



Quick start guide
for
Sectigo® Certificate Manager
23.8

August 2023

Sectigo Certificate Manager

Quick start guide, 23.8 SCMQG

Copyright © 2008, 2023, Sectigo.

All rights reserved.

Primary 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.....	1
Audience	1
Related documentation.....	1
Introduction	2
About SCM trials	2
Understanding SCM.....	3
Organizations, departments, and domains.....	3
Administrators	3
Certificates	3
Certificate profiles.....	4
Public vs private certificates.....	4
Enrollment options	4
Agents and certificate discovery	5
Notifications	5
Getting started	6
Logging into SCM.....	6
Using the Sectigo Certificate Manager Documentation dialog.....	6
Understanding the main SCM UI.....	6
Reviewing your details	7
How to review your administrator details	7
How to review organization details.....	8
First time setup.....	9
Adding organizations and departments	11
How to validate organizations.....	12
Adding administrators.....	14
Adding and delegating domains.....	17
How to add domains.....	17
How to validate domains	18
Setting up notifications	19
SSL certificates.....	21
How to add SSL certificate profiles.....	21
How to add endpoint accounts for enrollment form	22
How to add network agents for SSL certificate discovery.....	23
How to add discovery tasks	24
Client certificates.....	28
How to add client certificate profiles.....	28
How to configure Key Escrow	29
Code Signing certificates	30
How to add Code Signing certificate profiles.....	30
Device certificates	31
How to add device certificate profiles	32
How to add Device certificate enrollment endpoints.....	33

Managing certificates.....	35
Requesting and issuing SSL certificates	35
How to manually request an SSL certificate.....	36
How to collect SSL certificates	40
Requesting and issuing client certificates	41
How to add a client certificate end user	41
Requesting and issuing code signing certificates.....	43
How to add code signing certificates.....	43
Requesting and issuing device certificates	45
How to add device certificates.....	46
Generating reports	47

Preface

This document explains how to set up Sectigo Certificate Manager (SCM) and use it to manage SSL, client, code signing, and device certificates. For more information, see *Sectigo Certificate Manager Administrator's Guide*.

Audience

This document is intended for Master Registration Authority Officer (MRAO) administrators working with a full version of 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

- *Sectigo Certificate Manager Administrator's Guide*
- *Sectigo Certificate Manager Trial Quick Start Guide*
- *SCM Release Notes*
- *SCM REST API Reference*
- *SCM Web Service SSL API*

1 Introduction

SCM is a web-based application used by enterprises to manage the lifecycle of their digital certificates. Using SCM, you can manage the lifespan, issuance, deployment, renewal, and revocation of certificates on an organization, department, and individual basis. By consolidating and automating the often disparate processes involved in complex enterprise-wide PKI deployments, SCM reduces the need for manual certificate management and creates a more efficient, productive, and secure certification environment.

This document describes common tasks associated with setting up and using SCM to manage your PKI infrastructure and includes the following topics:

- [Understanding SCM](#)
- [Getting started](#)
- [First time setup](#)
 - [Adding organizations and departments](#)
 - [Adding administrators](#)
 - [Adding and delegating domains](#)
 - [Setting up notifications](#)
 - [SSL certificates](#)
 - [Client certificates](#)
 - [Code Signing certificates](#)
 - [Device certificates](#)
- [Managing certificates](#)
 - [Requesting and issuing SSL certificates](#)
 - [Requesting and issuing client certificates](#)
 - [Requesting and issuing code signing certificates](#)
 - [Requesting and issuing device certificates](#)
- [Generating reports](#)

Depending on your access level and configuration, some UI elements may not be visible to you.

1.1 About SCM trials

The trial version allows you to use SCM for 30 days. Once the trial period has expired, you must purchase the full version to continue using SCM.

You cannot order publicly trusted certificates or validate domains using the trial version. Certificates issued using a private certificate authority (CA) have a lifetime of 30 days. For information on using your trial, see the *Sectigo Certificate Manager trial quick start*.

2 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.

2.1 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, or code signing 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. (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.

2.2 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).

2.3 Certificates

Depending on the features enabled for your account, SCM can be used to request and manage the following types of digital 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** 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).

2.3.1 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 (i.e., 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.

2.3.2 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.

2.3.3 Enrollment options

Whether from a public or private CA, certificates can be enrolled in the following 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).

For information on using ACME or SCEP with SCM, see the *Sectigo Certificate Manager Administrator's Guide* or contact your Sectigo account manager.

2.4 Agents and certificate discovery

You may already have a variety of certificates issued by Sectigo or other vendors. To bring these existing certificates under SCM management, 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, and to incorporate Active Directory (AD) domains into SCM.

2.5 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.

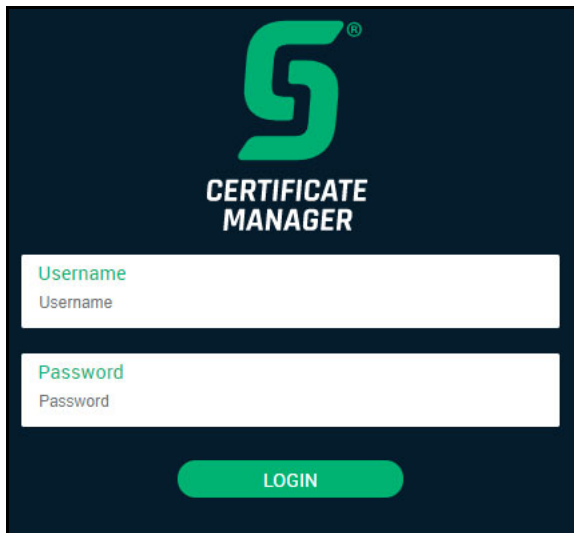
3 Getting started

The following sections describe how to log in, use the SCM UI, and review your details.

3.1 Logging into SCM

Once your organization has subscribed for a Sectigo account, you will be provided with a user name, password, and login URL for SCM.

The default format of this URL is `https://cert-manager.com/customer/<customer URI>/`, where `<customer URI>` is a path segment specific to your company.



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.

If you have not been supplied with your login details or are not able to log in, contact your Sectigo account manager or click **SCM Support** to create a support ticket.

You may be prompted to change your password after first login, if this is how your administrator configured your account in the access control settings.

3.2 Using the Sectigo Certificate Manager Documentation dialog

When you first access SCM, you are presented with the **Sectigo Certificate Manager Documentation** dialog.

You can launch the **Sectigo Certificate Manager Documentation** dialog at any time by clicking your user name in the upper-right corner and selecting **Documentation**. You will be redirected to the Sectigo docs website to read the existing documentation on SCM.

3.3 Understanding the main SCM UI

The SCM UI has a left pane that provides access to most of the settings.

The main functional areas of SCM are presented as a series of eight (or fewer, depending on your permissions level) pages: **Dashboard**, **Certificates**, **Discovery**, **Domains**, **Organizations**, **Persons**, **Reports**, **Enrollment**, **Issuers**, **Integrations**, **Settings**, and **About**.

3.4 Reviewing your details

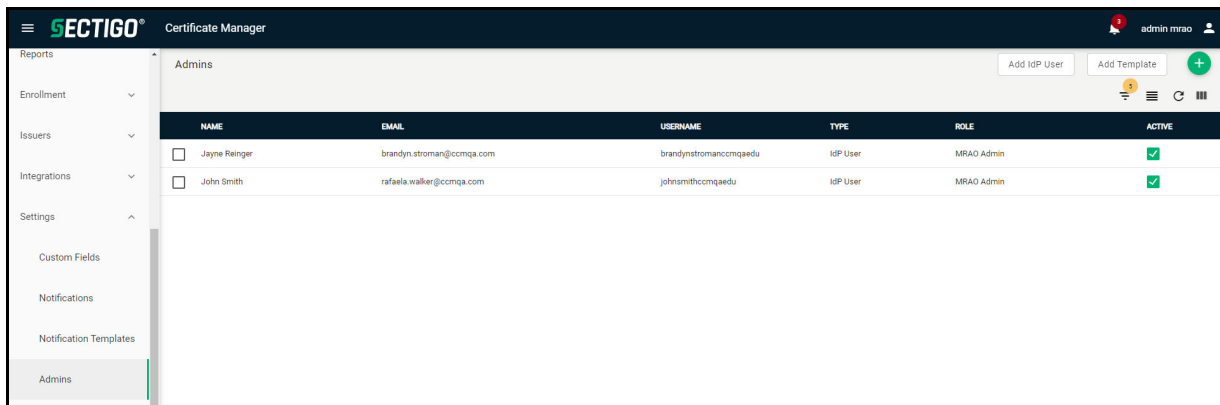
When you first access SCM, it will typically have the following items configured:

- An MRAO administrator. This is the account you used to log in. An MRAO administrator has full privileges to request certificates, create organizations and departments, create and delegate domains, add users and other administrators, modify SCM settings, and more.
- At least one organization validated by Sectigo. The details for this organization are based on the details you provided to Sectigo.

A number of other features may also be configured, depending on your agreement with Sectigo. For more information, contact your account manager.

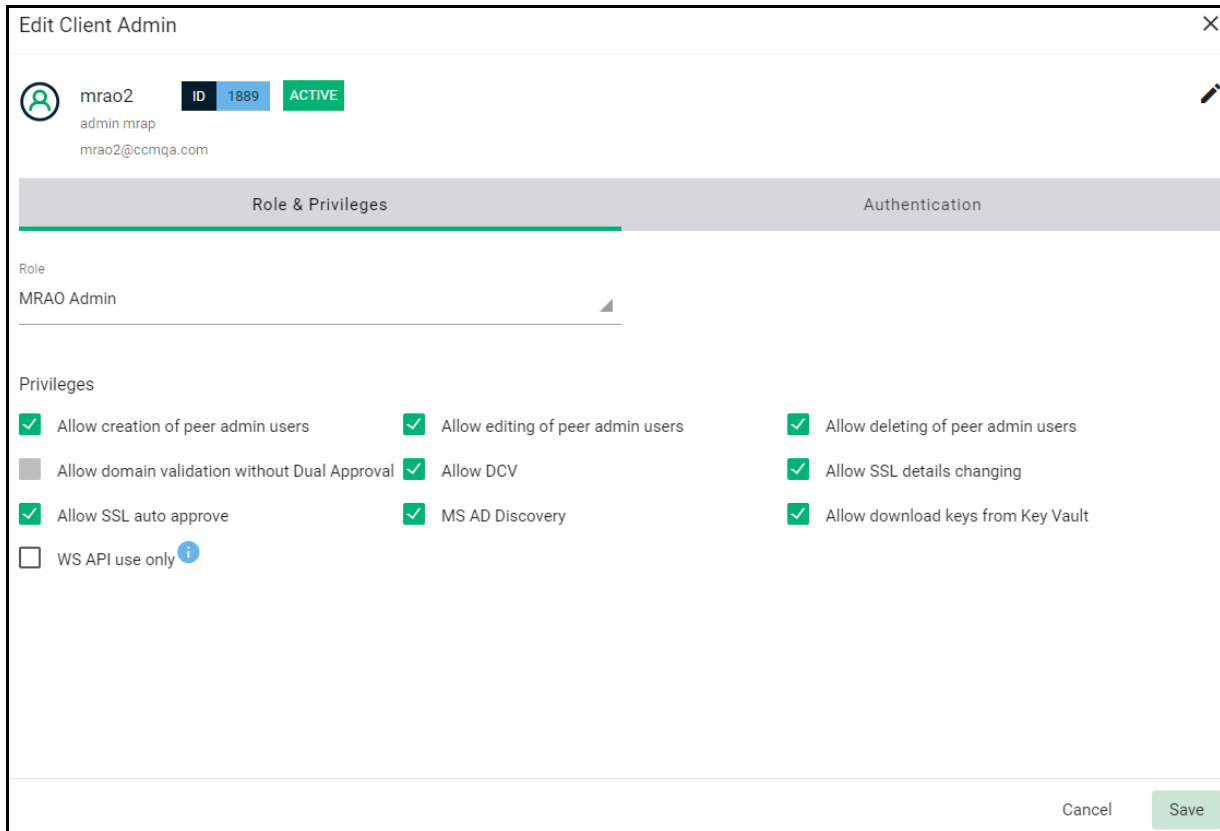
3.4.1 How to review your administrator details

The **Admins** page in **Settings** enables you to manage administrative personnel. As organizations or departments are added, you can, for example, add administrators with specific roles and permissions to manage them.



To review the administrator details, do the following:

1. Navigate to **Settings > Admins**, select the administrator in the list, and click **Edit**.
This displays the **Edit Client Admin** dialog.



2. Verify that the credentials are correct and click **Save** when done.

3.4.2 How to review organization details

Organizations are umbrella entities created by administrators for the purposes of requesting, issuing, and managing certificates for domains and employees. The **Organizations** page is used to add and modify the organizations.

To review the organization details, do the following:

1. Navigate to **Organizations**, select the organization in the list, and click the **Edit** icon on the details card.

This displays the **Edit Organization Details** dialog.

When certificates are brought under SCM management they are assigned to an organization. Ideally, you want to match certificates to organizations in SCM according to the organization (O) in the subject field of the certificate.

2. Verify that the details are correct and click **Save** when done.

4 First time setup

The following chart outlines the basic SCM features used in a typical configuration.



The following table summarizes the SCM features described in this guide.

Feature	Requirements
Organizations and Departments	Your account comes with at least 1 organization configured. <ul style="list-style-type: none"> • Required for issuing any type of certificate. • Must have at least 1 domain delegated to it. • Must be validated to issue public OV certificates.
Administrators	Your account comes with 1 MRAO configured. <ul style="list-style-type: none"> • Administrators can be added to manage organizations and departments.
Domains	<ul style="list-style-type: none"> • Required for issuing SSL, client, and code signing certificates. • Must be delegated to organizations. A single domain can be delegated to multiple organizations and departments. • Must pass DCV before publicly trusted certificates can be issued for it.
Notifications	<ul style="list-style-type: none"> • For automated alerts to administrators and users of events and activity.
Private CA	If enabled for your account, root and issuing private CAs will be set up for you by Sectigo. <ul style="list-style-type: none"> • For issuing privately trusted certificates. • Required for issuing device certificates.
SSL Certificates	
Certificate Profile	<ul style="list-style-type: none"> • Required for issuing SSL certificates.
SSL Enrollment Endpoint	<ul style="list-style-type: none"> • Endpoint account required for each organization for which you want to use the SSL enrollment form to enroll certificates.

Feature	Requirements
Network Agent	<ul style="list-style-type: none"> • For SSL certificate discovery on internal networks. • For auto-installation and renewal of SSL certificates on a server.
Discovery Tasks	<ul style="list-style-type: none"> • For running discovery scans.
Client Certificates	
Certificate Profile	<ul style="list-style-type: none"> • Required for issuing client certificates.
Client Certificate Enrollment Endpoint	<ul style="list-style-type: none"> • Endpoint account required for each organization for which you want to use the client certificate enrollment form to enroll certificates.
Key Escrow	<ul style="list-style-type: none"> • For storing private keys of client certificates for later recovery; certificates are revoked when their keys are recovered.
Sectigo Key Vault	<p>If enabled for your account, the key vault will be set up for you by Sectigo.</p> <ul style="list-style-type: none"> • For storing private keys of client certificates for later retrieval by authorized users and services. • Required for external services using client certificates, such as Sectigo Mobile Certificate Manager and MS Intune PFX Certificate Connector.
Code Signing Certificates	
Certificate Profile	<ul style="list-style-type: none"> • Required for issuing code signing certificates.
Device Certificates	
Certificate Profile	<ul style="list-style-type: none"> • Required for issuing device certificates.
Device Certificate Enrollment Endpoint	<ul style="list-style-type: none"> • Required for each organization for which you want to use the device certificate enrollment form to enroll certificates.

The following additional services may need to be configured if enabled for your account:

- ACME—Automates SSL certificate installation, renewal, and domain validation
- SCEP—Enables external services to enroll client and device certificates
- EST—Enables external services to enroll client and device certificates
- Private Key Store—For archiving the private keys of SSL certificates
- Microsoft Azure Key Vault—For encrypting and managing keys
- Microsoft Intune—For enrolling and managing client and device certificates
- Microsoft Intune Exporter—For exporting client certificates from Sectigo Key Vault to Intune
- MS Agent—For scanning and integrating Active Directory servers

For information on configuring these additional services, see the *Sectigo Certificate Manager Administrator's Guide* or contact your Sectigo account manager.

4.1 Adding organizations and departments

Any certificate ordered through SCM must be assigned to an organization. Each organization can have multiple departments.

NOTE: We recommend that you plan your organization and department structure before adding organizations.

Once an organization or department has been created, you can do the following (depending on your privilege level):

- Request and delegate domains to that organization or department.
- Request, approve, or decline requests and manage certificates on behalf of that organization or department.
- Assign users to organizations and departments, or approve their requests for enrollment, so they may receive client certificates.
- Run a certificate discovery scan on networks to discover certificates and assign them to organizations specified during scan configuration.

The organization and department names feature as the **O** (Organization) and **OU** (Organization Unit/Department) relative distinguished names in the subject field of your issued certificate. Once issued, you cannot reassign a certificate to the auspices of another organization in SCM.

You add an organization as follows:

1. Navigate to **Organizations**.
2. In the upper-right corner, click **Add** to open the **Add New Organization** dialog.

The screenshot shows a dialog box titled "Add New Organization" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

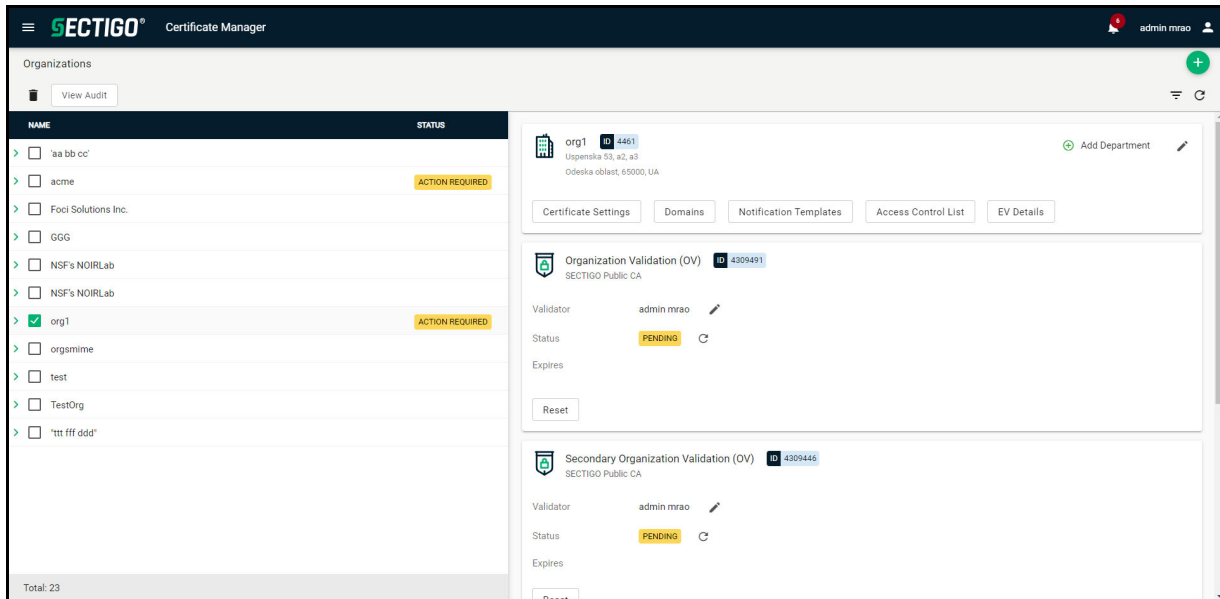
- Organization Name * (required)
- Address1 * (required)
- Address2
- Address3
- City * (required)
- State name * (required)
- Postal Code
- Country * (required) with a dropdown menu currently showing "United States"
- Buttons: "Cancel" and "Next" (highlighted in green) at the bottom right.

3. Complete organization details, and then click **Next**.

The new organization is added to the list on the **Organizations** page.

To add a department under an organization, do the following:

1. Navigate to **Organizations**.
2. Select the appropriate organization and click **Add Department**.



3. In the upper-right corner, click **Add** to open the **Add New Department** dialog. This dialog is similar to the **Add New Organization** dialog. The settings made here apply only to the new department.

4.1.1 How to validate organizations

To issue OV SSL certificates for organizations and their departments, your SCM account should have been enabled for OV certificates, and the organization should be validated by Sectigo. The validation process for newly created organizations can be initiated by MRAOs and when the process is completed successfully, the **Validation Status** displays Validated.

You can start the validation process by doing the following:

1. Navigate to **Organizations**.
2. Either select an unvalidated organization and click **Validate**, or select a validated organization and click **Revalidate**.

The dialog displays the validation status and contains all verified information about the organization (address, contact details, and so on). This information is then used to accelerate the issuance of subsequent OV level certificates for the organization.

The validation status of new organizations is initially **Not Validated**.

3. To change the administrator responsible for validating the organization, click **Edit** next to the **Validator** field, select an administrator, and click **Save**.

	NAME	EMAIL
<input type="checkbox"/>	mrao kv	mraokv@ccmqa.com
<input type="checkbox"/>	12 12	12@ccmqa.com
<input type="checkbox"/>	IdpUser IdpUser02;Id	user02@ccmqa.com
<input checked="" type="checkbox"/>	IdpUser12345 IdpUsi	user01@ccmqa.com
<input type="checkbox"/>	Sr sosiedov	ihor.sosiedov@sectigo.com
<input type="checkbox"/>	IdpUser IdpUser02	user02@ccmqa.com
<input type="checkbox"/>	gn sn	test01@ccmqa.com
<input type="checkbox"/>	02	test02@ccmqa.com
<input type="checkbox"/>	IdpUser IdpUser03	user03@comodo.com

Address details in the **General** page of the **Edit Organization** dialog are used for the validation process. This information cannot be edited while the validation status is Pending. The details can be edited only when the validation status is Validated, Expired, or Failed.

When a new department is added to a validated organization, its address details are fetched from the organization's anchor certificate. These details auto-populate the department's **General** page. The department name is blank for the administrator to complete. This name is to be shown as the Organizational Unit (OU) in the final certificate. If a department was added with different address details before the parent organization has been validated, then these details are replaced with those in the anchor certificate the next time an OV certificate is ordered for the department.

4.2 Adding administrators

Once you have created organizations and departments, you can assign administrators to them. Administrators can procure and manage certificates for organizations and departments.

MRAOs can create and set the permissions of other administrators and users of any organization or department.

RAOs can create departments and DRAO administrators for their own organization. These must be approved by a MRAO. RAOs cannot create new organizations or edit the general settings of an organization even if they have been delegated control of that organization. The RAO role is divided into sub-roles for each certificate type—RAO SSL, RAO Client Certificate, RAO Code Signing, and RAO Device Certificate.

DRAOs can see and request certificates for only the departments that have been delegated to them. They have no ability to manage certificates belonging to organizations or departments over which they have not been granted permissions. The DRAO role is divided into subroles for each certificate type—DRAO SSL, DRAO Client Certificate, DRAO Code Signing, and DRAO Device Certificate.

You can assign multiple administrative roles to one individual. For example, the same person could be a RAO SSL and RAO Client Certificate administrator.

To add an administrator, do the following:

1. Navigate to **Settings > Admins**.
2. In the upper-right corner, click **Add** to open the **Add New Client Admin** dialog.

Add New Client Admin
✕

Username *

Email *

Forename *

Surname *

Title

Telephone Number

Street

Cancel
Next

3. Complete the fields based on the information in the following table and click **Next**.

Field	Description
Username	The new administrator's login name.
Email	The full email address of the new administrator.
Forename, Surname	The first name and surname of the new administrator.
Title	The title for the new administrator.
Telephone Number	The contact phone number for the new administrator.
Street, Locality, State / Province, Postal Code, Country	The address details of the new administrator.
Relationship	The role of the new administrator.
Certificate Auth	Specifies whether or not the new administrator must authenticate with their client certificate over a https connection prior to being granted login rights. The list includes the client certificates issued by SCM for the new administrator based on their email address specified in the Email field.

Field	Description
Identity Provider	Specifies the IdP account to be used by the administrator to log into SCM. You can enable IdP login for the administrator at any time by sending an IdP invitation or by editing the administrator account.
IdP Person Id ^a	The unique identifier for the administrator in the IdP realm. The identifier can be obtained from meta data provided by the IdP service provider.
Password, Confirm password	The password for the new administrator. The new administrator has to change the password on first login.
Privileges	
Allow creation of peer admin users	When enabled, the new administrator can add other administrators of their own level or of lower level in the hierarchy.
Allow editing of peer admin users	When enabled, the new administrator can edit other administrators of their own level or of lower level in the hierarchy.
Allow deleting of peer admin users	When enabled, the new administrator can remove other administrators of their own level or of lower level in the hierarchy.
Allow domain validation without Dual Approval ^b	The new administrator's privileges are sufficient so that domains created or delegated by this administrator are activated immediately, without requiring approval by a second appropriately privileged RAO or a MRAO.
Allow DCV ^c	Enables the new MRAO, RAO SSL, and DRAO SSL to initiate DCV for newly created domains.
Allow SSL details changing	Enables the new MRAO, RAO SSL, and DRAO SSL to change the details of SSL certificates by navigating to Certificates > SSL Certificates .
Allow SSL auto approve	SSL certificates requested by the MRAO are automatically approved, and those requested by a RAO SSL and DRAO SSL are automatically approved by the administrator of same level and await approval from higher level administrator.
WS API use only	The administrator account can only be used via API integration. Access to the SCM UI is not allowed for this account.
Approve Domain Delegation	Enables the new RAO administrator to approve domain delegation requests by other RAOs or subordinate DRAOs.
MS AD Discovery	Enables the new MRAO administrator to access the Settings > MS Agents page, download and install MS Agents, and view the certificates and web servers discovered by MS Agents by scanning respective AD servers.
Allow download keys from Key Vault ^d	Enables the new MRAO administrator to download client certificate private keys stored in Sectigo Key Vault.
Role^e	

Field	Description
	<p>New administrators can be assigned to a particular organization (RAO) or department (DRAO) by selecting the appropriate organization or department from the list that appears after selecting a role. All organizations are listed by default. Clicking the plus sign (+) beside the organization name expands the tree structure to display the departments associated with the organization. Clicking Expand or Collapse All expands or collapses the entire tree structure.</p>

- a. Usually the **IdP Person Id** can be obtained from the value of the **Person Principal Name (PPn)** field in the meta data. This may vary for different IdP service providers. Contact your IdP service provider for help.
- b. Only available if Dual Approval for domains is enabled for your account. Contact your Sectigo account manager.
- c. Only available if DCV enabled for the account. Contact your Sectigo account manager.
- d. Only available if Sectigo Key Vault is enabled for your account.
- e. The same RAO can be assigned as RAO SSL, RAO Client Certificate, and RAO Code Signing as required. Similarly, same DRAO can be assigned as DRAO SSL, DRAO Client Certificate, and DRAO Code Signing as required.

Communicate the login URL for SCM, user name, and password to the new administrator through an out-of-band communication.

4.3 Adding and delegating domains

You can add your domains and delegate them to organizations or departments. Domains added by RAOs and DRAOs must be approved by an administrator of a higher authority level.

Certificates cannot be issued for a domain unless it is delegated to an organization or department. Domains can be delegated to any number of organizations and departments.

To issue publicly trusted certificates for a domain, the domain must also pass DCV. Privately trusted certificates do not require a domain that has passed DCV.

4.3.1 How to add domains

To add and delegate a new domain, do the following:

1. Navigate to **Domains**.
2. In the upper-right corner, click **Add** to open the **Create Domain** dialog.

Create Domain
✕

Active

Domain *

Description

ORGANIZATIONS/DEPARTMENTS	SSL CERTIFICATE	CLIENT CERTIFICATE	CODE SIGNING CERTIFICATE
> <input type="checkbox"/> acme	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> <input type="checkbox"/> inwodep	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> <input type="checkbox"/> org1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> <input type="checkbox"/> org3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> <input type="checkbox"/> orgintune	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> <input type="checkbox"/> orgscep	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> <input type="checkbox"/> orgsmime	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> <input type="checkbox"/> scepwodep	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Save

3. Enter the name of the domain in the **Domain** field and, optionally, a description of the domain in the **Description** field.
4. Select the **Active** option (you cannot order certificates for inactive domains).
5. Select the organizations and departments to which the domain should be delegated.
6. Select the types of certificates that can be ordered for the domain.
7. Click **Save**.

The domain is added to SCM and delegated to the selected organizations and departments. The delegation status is **Approved** if the request was made by a MRAO, or the status is **Requested** if the request was made by any other level of administrator.

4.3.2 How to validate domains

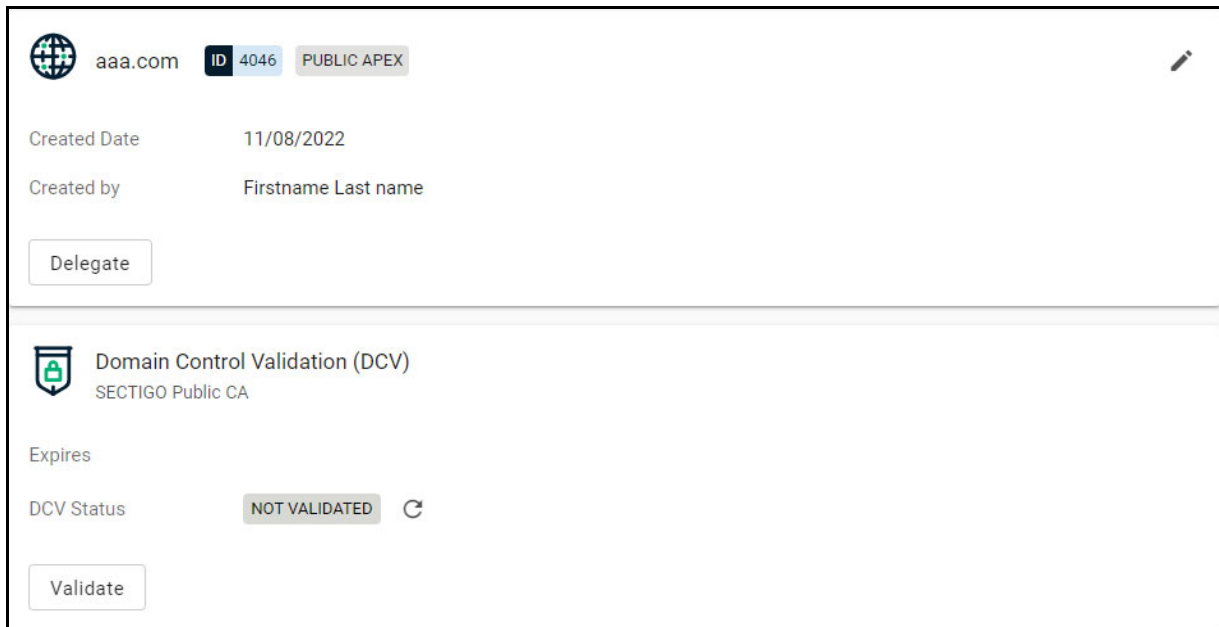
DCV can be carried out in the following ways:

- **Email**—An activation email is sent to the domain administrator. The domain is validated after the domain administrator clicks the validation link in the email.
- **HTTP/HTTPS**—SCM generates a text file to be placed in the root of the web server. You can download and forward the `.txt` file to the domain administrator and instruct them to place the file in the web server. SCM can validate the domain by the presence of the text file in the server.
- **CNAME**—SCM creates a DNS CNAME record for the domain. You can forward the record to the domain administrator and instruct them to create a DNS record using the same. SCM can validate the domain through its DNS record.

This section describes the email method of DCV. For details on the other methods, see *Sectigo Certificate Manager Administrator's Guide*.

To initiate DCV by email, do the following:

1. Navigate to **Domains**.
2. Select the appropriate domain and click **Validate** to open the **Validate domain** dialog.



3. Select **Email** and click **Next**.
4. Select an email address from the list and click **Submit**.
5. Click **OK**.

An automated email is sent to the selected Domain Administrator email address. The DCV status of the domain is changed to **Submitted**.

Upon receiving the email, the administrator should click the validation link and enter the validation code in the validation form that appears to complete the validation process. Once completed, the DCV status of the domain is changed to **Validated**.

4.4 Setting up notifications

Notifications allow you to customize email alerts for events in SCM. For example, you can create notifications for when certificates are due to expire, and specify who should be notified, the event for which they will be notified, when the notification should be sent, and more.

To create or edit a notification, do the following:

1. Navigate to **Settings > Notifications**.
2. In the upper-right corner, click the **Add** icon or select a notification and click **Edit**.

Add Notification ✕

Notifications allow you to stay ahead of various events, such as, certificate expiries, revocations, renewal failures, etc.

Name *

Type

Client Certificate Revoked ▾

Cancel Next

3. Give the notification a name and select a type.
4. Click **Next**.
5. Complete the **Details** tab fields and click **Save**.

4.5 SSL certificates

The following configuration is required for SSL certificates:

- **SSL certificate profiles**—A minimum of one SSL certificate profile is required for requesting SSL certificates. Typically your account will have several configured, depending on your agreement with Sectigo.

The following configurations are optional for SSL certificates:

- **SSL enrollment endpoint accounts**—If you want external users to be able to enroll SSL certificates, you must add SSL enrollment endpoint accounts for the organizations and departments on behalf of which they will be ordering certificates. These accounts provide access to the web form where they can enroll their certificate.
- **Network agent**—If you want to run SSL certificate discovery scans of your internal networks, you must install and configure network agents. Network agents are also used for auto-installation and renewal of SSL certificates on servers.
- **Discovery tasks**—Set up automated discovery tasks to scan your networks for SSL certificates to bring them under SCM management.

4.5.1 How to add SSL certificate profiles

To add an SSL certificate profile, do the following:

1. Navigate to **Enrollment > Certificate Profiles**.
2. In the upper-right corner, click the **Add** icon to display the **Create Certificate Profile** dialog.

The screenshot shows a 'Create Certificate Profile' dialog box. It has a title bar with a close button (X). The dialog contains the following fields and values:

- Name**: profile23
- CA Backend**: SECTIGO Public CA
- Certificate Type**: SSL Certificate
- Certificate Template**: Instant SSL
- Description**: comment

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

3. Enter a name for the profile in the **Name** field and, optionally, a description in the **Description** field.
4. Select the **CA Backend** to use for enrolling certificates that use this profile.
5. Set the **Certificate Type** field to **SSL Certificate**.

6. Choose a certificate template. The template controls the certificate policies as set by Sectigo.
7. Click **Next**.
8. Select the terms to allow for certificates enrolled using this profile.
9. Select the key types (algorithm and size or curve) to allow for certificates enrolled using this profile.
10. Optionally, set the **Requires approval** option.
11. Click **Save**.

4.5.2 How to add endpoint accounts for enrollment form

The SSL and client self-enrollment forms use a single shared endpoint each—the SSL Web Form endpoint and Client Certificate Web Form endpoint respectively. Access to these shared endpoints is managed by setting up accounts that grant access for an organization or department using an access code. The account also specifies which certificate profiles will be available for enrolling certificates.

To access the forms, applicants must have an email from a domain delegated to the account organization or department, and the access code.

The URL for the SSL self enrollment form is similar to the following:

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

The URL for the Client self enrollment form is similar to the following:

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

The access code should be conveyed to the applicant along with the URL of the endpoint. To request a certificate using the self-enrollment form, applicants must navigate to the form and fill out the information, including the code.

You create and manage web form endpoint accounts by navigating to **Enrollment > Enrollment Forms**, selecting the SSL, device, client or code signing web form endpoint, and clicking **Accounts**.

This displays the **SSL, Device, Code Signing** or **Client Certificate Web Form Accounts** dialog, which lists the accounts that have been configured for the selected endpoint.

To add or modify a Web Form account, do the following:

1. Navigate to **Enrollment > Enrollment Forms** and select the Enrollment Form.
2. To add an account, click **Accounts** on the Enrollment Forms dialog.
3. Click the **Add** icon.

To edit an account, select the account and click **Edit**.

The screenshot shows a dialog box titled "Create SSL Web Form Account". It contains the following fields and options:

- Name ***: A text input field.
- Organization ***: A dropdown menu with "acme" selected.
- Department**: A dropdown menu with "None" selected.
- Profiles**: A list box containing one item, "Profiles", with a "Remove All" button and a plus sign (+) to the right.
- CSR Generation method ***: A dropdown menu with "Browser" selected.
- Automatically approve certificate requests
- Allow Auto Renew SSL Certificates
- Allow Empty PKCS12 Password for Compatible TripleDES-SHA1

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

4. Enter a name for the account into the **Name** field. For example, "MyOrg SSL Form".
5. Select the organization and, optionally, department for the account from the **Organization** field. Only users with an email from a domain delegated to the organization will be able to use this account.
6. Select the CSR Generation method.
7. From the **Profiles** list, select the certificate profiles that will be available for certificates enrolled using the account by using the arrow buttons or dragging the certificate profiles from the **Available Certificate Profiles** list to the **Assigned Certificate Profiles** list.
8. For client accounts, select the **Allow Empty PKCS12 Password** to not password protect the client certificates issued using the account. (Typically, you would not enable this option.)
9. For SSL accounts, select **Automatically approve certificate requests** to have SSL certificate requests submitted through the self-enrollment form be automatically approved.
10. Select the authorization method.
11. Click **Save**.

4.5.3 How to add network agents for SSL certificate discovery

As part of our ongoing efforts to improve our documentation, the content previously covered in this section has been moved online. Information about the SCM agents can now be found in the following location: [Network agents](#)

4.5.4 How to add discovery tasks

A discovery scan identifies existing certificates on your network and imports them into SCM for further management. Discovered certificates that were not ordered through SCM are given an **External** status. Once imported, you can renew or replace external certificates with Sectigo equivalents.

When a task is run, discovered certificates can be automatically assigned to an organization or department by using assignment rules. You can then receive notifications relevant to the certificate for your organization or department (for example, certificate expiry reminders).

You are advised to create the organization or department structure you would like before creating and running a discovery scan. Then run a scan at the earliest opportunity so that you can gain a firm inventory of your company's certificate assets. Discovery scans are, however, optional and can be run anytime.

To scan your internal network, you must first create a **Discovery Task** by specifying the network agent to use for the scan.

4.5.4.1 Adding discovery tasks

You create a new discovery task or modify an existing one as follows:

1. Navigate to **Discovery > Network Discovery Tasks**.
2. Click **Add** or select a task and click **Edit**. The **Add** dialog is shown on the following page.
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.

Add Network Discovery Task

Common Schedule

Name *

Agent
Cloud

Certificate Buckets *
07.03.23 AD Rules

Ranges to Scan

Cancel Save

5. To add or modify the ranges, click **Add** or select a range and click **Edit**.

The **Add Scan Range** dialog is shown in the following illustration.

Add 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

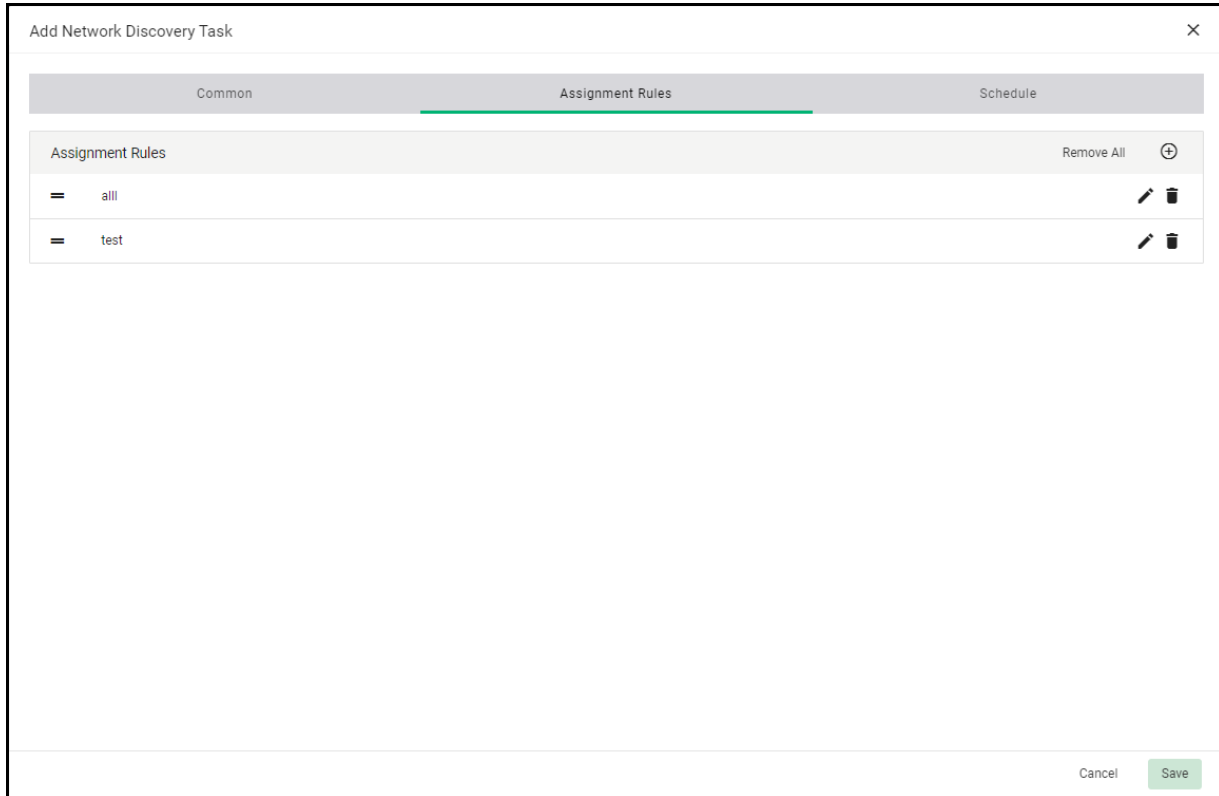
Host name
e.g. host1.domain.com

Port
443

Cancel OK

6. 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.

7. Enter the port number to use.
8. Click **OK** to add the scan range.
You can add multiple ranges. To remove a scan range, select it and click **Remove**.
9. Select **Assignment Rules**. Assignment Rules enable you to add rules that assign discovered certificates to a specific organization and department based on criteria you define.



10. Click **Add** to add a rule.
11. Enter a name for the rule.
12. Set the conditions for the rule. For example, Organization, Matches, and the name of your organization (assuming it matches the O in the subject of one or more of your certificates).
13. Using the **Assign to** field, assign the matching certificates to an organization.
14. Click **OK**. The rule is added to **Available rules**.
15. To add a rule to the task, move the rule from **Available rules** to **Assigned rules** using the arrows or by dragging.

NOTE: Network Discovery Tasks require a minimum of one assigned rule.

16. Complete the **Schedule** area shown in the following illustration to set the scan day, date, and start time, as well as the frequency of the task.

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

The screenshot shows a dialog box titled "Add Network Discovery Task" with a close button (X) in the top right corner. The dialog is divided into three tabs: "Common", "Assignment Rules", and "Schedule". The "Schedule" tab is currently selected and highlighted with a green underline. Below the tabs, the following configuration is visible:

- Frequency:** Weekly
- Day of Week:** Sunday
- Time zone:** UTC+02:00 - CAT, CEDT, CEST, EET, HAEC...
- Time:** 12:14 AM
- Next 5 scans:**
 - 11/21/2021 00:14:26 UTC+2
 - 11/28/2021 00:14:26 UTC+2
 - 12/05/2021 00:14:26 UTC+2

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

17. Click **Save**.

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

4.5.4.2 Running network discovery tasks

Launch scans using this task, as follows:

1. Navigate to **Discovery > Network Discovery Tasks**.
2. Select the appropriate task and click **Scan**.

Discovered and imported certificates can be reviewed using the following tabs:

- **Dashboard**—Displays an overview of your managed (i.e., assigned to organizations) certificates using charts.
- **Network Assets**—Lists all discovered certificates, including those that have not been assigned to an organization, i.e., that did not match an assignment rule when a scan was run. Using the **Assign To** option, you can manually assign these certificates to an organization.
- **SSL Certificates**—Lists the certificates that have been assigned to an organization or department.

4.6 Client certificates

The following configuration is required for client certificates:

- Client certificate profiles—A minimum of one client certificate profile is required for issuing client certificates. Typically your account will have several configured, depending on your agreement with Sectigo.

The following configuration options are optional for client certificates:

- Key escrow—A backup service for storing the private keys of end-user client certificates so that these keys can be recovered at a later date by appropriately privileged administrators. When a private key is recovered from escrow, the client certificate is revoked.
- Sectigo Key Vault—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. If enabled for your account, the key vault will be configured by your Sectigo account manager.
- Client certificate enrollment endpoint accounts—If you want external users to be able to enroll client certificates, you must add client enrollment endpoint accounts for the organizations and departments on behalf of which they will be ordering certificates. These accounts provide access to the web form where they can enroll their certificate. See [“How to add endpoint accounts for enrollment form” on page 22.](#)

4.6.1 How to add client certificate profiles

To add or edit a client certificate profile, do the following:

1. Navigate to **Enrollment > Certificate Profiles**.
2. Click **Add** to display the **Add Certificate Profile** dialog shown in the following illustration.

The screenshot shows a 'Create Certificate Profile' dialog box with the following fields and values:

Field	Value
Name *	profile23
CA Backend *	SECTIGO Public CA
Certificate Type *	SSL Certificate
Certificate Template *	Instant SSL
Description	comment

Buttons: Cancel, Next

3. Enter a name for the profile in the **Name** field and, optionally, a description in the **Description** field.
4. Select the **Enrolling Backend** to use for enrolling certificates that use this profile.
5. Set the **Certificate Type** field to **Client Certificate**.
6. Choose a certificate template. The template controls the certificate policies as set by Sectigo.
7. Select the terms to allow for certificates enrolled using this profile.
8. Select the key types (algorithm and size or curve) to allow for certificates enrolled using this profile.
9. Click **Save**.

4.6.2 How to configure Key Escrow

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 in the **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:

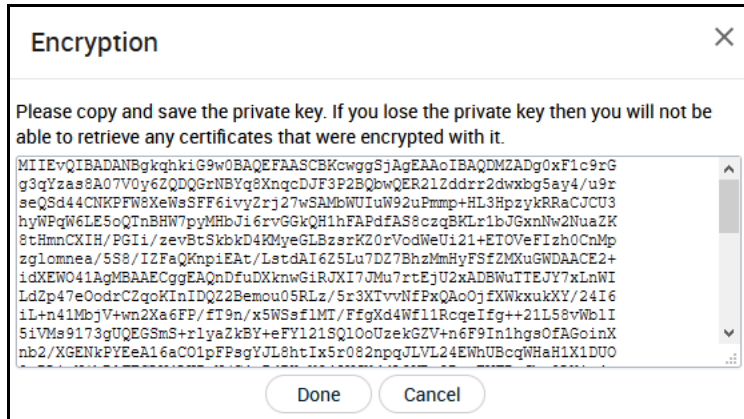
- **Allow Key Recovery by Department Administrators**—If selected, the DRAO Client Certificate can recover the private keys of client certificates issued by this department. At the time of creation, each client certificate is encrypted with the DRAO's master public key before being placed into escrow. In addition, if this option is selected, the department cannot issue a client certificate until the DRAO has initialized their master key pair in the **Encryption** page.

The key recovery options are in the **Client Certificates** page of the **Add New Organization** and **Add New Department** dialogs. (See [“Adding organizations and departments”](#) on page 11.)

If key recovery was specified during the creation of an organization or department, then MRAO, RAO Client Certificate, and DRAO Client Certificate administrators must initialize key encryption, as client certificates cannot be issued until the master key pairs have been initialized.

4.6.2.1 How to initialize private key encryption

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 an 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.

4.7 Code Signing certificates

The following configuration option is available for code signing certificates:

- **Certificate Profiles**—A minimum of one code signing certificate profile is required for requesting code signing certificates.

4.7.1 How to add Code Signing certificate profiles

To add or edit a code signing certificate profile, do the following:

1. Navigate to **Enrollment > Certificate Profiles**.
2. Click **Add** to display the **Add Certificate Profile** dialog shown in the following illustration.

The screenshot shows a dialog box titled "Add Certificate Profile". It contains the following fields and options:

- CA Backend:** SECTIGO Public CA
- Certificate Type:** Code Signing
- Certificate Template:** SECTIGO Public CA CS Certificate Template
- Trust Level:** Publicly Trusted
- Name:** SECTIGO Public CA CS Certificate Template
- Description:** (empty text field)
- Term:** None (with a "Select..." dropdown button)
- Allowed Key Types:** None (with a "Select..." dropdown button)

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

3. Enter a name for the profile in the **Name** field and, optionally, a description in the **Description** field.
4. Select the **Enrolling Backend** to use for enrolling certificates that use this profile.
5. Set the **Certificate Type field** to **Code Signing**.
6. Choose a certificate template. The template controls the certificate policies as set by Sectigo.
7. Select the terms to allow for certificates enrolled using this profile.
8. Select the key types (algorithm and size or curve) to allow for certificates enrolled using this profile.
9. Click **Save**.

4.8 Device certificates

The following configuration options are required for device certificates:

- **Private CA**—Device certificates are privately trusted and are issued by a private CA. A root and issuing private CA will be set up and configured for you by Sectigo.
The CA certificates can be obtained by navigating to **Issuers > Private CAs**, selecting a CA, and clicking **Download**. The root CA certificate should be downloaded and installed in your trust store.
- **Certificate Profiles**—A minimum of one device certificate profile is required for requesting device certificates.

The following configuration is optional for device certificates:

- Device certificate enrollment endpoints—If you want external users to be able to enroll device certificates, you must add device certificate enrollment endpoints for the organizations and departments on behalf of which they will be ordering certificates. The endpoint is a web form where they can enroll their certificate.

4.8.1 How to add device certificate profiles

To add device certificate profiles, do the following:

1. Navigate to **Enrollment > Certificate Profiles**.
2. Click **Add** to open the **Add Certificate Profile** dialog.
3. Enter a name for the profile in the **Name** field and, optionally, a description in the **Description** field.
4. Set the **Enrolling Backend** field to your private CA.
5. Set the **Certificate Type** field to **Device Certificate**.
6. Choose a certificate template. The template controls the certificate policies as set by Sectigo.

The screenshot shows the 'Add Certificate Profile' dialog box. The fields are as follows:

- CA Backend**: SECTIGO Public CA
- Certificate Type**: Device Certificate
- Certificate Template**: nonDefault
- Trust Level**: Private
- Name**: nonDefault
- Description**: (empty)
- Term**: None
- Allowed Key Types**: None

7. Depending on the selected template, set the term, allowed key types, key usage, and extended key usage for the profile.

The key usage and extended key usage determine cryptographic purposes for which the certificate can be used, such as key digital signing or encryption. Drag the items you want for the profile from the **Available** list to the **Assigned** list.

8. Click **Save**.

4.8.2 How to add Device certificate enrollment endpoints

External users can enroll device certificates using a Device Certificate Enrollment form. Before applicants can access the form, you need to configure an endpoint. The endpoint specifies the organization and, optionally, department that can access the form, the URL, and the certificate profiles that will be available for enrolling certificates.

The URL for the Device Certificate Enrollment form is similar to the following:

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

The URL of the endpoint should be conveyed to the applicant. To request a certificate using the self-enrollment form, applicants must navigate to the form and fill out the information. To access the form, applicants must have an email from a domain delegated to the organization or department specified by the endpoint.

To add device enrollment endpoints, do the following:

1. Navigate to **Enrollment > Enrollment Forms**.
2. To add an endpoint, click **Add**, or select an endpoint and click **Edit**. The **Create Enrollment Endpoint** dialog is shown in the following illustration.

The screenshot shows a 'Create Enrollment Endpoint' dialog box. It features a title bar with a close button (X). The main content area includes several input fields: 'Type' (a dropdown menu with 'Device certificate self-enrollment form' selected), 'Name' (a text input field with a red asterisk), 'Organization' (a dropdown menu with 'check.16' selected), 'Department' (a dropdown menu with 'None' selected), 'Profiles' (a button labeled 'Profiles' and 'Remove All' with a plus icon), 'URI Extension' (a text input field with a red asterisk and a 'Generate' button), and 'Help Link Text' (a text input field). At the bottom right, there are 'Cancel' and 'Save' buttons.

3. Set the type of endpoint to Device certificate enrollment form.

4. Enter a descriptive name for the endpoint.
5. Select an organization and, optionally, department. End-users enrolling certificates using the form must have an email from a domain delegated to this organization or department.

NOTE: Once an endpoint is created, the organization/department cannot be changed.

6. Specify the certificate profiles to be available when enrolling certificates using this endpoint. Use the arrow buttons or drag the certificate profiles from the **Available Certificate Profiles** list to the **Assigned Certificate Profiles** list.
7. Enter the URI extension. 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.

8. Optionally, enter a link name and address. This allows you to add a link to the enrollment form to, for example, a corporate intranet page with more information.
9. Optionally, enter help text. The text is displayed on the self-enrollment page to provide additional information or direction to users. The input limit is 2048 characters.
10. Click **Save**.

If you are adding an endpoint, the endpoint is added to the list of endpoints on the **Enrollment Forms** page.

5 Managing certificates

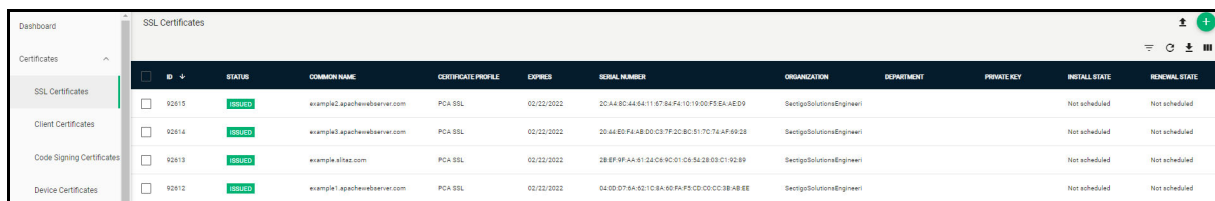
You can request the following types of certificates:

- [Requesting and issuing SSL certificates](#)
- [Requesting and issuing client certificates](#)
- [Requesting and issuing code signing certificates](#)
- [Requesting and issuing device certificates](#)

If you do not know which type of certificate is appropriate for you, contact your Sectigo account manager.

5.1 Requesting and issuing SSL certificates

SSL certificates are managed from the **Certificates > SSL Certificates** page.



ID	STATUS	COMMON NAME	CERTIFICATE PROFILE	EXPIRES	SERIAL NUMBER	ORGANIZATION	DEPARTMENT	PRIVATE KEY	INSTALL STATE	RENEWAL STATE
92615	ISSUED	example2.apachehttpserver.com	PCA SSL	02/22/2022	2044804464116784FA101900F5EA4E09	SectigoSolutionsEngineer			Not scheduled	Not scheduled
92614	ISSUED	example3.apachehttpserver.com	PCA SSL	02/22/2022	2044E0FA4B00C87F20BC817C76AF4928	SectigoSolutionsEngineer			Not scheduled	Not scheduled
92613	ISSUED	example1.thz.com	PCA SSL	02/22/2022	288F9FAA9124C69C01C5542803C19289	SectigoSolutionsEngineer			Not scheduled	Not scheduled
92612	ISSUED	example1.apachehttpserver.com	PCA SSL	02/22/2022	0400D76A021C8490FAF5C0CC0C3B4BEE	SectigoSolutionsEngineer			Not scheduled	Not scheduled

You can apply for SSL certificates in the following ways:

- **Built-in Wizard**—You can request SSL certificates from SCM using the built-in wizard. After the form is submitted and the request is approved, SCM sends a collection email to you (or to you and an external applicant if required). You or the external applicant can download the certificate and install it on the target server.
- **Self-enrollment by external applicant**—You can direct applicants to the request form to order SSL certificates for their domains. Applicants must validate their application by entering the appropriate access code for their organization or department. The email address entered on the form must be from the domain that is subject to the certificate application, and the domain must be delegated to the same organization or department.
- **Automatic enrollment, request, and installation**—SCM can create certificate requests for enrolled domains, then automatically install the certificate on the web server. Agents installed on a server can automatically generate a Certificate Signing Request (CSR) and forward it to SCM to create a certificate request for administrator approval. Once approved and issued, the agent collects the certificate and installs it on the target server. The agent can also renew an expiring certificate in the same manner.

The remainder of this section explains request and issuance of the certificate using the built-in wizard (manual CSR generation). For information on the other methods, see *Sectigo Certificate Manager Administrator's Guide*.

Before beginning the application, you will need to create the CSR. The public key included in the CSR should have at minimum an 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 Relative Distinguished Name (RDN) fields:

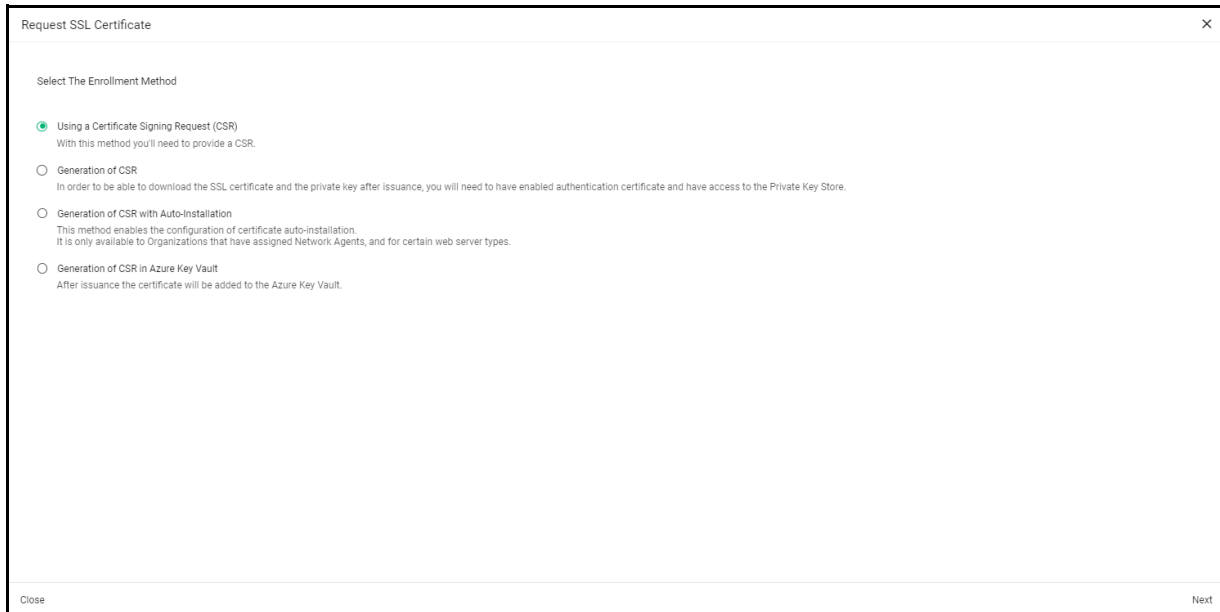
- CN—Common name, e.g., registered domain name

- 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)

5.1.1 How to manually request an SSL certificate

To apply for an SSL certificate, do the following:

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

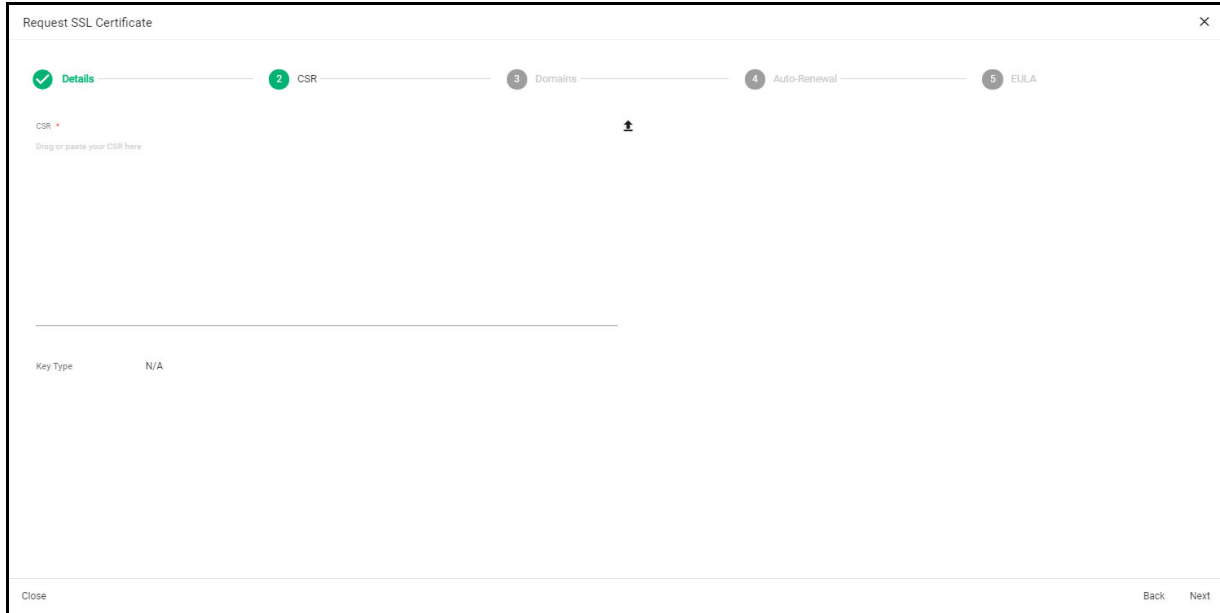


2. Select **Using a Certificate Signing Request (CSR)** and click **Next** to open the **Details** page.

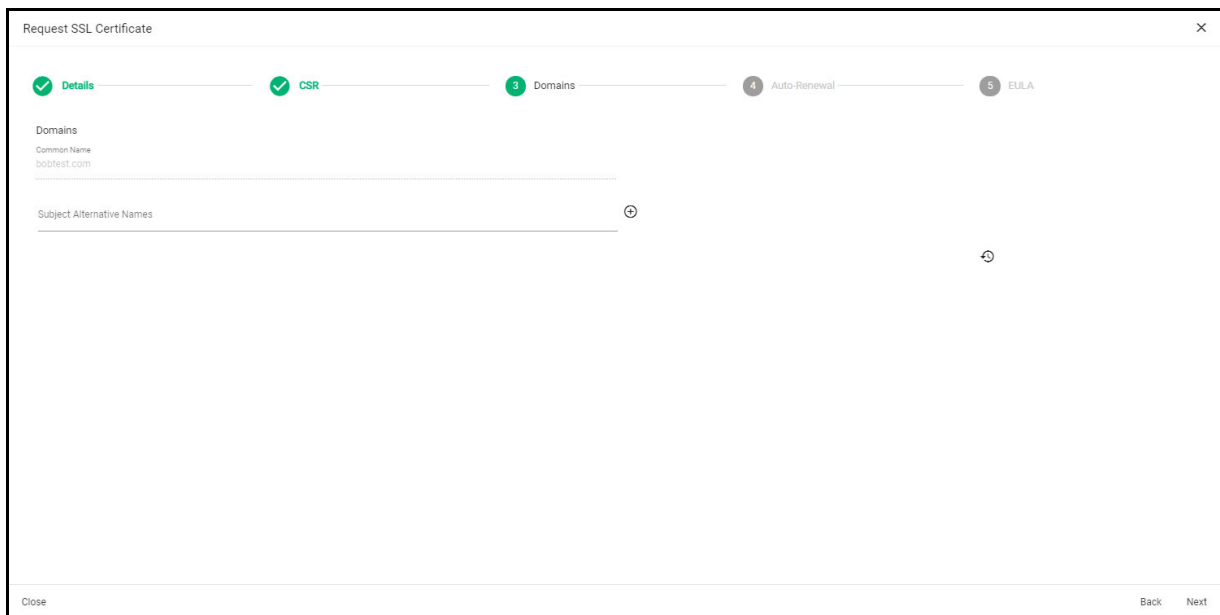
3. Complete the **Details** fields based on the information in the following table. Mandatory settings are marked by a red asterisk.

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 (if provided) is also displayed.
Certificate Term	The validity period of the certificate.
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.
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 (to view this, open the Certificates area and click View next to the subject certificate). The email address of the external requester is displayed as the External Requester in the View dialog of an issued certificate.

4. Click **Next** to open the **CSR** page shown in the following illustration.

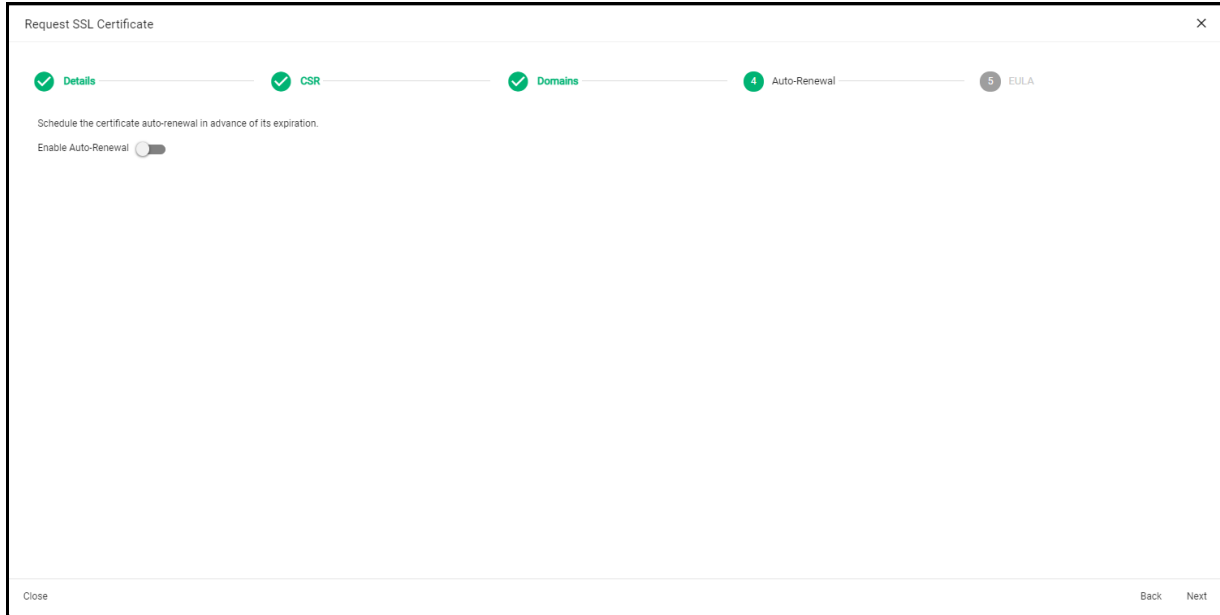


5. Paste or drag your CSR into the **CSR** field, or upload it as a `.txt` file.
6. Click **Next** to open the **Domains** page shown in the following illustration.

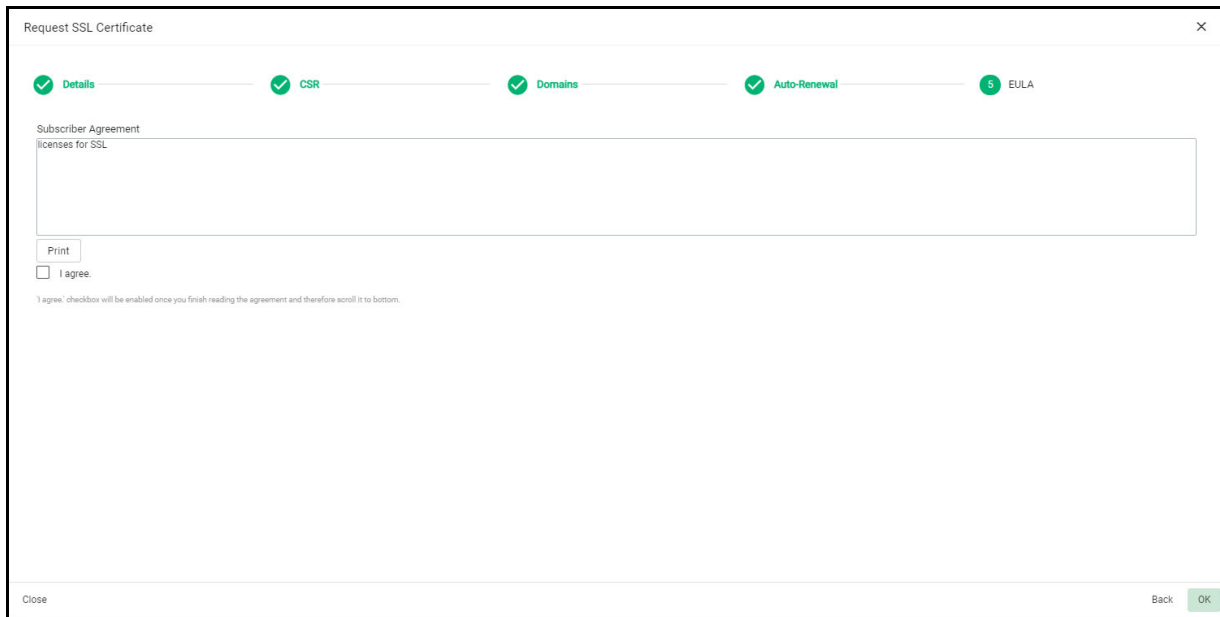


7. Add **Subject Alternative Names**. For EV-level certificates, complete the **EV Details** page.

NOTE: The details you need to complete depend on the EV mode activated for your account. This is the same information as provided in the EV details page when adding a new organization. If the EV type is **RA**, for your account, this is auto-populated.
8. Click **Next** to open the **Auto-Renew** page shown in the following illustration.



9. To have SCM apply for a new certificate when the current one approaches expiry, select **Enable Auto-Renewal**.
10. Click **Next** to open the **EULA** page shown in the following illustration.
11. Read the EULA and accept it by selecting **I Agree**, and then click **OK** to submit the application.

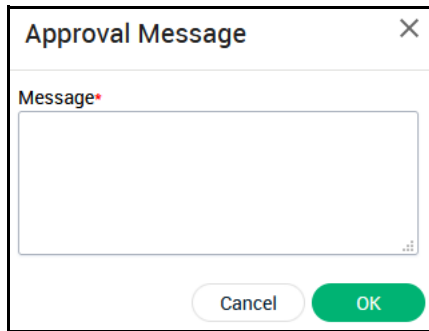


The certificate is added to the **Certificates > SSL Certificates** page with the status of Requested.

To approve the request, do the following:

1. Navigate to **Certificates > SSL Certificates**.

2. Select the appropriate certificate and click **Approve** to open the **Approval Message** dialog shown in the following illustration.



3. Enter a message to be sent with the approval notification email and click **OK**.
Once the request has been approved, the certificate status changes to **Approved**.
SCM forwards the application to Sectigo and the status changes to **Applied**.
Sectigo issues the certificate if validation is successful.
SCM sends a Certificate Collection email to the certificate requester and the **Status** of the certificate is changed to **Issued**.

5.1.2 How to collect SSL certificates

The next step is to collect the certificate, which can be done in one of two ways:

- Collection via email.
- Collection via SCM.

To collect the certificate via email:

Once the certificate has been issued, SCM automatically sends a collection email to you and the external applicant, if applicable.

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

Click the link in the collection email to download the certificate file for installation on the appropriate server.

To collect the certificate in SCM, do the following:

1. Navigate to **Certificates > SSL Certificates**.
2. Select the certificate and click **View**.
3. Click **Download** in the upper-right corner.
4. Select on the appropriate certificate format to download the certificate.

5.2 Requesting and issuing client certificates

Client certificates are managed from the **Certificates > Client Certificates** page.

ID	STATUS	ORDER NUMBER	CERTIFICATE PROFILE	TERM	REQUESTED VIA	SUBJECT	EXPIRES	SERIAL NUMBER	NAME	EMAIL	REQUESTED	ISSUED	DOWN
2119	DOWNLOADED	3054192	imune_new	365	Self Enrollment	Eradmin2019@comqa	11/17/2023	6F5F5E0B022A	Administrator 20	admin2019@comqa.com	11/16/2021 18:40	11/16/2021 02:00	11/16
2092	ISSUED	3048969	imune_new	365	Self Enrollment	Eh1205@comqa.com	11/12/2023	CE4E414E41EE	Jordan Key	1205@comqa.com	11/11/2021 19:03	11/11/2021 02:00	
2088	DOWNLOADED	2974090	imune	730	Self Enrollment	Ehkrakasa@comqa.o	09/18/2023	F2215B9625CD	Kira Kaa	krakasa@comqa.com	09/17/2021 15:20	09/17/2021 03:00	09/17

You can issue client certificates to enrolled users for domains which have been delegated to an organization or department.

Add client certificate users to SCM in one of the following ways:

- Manually enter the details of each user via the **Add New Person** form.
- Import a list of users from a CSV file.
- Auto-enroll users through Active Directory (AD) Integration by integrating your AD server with SCM via installing an MS agent. You can then automatically import users and provision them with client certificates.

Users can also enroll themselves and their client certificates using the self-enrollment form. This section explains the process of manually adding the users and enrolling their certificates by invitation. For more information on importing users, configuring and using the client self-enrollment form, or auto-enrolling users through AD Integration, see *Sectigo Certificate Manager Administrator's Guide*.

5.2.1 How to add a client certificate end user

To add a user manually, do the following:

1. Navigate to **Persons**.
2. Click the **Add** icon in the upper-right corner to open the **Add New Person** dialog.
3. Choose the organization and, if applicable, department to which the end user will belong.
4. Choose the domain with which the end user is associated. The end user's email should use this domain.
5. Enter the end user's email address. The domain of the address is automatically set.
6. Enter the end user's personal details. For client certificates, you typically specify the end-user's full name as the common name.
7. Enter any alternative email addresses separated by commas.
8. To allow the user to use the self-enrollment form to enroll client certificates, enter a secret ID.
9. Set the validation type. Typically, this will be Standard.
10. Click **Save**.

Repeat this process to add more users.

The screenshot shows a web form titled "Add New Person" with a close button (X) in the top right corner. The form is organized into several sections:

- Organization:** A dropdown menu with "acme" selected.
- Department:** A dropdown menu with "None" selected.
- Domain:** A dropdown menu with "ccmqa.com" selected.
- Personal Information:** A section containing two text input fields:
 - First Name ***: A required field, indicated by a red asterisk.
 - Middle Name**: An optional field.

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

To edit an existing end-user's details, navigate to **Certificates > Client Certificates**, select the end-user and click **Edit**.

NOTE: If any information is altered, with the exception of Secret ID, any previously issued client certificates for this email address is automatically revoked.

5.3 Requesting and issuing code signing certificates

Code signing certificates are managed from the **Certificates > Code Signing Certificates** page.

STATUS	ORDER NUMBER	CERTIFICATE PROFILE	TERM	REQUESTED VIA	SUBJECT	EXPIRES	SERIAL NUMBER	ORGANIZATION	DEPARTMENT	NAME	EMAIL	ISSUED	REQUESTED
REVOKED	F5U9N8hMunHq6	CS.pca	365	PKCS10		11/18/2021	50:54:8C:2A:4F:A5:D	Org1		12 21	12@boom.com	11/18/2020	11/18/2020
INVITED		CS.pca	365	PKCS10				Org1		12321	12@boom.com	07/09/2021	
EXPIRED			366	Discovery		05/25/2021	62:90:D8:91:CA:58:8f	iconlab		Administrator 42			
REVOKED	Fm5j8t9Fiv7w8K4	CS.pca	365	PKCS10		02/17/2022	58:89:D5:88:A4:96:7f	Org1		Dwight.Hodge	dwhight.hodge@sectigo.com	02/17/2021	02/17/2021
ISSUED			730	Discovery		05/28/2022	38:60:00:01:58:88:8f	iconlab		local2			
DOWNLOADED	Fm59gOZPj7w8KA	CS.pca	365	PKCS10		02/17/2022	41:45:58:78:07:88:8f	Org1		Murray Demo	murray.mocullgh@sectigo.com	02/17/2021	02/17/2021

You can issue code signing certificates to users with email addresses at domains you have added to SCM. Each domain should have been delegated to an organization or department and should have passed DCV.

You can add code signing certificate users to SCM in the following ways:

- By manually entering the details of each user.
- By importing a list of users and their details from a CSV file that you have created. Each entry in this file should have four mandatory and two optional fields for the details, listed in a specified order. You can upload the `.csv` file using the **Certificates > Code Signing Certificates** page.

Once the users are added, SCM automatically sends the invitation email. Upon clicking the validation link in the email, the user is presented with a registration form which the user needs to fill out and submit. Once the form has been submitted and validated, SCM sends the user an email containing a link to download their certificate. For information on importing users from a `.csv` file, see *Sectigo Certificate Manager Administrator's Guide*.

5.3.1 How to add code signing certificates

You add a code signing certificate user manually as follows:

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

The screenshot shows a 'Send Invitation' dialog box with the following fields and values:

- Email ***: unknownemail@test.com
- Details**
 - Enrollment Endpoint ***: cs19
 - Account ***: 1
- Profile**: CS pca

Buttons at the bottom: Cancel, Send

3. 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.

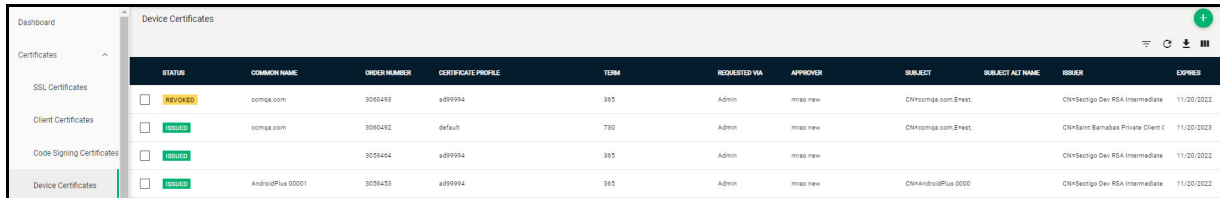
If the requester is an existing user, the corresponding certificate is automatically added to SCM and a certificate collection email is sent to the end-user.

If the requester is a new end-user, an invitation mail is sent to initiate the self-enrollment process. Upon clicking the link in the mail, the email address is validated and the applicant is taken to the **User Registration** form. Upon completion of user registration and validation processes, the

certificate request is sent to SCM for approval. Once the certificate is issued, a collection form is sent via email, enabling the end-user to download and save the certificate.

5.4 Requesting and issuing device certificates

Device certificates are managed from the **Certificates > Device Certificates** page.



STATUS	COMMON NAME	ORDER NUMBER	CERTIFICATE PROFILE	TERM	REQUESTED VIA	APPROVER	SUBJECT	SUBJECT ALT NAME	ISSUER	EXPIRES
REVOKED	comqa.com	3050493	ad99994	365	Admin	mtao new	CN=comqa.com.Erect	CN=Sectigo Dev RSA Intermediate	CN=Sectigo Dev RSA Intermediate	11/20/2022
ISSUED	comqa.com	3050492	default	730	Admin	mtao new	CN=comqa.com.Erect	CN=Saint Barnabas Private Client C	CN=Sectigo Dev RSA Intermediate	11/20/2023
ISSUED	comqa.com	3050464	ad99994	365	Admin	mtao new	CN=comqa.com.Erect	CN=Sectigo Dev RSA Intermediate	CN=Sectigo Dev RSA Intermediate	11/20/2022
ISSUED	AndroidPlus 00001	3050453	ad99994	365	Admin	mtao new	CN=AndroidPlus 0000	CN=Sectigo Dev RSA Intermediate	CN=Sectigo Dev RSA Intermediate	11/20/2022

You can apply for device certificates in the following ways:

- **Active Directory**—Device certificates can be issued from SCM as a proxy and from MS CA devices that have been enrolled to Active Directory (AD).
- **SCEP**—Using the built-in SCEP server, certificates can be requested and issued for devices that have been configured with a suitable configuration profile.
- **API integration**—Mobile Device Management (MDM) solutions can be integrated with SCM through APIs. Administrators can apply configuration profiles to managed devices to enroll for certificates from SCM.
- **Self-enrollment**—Device certificates can be requested by applicants using the self-enrollment form for issuance of certificates from private CAs. The self-enrollment form is available by clicking the link provided by an administrator.
- **Manually**—Device certificates can be requested from the **Certificates > Device Certificates** page.

The remainder of this section explains how to request certificates manually from SCM. For information on the other methods, see *Sectigo Certificate Manager Administrator's Guide*.

Before beginning the application, you will need to create the CSR. The public key included in the CSR should have at minimum an 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 Relative Distinguished Name (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.

5.4.1 How to add device certificates

Add a device certificate by doing the following:

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

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 device certificate profile.
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.

6 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: [Generating reports](#)