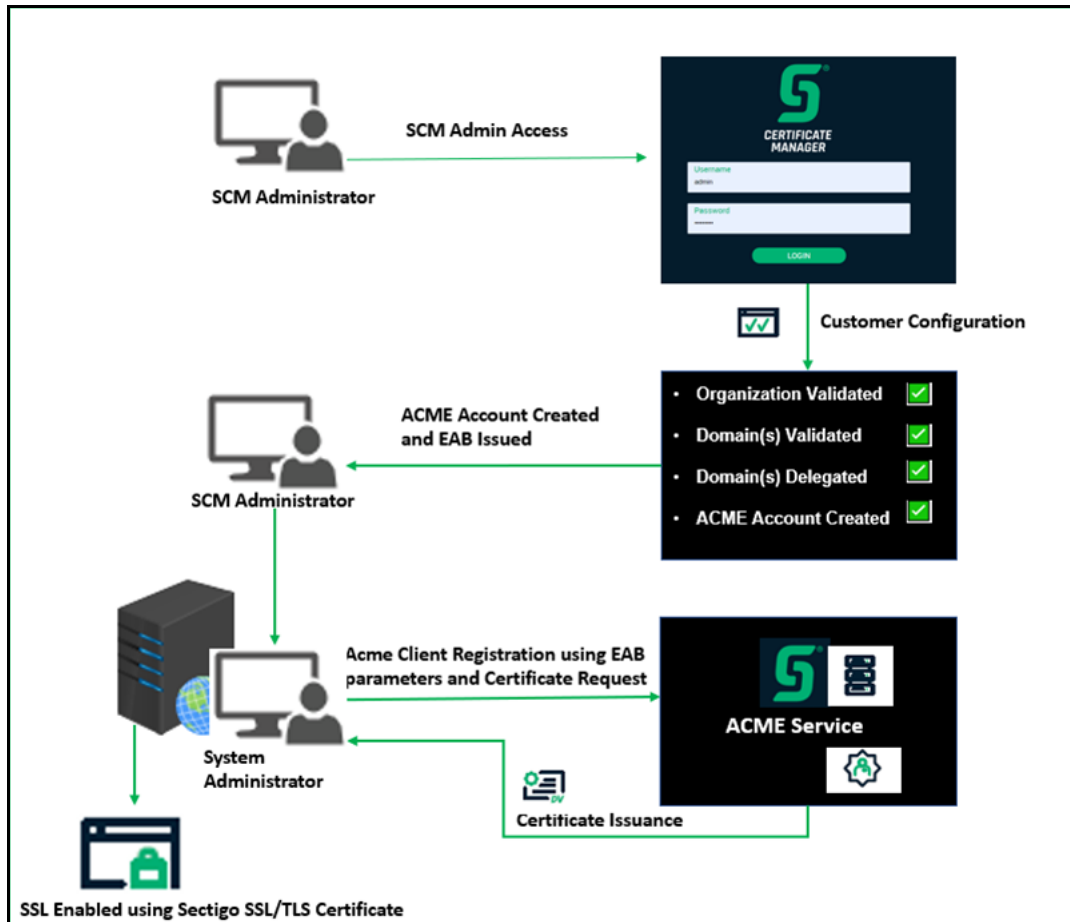
- [Sectigo ACME service overview](#)
- [Configuring ACME endpoints](#)
- [ACME clients overview](#)

8.1 Sectigo ACME service overview

The ACME protocol for issuing SSL certificates automates interactions between web servers and CAs, including certificate installation, renewal, and domain validation. For more information, see <https://tools.ietf.org/html/rfc8555>.

The Sectigo implementation of the ACME protocol is known as the Sectigo ACME service. It enables the following:

- SSL certificate enrollment through a third-party ACME client.
All validation levels—DV, OV, and EV—are supported, as well as SDC, MDC, and WC certificate profiles.
Domains that are pre-validated in SCM are not issued validation challenges through ACME. Domains that are not pre-validated in SCM are subject to ACME validation challenges. Validation done through ACME does not change the **Validation Status** of domains in SCM.
- Re-issuance of SSL certificates with new certificates to add or remove one or more domains.
- Automatic and manual renewal of SSL certificates.
- Visualization and revocation of SSL certificates via SCM, as described in [“Managing SSL Certificates”](#) on page 20, [“Understanding the SCM dashboard”](#) on page 8, and [“Generating reports”](#) on page 159. This requires creation of an externally-bound ACME account in SCM. For information on external account binding (EAB), see the ACME specification at <https://tools.ietf.org/html/rfc8555#section-7.3.4>.



To deploy ACME, do the following:

1. In SCM, add an ACME account for an enrollment endpoint (ACME server) to bind the SCM account with the ACME server.
 - This creates External Account Binding (EAB) (aka authorization code) values for the ACME account for that specific endpoint.
 - For information on configuring accounts for ACME server endpoints, see [“Configuring ACME endpoints” on page 185](#).
2. Using your ACME client (e.g., Certbot), send the EAB values (KeyID and HMAC Key) along with other certificate-related information to the enrollment endpoint (ACME server).
 - The ACME server checks the EAB values, links the ACME client, and creates the ACME account for the client.
 - EAB values can be reused to support multiple ACME clients.
 - ACME Client Account key pair will be used for authentication and secure communication for subsequent certificate management with Sectigo ACME server(s).
 - For information on using ACME clients with the Sectigo ACME Service, see [“ACME clients overview” on page 190](#).

If successfully validated by the Sectigo ACME server, then the certificates issued by Sectigo CA(s) can be directly installed on a web server using respective client plug-ins or manually installed on the corresponding domain validated web servers.

8.2 Configuring ACME endpoints

ACME must be enabled for your account and the ACME server endpoints configured by Sectigo. For assistance, contact your Sectigo account manager.

Depending on how your account is configured, ACME accounts may connect to the following Sectigo ACME server endpoints:

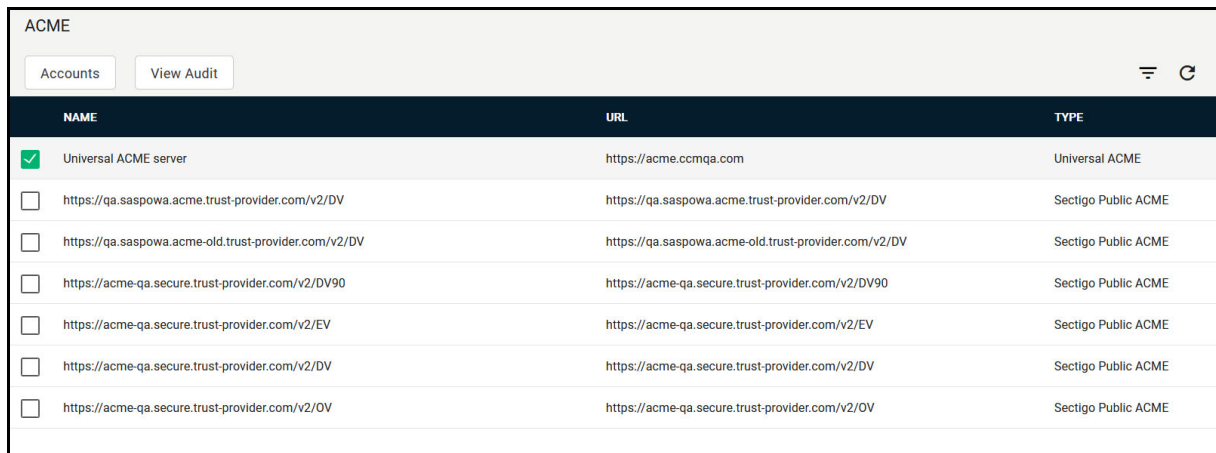
- Public CA - DV
- Public CA - OV
- Public CA - EV
- Private CA

RAO and DRAO administrators can only create and modify ACME accounts for organizations and departments that are delegated to them.

8.2.1 How to manage ACME accounts

1. Navigate to **Enrollment > ACME**.

The ACME endpoints configured for your account by Sectigo are listed, along with any other endpoints that are configured for your account.

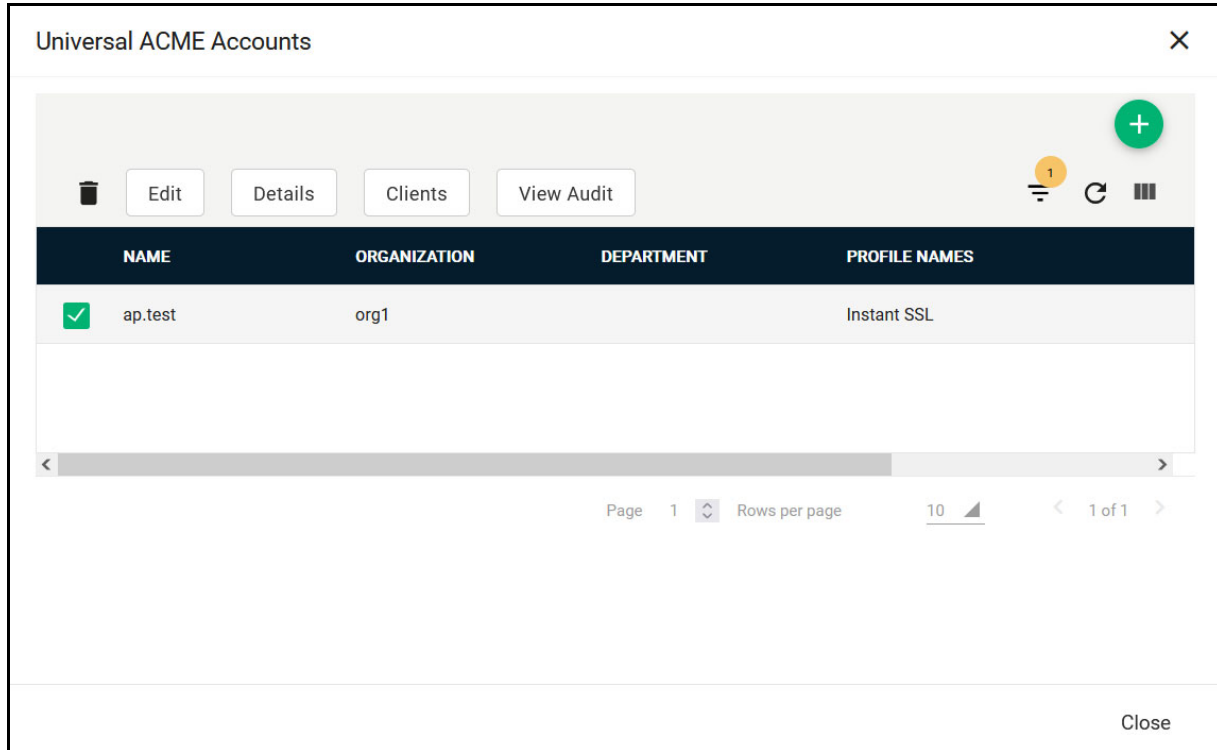


The screenshot shows the 'ACME' configuration page. At the top, there are two buttons: 'Accounts' and 'View Audit'. Below the buttons is a table with three columns: 'NAME', 'URL', and 'TYPE'. The table contains seven rows of ACME endpoints. The first row is selected, indicated by a green checkmark in the left margin. The other rows have empty checkboxes. The table also includes a filter icon and a refresh icon in the top right corner.

NAME	URL	TYPE
<input checked="" type="checkbox"/> Universal ACME server	https://acme.ccmqa.com	Universal ACME
<input type="checkbox"/> https://qa.saspowa.acme.trust-provider.com/v2/DV	https://qa.saspowa.acme.trust-provider.com/v2/DV	Sectigo Public ACME
<input type="checkbox"/> https://qa.saspowa.acme-old.trust-provider.com/v2/DV	https://qa.saspowa.acme-old.trust-provider.com/v2/DV	Sectigo Public ACME
<input type="checkbox"/> https://acme-qa.secure.trust-provider.com/v2/DV90	https://acme-qa.secure.trust-provider.com/v2/DV90	Sectigo Public ACME
<input type="checkbox"/> https://acme-qa.secure.trust-provider.com/v2/EV	https://acme-qa.secure.trust-provider.com/v2/EV	Sectigo Public ACME
<input type="checkbox"/> https://acme-qa.secure.trust-provider.com/v2/DV	https://acme-qa.secure.trust-provider.com/v2/DV	Sectigo Public ACME
<input type="checkbox"/> https://acme-qa.secure.trust-provider.com/v2/OV	https://acme-qa.secure.trust-provider.com/v2/OV	Sectigo Public ACME

2. Select the endpoint and click **Accounts**.

This displays the **ACME Accounts** dialog which lists the accounts that have been configured for the selected ACME server endpoint.



3. Select an account. From ACME Accounts dialog you can do any of the following:
 - Click **Details** to see the ACME Account Details page.
 - Click **Clients** to see the list of ACME clients registered with that account. Select a client to either view the client details or the SSL certificates enrolled using that client.
 - Click **View Audit** to see a list of audits on that account. Select an audit and click **View** or **Audit Chain** to see more details.

8.2.2 How to add and modify accounts for Sectigo public ACME servers

To add or modify a Sectigo public ACME account, do the following:

1. Navigate to **Enrollment > ACME**, and click **Accounts**.
2. To add an account, click **Add**.
 - To edit an account, select the account and click **Edit** to open the **Edit ACME Account** dialog.
 - To display a client, select the account and click **Clients** to open the **ACME Clients** dialog.
3. Provide a descriptive name for the account.
4. If you are adding an account, select the organization and, optionally, the department for which the ACME account will serve as endpoint. Once created, the organization and department cannot be changed.

Create ACME Account

Name *

Organization *
check.16

Department
None

Validation Type OV

Domains
No domains are available.

Cancel Save

5. Select the domains you want to assign to the new ACME account.
 - If the **Validation Type** of the server is DV or OV, then the domains are already available.
 - If the **Validation Type** of the server is EV, click **EV Details** > **Edit** to complete the **Edit EV Details** dialog for the organization.
6. Use the arrow buttons or drag the domains to assign to the new ACME account from the **Available domains** list to the **Assigned domains** list.

Selecting domains for an ACME account controls the boundaries of the account. In addition, the current validation status of the domain affects the ACME client.

7. Click **Save**.

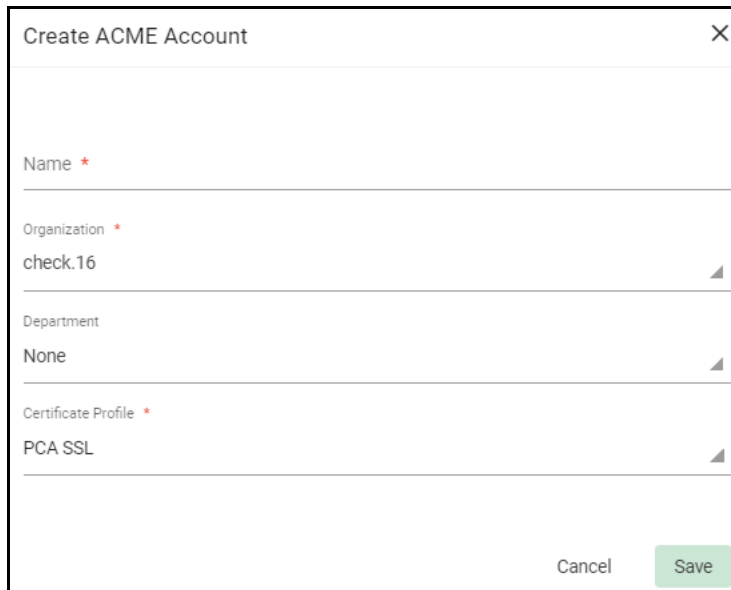
If you are adding an account, the account is added to the list of accounts in the **ACME Accounts** dialog and the **ACME Account Details** dialog is displayed.

8.2.3 How to add and modify accounts for Universal ACME servers

To add or modify an account for the Universal ACME endpoint, do the following:

1. Navigate to **Enrollment** > **ACME**, select a Universal ACME endpoint, and click **Accounts**.
2. To add an account, click **Add**.
 - To edit an account, select the account and click **Edit** to open the **Edit ACME Account** dialog.

- To display a client, select the account and click **Clients** to open the **Universal ACME Clients** dialog.



Create ACME Account

Name *

Organization *
check.16

Department
None

Certificate Profile *
PCA SSL

Cancel Save

3. Provide a descriptive name for the account.
4. Select the organization and, optionally, the department for which the ACME account will serve as endpoint. Once created, the organization and department cannot be changed.
5. Select the certificate profile to use for certificates enrolled using the endpoint.
6. Click **Save**.

The account is added to the list of accounts in the **ACME Accounts** dialog and the **ACME Account Details** dialog is displayed.

8.2.4 How to view account details

When an account is created for an ACME endpoint, the **Key ID**, **HMAC Key**, and **Account ID** are created. The Key ID and HMAC Key are based on the external account binding (EAB) ID and key respectively and act similarly to a username and password pair. They, along with the ACME URL, are required when accessing the Sectigo ACME service to proceed with enrolling SSL certificates using the service.

The **Key ID**, **HMAC Key**, **ACME URL**, and **Account ID** for **Pending** accounts can be viewed any time using the **Details** option.

To view ACME account details, do the following:

1. In the **ACME Accounts** dialog, select an account and click **Details** to open the **ACME Account details** dialog.

The **ACME URL** field shows the URL of the ACME account server.

2. Take a note of this URL, as this information is required to access the Sectigo ACME service to proceed with the SSL certificates enrollment.

If the account status is **Pending**, you can copy values from the **Key ID** and **HMAC Key** fields to the clipboard. The **EAB** information is not displayed for accounts with any other status.

The **How to use External Account Binding (EAB) with Certbot** field provides an example Certbot command. See [“Using the Sectigo ACME Service” on page 183](#) for more information on using the Sectigo ACME service with Certbot.

8.2.4.1 Deleting ACME Accounts

To delete an ACME account, select the account in the **ACME Accounts** dialog, click **Delete**, then click **OK** to confirm.

An ACME Account can handle multiple ACME clients. To deactivate all the clients, delete the ACME Account.

8.3 ACME clients overview

ACME clients communicate with Sectigo ACME servers to request and manage certificates. The following section provides information on ACME clients details and some examples of how the Certbot client can be used with the Sectigo ACME service.

NOTE: If the ACME client does not specify a validity term for certificates, the validity period of certificates will default to the shortest term available for your account. Contact your Sectigo account manager.

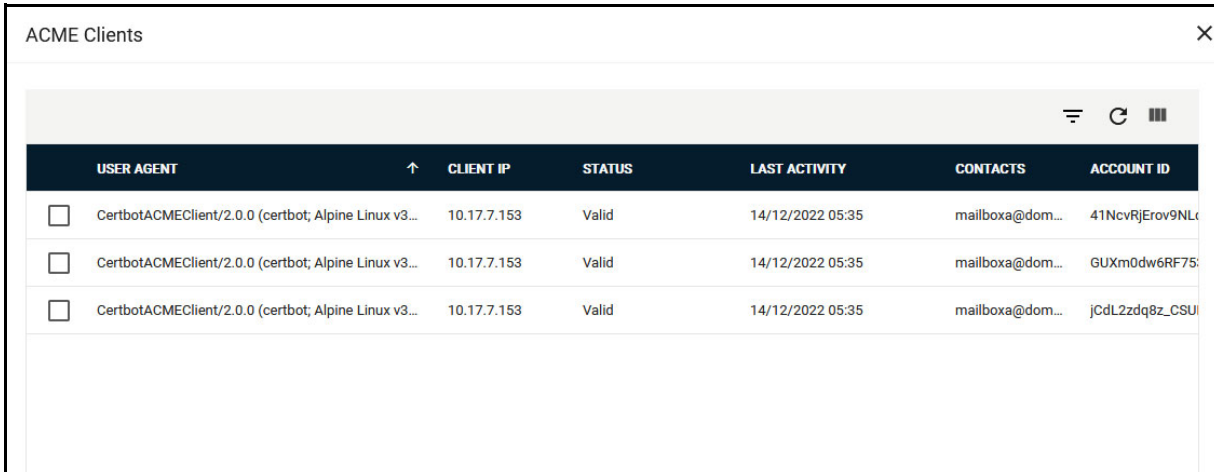
The following table lists options available in the **ACME Clients** dialog.

Column	Description
Client IP	The IP address of the ACME client
User Agent	The name of the ACME client user agent
Status	The status of the ACME client. It can be one of the following: <ul style="list-style-type: none"> Valid – The client is active. Deactivated – The client has been deactivated.
Last Activity	The date and time of the last activity of the ACME client
Contacts	The client's email address
ACME URL	The URL used for ACME
Account ID	The ID of the account

8.3.1 How to view ACME clients details

1. In the **ACME Accounts** dialog, select an account and click **Clients** to open the **ACME Clients** dialog.

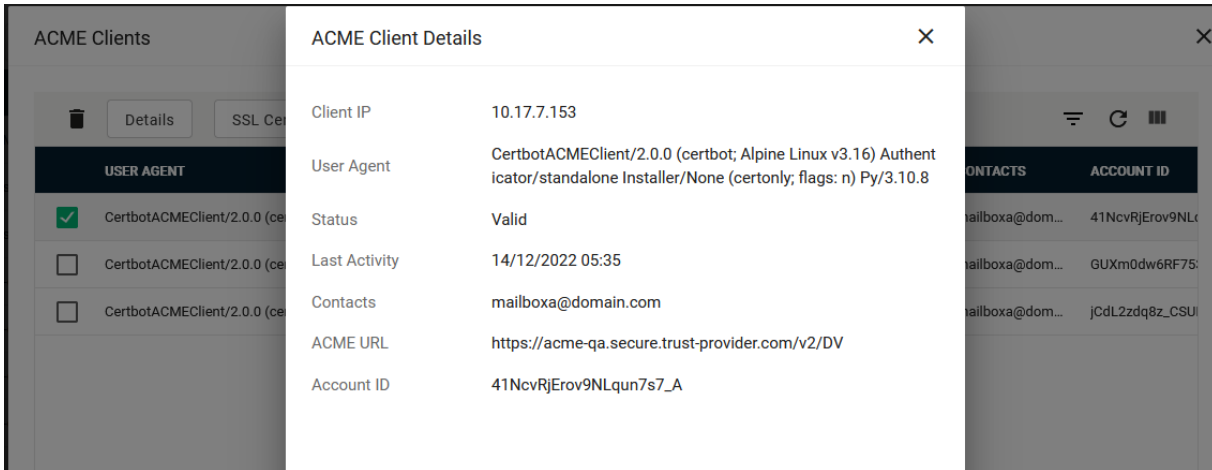
NOTE: An ACME Account can handle multiple ACME clients and every client will be managed individually.



The screenshot shows a window titled "ACME Clients" with a close button (X) in the top right corner. Below the title bar is a header area with a search icon, a refresh icon, and a menu icon. The main content is a table with the following columns: USER AGENT, CLIENT IP, STATUS, LAST ACTIVITY, CONTACTS, and ACCOUNT ID. There are three rows of data, each with a checkbox in the first column.

	USER AGENT	CLIENT IP	STATUS	LAST ACTIVITY	CONTACTS	ACCOUNT ID
<input type="checkbox"/>	CertbotACMEClient/2.0.0 (certbot; Alpine Linux v3...	10.17.7.153	Valid	14/12/2022 05:35	mailboxa@dom...	41NcvRjErov9NLC
<input type="checkbox"/>	CertbotACMEClient/2.0.0 (certbot; Alpine Linux v3...	10.17.7.153	Valid	14/12/2022 05:35	mailboxa@dom...	GUXm0dw6RF75:
<input type="checkbox"/>	CertbotACMEClient/2.0.0 (certbot; Alpine Linux v3...	10.17.7.153	Valid	14/12/2022 05:35	mailboxa@dom...	jCdL2zdzq8z_CSUI

2. Select the ACME client and click **Details** as shown in the following illustration.



8.3.2 How to use Certbot

Certbot enables enrollment, installation, and management of SSL certificates.

For information on the Certbot installation, navigate to <https://certbot.eff.org/> and generate a list of instructions by selecting your server software and operating system.

Your experience using Certbot may differ depending on the server software, operating system, and Certbot plugins you have installed.

The following table provides a subset of common Certbot commands. A complete list of Certbot commands can be found at <https://certbot.eff.org/docs/using.html#certbot-command-line-options>.

Command	Description
<code>register</code>	Register a Sectigo ACME account
<code>certonly</code>	Initiates the enrollment of a certificate
<code>certbot run</code>	Obtains and installs a certificate in your current web server
<code>--server</code>	Specifies which ACME server to contact. The following commands are applicable to each primary Sectigo ACME server, whose URLs must be specified exactly. Use the URL of the ACME account server specified in the ACME URL field for your account.
<code>--server https://acme.sectigo.com/v2/DV</code>	Specifies the Sectigo ACME server for DV SSL certificates
<code>--server https://acme.sectigo.com/v2/OV</code>	Specifies the Sectigo ACME server for OV SSL certificates

Command		Description
<code>--server https://acme.sectigo.com/v2/EV</code>		Specifies the Sectigo ACME server for EV SSL certificates
<code>--domain</code> <code>-d</code>		Indicates the domains to be included. Multiple domains can be added with further domain tags. The initial domain is treated as the subject CN of the certificate. All subsequent domains are SANs on the certificate.
<code>run</code>		Tells the authenticator plugin and installer plugin to initiate the acquisition and installation of a certificate
	<code>--authenticator</code> <code>-a</code>	Specifies the authenticator plugin to be used
	<code>--installer</code> <code>-i</code>	Specifies the installer plugin to be used
<code>renew</code>		Renews all previously obtained certificates that are near expiry
<code>certbot revoke</code>		Revokes a certificate regardless of the remaining time until expiration
<code>--force-renewal</code>		Renews a certificate regardless of the remaining time until expiration
<code>--expand</code>		Updates an existing certificate with a new certificate that includes one or more new domains
<code>--non-interactive</code>		Runs the command line without requesting further user input. This may require the addition of other commands (such as <code>--agree-tos</code>).
<code>--agree-tos</code>		Indicates that you agree to the Sectigo ACME terms of service
<code>--eab-kid</code>		Specifies the key identifier for external account binding. This is the EAB ID in an SCM ACME account.
<code>--eab-hmac-key</code>		Specifies the HMAC key for external account binding. This is the EAB Key in an SCM ACME account.
<code>--cert-name</code>		Specifies the name for returned certificate in your system
<code>unregister</code>		Unregister an SCM ACME account. Once unregistered, the ACME account is deactivated on the ACME server and cannot be restored.

The following table provides sample commands for performing various ACME tasks using Certbot. The examples do not necessarily represent the commands required in your specific environment.

Register account
<pre>certbot register --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/DV --eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV-nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNIln0gEw</pre>

Obtain a DV certificate
Apache authenticator
<pre>certbot certonly --apache --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/DV --eab- kidbxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name dv01</pre>
NGINX authenticator
<pre>certbot certonly --apache --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/DV --eab- kidbxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name dv01</pre>
Standalone authenticator
<pre>certbot certonly --standalone --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/DV --eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name dv01</pre>
Obtain an OV certificate
Apache authenticator
<pre>certbot certonly --apache --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/OV --eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name ov01</pre>
NGINX authenticator
<pre>certbot certonly --nginx --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/OV --eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name ov01</pre>
Standalone authenticator
<pre>certbot certonly --standalone --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/OV --eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt- 5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name ov01</pre>

Obtain an EV certificate
Apache authenticator
<pre>certbot certonly --apache --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/EV --eab- kidbxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name ev01</pre>
NGINX authenticator
<pre>certbot certonly --nginx --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/EV --eab- kidbxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name ev01</pre>
Standalone authentication
<pre>certbot certonly --standalone --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/EV --eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name dv01</pre>
Obtain and install a certificate
Apache authenticator/installer
<pre>certbot run --apache --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/DV --eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name dv01</pre>
NGINX authenticator/installer
<pre>certbot run --nginx --non-interactive --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/DV --eab-kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name dv01</pre>
Obtain and install a certificate using a different authenticator and installer
Webroot authenticator / Apache installer
<pre>certbot run -a webroot -i apache -w /var/www/html --non-interactive --agree-tos -- email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/DV --eab- kid bxFGQVK9ed1oNRRVuz3FZg --eab-hmac-key ek2TIQpQcG8Tlt-5OjMEteSBISa7-fvWAWDyMpczV- nRXc7PkSMtuvW31YQ1xA8t0vTf0zOz3xAwEGNI1n0gEw --domain scmexample.com --cert-name dv01</pre>

Expand a certificate to include further domains (Apache)
<pre>certbot certonly --expand --apache -d scmexample.com,scmdomaintobeadded.com --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/DV --eab-kid Ls3dE7b4vy_947D7MScwqg --eab-hmac-key LT3_ebbI5bQ_dadLjdS86z_c4nevXcBg4T5Ci7CLqKpB3nLw6e8Y08VWacEeahHQXsb8KeRh2C2PoxHKwPLuiQ</pre>
Force the renewal of a certificate (Apache)
<pre>certbot certonly --force-renewal --apache --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/DV --eab-kid Ls3dE7b4vy_947D7MScwqg --eab-hmac-key LT3_ebbI5bQ_dadLjdS86z_c4nevXcBg4T5Ci7CLqKpB3nLw6e8Y08VWacEeahHQXsb8KeRh2C2PoxHKwPLuiQ --domain scmexample.com</pre>
Duplicate an existing certificate (Apache)
<pre>certbot certonly --duplicate --apache --agree-tos --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/DV --eab-kid Ls3dE7b4vy_947D7MScwqg --eab-hmac-key LT3_ebbI5bQ_dadLjdS86z_c4nevXcBg4T5Ci7CLqKpB3nLw6e8Y08VWacEeahHQXsb8KeRh2C2PoxHKwPLuiQ --domain scmexample.com</pre>
Revoke an existing certificate
<pre>certbot revoke --eab-kid_spjQh6WEPMGUqyVCPW7w --eab-hmac-key K39ss5B_4gQ7bFTmGxjzPO5g-BWcZIAux9rgLOFONDqGMvjL9LtDda5382-9dNzmWgIAGK1c5THZs7J2Pvca --server https://acme.sectigo.com/v2/DV --cert-path /etc/example/archive/testCert/cert1.pem --reason keycompromised</pre>
Unregister an ACME account
<pre>certbot unregister --email <CUSTOMER_EMAIL>@<DOMAIN.COM> --server https://acme.sectigo.com/v2/DV --domain scmexample.com --account 18f63f589759f00d14718ecf8325bba4</pre>

The following Certbot commands are not currently supported by the Sectigo ACME service:

- `--test-cert`
- `--staging`
- `--must-staple`
- `--staple-ocsp`

Managing issuers

Issuers page contains the following sub-pages:

- CA Backends
- Private CAs

9.1 CA Backends

As part of our ongoing efforts to improve our documentation, the content about CA Backends previously covered in this chapter has been moved online.

Information about the CA backends can now be found in the following location:

- [CA Backends](#)

9.2 How to manage private CAs

The **Private CAs** page shown in the following illustration enables you to view and download certificates for the private CAs that have been configured for your account.

To download and install certificates, select a private CA with a state of **Signed** and click **Download Certificate**. Certificates are downloaded in `.cer` format for installation in your trust store.

Private CAs							
NAME	TRIAL MODE	SUBJECT	KEY TYPE	SIGNATURE	STATE	SERIAL NUMBER	EXPIRATION DATE
<input type="checkbox"/> 6		CN=testpca Root CA,O=testpca,L=I	RSA-2048	SHA 512	SIGNED	7823304c64f12765FA8E9BD4F8C	01/01/2031
<input type="checkbox"/> 3.2048		CN=1 Issuing CA,O=1,L=Odesa,ST=	RSA-2048	SHA 256	SIGNED	74A00FDBB39ABF602EB66C4FE1	09/17/2025
<input type="checkbox"/> 5.1		CN=testpca Issuing CA,O=testpcaJ	EC-P-256	SHA 512	SIGNED	7D537F4F20FDE7D70B8F17FE47F	09/17/2030
<input type="checkbox"/> 5		CN=Sectigo Demo Portal Authentic	EC-P-256	SHA 512	SIGNED	69BC71D9A54AA7DA9FE726CC1C	09/17/2050
<input type="checkbox"/> 4.1		CN=testpca Issuing CA,O=testpcaJ	EC-P-384	SHA 384	SIGNED	2DAEB21AE06A609E6FA1F87499I	09/17/2030
<input type="checkbox"/> 4		CN=testpca Root CA,O=testpca,L=I	EC-P-384	SHA 384	SIGNED	59B5DA90560541CED6B3F1DA6C	09/17/2040
<input type="checkbox"/> 3.1		CN=testpca Issuing CA,O=testpcaJ	RSA-4096	SHA 256	SIGNED	12EA803193EFA8D9539AB50658I	09/17/2030
<input type="checkbox"/> 3		CN=testpca Root CA,O=testpca,L=I	RSA-4096	SHA 256	SIGNED	296F338B81F84730FA00D70C6EC	09/17/2040
<input type="checkbox"/> 2		CN=Common Name,OU=private ca	RSA-2048	SHA 512	SIGNED	50388FB020100C6E04064442062	09/17/2021

The following table lists settings and elements of the **Private CAs** page.

Field / Element	Description
Name	The name of the private CA
Trial Mode	Indicates whether or not the private CA is in trial mode. For more information, see "Requesting and adding a trial private CA" on page 197.
Subject	The contents of the Subject field of the certificate
Key Type	The type of algorithm used for encryption
Signature	The type of signature algorithm used for the signing of the certificate
State	The state of the private CA certificate
Serial Number	The serial number of the private CA certificate that is unique and can be used to identify the certificate
Expiration Date	The expiration date of the private CA certificate
Add ^a	Adds a new trial private CA
Download Certificate ^b	Downloads signed private CA certificates for installation on your trust store. Certificates are downloaded in <code>.cer</code> format.

a. Control appears only if private CA trial mode is enabled for your account. Contact your Sectigo account manager.

b. Control appears only after selecting a private CA with a Signed certificate.

9.2.1 Requesting and adding a trial private CA

A 30-day private CA trial allows MRAOs to add and configure private CAs. To request a trial, contact your Sectigo account manager.

NOTE: If you are running a SCM trial, private CA trial mode is available by default.

A private CA allows you to issue your own private trust level certificates. Private trust level certificates can be used to secure enterprise infrastructure, such as:

- **Internal servers**—Issue and manage private SSL certificates to secure internal web servers, user access, connected devices, and applications.
- **Corporate email**—Issue and manage private client certificates.

Configuring and using a trial private CA involves the following general steps:

1. Add a root private CA.
2. Add an issuing private CA with the root CA as the parent issuer.
3. Add certificate profiles for the certificate types you want to issue using the private CA, setting the enrolling backend for each profile to the issuing private CA.
4. Issue certificates.

Certificates enrolled during trial have a lifetime of 30 days. For seamless transition from the trial to the full version, ensure that the information you enter during the trial is accurate. Trials are for online root private CAs only, and you cannot transition from an online to offline root.

Five days prior to the scheduled end of your trial, you start receiving daily notification emails from Sectigo. You can contact your Sectigo account manager to request either an extension of the trial or the full private CA feature to be added to your account. Alternatively, you can let the trial expire, in which case you would not be able to order certificates. The certificates ordered during trial are not revoked and continue to be available after the expiration of the trial.

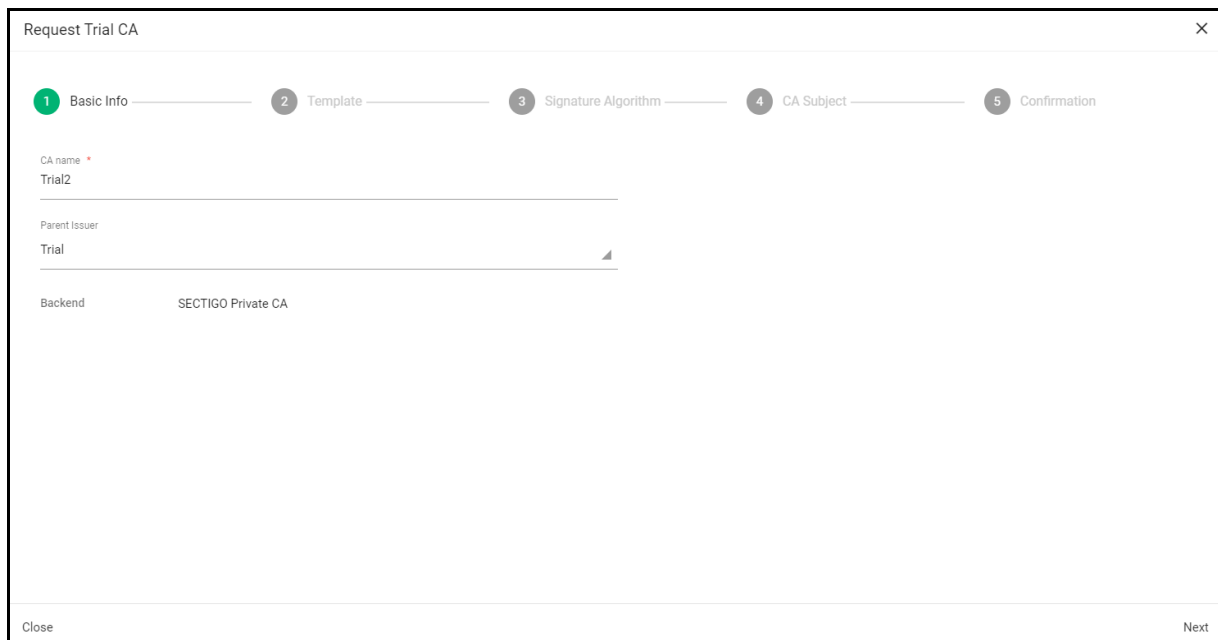
Once the Private CA trial mode has been activated for your account, an **Add** button appears on the **Private CAs** page.

Because end-entity certificates are not issued from a root CA, you first add a root CA, and then an issuing CA that uses the root as its parent. The steps for adding both are the same.

You add a trial private CA as follows:

1. Navigate to **Issuers > Private CAs**.
2. Click **Add** to open the **Request Trial CA** wizard shown in the following illustration.

If the **Add** button is not displayed, your trial is not active and you need to contact Sectigo Support.



The screenshot shows a wizard window titled "Request Trial CA" with a close button (X) in the top right corner. The wizard has five steps: 1. Basic Info (active), 2. Template, 3. Signature Algorithm, 4. CA Subject, and 5. Confirmation. The "Basic Info" step contains the following fields:

- CA name ***: Trial2
- Parent Issuer**: Trial (with a dropdown arrow)
- Backend**: SECTIGO Private CA

At the bottom left is a "Close" button and at the bottom right is a "Next" button.

3. Enter a name for the CA in the **CA name** field.
4. Select the **Parent Issuer**.
 - To add a root CA, choose the **None (Self Issued Root)** option.
 - To add an issuing CA, choose a root CA you have already added.
5. Click **Next** to open the **Template** page shown in the following illustration.

Request Trial CA

Basic info — 2 Template — 3 Signature Algorithm — 4 CA Subject — 5 Confirmation

Template
rsa-4096-root

Key Type	RSA-4096
Lifetime	20 Years

Close Back Next

6. Use the **Template** field to select the template to use. The template determines the key type that the CA will use, as well as the lifetime of the CA certificate.

The lifetime is 5 years for RSA-2048, and 10 years for all other key types.

For self-issued roots, RSA-2048 has a fixed expiry of December 31, 2030, and the lifetime is 20 years for all other key types.

7. Click **Next** to open the **Signature Algorithm** page shown in the following illustration.

Request Trial CA

Basic info — Template — 3 Signature Algorithm — 4 CA Subject — 5 Confirmation

Signature Algorithm
SHA 256

Close Back Next

8. Use the **Signature Algorithm** field to select one of the following algorithms:
 - SHA-1

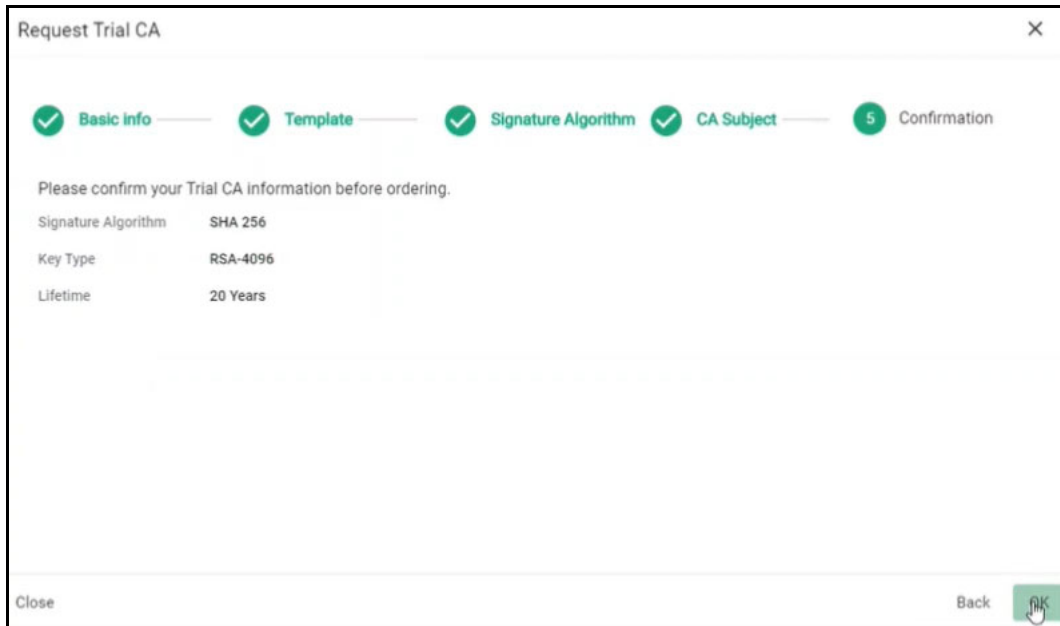
- SHA-256
- SHA-384
- SHA-512

If you are adding an issuing CA, the algorithm of the parent root CA is automatically selected.

9. Click **Next** to open the **CA Subject** page shown in the following illustration.

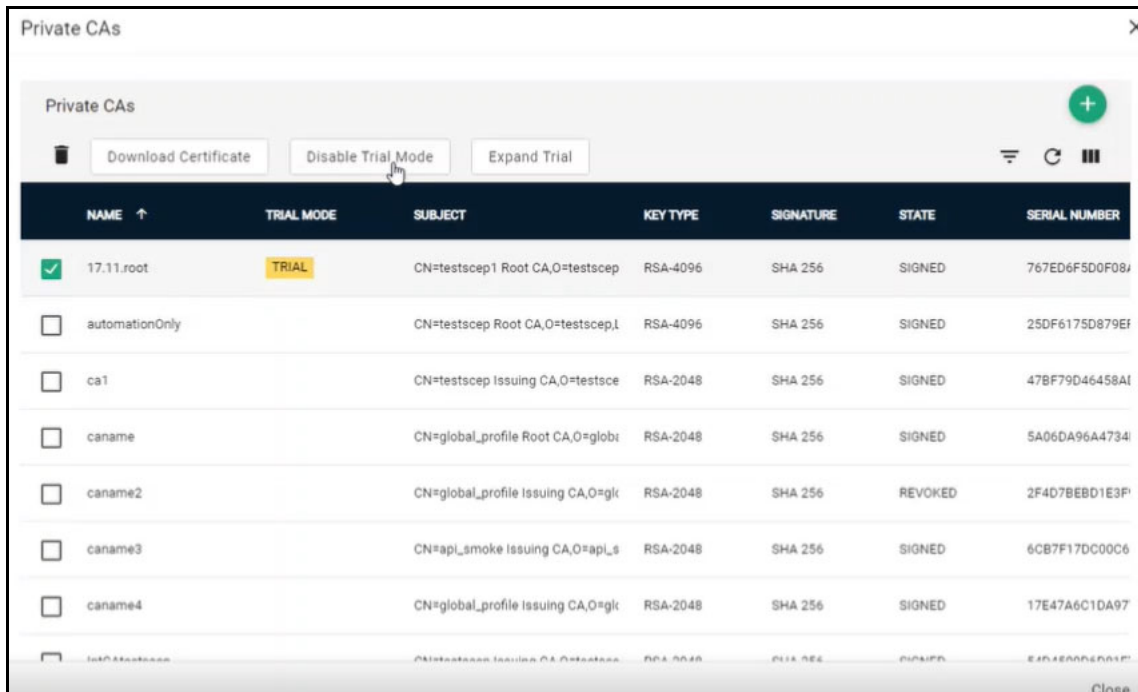
The screenshot shows a web form titled "Request Trial CA" with a close button (X) in the top right corner. At the top, there is a progress bar with five steps: "Basic info" (checked), "Template" (checked), "Signature Algorithm" (checked), "4 CA Subject" (current step, highlighted), and "5 Confirmation" (not started). Below the progress bar are four input fields, each with a red asterisk indicating a required field: "Customer Name", "City or Locality", "State or Province", and "Country". The "Country" field has a dropdown menu with "United States" selected. At the bottom left is a "Close" button, and at the bottom right are "Back" and "Next" buttons.

10. Enter your customer name in the **Customer Name** field. This value is used for the Organization (O) and Common Name (CN) fields when generating the private CA certificate. In the case of CN, either Root CA or Issuing CA is appended depending on whether the parent issuer is set to self-issued root or another CA.
11. Enter your city in the **City or Locality** field.
12. Enter your state or province in the **State or Province** field.
13. Select your country.
14. Click **Next** to open the **Confirmation** page shown in the following illustration.



15. Click **OK** to confirm your trial.

The private CA is added to the **Private CAs** page; trial mode is indicated in the **Trial Mode** column. You can now disable or expand the trial by clicking the appropriate buttons.



To enroll certificates against a new issuing CA, you first need to add certificate profiles for each type of certificate you want to issue using the new CA. Certificate templates, one each for client, code signing, SSL, and device profiles, are provided with the new CA for this purpose. See [“How to manage certificate profiles”](#) on page 160.

NOTE: Regardless of any term set for certificate profiles that you create, all certificates enrolled against a trial private CA are limited to 30 days.

Using SCM with Microsoft Azure and Intune

This chapter provides information on how to integrate SCM with Microsoft Azure and configure Microsoft Intune for enrollment and management of client and device certificates.

This chapter describes the following topics:

- [Microsoft Azure configuration overview](#)
- [Configuring Azure for Azure Key Vault](#)
- [Configuring Azure for Intune SCEP](#)
- [Configuring Azure for Intune Exporter](#)
- [Registering applications in Azure](#)
- [Configuring SCM Azure accounts](#)

10.1 Microsoft Azure configuration overview

The SCM integration with Microsoft Azure enables you to do the following:

- Use Azure Key Vault for automatic CSR generation and SSL certificate storage when enrolling SSL certificates using the built-in wizard in SCM.
- Use Microsoft Intune configured for SCEP to issue and manage certificates for mobile devices.
- Automatically export client certificates and private keys from SCM to Intune.

SCM can be integrated with the Microsoft Azure for the following:

- Azure Key Vault—generate CSRs automatically and store SSL certificates when enrolling certificates using the built-in wizard.
- Intune with SCEP—issue and manage certificates for mobile devices.
- Intune Exporter—export client certificates and private keys from SCM to Intune.

Connecting to an Azure service from SCM requires the following:

- In Azure—Registering an application for each service that you will be using.
You add an application registration in Azure for each service you will be using with SCM.
- In Azure—Configuring the application for the service that you will be using.
Each type of service you will be using with SCM (Azure Key Vault, SCEP, and Intune Exporter) requires configuring for the specific requirements of the service.
- In SCM—Creating a corresponding Azure Account for each registered application.
SCM uses Azure accounts to authenticate itself with the Azure application.

Azure integration requires the following:

- an active Azure subscription
- at least one resource group configured

10.2 Configuring Azure for Azure Key Vault

This section assumes that you have at least one resource group configured in Azure and at least one key vault assigned to the resource group.

Azure key vault is only available if enabled for your account. Contact your Sectigo account manager.

The process of configuring Azure and SCM for use with Azure Key Vault involves the following:

- In Azure:
 - Register an application—an application must be added to Azure to allow SCM to authenticate and access the vault. This process generates the Application ID and Directory ID you will use to create an Azure Account in SCM. See [“Registering applications in Azure” on page 223](#).
 - Set API permissions for the application to grant the application access to the Azure Key Vault API. This process also generates the client secret that will be used to authenticate SCM to the application.
 - Grant the application access to resource groups containing the key vaults you want to use.
 - Grant the application access to key vaults.
- In SCM:
 - Set up an SCM Azure Account—SCM connects to Azure applications via Azure accounts configured in SCM, using the application ID, directory ID, and client secret. See [“Configuring SCM Azure accounts” on page 226](#).

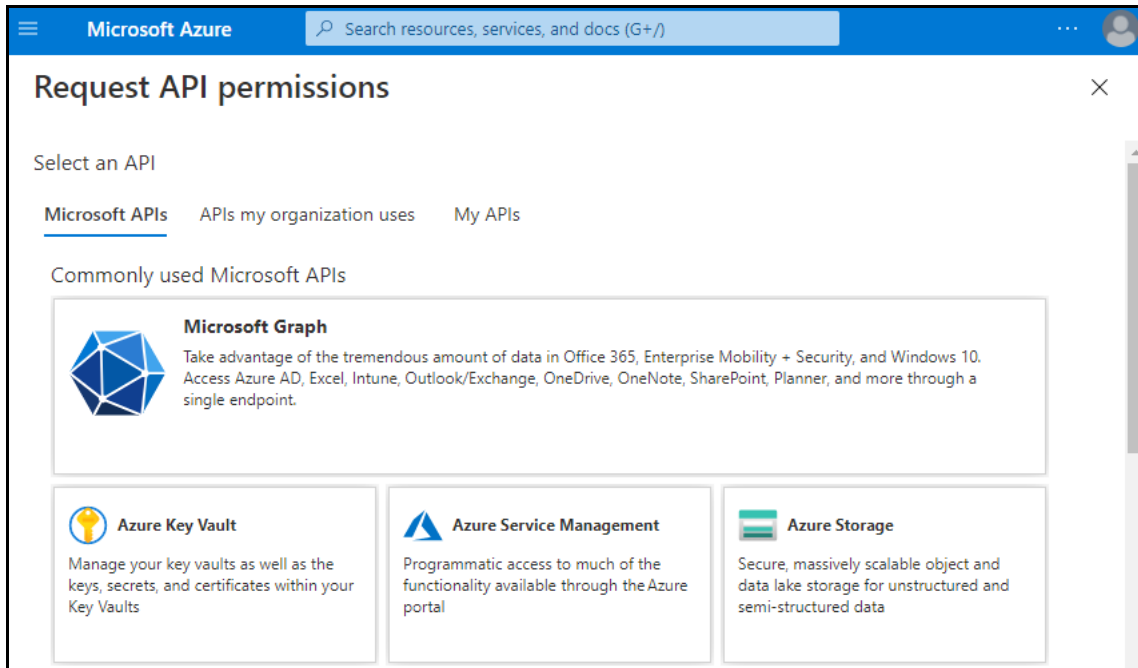
For information on enrolling SSL certificates in Azure Key Vault, see [“Generation of CSR in Azure Key Vault” on page 65](#).

10.2.1 How to set API permissions for Azure Key Vault

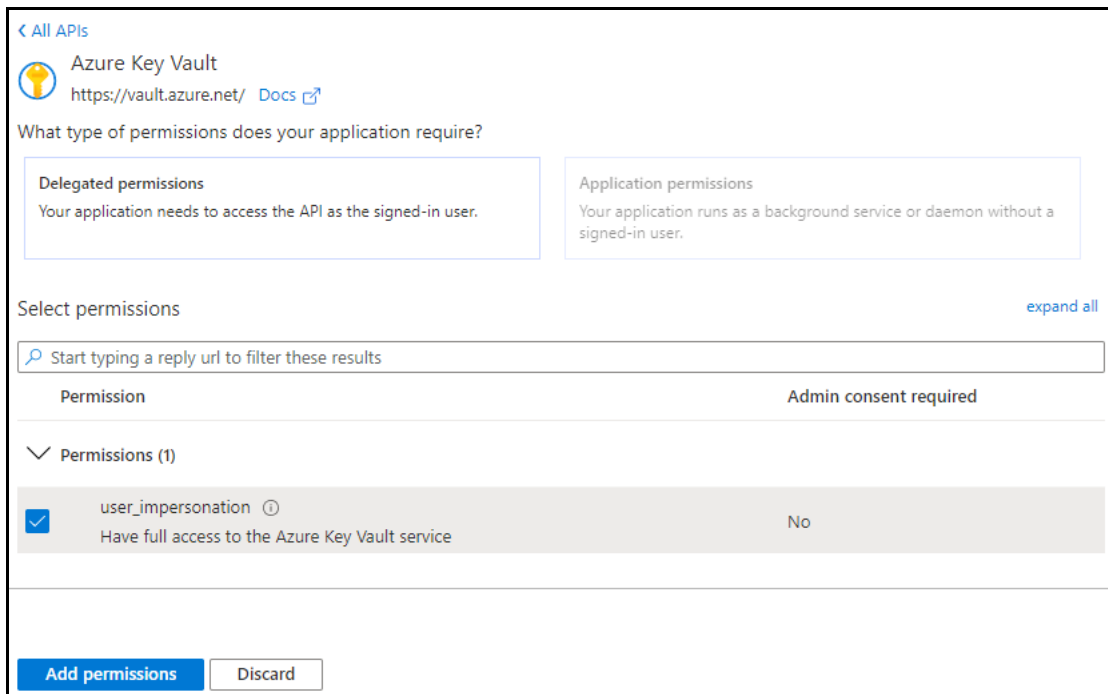
This section assumes that you have registered an application in Azure for use with Azure key vault (see [“Registering applications in Azure” on page 223](#)).

To set the API permissions for your Azure Key Vault application in Azure:

1. Sign in to Microsoft Azure portal at <https://portal.azure.com>
2. Navigate to the **App registrations** page.
3. Select the application you registered for Azure Key Vault.
4. Under **Manage**, select **API permissions** and click **Add a permission** to open the **Request API permissions** page, as shown in the following illustration.



5. Select **Azure Key Vault** to display the **Azure Key Vault** options.



6. Under **Select permissions**, select **user_impersonation**.

7. Click **Add permissions**.

8. Under **Manage**, select **Certificates & secrets**.

The screenshot shows the Microsoft Azure portal interface for managing a Sctigo Certificate Manager application. The left-hand navigation pane is expanded to 'Certificates & secrets'. The main content area displays instructions on credentials and certificates, followed by an 'Upload certificate' button. Below this, a table with columns 'Thumbprint', 'Start Date', and 'Expires' is shown, indicating no certificates are currently added. Further down, there is a 'New client secret' button and another table with columns 'Description', 'Expires', and 'Value', also indicating no client secrets are currently created.

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

The 'Add a client secret' dialog box contains a text input field for 'Description'. Below it, the 'Expires' section has three radio button options: 'In 1 year' (which is selected), 'In 2 years', and 'Never'. At the bottom of the dialog, there are two buttons: 'Add' and 'Cancel'.

10. Provide a description (such as SCM Access), select **Never**, and click **Add**.

The client secret is added to the **Client secrets** list.

11. Copy and record the secret **Value**.

This value is needed to create the SCM Azure Account that will be used to connect to your Azure application.

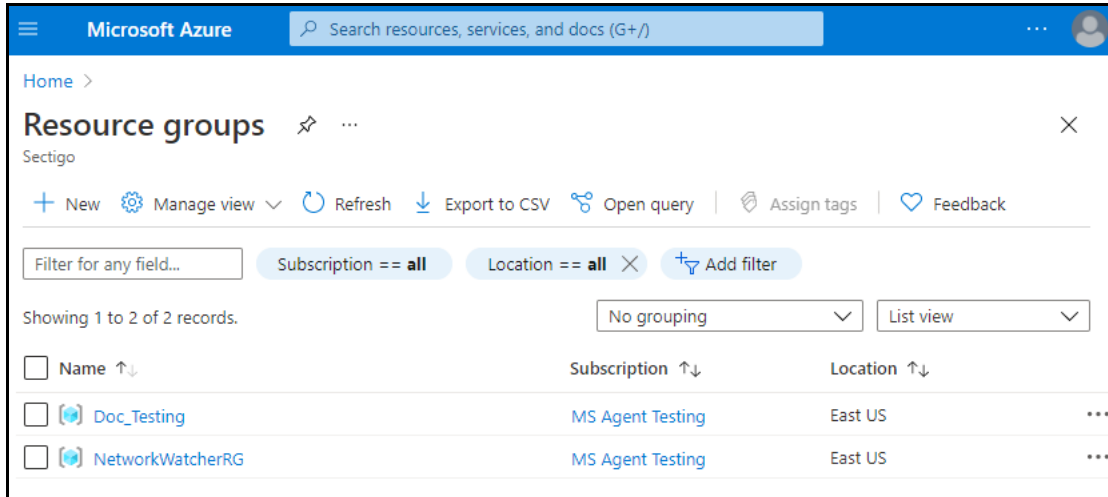
NOTE: The secret value is equivalent to a password and is not accessible after you leave the window. Copy and save it in a private location.

10.2.2 How to grant an application access to resource groups

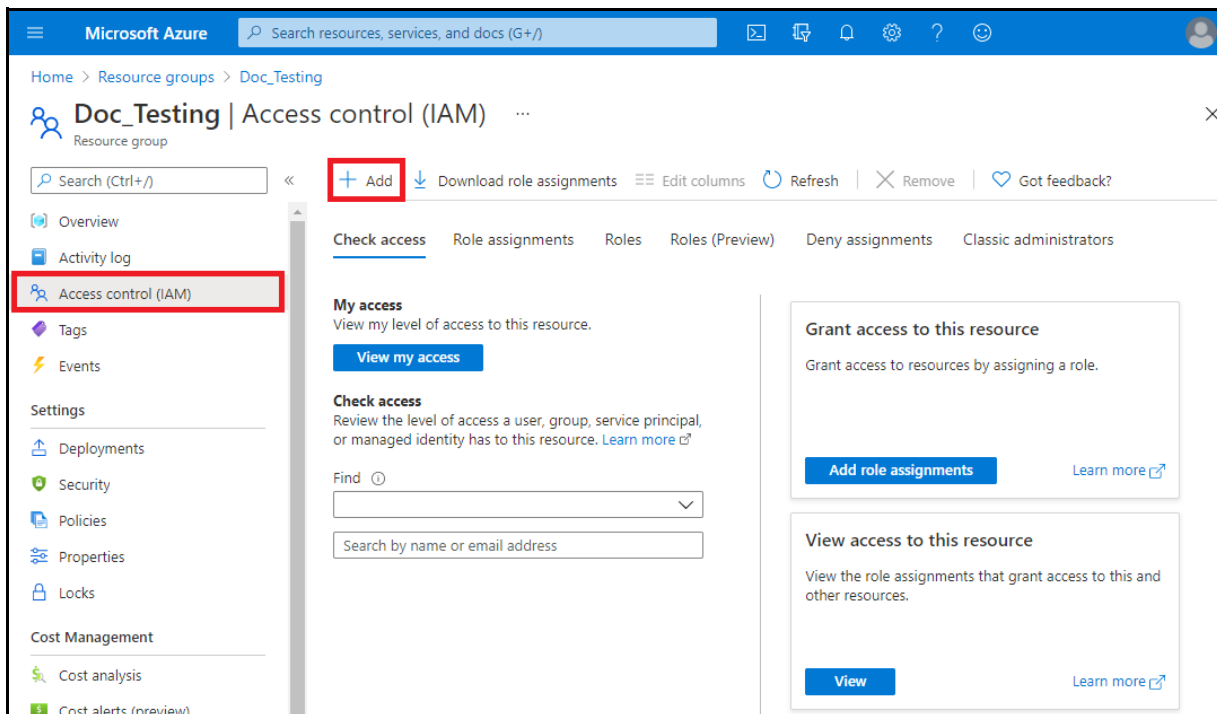
To give the registered application access to resource groups and key vaults, do the following:

1. Sign in to Microsoft Azure portal at <https://portal.azure.com>
2. Navigate to the **Resource groups** page shown in the following illustration.

NOTE: Access can also be given at the **Subscription** level, if necessary.



3. Select the resource group containing the appropriate Key Vault.
4. Select **Access control**, as shown in the following illustration.



5. Click **Add > Add Role Assignment**.

6. Complete the **Add role assignment** fields based on the information provided in the following table, then click **Save**.

Field	Value
Role	Key Vault Contributor
Assign access to	Azure AD user, group, or service principal
Select	The name given to the application during registration, e.g., Sectigo Certificate Manager Key Vault.

10.2.3 How to grant an application access to Key Vaults

To enable the registered application to create a certificate in the Key Vault, do the following:

1. Sign in to Microsoft Azure portal at <https://portal.azure.com>
2. Search for **Key vaults** to navigate to the **Key vaults** page.
3. Select the appropriate key vault.
4. Select **Access policies** for this key vault.
5. Click **Add Access Policy**.
6. Complete the **Add access policy** fields based on the information in the following table and click **Add**.

Field	Value
Configure from template	Certificate Management
Key permissions	Default
Secret permissions	Default
Certificate permissions	Default
Select principal	The name given to the application during registration, e.g., Sectigo Certificate Manager Key Vault.
Authorized application	Default

10.3 Configuring Azure for Intune SCEP

SCEP is a certificate enrollment protocol standard designed to provide scalability to digital certificate issuance. SCEP is only available if enabled for your account. Contact your Sectigo Account Manager.

The process of integrating SCM with Microsoft Azure and configuring Microsoft Intune for SCEP involves the following:

- In Azure:
 - **Register** an application—an application must be added to Azure to allow SCM to authenticate and perform SCEP request validation. This process generates the Application ID and Directory ID you will use to create an Azure Account in SCM. See [“Registering applications in Azure” on page 223](#).
 - **Set** API permissions for the Intune application to allow access to SCEP request validation resources. This process generates the client secret that will be used to authenticate SCM to the application.
- In SCM:
 - **Set up** an SCM Azure Account—SCM connects to Azure applications via Azure accounts configured in SCM, using the application ID, directory ID, and client secret. See [“Configuring SCM Azure accounts” on page 226](#).
 - **Add** client and/or device certificate Intune SCEP endpoints—The Intune SCEP endpoints define the URLs that Intune applications use to connect to the SCM SCEP server.
- In Microsoft Endpoint Manager (MEM):
 - **Create** a trusted profile—The trusted profile is configured with a trusted certificate provided by Sectigo. This is used to secure communication with the SCM SCEP server.
 - **Create** a SCEP profile for each platform (e.g., Android, iOS)—SCEP profiles must be created for each target device platform, and configured with the trusted profile and the appropriate SCM Intune SCEP endpoint URL.

Additionally, for certificates to be enrolled on target devices, the Intune Company Portal must be installed on the device, using the application store associated with the particular platform (i.e., Google Play for Android or Apple App Store for iOS). If everything is configured correctly, enrollment is completed after the first sign-on to the Intune Company Portal. The Intune Company Portal may take measures to enforce security. For example, it can run on password-protected devices. Each group for which enrollment of device certificates through Intune is enabled must have only one set of Profiles assigned. This also implies that these profiles must be created for use on one particular platform.

Everything else, including reading of profiles, request and validation of the certificate, as well as the subsequent certificate enrollment and notification about the process completion occurs seamlessly in the background of the device.

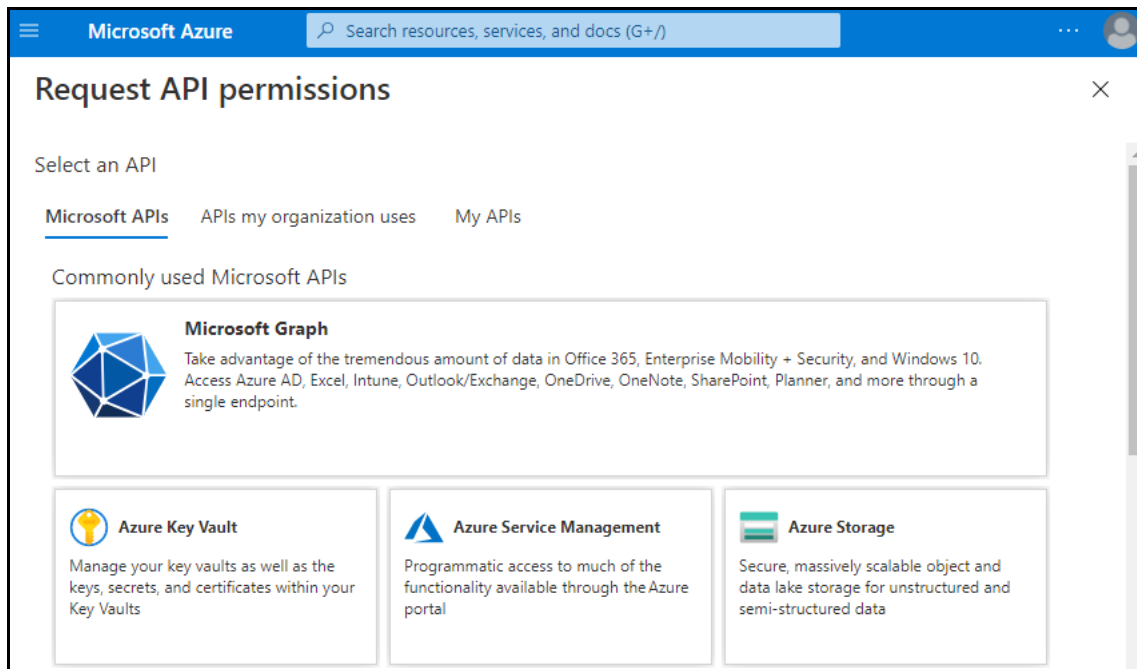
NOTE: The application configuration and profile registration processes are platform-dependent. The procedures described are applicable to iOS devices only, unless stated otherwise.

10.3.1 How to set API permissions for Intune SCEP

This section assumes that you have registered an application in Azure for use with Intune SCEP (see “[Registering applications in Azure](#)” on page 223).

To set the API permissions for your Intune SCEP application in Azure:


1. Sign in to Microsoft Azure portal at <https://portal.azure.com>
2. Navigate to the **App registrations** page.
3. Select the application you registered for Intune SCEP.
4. Under **Manage**, select **API permissions** and click **Add a permission** to open the **Request API permissions** page, as shown in the following illustration.



5. Under **Microsoft APIs**, select **Intune** to display the **Request API Permissions** page shown in the following illustration.

Request API permissions ✕

[← All APIs](#)


Intune
<https://api.manage.microsoft.com/> [Docs](#)

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.

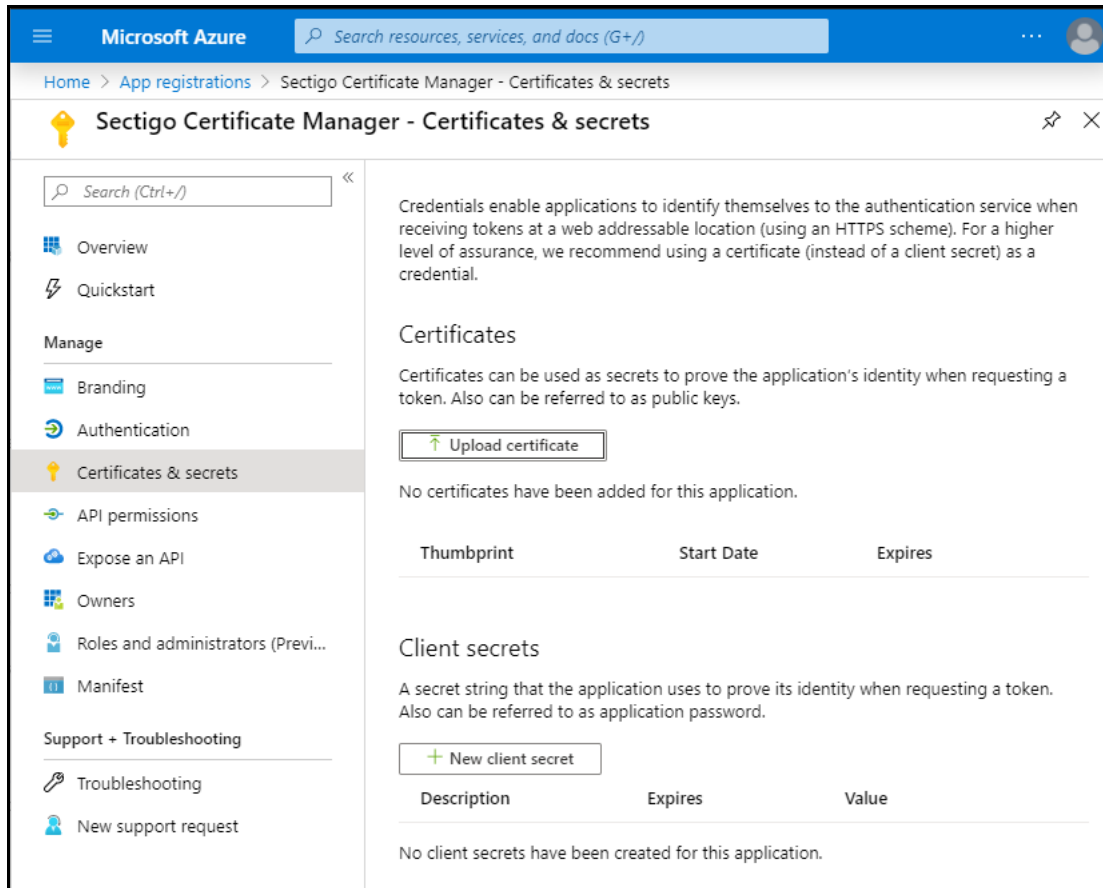
Select permissions [expand all](#)

	Permission	Admin consent required
✓	Permissions (1)	
<input type="checkbox"/>	get_data_warehouse ⓘ Get data warehouse information from Microsoft Intune	Yes
<input type="checkbox"/>	get_device_compliance ⓘ Get device state and compliance information from Microsoft Intune	Yes
<input type="checkbox"/>	manage_partner_compliance_policy ⓘ Manage partner compliance policies with Microsoft Intune.	Yes
<input type="checkbox"/>	pfx_cert_provider ⓘ PFX certificate management	Yes
<input checked="" type="checkbox"/>	scep_challenge_provider ⓘ SCEP challenge validation	Yes

Add permissions
Discard

6. Select **Application permissions**.
7. Select **SCEP challenge validation**, and then click **Add permissions**.
It is essential to perform this step, as Microsoft Intune differentiates between added permissions and granted permissions.
8. Under **Manage**, select **API permissions** and click **Add a permission** to open the **Request API permissions** page.
9. Select **Microsoft Graph**, and then select **Application permissions**.
10. Use search to locate and enable the following permission: Application.Read.All
11. Click **Add permissions**.
12. If you are an administrator in Azure, click **Grant admin consent for Sectigo**. If you are not an administrator in Azure, you need to wait for an Azure administrator to approve the permissions before continuing.

13. Under **Manage**, select **Certificates & secrets**.



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

The 'Add a client secret' dialog box contains the following elements:

- A text input field labeled 'Description'.
- An 'Expires' section with three radio button options: 'In 1 year' (which is selected), 'In 2 years', and 'Never'.
- 'Add' and 'Cancel' buttons at the bottom.

15. Provide a description (such as SCM Access), select **Never**, and click **Add**.

The client secret is added to the **Client secrets** list.

16. Copy and record the secret **Value**.

This value is used to create the SCM Azure Account that will be used to connect to your Azure Intune SCEP application.

NOTE: The secret value is equivalent to a password and is not accessible after you leave the window. Copy and save it in a private location.

10.3.2 How to add Intune SCEP endpoints in SCM

RAO and DRAO administrators can only create and modify enrollment endpoint accounts for organizations and departments that are delegated to them.

The following requirements must be met for the process to succeed:

- Your account must have SCEP enabled for device and/or client certificates and corresponding RA certificates configured. Contact your Sectigo account manager for details.
- Your account must have Intune enabled. Contact your Sectigo account manager for details.
- You must have at least one certificate profile configured for use with client or device certificates. For more information on certificate profiles, see [“How to manage certificate profiles” on page 160](#).
- You added an SCM Azure Account that is linked to a registered Azure application that has been configured for Intune SCEP (see [“How to add an Azure account” on page 227](#)).

To add or modify Intune SCEP enrollment endpoints, do the following:

1. In SCM, navigate to **Enrollment > SCEP**.
2. Click **Add** to display the **Create Enrollment Endpoint** dialog, and select **Client certificate Intune SCEP** or **Device certificate Intune SCEP** from the **Type** list.

To modify an Intune SCEP endpoint, select the endpoint and click **Edit**.

The screenshot shows a dialog box titled "Create Enrollment Endpoint" with a close button (X) in the top right corner. The dialog contains the following elements:

- A "Name" field with a red asterisk (*) indicating it is required.
- A "Type" dropdown menu currently set to "Client certificate Intune SCEP".
- An information box (i) containing the text: "The SCEP enrollment endpoint allows for enrollment of Client certificates using the Simple Certificate Enrollment Protocol as described in RFC 8894. Sectigo Certificate Manager supports the Intune challenge validation process using assigned Azure account."
- At the bottom, there are two buttons: "Cancel" and "Next".

3. Click **Next** and complete the **Create Enrollment Endpoint** form.

4. Complete the fields referring to the following table, then click **Save**.

Field / Element	Description
Type	The type of endpoint to add. Intune SCEP Options include Client certificate Intune SCEP and Device certificate Intune SCEP. This option is only available when adding an endpoint.
Name	A descriptive name for the endpoint.
Organization	The organization associated with the endpoint. Once an endpoint is created, the organization cannot be changed.
Department	The department associated with the endpoint. Once an endpoint is created, the department cannot be changed.
SCEP RA Certificate	The RA certificate associated with the endpoint. The RA certificate should be issued from the same backend that will be used to issue the certificates. For information about viewing your RA certificates, see “Managing SCEP RA certificates” on page 176 .
GetCert Response Format	The format of the CA certificate that is provided to SCEP.

Field / Element	Description
GetCACert Response Format	The format of the RA certificate that is provided to SCEP.
Profile	The certificate profile that is used when enrolling certificates using this endpoint.
Term	The term for certificates enrolled via the endpoint.
Azure Account	The SCM Azure account that connects to your registered Azure Intune SCEP application.
URI Extension	The URI extension used to create a unique URL for the endpoint that SCEP clients will use to connect to the SCM SCEP server. The URL is automatically shown below the URI Extension field, and should be used in the SCEP profile so the client can access the SCEP server.

10.3.3 How to create trusted certificate profiles

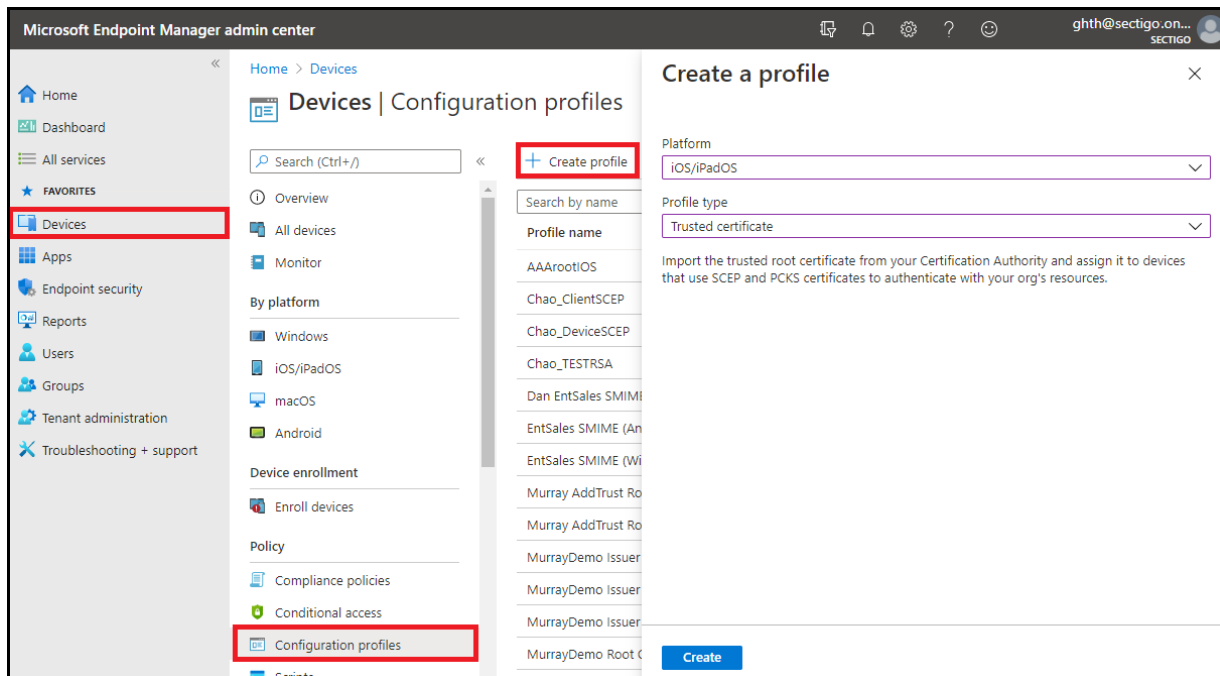
Trusted certificate profiles must be created in MEM for each platform (e.g., iOS, Android). Each profile contains a trusted certificate that allows enrolled devices to trust the SCEP server.

The trusted certificate files are provided by Sectigo, and include root and intermediate certificates. You will create trusted certificate profiles for both root and intermediate for each platform you want to support.

For more information on creating trusted root certificate profiles in Intune, visit <https://docs.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root>.

You can create and assign trusted certificate profiles as follows:

1. Sign in to MEM portal at <https://endpoint.microsoft.com>.
2. Select **Devices > Configuration profiles**.
3. Click **Create profile**, and then do the following:
 - a. Select the platform (for example, iOS/iPadOS).
 - b. Select **Templates > Trusted certificate** as profile type.
 - c. Click **Create**.



4. In the **Trusted certificate** screen, do the following:
 - a. Enter the profile name. It is recommended to combine information about the platform and type of trusted certificate (for example, iOS CA Root).
 - b. Enter a description.
 - c. Click **Next**.
 - d. Upload the DER-encoded trusted certificate file you received from Sectigo. This file is issued by your CA as a public certificate. It can also come from any device that trusts your issuing CA.
 - e. Click **Next**.
 - f. Add a group to assign or click **Add all devices**.
 - g. Click **Next**.
 - h. Click **Create**.

These steps must be performed for each trusted certificate.

10.3.4 How to create SCEP profiles

Before creating a SCEP profile, you will need the following:

- The trusted profile created in “[How to create trusted certificate profiles](#)” on page 215.
- The Intune SCEP endpoint URL configured in SCM. See “[How to add Intune SCEP endpoints in SCM](#)” on page 213.

For more information on creating SCEP certificate profiles in Intune, visit <https://docs.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep>.

You can create a SCEP profile and point it to SCM as follows:

1. Sign in to MEM portal at <https://endpoint.microsoft.com>.
2. Select **Devices > Configuration profiles**.
3. Click **Create profile**, and then do the following:
 - a. Select the platform (for example, iOS/iPadOS).
 - b. Select **SCEP Certificate** as profile type.
 - c. Click **Create**.
4. In the **SCEP certificate** screen, do the following:
 - a. Enter the profile name. It is recommended to combine information about the platform and type of trusted certificate (for example, iOS SCEP).
 - b. Enter a description.
 - c. Click **Next**.
 - d. Set the certificate type to **User** to issue client certificates, or **Device** to issue device certificates.
 - e. If the certificate type is **User**, set the **Subject name format** to `CN={{UserName}}@<domain>`, where domain is the domain of organization or department of the users who will be issued the certificates.
 If the Certificate type is **Device**, set the **Subject name format** to `CN={{AAD_Device_ID}}`.
 - f. Set the **Subject Alternative Name** to one of the values, such as an email address.
 It is recommended that you only set one option, as multiple options may cause errors in the Intune company profile. Optionally, you may select a **User Principal Name (UPN)** to be included in the client certificate, in which case this additional name (UPN) is appended to the RFC822 name in the Subject Alternative Name field. For a UPN to be sent with the request, the **Allow Principal Name** option must be enabled (it is off by default) for the appropriate organization or department in SCM (see Edit certificate settings).
 - g. Set the certificate validity period to **1 year**.
 - h. Set **Key usages** to **Digital signature** (Device) or **Digital signature and Key encipherment** (User).
 - i. Set **Key size** to **2048**.
 - j. Set **Root Certificate profile** to the intermediate trusted profile created in ["How to create trusted certificate profiles"](#) on page 215.
 - k. Specify **Extended key usage** by selecting **Client Authentication**.
 - l. Set SCEP Server URLs to the Intune SCEP endpoint URLs configured in SCM.

NOTE: If the profile is for Windows, delete `pkiclient.exe` from the SCEP URL, as this will be automatically appended by Windows.
 - m. Click **Next**.
 - n. Add a group to assign or click **Add all devices**.
 - o. Click **Next**.
 - p. Click **Create**.

10.3.5 Strong mapping in Microsoft Intune certificates

Microsoft Intune will soon be including the device or user SID in requests to the SCEP endpoint. It will be included as an URL in the SAN:

```
tag:microsoft.com,2022-09-14:sid:<value>
```

Visit <https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-implementing-strong-mapping-in-microsoft-intune-ba-p/4053376> for more details.

SCM will detect the SID and include it in requests to the Sectigo Private CA automatically. To include it within your private certificates, contact Sectigo to ensure your custom certificate templates include the SID value. The SID in the issued certificate can be formatted in either the URL in SAN format as requested or the previous certificate extension format (OID 1.3.6.1.4.1.311.25.2).

A SCEP profile is loaded on each device requiring certificates from SCM. SCEP profiles must be created in MEM for each target device platform, and configured with the corresponding trusted profile and the appropriate SCM Intune SCEP endpoint URL.

10.3.6 Issues and limitations related to different platforms

On iOS devices, Apple MDM Push Certificate must be installed to allow access to Microsoft Intune. The process includes downloading the MDM Certificate from Microsoft Azure and sending it to the Apple portal. For more information, see the following:

- Get an Apple MDM push certificate at <https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get>
- Intune and the APNs certificate: FAQ and common issues at <https://techcommunity.microsoft.com/t5/Intune-Customer-Success/Intune-and-the-APNs-certificate-FAQ-and-common-issues/ba-p/280121>

On Android devices, Microsoft Azure displays the enrollment status as **Failed** for a few minutes after accepting the new certificate by the device owner following a successful certificate enrollment. This status changes to **Successful** in the background during the device synchronization.

10.4 Configuring Azure for Intune Exporter

Intune Exporter enables you to automatically export client certificates and private keys from the SCM Sectigo Key Vault to Intune for use with mobile device management.

Intune Exporter is only available if enabled for your account. Contact your Sectigo account manager.

Before configuring Intune Exporter, you must ensure that SCM can map to your Intune account. SCM can map persons to users in your Intune account when one of the following requirements is satisfied:

- The Principal Name (UPN) for the person account (client certificate) in SCM must be the same as the **user name** in Azure. It is recommended that you choose this approach.

- The **Email** for the person account (client certificate) in SCM must be the same as the **mail** attribute in Azure. For more information on how to configure the Azure's **mail** attribute, consult Microsoft's documentation.

The process of configuring Azure and SCM for Intune Exporter involves the following:

- In Azure:
 - Register an application—an application must be added to Azure to allow SCM to authenticate and access Intune. This process generates the **Application ID** and **Directory ID** you will use to create an Azure Account in SCM. See [“Registering applications in Azure” on page 223](#).
 - Set API permissions for the application to allow access to SCEP request validation resources. This process generates the client secret that will be used to authenticate SCM to the application.
- On your server:
 - Install and configure the **Certificate Connector for Microsoft Intune**.
This process generates the **Name**, **Provider name**, **Key name**, and **Public Key** that will be used to authenticate SCM to the Certificate Connector for Microsoft Intune.
- In SCM:
 - Set up an SCM Azure Account—SCM connects to Azure applications via Azure accounts configured in SCM, using the application ID, directory ID, and client secret. See [“Configuring SCM Azure accounts” on page 226](#).
 - Create the Intune Exporter—Intune Exporter connects to Azure using the Azure Account, and to the Certificate Connector for Microsoft Intune using the **Name**, **Provider name**, **Key name**, and **Public Key**.

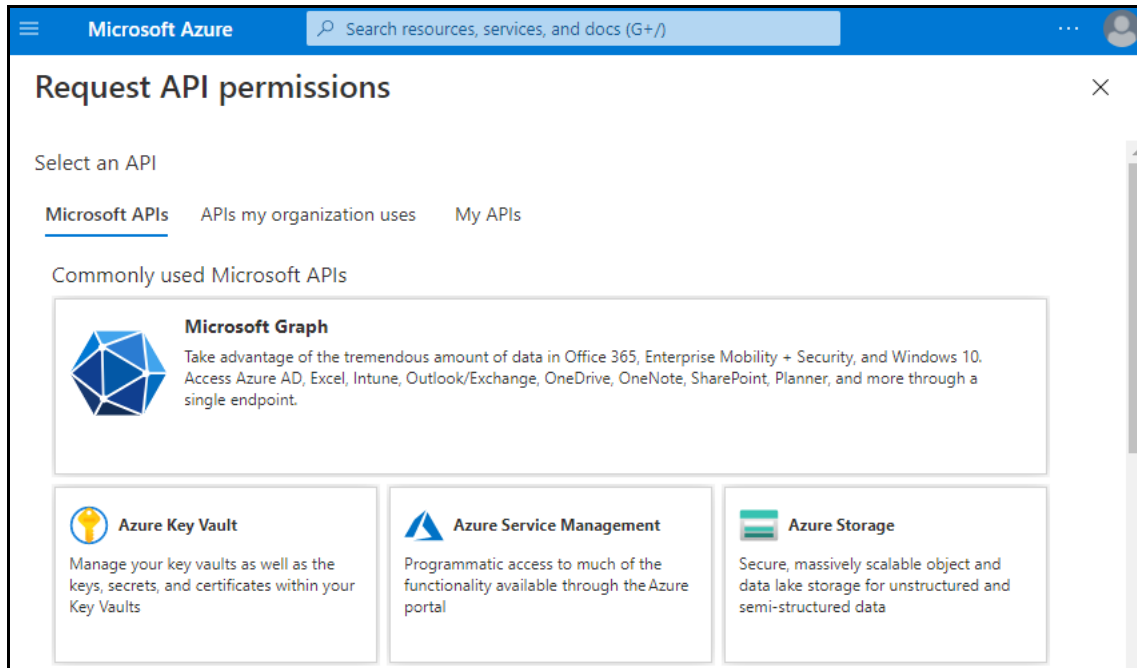
Client certificates can be manually exported to Intune using the **Export to Intune** option in the **Certificates for** dialog. See [“How to view end-user Client Certificates” on page 84](#).

10.4.1 How to set application API permissions for Intune Exporter

This section assumes that you have registered an application in Azure for use with Intune Exporter (see [“Registering applications in Azure” on page 223](#)).

To set the API permissions for your Intune Exporter application in Azure:

1. Sign in to Microsoft Azure portal at <https://portal.azure.com>
2. Navigate to the **App registrations** page.
3. Select the application you registered for Intune Exporter.
4. Under **Manage**, select **API permissions** and click **Add a permission** to open the **Request API permissions** page, as shown in the following illustration.



5. Select **Microsoft Graph**, and then select **Application permissions**.
6. Use search to locate and enable the following permissions:
 - Application.Read.All
 - User.Read.All
 - Directory.Read.All
 - DeviceManagementConfiguration.ReadWrite.All
7. Click **Add permissions**.
8. If you are an administrator in Azure, click **Grant admin consent for Sectigo**. If you are not an administrator in Azure, you need to wait for an Azure administrator to approve the permissions before continuing.
9. Under **Manage**, select **Certificates & secrets**.
10. Click **New client secret** to display the **Add a client secret** dialog.
11. Provide a description (such as SCM Access), select **Never**, and click **Add**.
The client secret is added to the **Client secrets** list.
12. Copy and record the secret **Value**.
This value is used to create the SCM Azure Account that will be used to connect to your Azure Intune SCEP application.

NOTE: The secret value is equivalent to a password and is not accessible after you leave the window. Copy and save it in a private location.

10.4.2 How to configure Intune to use imported certificates

To configure your Intune infrastructure for using imported PKCS certificates, do the following:

1. Navigate to <https://docs.microsoft.com/en-us/intune/protect/certificates-imported-pfx-configure> and use the Microsoft documentation complete the following steps:

- a. Download, install, and configure the Certificate Connector for Microsoft Intune.
- b. Build PFXImport PowerShell Project cmdlets.
- c. Create the encryption public key.

You must export the key to a file using the following command:

```
Export-IntunePublicKey -ProviderName "<ProviderName>" -KeyName  
"<KeyName>" -FILEFORMAT "PEM" -FilePath "<File path\Filename.PFX>"
```

When following the Microsoft documentation, skip the **Import PFX Certificates** and **To import the PFX certificate** sections.

- d. Create a PKCS imported certificate profile.
2. Record your **Name**, **Provider name**, **Key name**, and **Public Key**.

10.4.3 How to configure SCM for Intune Exporter

Intune Exporter is only available if enabled for your account. Contact your Sectigo account manager.

The following requirements must be met for the process to succeed:

- Intune must be enabled for your account. Contact your Sectigo account manager.
- Sectigo Key Vault must be enabled for your account. Contact your Sectigo account manager.
- You configured Intune to use imported certificates and obtained the name, provider name, key name, and public key (see ["How to configure Intune to use imported certificates" on page 220](#)).
- You added an SCM Azure Account that is linked to a registered Azure application that has been configured for Intune SCEP (see ["How to add an Azure account" on page 227](#)).

To configure SCM for Intune Exporter, do the following:

1. From SCM, navigate to **Integrations > Intune Exporter**.
2. In the upper-right corner, click **Add** to open the **Intune Certificate Exporter Settings** shown in the following illustration.

Intune Certificate Exporter Settings

Certificate Manager needs to authenticate to Microsoft Intune to import certificates and private keys. To authenticate an app registration must be created in Azure and client secret created. The app registration must also be authorized to call the Microsoft Graph API. After app registration, add graph User.Read.All, Directory.Read.All and DeviceManagementConfiguration.ReadWrite.All permissions.

Azure Account *

NONE ▲ Test Connection

Certificate Manager needs to encrypt the exported certificates/private keys for a Microsoft PFX Connector. To encrypt the public key and key provider information is required.

Name *

Purpose

General ▲

Microsoft Graph Deployment

https://graph.microsoft.com ? [Read more](#)

Provider name *

Cancel Save

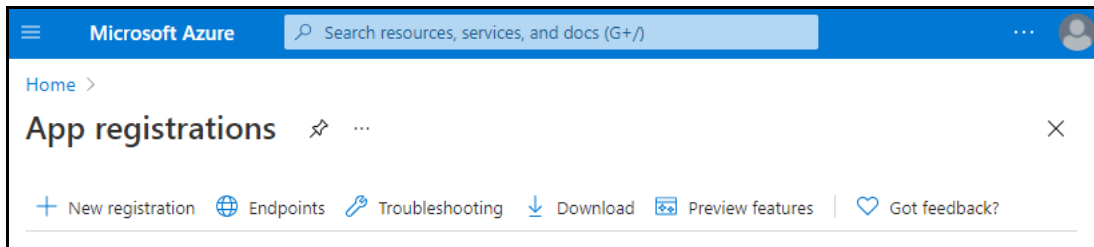
3. Select the Azure account linked to the application configured for Intune Exporter.
4. Click **Test Connection** to validate the data.
5. Select the purpose for the exported certificate.
6. Enter the URL of the Microsoft Graph Deployment.
7. Complete the **Name**, **Provider name**, **Key name**, and **Public Key** fields using the values you recorded during the Certificate Connector configuration.
8. Click **Save**.

10.5 Registering applications in Azure

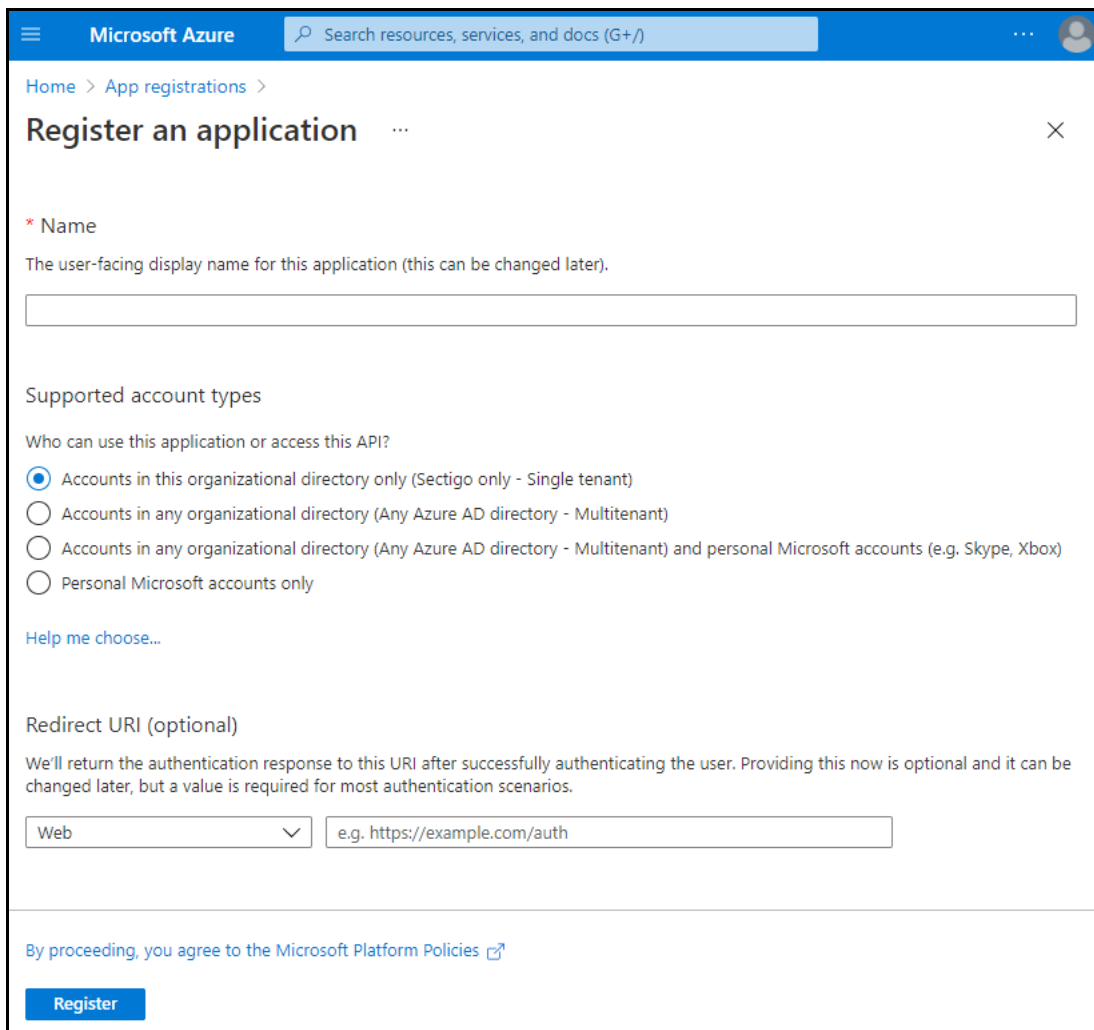
Whether you are adding an application to Azure for Azure Key Vault, Intune SCEP, or Intune Exporter, the steps for registering an application in Azure are the same.

To register an application in Azure, do the following:

1. Sign in to Microsoft Azure portal at <https://portal.azure.com>
2. Navigate to the **App registrations** page shown in the following illustration.



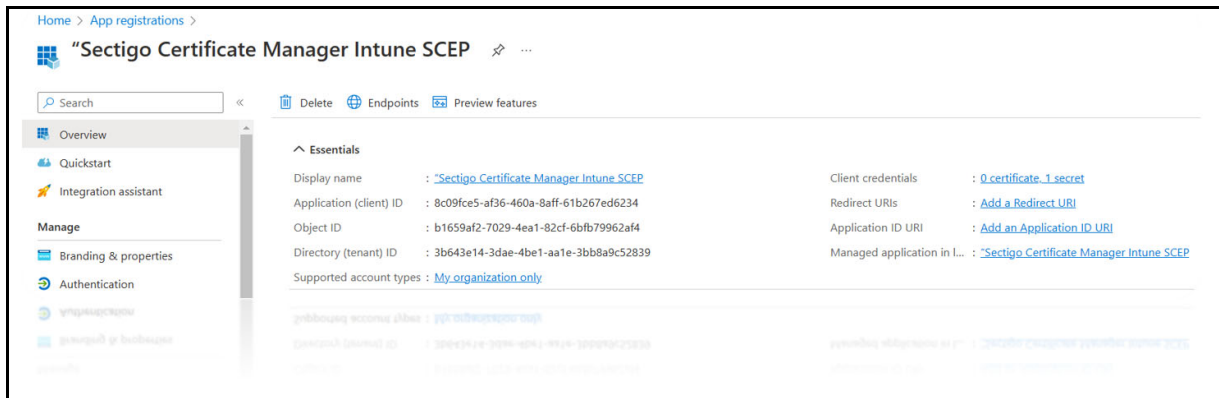
3. Click **New registration** to open the **Register an application** page.

A screenshot of the 'Register an application' page in the Microsoft Azure portal. The top navigation bar is blue with the 'Microsoft Azure' logo, a search bar, and a user profile icon. The breadcrumb is 'Home > App registrations >'. The main heading is 'Register an application' with a share icon and a close button. Below the heading, there is a form with the following sections:

- * Name**: A text input field with the placeholder text 'The user-facing display name for this application (this can be changed later)'. The field is currently empty.
- Supported account types**: A section titled 'Who can use this application or access this API?' with four radio button options:
 - Accounts in this organizational directory only (Sectigo 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 onlyA link 'Help me choose..' is located below the options.
- Redirect URI (optional)**: A section with the text 'We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.' Below this text is a dropdown menu set to 'Web' and a text input field containing 'e.g. https://example.com/auth'.

At the bottom of the page, there is a link 'By proceeding, you agree to the Microsoft Platform Policies' and a blue 'Register' button.

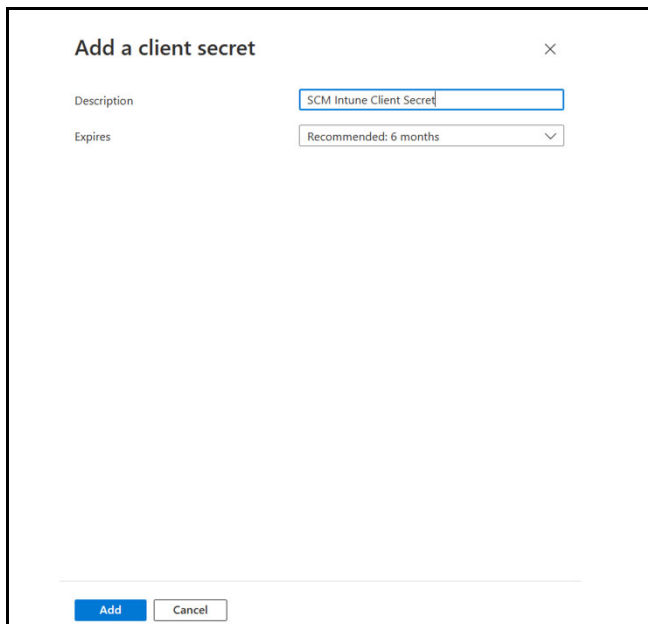
4. Enter a name for the application. For example:
 - for Azure Key Vault, enter **Sectigo Certificate Manager Key Vault**.
 - for Intune Exporter, enter **Sectigo Certificate Manager Intune Exporter**.
 - for Intune SCEP, enter **Sectigo Certificate Manager Intune SCEP**.
 5. Select **Accounts in this organizational directory only** (the default).
 6. Click **Register**.
- The application is created and displayed with the **Overview** selected.
7. Save the **Application (client) ID** and **Directory (tenant) ID** from the **Overview** section for the SCM registration.
 8. Select **Client Credentials** to create a new secret for SCM registration.



These values are used to create the SCM Azure Account that will be used to connect to the registered Azure application.

10.5.1 Creating Client Secret

1. Select **New Client Secret** and click **Add**.

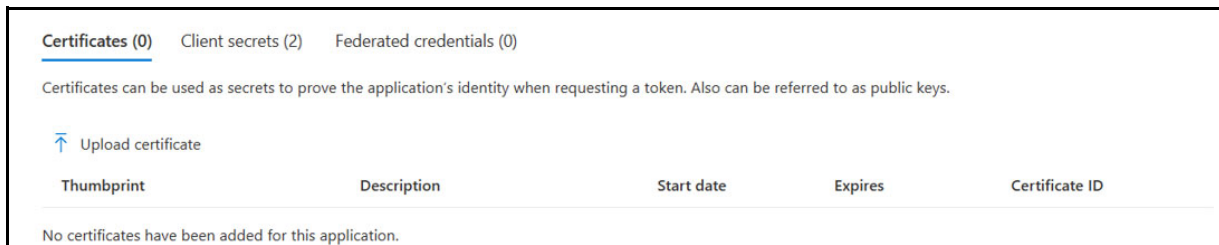


2. Copy and save the client secret.



10.5.2 Adding certificates

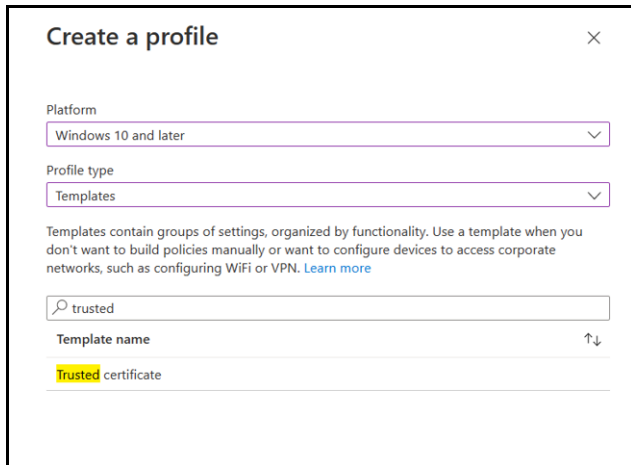
1. Select the **Certificates** tab.



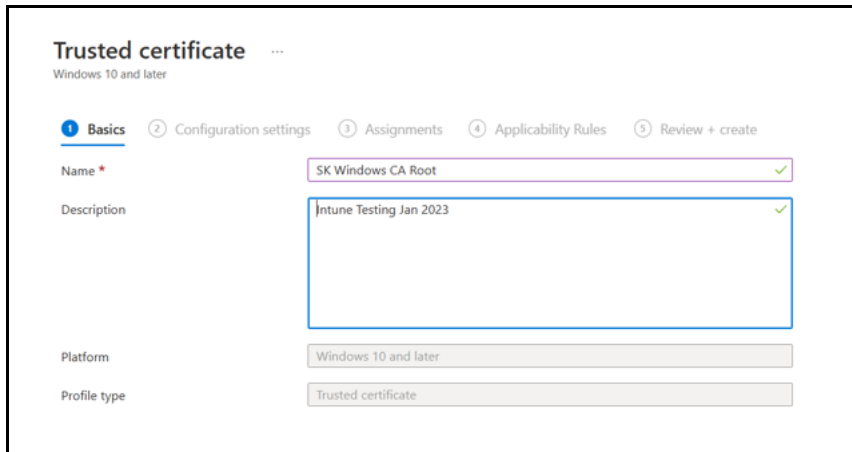
2. Click **Upload certificate > Add**.



3. Create a profile.



4. Add Trusted certificate details.



10.6 Configuring SCM Azure accounts

The **Integrations > Azure Accounts** tab shown in the following illustration enables you to manage the SCM Azure accounts used to connect SCM to Azure registered applications.

This section assumes that you have an active Azure subscription, at least one resource group configured, and have registered and configured the application that you want to connect to in Azure (see [“Registering applications in Azure”](#) on page 223).

Azure Accounts				
NAME	ENVIRONMENT	DIRECTORY ID	APPLICATION ID	DELEGATION MODE
<input type="checkbox"/> Azure Key Vault Account	Azure	3b643e14-3dae-4be1-aa1e-3bb8a9c52839	48e6b205-782c-4969-b40d-769d10b82f82	General

The following table lists settings and elements of the **Accounts** tab.

Field / Element	Description
Name	The name of the account.
Environment	The Azure environment.
Directory ID	The Directory (tenant) ID of the App registered in Azure.
Application ID	The Application (client) ID of the App registered in Azure.
Delegation Mode	The organizations and departments to which the account has been delegated.
Add	Enables you to add a new account.
Edit ^a	Enables you to edit the selected account.
Delete ^a	Deletes the selected account.
Delegate ^a	Enables you to delegate existing accounts to organizations and departments.

a. Controls appear only after selecting an account.

10.6.1 How to add an Azure account

You will need the **Directory ID** and **Application ID** for the registered application you are connecting to. These can be obtained in Azure from the **Overview** section for the application. You will also need the **Client Secret** that you created when you set API permissions for the application in Azure.

To add an Azure account, do the following:

1. Navigate to **Integrations > Azure Accounts** and click **Add** to display the **Add Azure Account** dialog shown in the following illustration.

Add Azure Account

Please delegate the account to proper organization(s) after creation

Name *

Environment *
Azure

Directory ID *

Application ID *

Application (client) Secret *

2. Enter a name for the account.
3. Choose the environment for the account.
4. Enter the registered app's **Directory ID**, **Application ID**, and **Client Secret**.
5. Click **Test Connection** to validate the data.
6. Click **Save**.

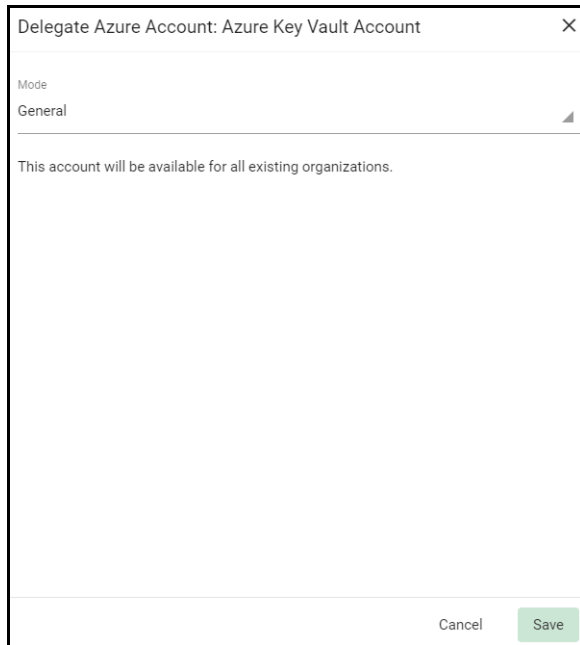
To edit or remove a connection between SCM and Azure Key Vault, navigate to **Integrations > Azure Accounts**, select the account, and click **Edit** to make changes or click **Reset** to remove the connection.

10.6.2 How to delegate Azure accounts

Azure accounts can be delegated for use with specific organizations and departments.

To delegate an Azure account, do the following:

1. Navigate to **Integrations > Azure Accounts**.
2. Select a certificate profile and click **Delegate** to open the **Delegate Azure Account** dialog shown in the following illustration.



Delegate Azure Account: Azure Key Vault Account

Mode
General

This account will be available for all existing organizations.

Cancel Save

3. Set the mode to **Customized** to select each organization and/or department that should have access to the Azure account, or to **General** to make it available to all existing organizations.
4. Click **Save**.

SCM agent integrations

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the SCM agents can now be found in the following locations:

- [Network agents](#)
- [PKS agents](#)
- [MS agents](#)
- [CA connectors](#)

Configuring settings

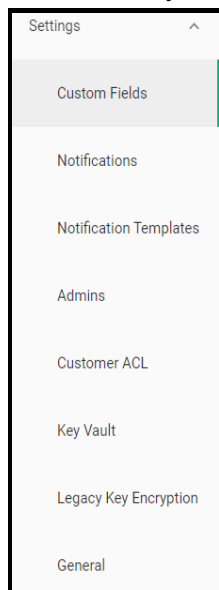
This chapter describes how to configure all settings available in SCM.

This chapter describes the following topics:

- The settings configuration overview
- Configuring organizations, departments, and domains
- Configuring notifications
- Configuring notification templates
- Configuring Key Escrow and encryption
- Successfully downloading the private key of a client certificate revokes that certificate.
- Configuring access control
- Managing SCM agents
- Configuring assignment rules
- Using Sectigo Key Vault
- Configuring Azure integration
- Managing General settings

12.1 The settings configuration overview

The **Settings** menu contains multiple areas that vary based on the features enabled for your account and your administrative privileges.



The **Custom Fields** page enables MRAOs to configure custom fields for use in certificate enrollment forms. SSL, client, and device certificates have a set of standard fields that contain information about the owner, domain, organization, department, address, etc. You can use custom fields to track additional information, such as an employee code or telephone number.

NAME	CERTIFICATE TYPE	MANDATORY FOR ADMIN UI	MANDATORY FOR REST API & ENDPOINTS	MANDATORY FOR SOAP API	MANDATORY FOR ENROLLMENT FORMS	ACTIVE
<input type="checkbox"/> ssl	SSL Certificate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> ssl*	SSL Certificate	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> client	Client Certificate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> client*	Client Certificate	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> device	Device Certificate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> device*	Device Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

The **Notifications** page enables you to set up and manage notifications sent to various recipients, including notifications triggered by the SSL certificate status, by the client certificate status, and by discovery scan summaries.

NAME	NOTIFICATION TYPE	ORGANIZATION/DEPARTMENT	CERTIFICATE PROFILE	CREATED
<input type="checkbox"/> SSL Expiration 3	SSL Expiration	org1/dep1, org1		admin n
<input type="checkbox"/> SSL Expiration	SSL Expiration	org1/dep1, org1		admin n
<input type="checkbox"/> Device Expiration	Device Certificate Expiration	ANY		admin n
<input type="checkbox"/> Client Expiration	Client Certificate Expiration	ANY		admin n
<input type="checkbox"/> CS Expiration	Code Signing Certificate Expiration	ANY		admin n
<input type="checkbox"/> Client admin created	Client Admin Creation	ANY		admin n
<input type="checkbox"/> Fun	Code Signing Certificate Enrolled (DL)	ANY		admin n
<input type="checkbox"/> Fun Email	Code Signing Certificate Enrolled (DL)	ANY		admin n

The **Notification Templates** page enables MRAOs to customize the contents of templates for event-based notifications.

NAME	RECIPIENT TYPE
<input checked="" type="checkbox"/> Auto Renewal Failed	Email
<input type="checkbox"/> Certificate is ready for manual installation	Email
<input type="checkbox"/> SSL Expiration	Email

The **Admins** page enables you to view and configure a list of administrative personnel. The contents of the list and availability of controls depends on your security role.

Admins						
Add IdP User Add Template +						
☰ ↻ ☰						
	NAME	EMAIL	USERNAME	TYPE	ROLE	ACTIVE
<input type="checkbox"/>	IdpUser12345 IdpUser012	user01@ccmqa.com	adminidp01	Standard	MRAO Admin	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Sr sosiedov	ihor.sosiedov@sectigo.com	ihor	Standard	MRAO Admin	<input checked="" type="checkbox"/>
<input type="checkbox"/>	IdpUser IdpUser02	user02@ccmqa.com	user02comodocom	IdP User	MRAO Admin	<input checked="" type="checkbox"/>
<input type="checkbox"/>	gn sn	test01@ccmqa.com	test01comodocom	IdP User	MRAO Admin	<input checked="" type="checkbox"/>
<input type="checkbox"/>	02	test02@ccmqa.com	test02comodocom	IdP User	MRAO Admin	<input checked="" type="checkbox"/>
<input type="checkbox"/>	IdpUser IdpUser03	user03@comodo.com	user03comodocom	IdP User	MRAO Admin	<input checked="" type="checkbox"/>

The **Customer ACL** page enables MRAOs to configure and limit incoming access to SCM to specific IP addresses and ranges. The access restrictions can be applied for all administrators or selectively for MRAO administrators only, or RAO and DRAO administrators only.

The **Departments** page is visible to DRAO administrators. It enables DRAOs to view all departments that have been delegated to them and to request new domains for those departments. See [“Configuring organizations and domains” on page 158](#).

Instead of **Departments**, MRAO and RAO administrators see the **Organizations** page that enables them to view, add, edit, and delete organizations, as well as assign departments and domains to the organizations.

The **Key Vault** page enables MRAOs to configure Sectigo Key Vault, used for storing and retrieving client certificate private keys.

Key Vault

Key Vault Recovery

Recovery Method Recover via iOS Mobilee Config or, PKCS#12 File

iOS Mobile Config Security

Digitally Sign iOS Mobile Config YES

Subject N/A

Issuer N/A

Serial Number N/A

Expires N/A

Exchange Configuration

Include Exchange Configuration in iOS Mobile Config YES

Exchange Server Host Name mail.office.com

Use SSL For Communication YES

Number of Past Days to Sync 30

Prevent Moving Messages to Another Account YES

The **Legacy Key Encryption** page enables you to configure Key Escrow for storing the private keys of client certificates so that these keys can be recovered at a later date by appropriately privileged administrators.

Legacy Key Encryption

SCOPE	NAME	STATUS
<input type="checkbox"/>	Master	testscep Public key is loaded

The **General** page enables MRAOs to configure the date format for displaying dates in SCM.

General

Settings

Date Format mm/dd/yyyy

Days before expiry validated domain is Action Required 30

12.2 Configuring organizations, departments, and domains

SCM enables MRAOs and RAOs SSL to create and maintain organizations and departments. DRAOs SSL can create and maintain departments.

Before you can request certificates, you first need to create domains and delegate them to organizations or departments. The delegated public domains must pass DCV that is initiated by a MRAO or RAO SSL, or DRAO SSL with sufficient privileges.

For more information, see [Understanding organizations and departments](#).

12.2.1 How to define custom fields

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the SCM custom fields can now be found in the following location:

- [Custom fields](#)

12.3 Configuring notifications

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the notifications can now be found in the following location:

- [Notifications](#)

12.4 Configuring notification templates

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the notification templates can now be found in the following location:

- [Notification templates](#)

12.5 Configuring Key Escrow and encryption

SCM key escrow is used to store the individual private keys of end-user client certificates so that these keys can be recovered at a later date by appropriately privileged administrators. The keys are stored in encrypted form.

You can specify that keys in escrow be independently retrieved by any of the three administrator levels: MRAO, RAO Client Certificate, and DRAO Client Certificate. SCM can store up to two encrypted versions of the private keys of client certificates of an organization and up to three versions for a department. Each version is separately encrypted by three different master public keys: the MRAO master key, the organization master key, and the departmental master key.

The master public keys are stored by SCM. The corresponding master private keys, which are required for decryption and retrieval, are not stored in SCM. The private keys must be saved in a secure location by the administrator who is creating the organization or department.

Retrieving the private key of an end-user's client certificate from escrow causes the revocation of that certificate. This is true if any administrator, regardless of level, chooses to retrieve a client certificate from escrow. A private key can be retrieved from escrow by clicking **Download** for a specific certificate. See [“How to recover an end-user's private key from Escrow” on page 241](#) for more information.

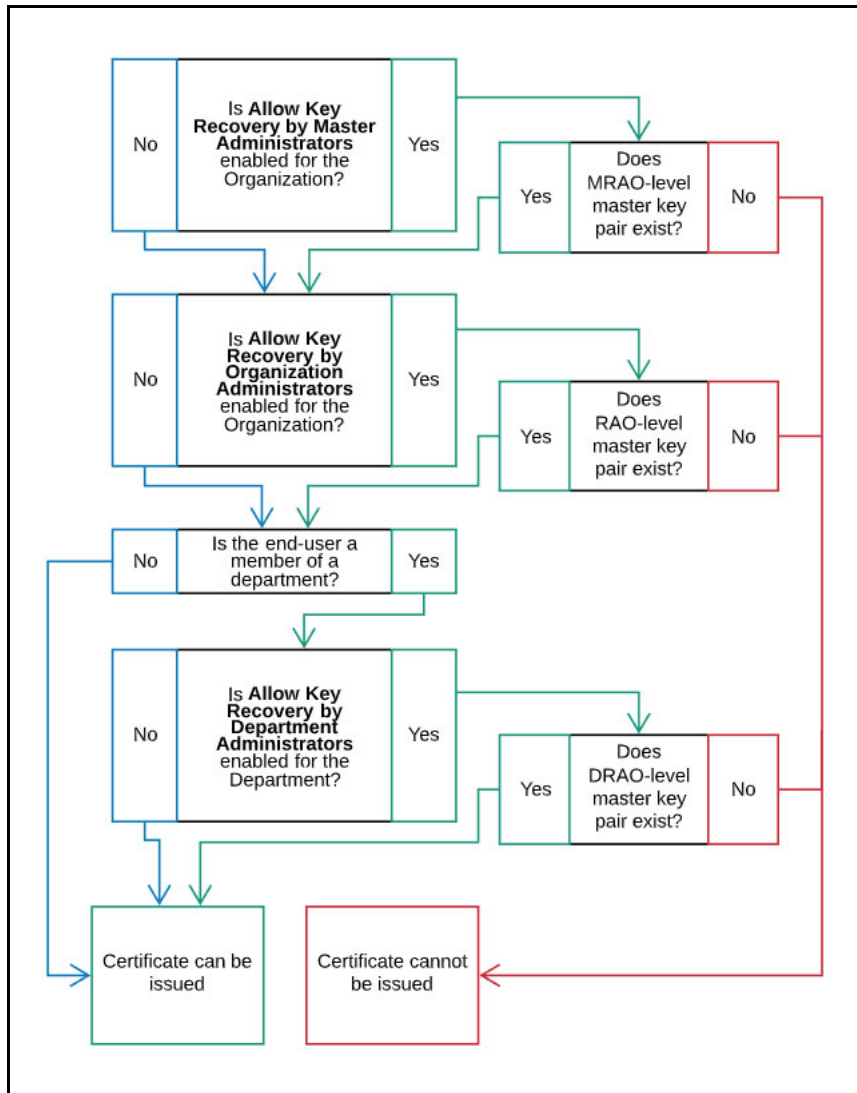
12.5.1 About the master key requirements for issuing Client Certificates

One master key pair is generated (if required) per organizational tier. Therefore, one master key pair is used by all RAO Client Certificate administrators of a particular organization. Similarly, if key retrieval is required at the departmental level, then one pair of master keys—Department Master Key—is used by all DRAO Client Certificate administrators of a particular department.

If key escrow has been configured for an organization or department and a master key pair has not been initialized, then the organization or department cannot issue client certificates. If key escrow is required through all tiers (MRAO, Organization, and Department), then a master key pair must have been initialized for each level. To check the initialization status, navigate to **Settings > Legacy Key Encryption**.

NOTE: Administrators can only see the initialization status of the master key pair for their own administrative level (Master, Organization, or Department).

The following illustration outlines the requirements for the master key pairs for the successful issuance of client certificates.



12.5.2 How to configure Key Escrow for an organization or department

Key recovery options are configured by a MRAO when creating an organization, or by a MRAO or RAO Client Certificate when creating a department. These options can only be configured when an organization or department is created, and once configured, cannot be modified.

The following key escrow options can be set for organizations or departments:

- **Allow Key Recovery by Master Administrators**—If selected, the MRAO can recover the private keys of client certificates issued by this organization. At the time of creation, each client certificate is encrypted with the MRAO's master public key before being placed into escrow. In addition, if this option is selected, the organization or department cannot issue client certificates until the MRAO has initialized their master key pair in the **Encryption** page.
- **Allow Key Recovery by Organization Administrators**—If selected, the RAO can recover the private keys of client certificates issued by this organization. At the time of creation, each client certificate is encrypted with the RAO's master public key before being placed into escrow. In addition, if this option is selected, the organization or department cannot issue

client certificates until the RAO has initialized their master key pair on the **Legacy Key Encryption** page.

Note that for departments these options are only active if a MRAO enabled the appropriate key recovery options when configuring client certificate options for the organization.

The following additional key escrow setting can be set for departments:

- **Allow Key Recovery by Department Administrators**—If selected, the DRAO Client Certificate can recover the private keys of client certificates issued by this department. At the time of creation, each client certificate is encrypted with the DRAO's master public key before being placed into escrow. In addition, if this option is selected, the department cannot issue a client certificate until the DRAO has initialized their master key pair on the **Legacy Key Encryption** page.

The key recovery options are in the **Client Certificates** page of the **Add New Organization** and **Add New Department** dialogs. (See [Edit certificate settings](#).)

For more information on creating and managing organizations and departments, see [Managing organizations and departments](#).

12.5.3 How to view and configure encryption settings

The **Legacy Key Encryption** page shown in the following illustration enables MRAO, RAO Client Certificate, and DRAO Client Certificate administrators to encrypt the private keys of the end-users' client certificates. If key recovery was specified during the creation of an organization or department, then you must complete this configuration, as client certificates cannot be issued until the master key pairs have been initialized.

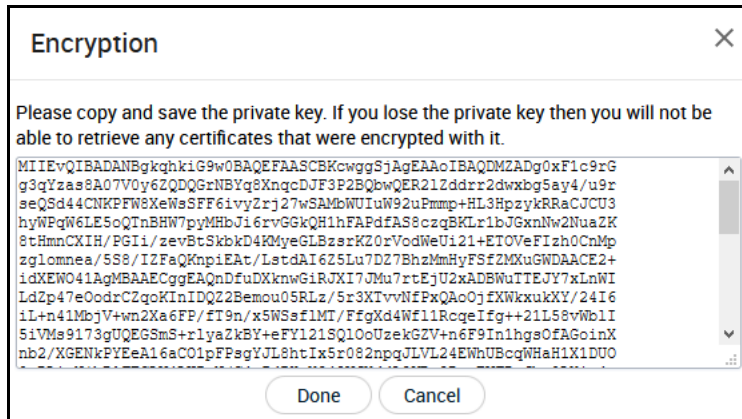
SCOPE	NAME	STATUS
<input checked="" type="checkbox"/>	Master	Public key is loaded

The following columns and controls are available:

- **Scope**—The hierarchy level of the organization or department. Valid values are Master, Organization, Department.
- **Name**—The name of the organization or department.
- **Status**—The status of private key encryption.
- **Initialize Encryption**—Starts the initial encryption process. This control is available only if the private keys have never been encrypted and the status is Not Initialized for the selected organization or department.
- **Re-encrypt**—Starts the re-encryption process of the private keys of the certificates of the end-users belonging to an organization or department. This control is available only if the private keys for the selected organization or department are already encrypted.

12.5.3.1 How to encrypt private keys

To initialize the private key encryption, navigate to **Settings > Legacy Key Encryption** and click **Initialize Encryption**. This starts the process and generates a master private key, which you need to copy and paste into a `.txt` file, and then store in a secure location.



The master private key is not stored in SCM. It is recommended that the private key be saved in a secure password-protected location. The key is required if an administrator decides to either re-encrypt the keys or download the end-user's client certificate.

When you click **Done** on the **Encryption** dialog, the status is changed to **Public key is loaded**.

All the private keys of the end-user client certificates are now encrypted using the master public key of the administrator who began this process. Decryption requires the private key that was saved earlier.

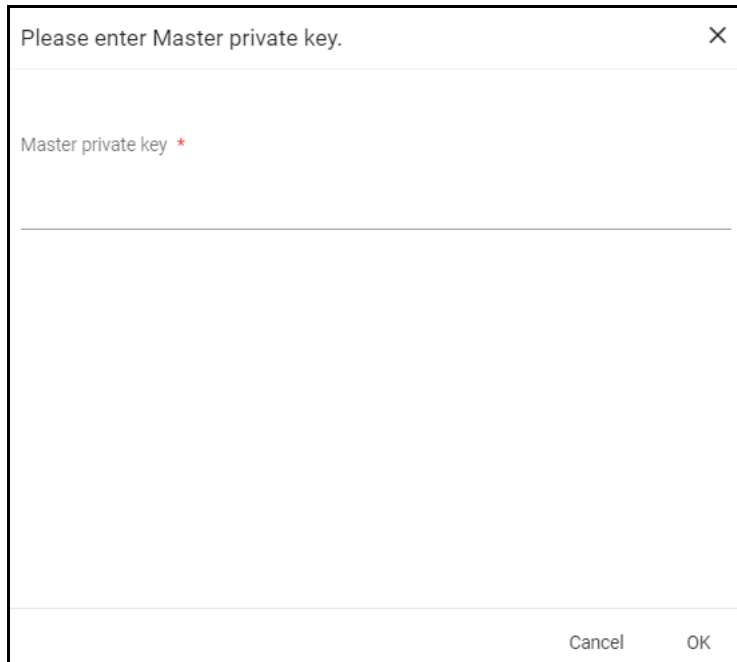
12.5.3.2 How to re-encrypt private keys

MRAO, RAO Client Certificate, and DRAO Client Certificate administrators can use re-encryption to change the master key pair and then automatically re-encrypt the existing end-user's key pairs with the new master public key. This may be necessary if the original private key becomes compromised or administrative personnel leave the company.

To re-encrypt the private keys, do the following:

1. Navigate to **Settings > Legacy Key Encryption**.
2. Select the scope and click **Re-encrypt** in the upper-left corner. Re-encrypt is available only if the private keys for the selected organization or department are already encrypted.

This opens the **Please enter Master private key** dialog shown in the following illustration.

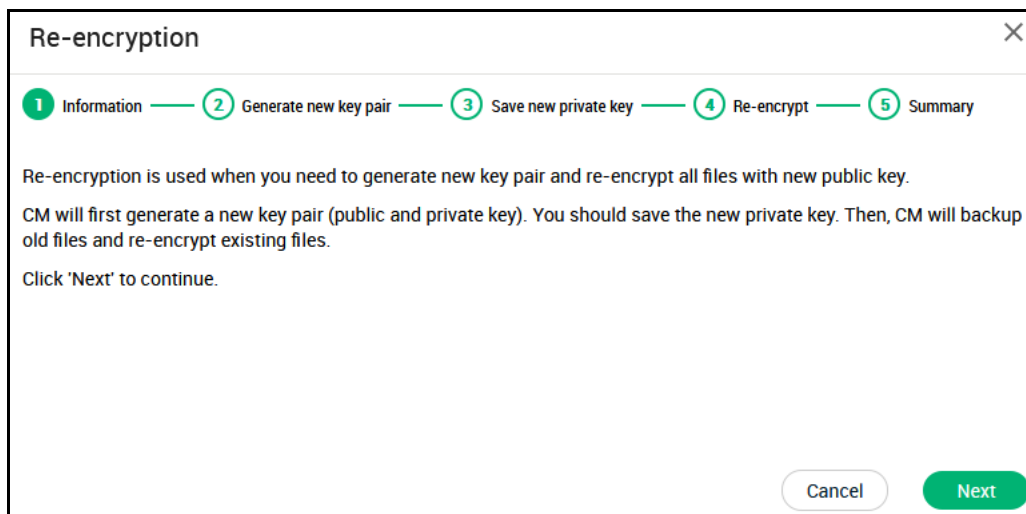


Please enter Master private key. [X]

Master private key *

Cancel OK

3. Paste the existing master private key into the **Master private key** field.
4. Click **OK** to open the **Re-encryption** wizard.



Re-encryption

1 Information — 2 Generate new key pair — 3 Save new private key — 4 Re-encrypt — 5 Summary

Re-encryption is used when you need to generate new key pair and re-encrypt all files with new public key.
CM will first generate a new key pair (public and private key). You should save the new private key. Then, CM will backup old files and re-encrypt existing files.
Click 'Next' to continue.

Cancel Next

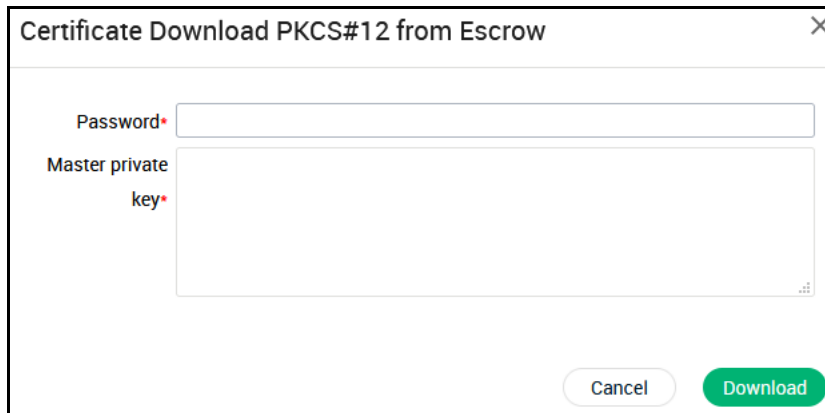
5. Click **Next** to continue.
6. Click **Generate key pair** to generate the new keys.
7. Copy and paste the private key into a `.txt` file, and save it in a secure password-protected location, then click **Continue** to start the re-encryption of the private keys.
8. Click **Proceed** to begin re-encrypting the private keys of client certificates.
You will see a message when it is completed successfully.

12.5.4 How to recover an end-user's private key from Escrow

You may need to recover an end-user's private key in order to decrypt data if, for example, the original client certificate belonging to an end-user was lost or if the end-user left the company. You should have your master private key ready, as it is required to complete this process.

To download an end-user's private key, do the following:

1. Navigate to **Certificates > Client Certificates**.
2. Select the certificate and click **Download**. This displays the **Certificate Download from Escrow** dialog shown in the following illustration.



The screenshot shows a dialog box titled "Certificate Download PKCS#12 from Escrow". It features a "Password*" field and a "Master private key*" text area. At the bottom, there are "Cancel" and "Download" buttons.

3. Enter a password in the **Password** field. This password is used to protect access to the .p12 file that is downloaded.
4. Paste your master private key into the **Master private key** field.
5. Click **Download**.

Successfully downloading the private key of a client certificate revokes that certificate.

12.6 Configuring access control

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the access control can now be found in the following location:

- [Understanding access restrictions](#)

12.7 Configuring a Private Key Store

MRAOs can create and maintain a secure Private Key Store (PKS) on their local network for archiving the private keys of SSL certificates generated by the auto-CSR. In addition, the PKS enables you to upload the private keys of existing certificates to the store.

Information about the PKS agent can now be found [here](#).

12.8 Managing SCM agents

SCM agents allow you to automate various processes, such as certificate discovery and installation.

For more information, see [“SCM agent integrations” on page 230](#).

12.9 Configuring assignment rules

Assignment rules are used during discovery tasks to assign external certificates to organizations and departments based on the criteria you specify.

For more information, see [“Managing assignment rules” on page 150](#).

12.10 Using Sectigo Key Vault

Sectigo Key Vault is used to store private keys of the client certificates managed by SCM and allows for later retrieval by authorized users and services, such as Sectigo Mobile Certificate Manager.

Sectigo Key Vault is only available if enabled for your account. Contact your Sectigo account manager.

When configured, client certificate private keys are automatically stored in the vault when the certificate is enrolled using the following methods:

- Client Certificate Web Form enrollment endpoint (including enrollment by access code, secret ID, and invitation).
- MS Agent, if the MS template has been configured for key archiving. See [“MS agents” on page 230](#).

Keys can also be uploaded to the vault using REST.

Some enrollment protocols, including SCEP and EST, do not support key archiving.

12.10.1 How to download an end-user's Private Key from Sectigo Key Vault

When Sectigo Key Vault is configured, client certificate private keys can be downloaded in the following ways:

- By an administrator from SCM, using the **Download from Key Vault** option on the **Certificates for** dialog. This option only appears if the **Allow download keys from Key Vault** privilege is enabled for the administrator.
- By end users, using the **Private Key Recovery** form accessed via your Key Vault URL. Your Sectigo Key Vault URL is displayed on the **About** page under **Additional Services**.

To download private keys from Sectigo Key Vault in SCM, do the following:

1. Navigate to **Certificates > Client Certificates**.

2. Select the **Person profile** containing one or more private keys you need to retrieve.
3. Click **Certificates**.
4. Select a certificate and click **Download from Key Vault**.
5. Select one of the following:
 - **Selected**—Downloads the private key for the selected certificate.
 - **All**—Downloads the private keys for all certificates assigned to the Person profile.
6. In the **Passphrase** field, provide a password to protect the PKCS #12 file.
7. Click **Download**.

To enable end users to download private keys from Sectigo Key Vault using the **Private Key Recovery** form, provide the Key Vault URL to the end user using an out-of-band communication such as email.

Accessing the Key Vault URL displays the **Private Key Recovery** form listing the end user's available client certificates. To access the form, the end user must authenticate using the configured SAML IdP and the assertion must contain an email address to lookup the person.

The end user can select one or more certificates with keys and click **Download** to download the certificates.

SCM delivers the certificates in a single PKCS#12 file (.p12 file), and the user is prompted to enter a password to protect the p12 file before it downloads. The end-user is asked for this password when they import the certificate(s) into the certificate store of their computer.

12.10.2 How to configure Sectigo Key Vault for use with iOS

By default, keys are downloaded in PKCS#12 format. Using the **Key Vault** settings, you can configure Sectigo Key Vault to provide keys in a format compatible with iOS when accessed from an iOS device.

Key Vault

Key Vault Recovery

Recovery Method Recover via iOS Mobilee Config or, PKCS#12 File

iOS Mobile Config Security

Digitally Sign iOS Mobile Config YES

Subject N/A

Issuer N/A

Serial Number N/A

Expires N/A

Exchange Configuration

Include Exchange Configuration in iOS Mobile Config YES

Exchange Server Host Name mail.office.com

Use SSL For Communication YES

Number of Past Days to Sync 30

Prevent Moving Messages to Another Account YES

To configure Sectigo Key Vault for iOS, do the following:

1. Navigate to **Settings > Key Vault**.
2. Complete the fields, referring to the following table, and click **Save**.

Field	Description
Enable iOS Mobile Config during recovery from Key Vault	Enables or disables inclusion of a mobile configuration file when downloading keys while accessing the Private Key Recovery form from a device running iOS.
Include Exchange Configuration in iOS Mobile Config	Enables inclusion of Exchange settings in the mobile configuration file. These settings configure an Exchange ActiveSync Contacts account on the device. Mail and Calendar are not configured using this account on iOS. The Principal Name of the device owner in SCM is used as Exchange login and is embedded into the ActiveSync profile.
Exchange Server Host Name	The Exchange server host name (or IP address).
Use SSL For Communication	Specifies whether the Exchange server uses SSL for authentication.
Past Days to Sync	The number of past days of mail to sync. Mail received before this number of days in the past will not be synchronized.

Field	Description
Prevent Moving Messages to Another Account	If enabled, messages may not be moved out of this email account into another account. Also prevents forwarding or replying from a different account than the message was originated from.
Digitally Sign iOS Mobile Config	Enables or disables digital signing of the mobile configuration file.
PKCS#12 File	The private key to use to digitally sign the mobile configuration file. Click Upload From File to select a certificate in PKCS#12 format.
Passphrase	The password of the PKCS#12 file being used to sign the file.

12.11 Configuring Azure integration

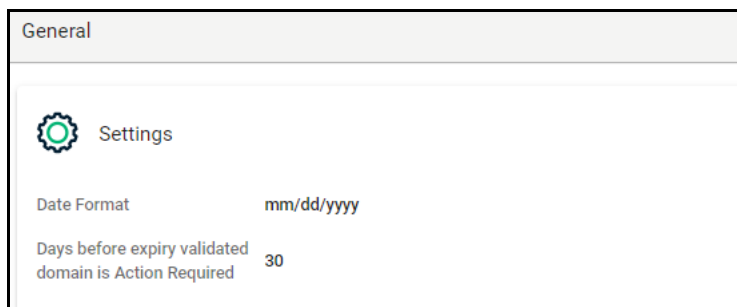
SCM can be integrated with the Microsoft Azure for the following:

- **Azure Key Vault**—generate CSRs automatically and store SSL certificates when enrolling certificates using the built-in wizard.
- **Intune with SCEP**—issue and manage certificates for mobile devices.
- **Intune Exporter**—export client certificates and private keys from SCM to Intune.

For more information, see [“Using SCM with Microsoft Azure and Intune” on page 203](#).

12.12 Managing General settings

The **General** page enables MRAO administrators to change the way in which dates will be displayed globally in SCM.



NOTE: Only affects the way dates are presented in SCM, for all users. This setting does not change the way time is handled on certificates.

Managing administrators

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about SCM administrators can now be found in the following locations:

- [Understanding administrators](#)
- [Adding administrators](#)
- [Managing administrators](#)

Appendix A: CSV import format requirements

This appendix describes the format of CSV files used for bulk import of data into SCM.

This appendix describes the following topics:

- [Network discovery task CSV file format](#)
- [SSL certificate CSV file format and importing guidelines](#)
- [End-user CSV file format and importing guidelines](#)
- [Code signing certificate CSV file format and importing guidelines](#)

A 1: Network discovery task CSV file format

When creating a .csv file for the bulk import of network discovery tasks, the columns must be populated using the information and order outlined in the following table.

Column	Field	Description
A	Task Name	The name of the task
B	Agent Name	The name of the agent that is to be used. If left empty, an agent is automatically assigned based on the ranges specified in the Scan Ranges column. You must have at least one agent configured to interact with your required scan ranges. For more information on configuring a network agent, see here .
C	Scan Ranges	The IP or IP range to be scanned. Ranges can be specified using a hyphen and can include a host name. CIDR format is supported.
D	Ports	The ports to be scanned. Multiple ports can be included using a comma-separated list enclosed in quotations ("233, 235, 255"). Port ranges can also be specified using a hyphen.
E	Schedule	The times when this network discovery task is to be run. Supported values are: Manual, Once, Daily, Weekly, Monthly, Quarterly, SemiAnnually, Annually. Tasks are scheduled for one minute following the upload of the CSV file and all tasks other than Manual and Daily are run on Sundays. You can also indicate a time zone by adding / followed by your UTC time zone.

Column	Field	Description
F	Bucket ID	The bucket ID of the task

The following is an example of a simple .csv file for the creation of two network discovery tasks.

	A	B	C	D	E	F
1	Example Task Name	01win38	10.101.66.1/24	443	Manual	397b80e0-4d08-4048-a070-055e85031919
2	Example Task Name 2	Cloud	sectigo.com	443	Run Once	397b80e0-4d08-4048-a070-055e85031919
3						

A.2 SSL certificate CSV file format and importing guidelines

The data for SSL certificate bulk enrollment requests must be structured correctly and submitted in a CSV format. Parameters specified for each separate certificate included in the request must be written on one line and separated by commas, except the last parameter in the line. All parameters are mandatory, except for Subject Alternative Names (SAN); if the certificate has no SANs, the parameter is left blank. If a parameter contains one or more commas within its string, this parameter must be placed in quotes.

The following parameters must be present in each line of the CSV file in the order listed:

1. Common Name—string.
2. SAN—the whole value must be in quotes, domains inside, comma separated.
3. Certificate Type—string, must be the same as the certificate profile **Name**.
4. Certificate Term—string, must be the same as it appears in the certificate profile.
5. Server Software—string. It is currently suggested that you populate this space with "OTHER".

For example, to request enrollment for an EliteSSL Certificate profile for 1 year with a common name of scmqa.com without SANs, the following line would be included in the CVS file:

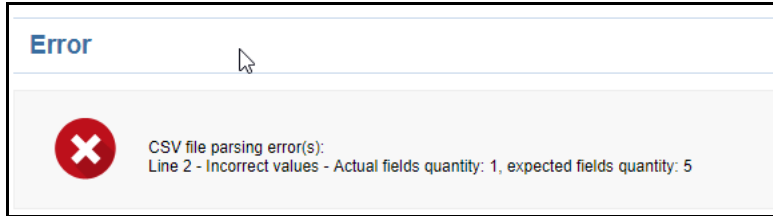
```
scmqa.com, , EliteSSL Certificate, 1 year, OTHER
```

The following example requests enrollment for an AMT Multi-Domain SSL Certificate for 2 years with a common name of scmqa.com, and with SANs fly.com and new.com:

```
scmqa.com, "fly.com, new.com", AMT Multi-Domain SSL Certificate, 2 years, OTHER
```

A.2.1 Bulk SSL certificate CSV file errors

When submitting a bulk enrollment request accompanied by a CSV file that contains errors, an error message similar to the one shown in the following illustration might appear.



The following table lists errors that may arise during parsing of an SSL Certificate CSV file.

Error ID	Error message	Reason
1	CSV file parsing error(s): Line <line ID> - Required field 'commonName' is not specified. (Displayed in red bold above every field.)	The CSV file contains a line without a common name.
2	CSV file parsing error(s): Line <line ID> - Required field 'certType' is not specified. (Displayed in red bold above every field.)	The CSV file contains a line without a certificate type.
3	CSV file parsing error(s): Line <line ID> - Required field 'certTerm' is not specified.	The CSV file contains a line without a certificate validity period (term).
4	CSV file parsing error(s): Line <line ID> - Required field 'serverSoftware' is not specified	The CSV file contains a line without a server software.
5	CSV file parsing error(s): Line <line ID> - Please use commas only to delimit domain alternative names (for example - domain_one.com, domain_two.com, etc.)	The CSV file contains a line in which not all parameters are separated by commas.
6	CSV file parsing error(s): Line <line ID> - field 'certType' contains disallowed value: <value>	The specified certificate type is not found among certificate profiles allowed for the organization for which this request is being submitted. Or this certificate type does not exist.
7	CSV file parsing error(s): Line <line ID> - field 'certTerm' contains disallowed value: <value>	The specified certificate term is not permitted for the certificate type specified in the same line.
8	CSV file parsing error(s): Line <line ID> - field 'serverSoftware' contains disallowed value: <value>	The specified server software is not found among the server software allowed for the organization for which the request is being submitted.
9	CSV file parsing error(s): Line <line ID> - Incorrect values - Actual fields quantity: <value>, expected fields quantity: <value>	The number of commas in a line of the CSV file is other than four.

Error ID	Error message	Reason
10	CSV file parsing error(s): Line <line ID> - Field 'san' contains non-empty value: '<0>'. Subject alternative names are not allowed for '<specified certType>' certificate type.	A line in the CSV file contains Subject Alternative Names, whereas the certificate type specified in the same line is not multi-domain.

A.3 End-user CSV file format and importing guidelines

The following table lists fields, with their possible values and formats, that can be imported from the CSV file for each end-user.

The fields in the CSV file differ depending on whether or not principal name support is enabled for the organization. For organizations for which the principal name support is not enabled (the default), the **Principal Name** field is not included. Principal name support is configured when adding or editing organizations or departments. For more information, see [Edit certificate settings](#).

Department is mandatory only if multiple end-users are being imported by a DRAO Client Certificate; MRAO, RAO Client Certificate, as well as DRAO Client Certificate administrators that are also MRAO or RAO Client Certificate administrators, can leave this field blank.

Optional fields without values must be included but left blank. If **Common Name** is left blank, it is automatically filled using **First Name** and **Last Name**.

The **Secret ID** field can be used to add a layer of authentication to the process. If specified, the end-user has to enter the identifier in the certificate enrollment form. For more information, see [“Enabling the end-user self-enrollment by secret identifier” on page 103](#).

With the exception of the **Secret ID** and **Phone** fields, ensure that the fields are imported using characters as per the following table, including commas and quotation marks.

Field	Required	Minimum characters	Maximum characters	Format	Supported characters
First Name	Yes	1	128		A-Z a-z 0-9 . - space
Middle Name	No	0	128		A-Z a-z 0-9 . - space

Field	Required	Minimum characters	Maximum characters	Format	Supported characters
Last Name	Yes	1	128		A-Z a-z 0-9 . - space
Email (Primary)	Yes	3	128	Valid email address	A-Z a-z 0-9 . - _ @
Email (Alternative)	Yes	3	128	Valid email addresses separated by a space	A-Z a-z 0-9 . - _ @ space
Validation Type	No				high standard
Organization	Yes	1	128		Any
Department	No	0	128		Any
Secret ID	No	0	128		Any
Phone	No	0	128		Any
Country	Yes	2	2	Valid two-letter country code	A-Z a-z
Principal Name	No	1	128		Any
EPPN	No	0	128		Any
Common Name	No	0	128		Any

The following example pertains to organizations for which principal name support is enabled:

```
First1,Middle1,Last1,User1-al@abc.com,User1-sec-al@abc.com,
standard,sysorg,sysdep,Secret1,380487000001,UA,User1-al@abc.com,User@System,
"First1 Last1"
```

NOTE: If an organization has principal name support enabled and a department belonging to that organization does not, when loading end-users of the department, the Principal Name field must be included but should be left blank.

The following example pertains to organizations for which principal name support is not enabled:

```
First1,Middle1,Last1,User1-al@abc.com,User1-sec-al@abc.com,  
standard,sysorg,sysdep,Secret1,380487000001,UA,User@System,  
"First1 Last1"
```

The following would result in failure to import end-users:

- Lines do not have the correct number of fields.
- Any mandatory field is not completed.
- The organization does not exist.
- The department, if present, does not exist.
- The department, if present, does not exist for the specified organization.
- The value provided in the Primary Email Address field is not in a valid format or the email domain cannot be determined.
- The domain of the primary email address is not delegated to the organization or is not active.
- The domain of the primary email address is not delegated to the department (if department is supplied).
- The value provided in the Secondary Email Address field (if supplied) is not in a valid format or the email domain cannot be determined.
- The domain of the secondary email address is not delegated to the organization or is not active.
- The domain of the secondary email address is not delegated to the department (if department is supplied).
- The administrator attempting the import does not have the correct permissions for the organization or department:
 - MRAO administrators have permission to import for any valid organization or department. MRAOs may leave the Department field blank.
 - RAO Client Certificate administrators have permission to import for organizations and any subordinate departments that have been delegated to them. RAO Client Certificate administrators may leave the Department field blank.
 - DRAO Client Certificate administrators have permission to import for departments that have been delegated to them. DRAO Client Certificate administrators cannot leave the Department field blank unless they are also a RAO Client Certificate for the same organization.

A.4 Code signing certificate CSV file format and importing guidelines

The following table lists fields, with their possible values and formats, that can be imported from the CSV file for each certificate.

Field	Required	Minimum Characters	Maximum Characters	Format	Supported Characters
Organization	Yes	1	128		Any
Department	No ^a	0	128		Any
Term	Yes	1	1	Integer	01/05/13
Email Address	Yes	3	128	Valid email address	A-Z a-z 0-9 . - _ @
Full Name	Yes	1	64	Valid name	A-Z a-z 0-9 . - ,
Contact Email	No	3	128	Valid email address	A-Z a-z 0-9 . - _ @

a. Department can be excluded but the comma following it must be kept.

The following example pertains to organizations that include a department:

```
"Test Organization","Test Department","1","jsmith@example.org","JOHN SMITH",
"jsmith@alternativeemail.com"
```

The following example pertains to organizations that do not include a department:

```
"Test Organization",,"1","jsmith@example.org","JOHN SMITH",
"jsmith@alternativeemail.com"
```

Appendix B: Sectigo root and intermediate certificates

This appendix provides supplementary information for use when importing Sectigo private root and intermediate certificates.

This appendix contains the following topics:

- [Sectigo root and intermediate certificates](#)
- [Importing the Sectigo root certificate](#)
- [Importing the Sectigo intermediate certificates](#)

B.1 Sectigo root and intermediate certificates

For SCM certificates to be trusted internally, the root and intermediate CA certificates must be imported into your environment. These certificates are provided by your Sectigo account manager during your initial account setup.

NOTE: Unless issued a Private CA by Sectigo for your organization, the root and intermediate certificates may still be Comodo CA root and intermediate certificates. These certificates are still valid.

B.2 Importing the Sectigo root certificate

As a domain administrator with access to the system where an AD is installed, you can import the Sectigo root certificate into the Trust Root CA certificate store in the AD as follows:

1. Log in as an administrator to the Windows system where the AD is installed.
2. Navigate to **Windows Control Panel > Administrative Tools > Group Policy Management**.
3. In the **Group Policy Management** dialog, expand **(Forest Name)**, expand **(your domain name) > Domains > (your domain name)**.
4. Right-click **Default Domain Policy** and select **Edit**.
5. In the **Group Policy Management Editor** dialog, expand **Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities**.
6. Right-click **Trusted Root Certification Authorities** and select **Import**.
7. On the **Welcome to the Certificate Import Wizard** dialog, click **Next**.
8. On the **File to Import** dialog, click **Browse**.

9. Locate and select the **Sectigo Root Certificate** to be imported, and then click **Next**.
10. In the **Certificate Store**, select **Place all certificates to the following store** and set the **Certificate store** to **Trusted Root Certification Authorities**.
11. Click **Next > Finish > OK**.

Computers apply the **GPO** and download the certificate on the client machines, the next time Group Policy is refreshed.

B.3 Importing the Sectigo intermediate certificates

As a domain administrator with access to the system where an AD is installed, you can import the Sectigo intermediate certificate into the Intermediate CA certificate store in the AD as follows:

1. Log in as an administrator to the Windows system where the AD is installed.
2. Navigate to **Windows Control Panel > Administrative Tools > Group Policy Management**.
3. In the **Group Policy Management** dialog, expand **(domain name) > Domains > (domain name)**.
4. Right-click **Default Domain Policy** and select **Edit**.
5. Right-click **Intermediate Certification Authorities** and select **Import**.
6. On the **Welcome to the Certificate Import Wizard** dialog, click **Next**.
7. On the **File to Import** dialog, click **Browse**.
8. Locate and select the **Sectigo Intermediate Certificate** that is to be imported, and then click **Next**.
9. In the **Certificate Store**, select **Place all certificates to the following store** and set the **Certificate store** to **Intermediate Certification Authorities**.
10. Click **Next > Finish > OK** to save your changes.

Computers apply the **GPO** and download the certificate on the client machines, the next time Group Policy is refreshed.