SECTIGO®

Administrator's Guide
for
Sectigo® Certificate Manager
24.12

December 2024

Sectigo Certificate Manager

Administrator's Guide, 24.12 SCMAG

Copyright © 2008, 2024, Sectigo.

All rights reserved.

Author: Sectigo

Table of Contents

3 Managing certificates

4 Performing certificate discovery tasks

5 Configuring organizations and domains

6 Generating reports

7 Managing enrollments

8 Managing issuers

9 Using SCM with Microsoft Azure and Intune

10 SCM agent integrations

11 Configuring settings

12 Managing administrators

Appendix A: CSV import format requirements

Appendix B: Sectigo root and intermediate certificates

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.
italic	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.
<text>	Italic type with chevron brackets indicates the required insertion of user or company specific text.

1

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.
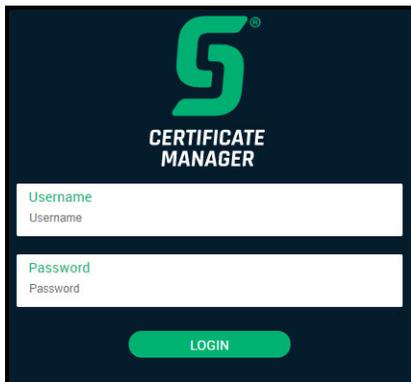
2.   Validate your identity using one of the following methods:
   • Enter your SCM credentials and click **Login**.
   • If configured, click the name of your identity provider and enter your SSO credentials.
3.   Depending on how your account was set up, you may be prompted to change your password 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 [icon] 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.

Notifications   ×

	Mark All As Read	Delete All

C

MESSAGE	CREATED DATE
☐ MS Agent 'Agent5' is connected now.	
☐ MS Agent 'Agent60' is connected now.	
☐ MS Agent '7.03.23' is connected now.	
☐ Private Key Agent is connected now.	
☐ MS Agent 'Agent60' is not active a long time.	
☐ MS Agent '7.03.23' is not active a long time.	
☐ MS Agent 'Agent8' is not active a long time.	
☐ Private Key Agent is not active a long time.	

Page 1   Rows per page   10 ◢   ‹ 1-10 of 260 ›

Close

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
_____

Telephone Number
_____

Street
Locality
                    .
_____

Zip / Postal Code
_____

Country
                                                        ◢
_____

Relationship
_____

Current locale
en   ◢
_____

Password	Change
Grid settings	Reset To Default
Recent Activity	Show

Cancel   Save

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

2

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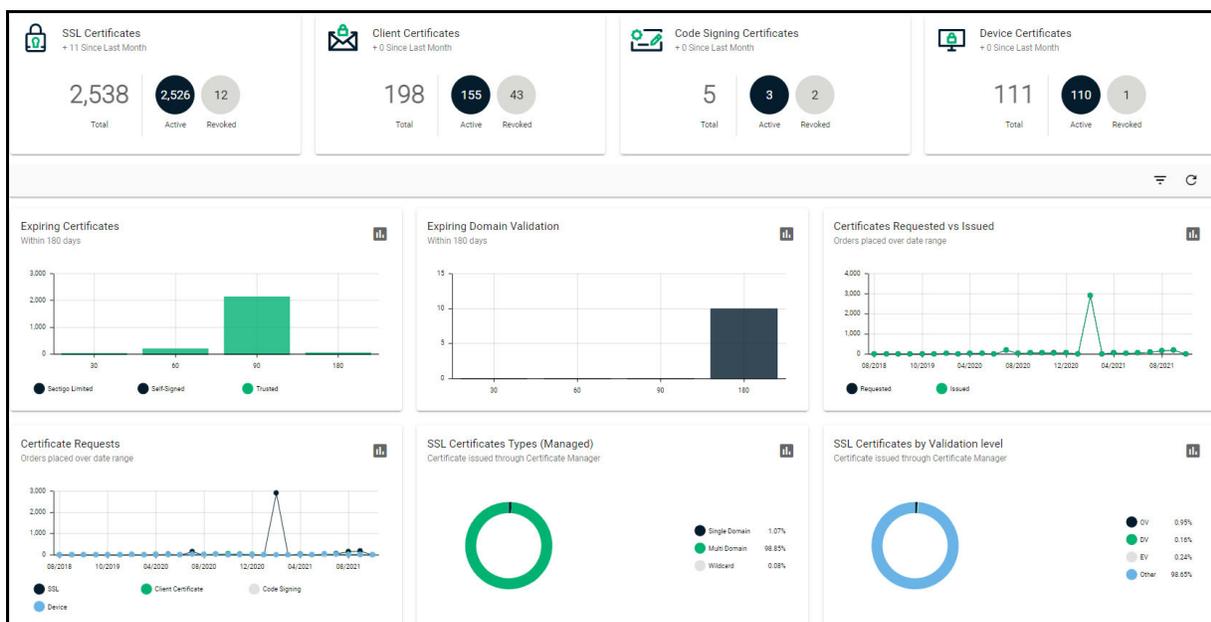
Clicking the chart icon ▮▮ in the upper right corner of a chart displays a report with the breakdown of the chart statistics. Hovering the cursor over a legend or chart sector displays additional information.

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.
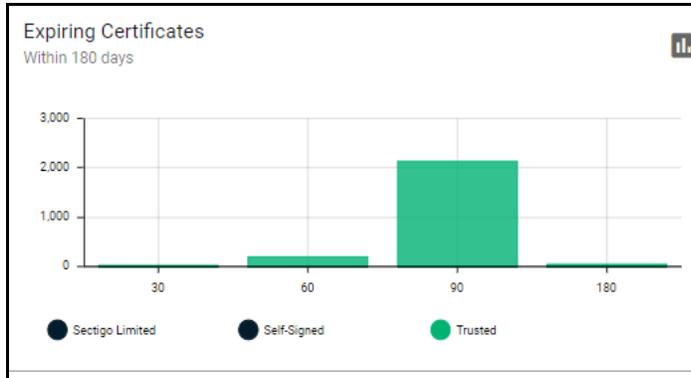
The following information is available:

- **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.
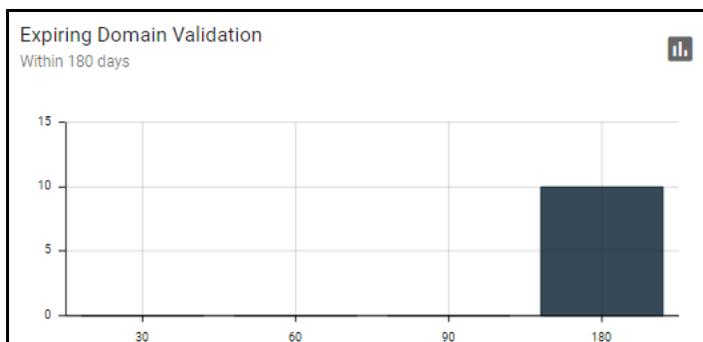
The following information is available:

- **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.
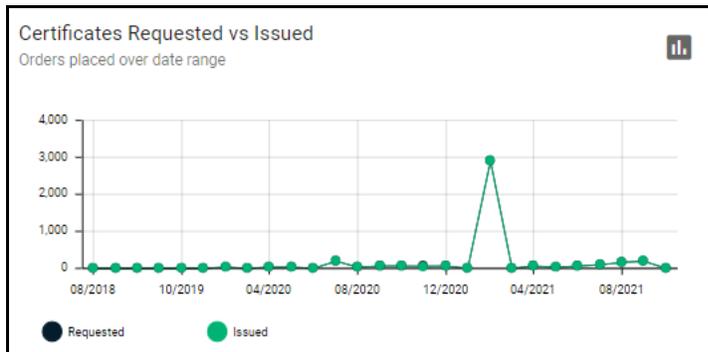- **Organization**—the name of the organization that has been issued with the certificate.
- **Department**—the department of the organization that is associated with the certificate. This column is blank when a department has not been delegated as the controlling entity.
- **Order Number**—the number 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.
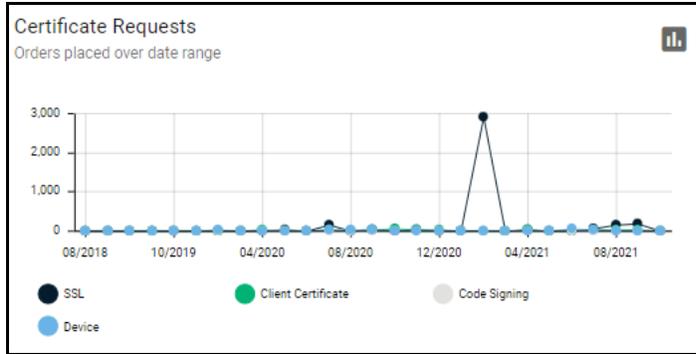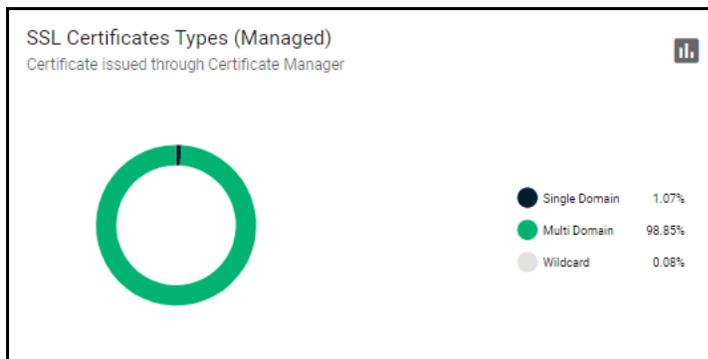
The following information is available:

- **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.
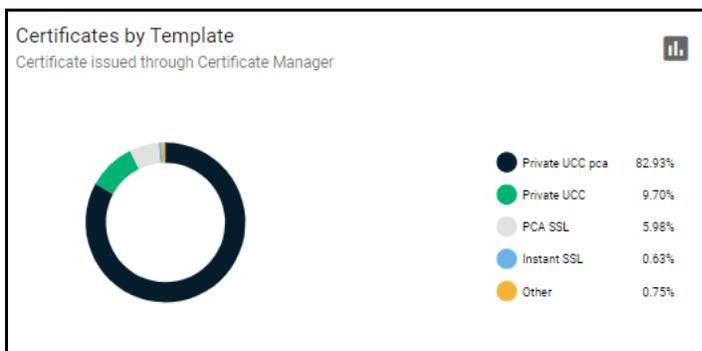
The following information is available:

- **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 **DVC 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.
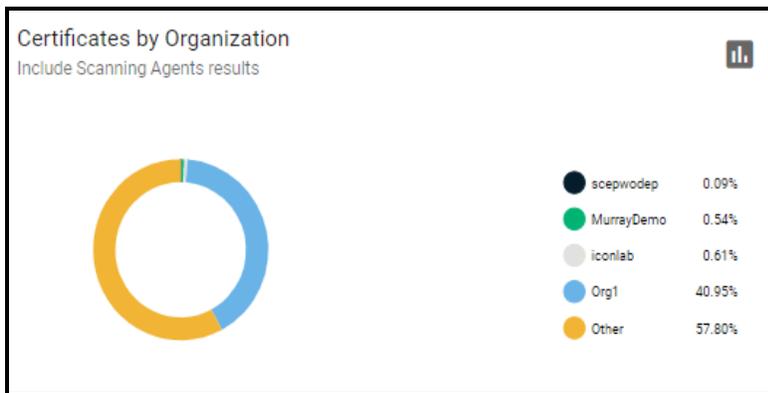

The following information is available:

- **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.
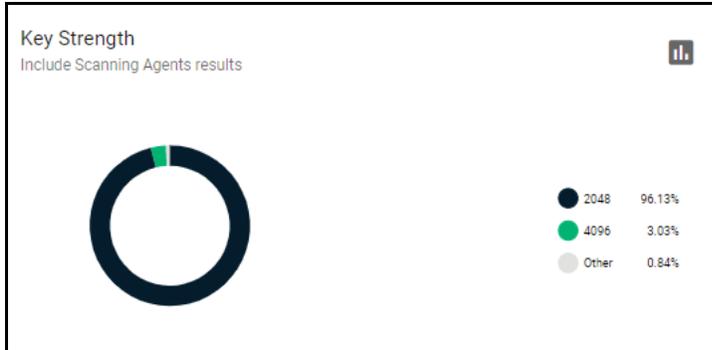

The following information is available:

- **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.
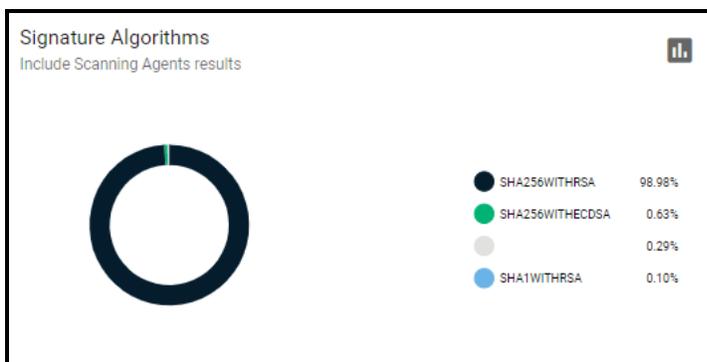
The following information is available:

- **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.
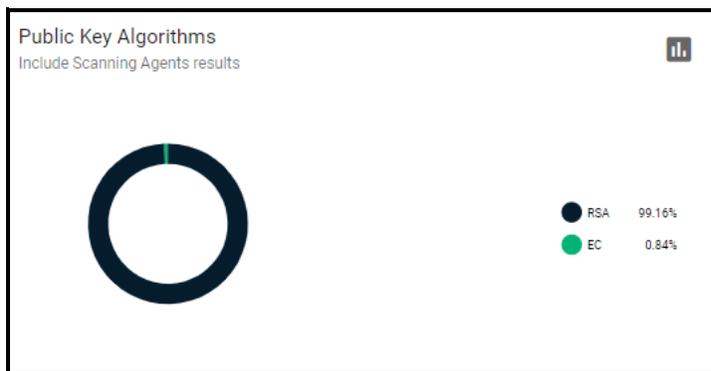

The following information is available:

- **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,S HA384 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,S HA384 with RSA, etc.
- **Key Algorithm**—the type of algorithm used, by the public and private keys, for encryption. For example, RSA, DSA, and EC.

3

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

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 115.

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 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 72.

- **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 75.

- **Revoke**—Revokes the certificate. See "How to revoke, replace, and delete SSL certificates" on page 78.

- **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 78.

- **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.
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.
Requested Via	How the certificate was requested. For example, via Discovery, Web Form, Client Admin, ACME.
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.

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.
Approver	The name of the person who approved the 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.
Comments	Comments that don't fit under any other heading.
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: • **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: • **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.
Renewed	The date the certificate was renewed.
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
- Renew or revoke the certificate
- 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.
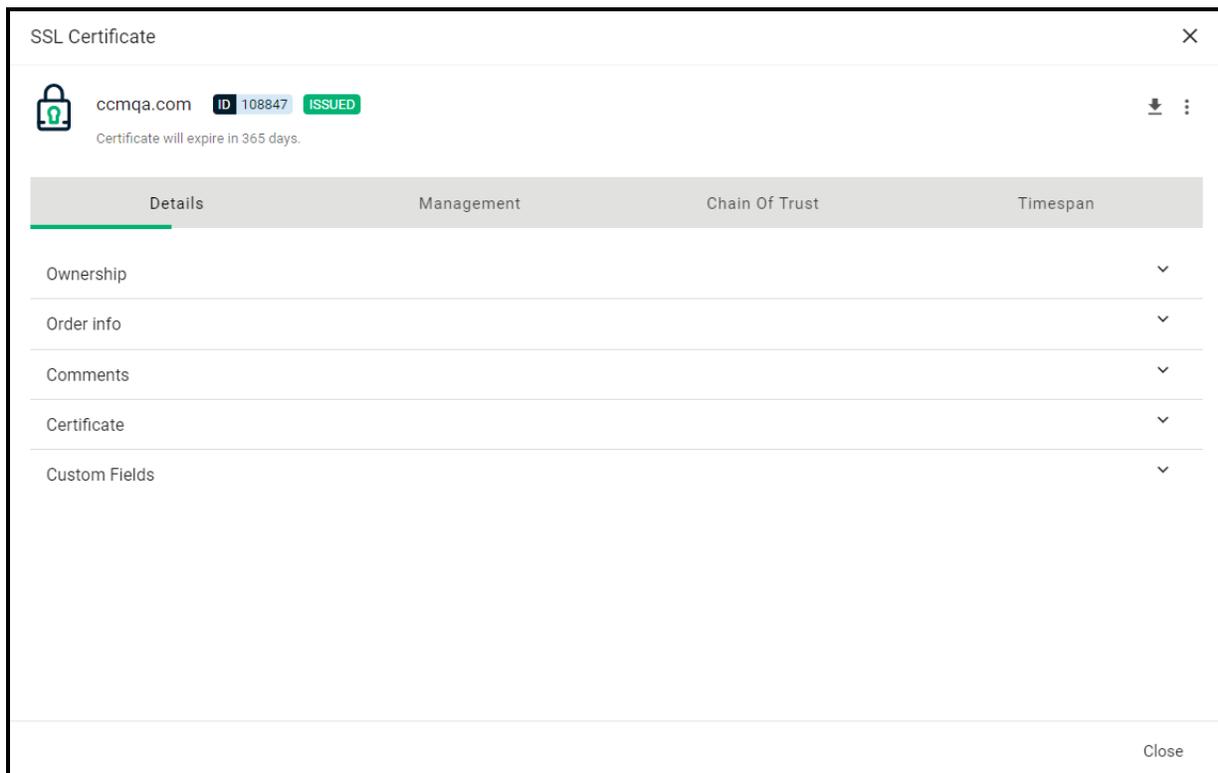
The Certificate summary panel displays the following information:

- 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** icon 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.
- The three vertical dots allows you to do the following:
  - **Renew** - Renews the certificate to extend its validity.
  - **Mark Renewed** - Marks the certificate as renewed manually.
  - **Revoke** - Revokes the certificate.
- 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
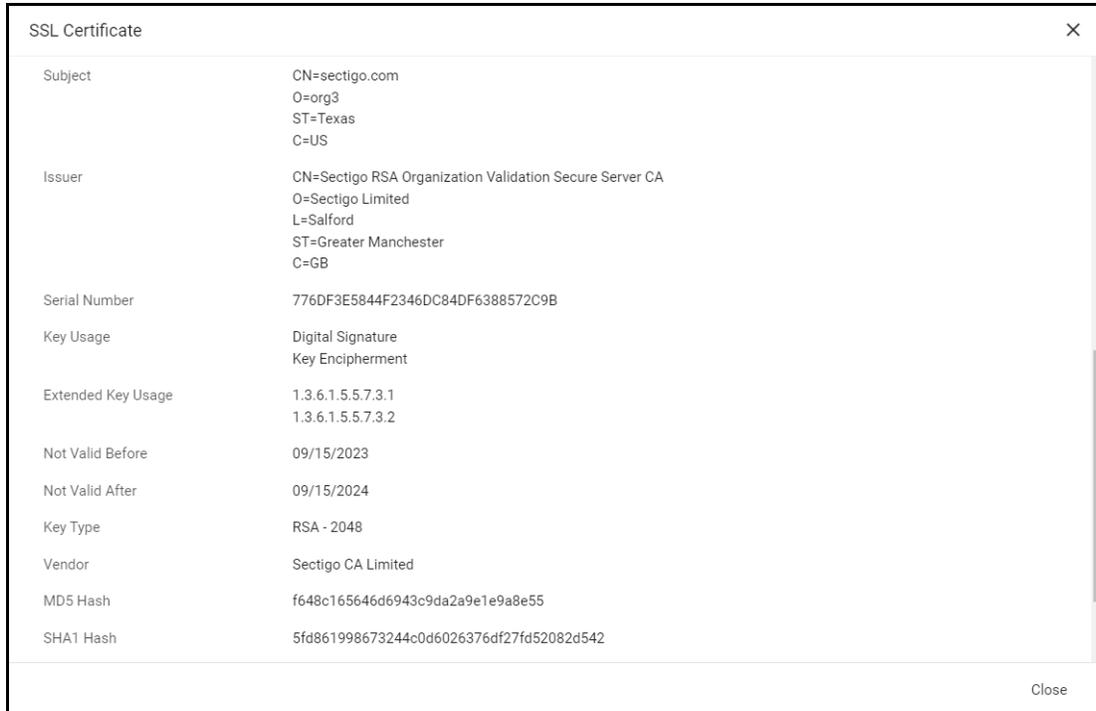
3.2.2.2 Using the Certificate Management tab

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.
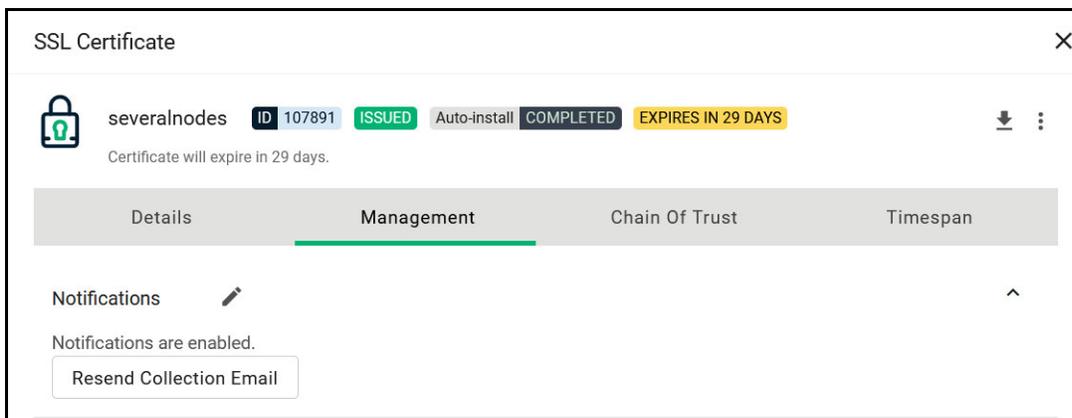
In **Auto-installation**, you have information about server nodes associated with the certificate.
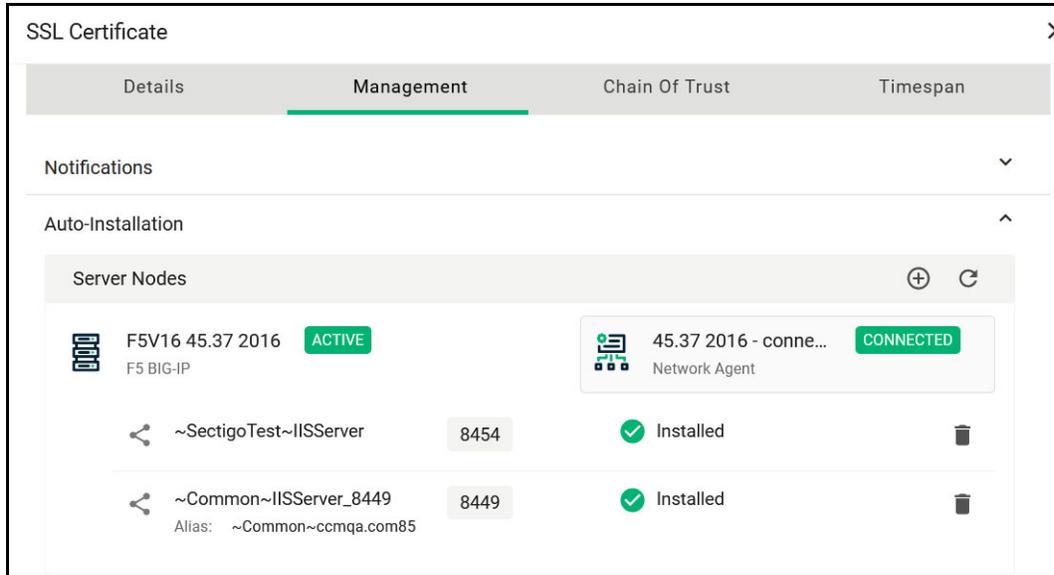
Locations describes where the certificate exists outside of SCM.

- 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

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.

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**.
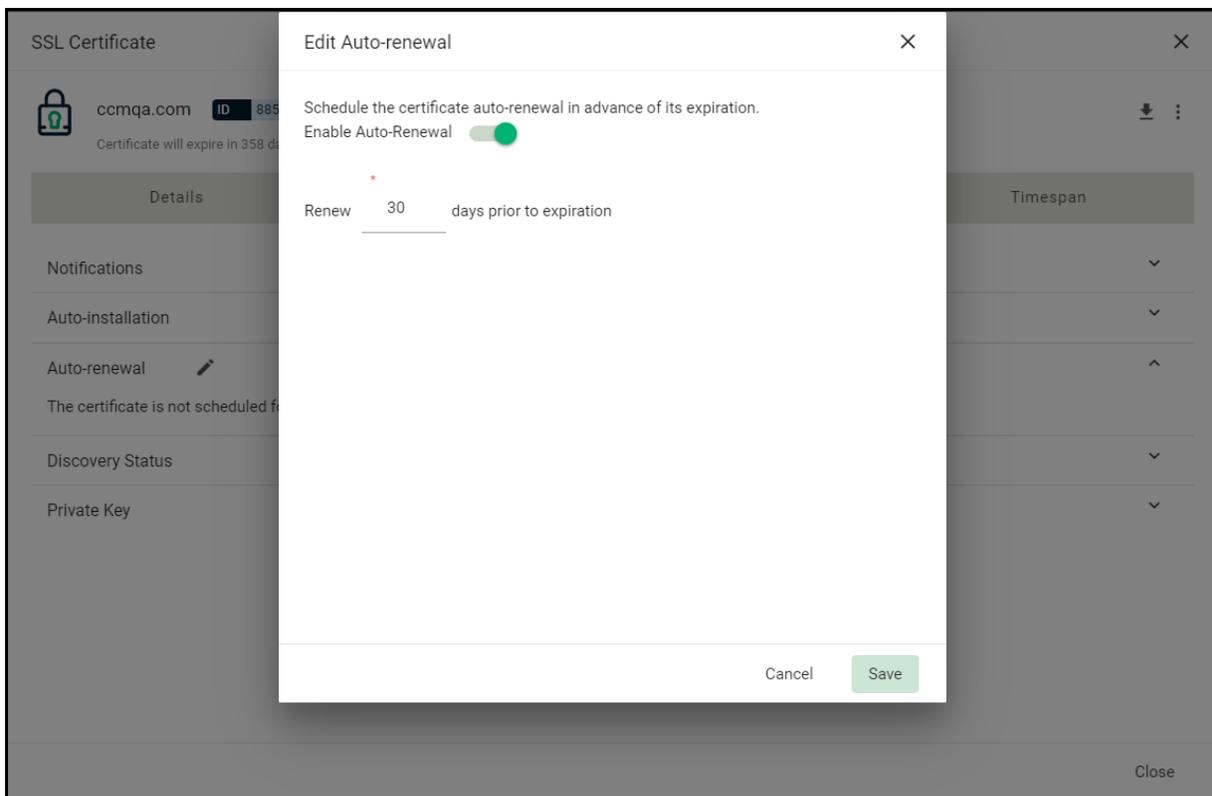
For more information, see "Automatic certificate renewal scheduling" on page 77.

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 72.

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).

- 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.

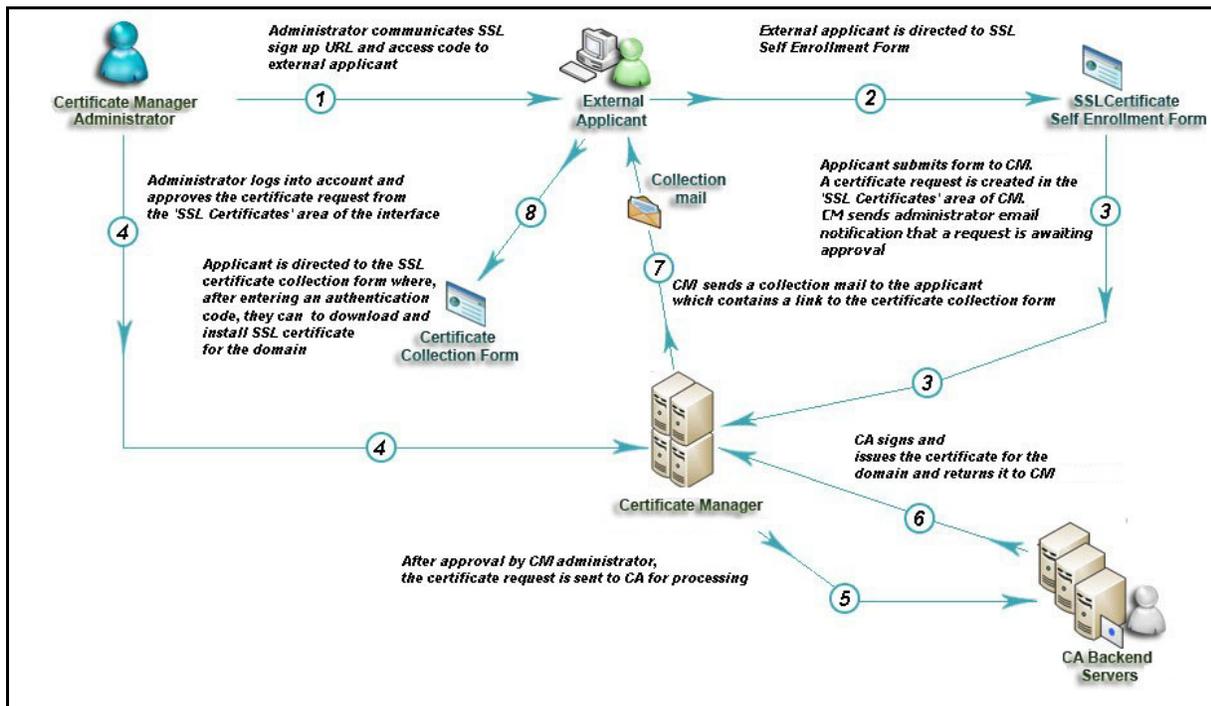### 3.2.3.1 Using the SSL certificate enrollment form

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.

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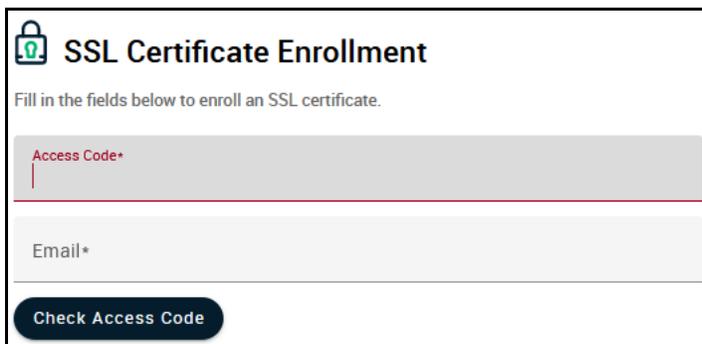
To access the full form, the applicant must enter the access code and an email address from a domain delegated to the organization or department of the enrollment endpoint account, and click **Check Access Code**. If both the access code and email address are successfully validated, the full certificate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

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 126.

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 `example.com`. For wildcard certificates, the domain name in the format of `*.example.com`. For MDC, the primary domain name in the format of `example.com`.
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.
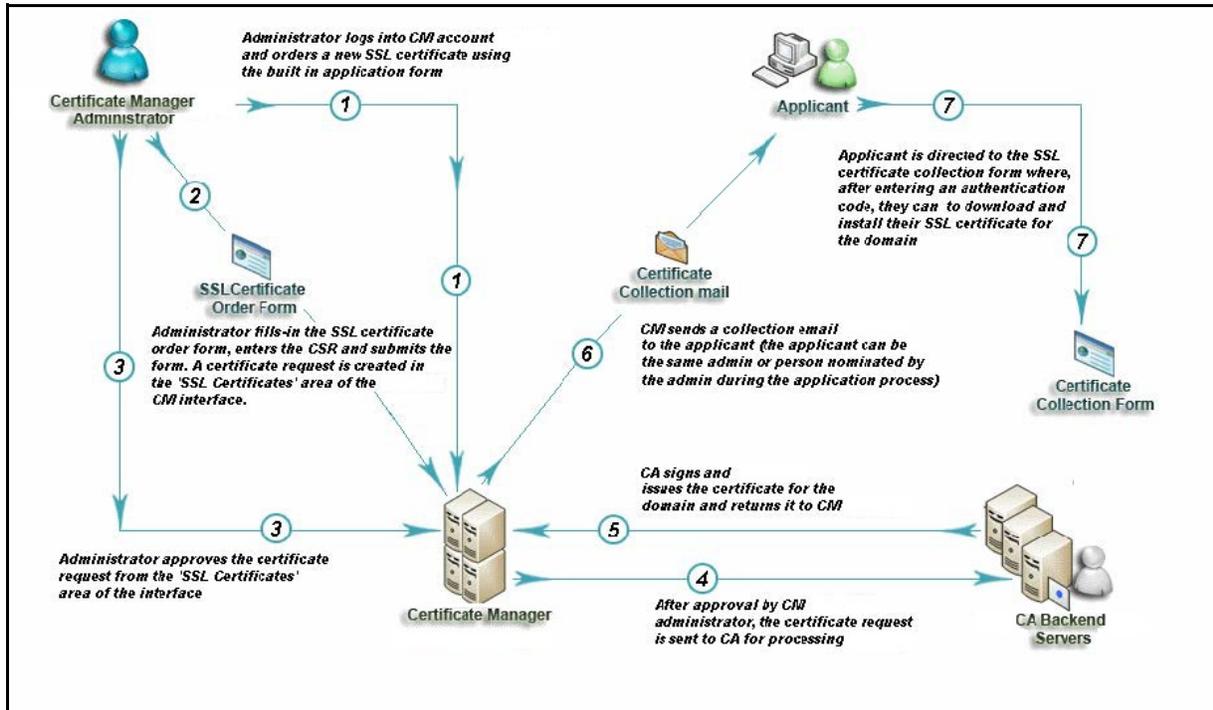
You can manually apply for new certificates as follows:

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

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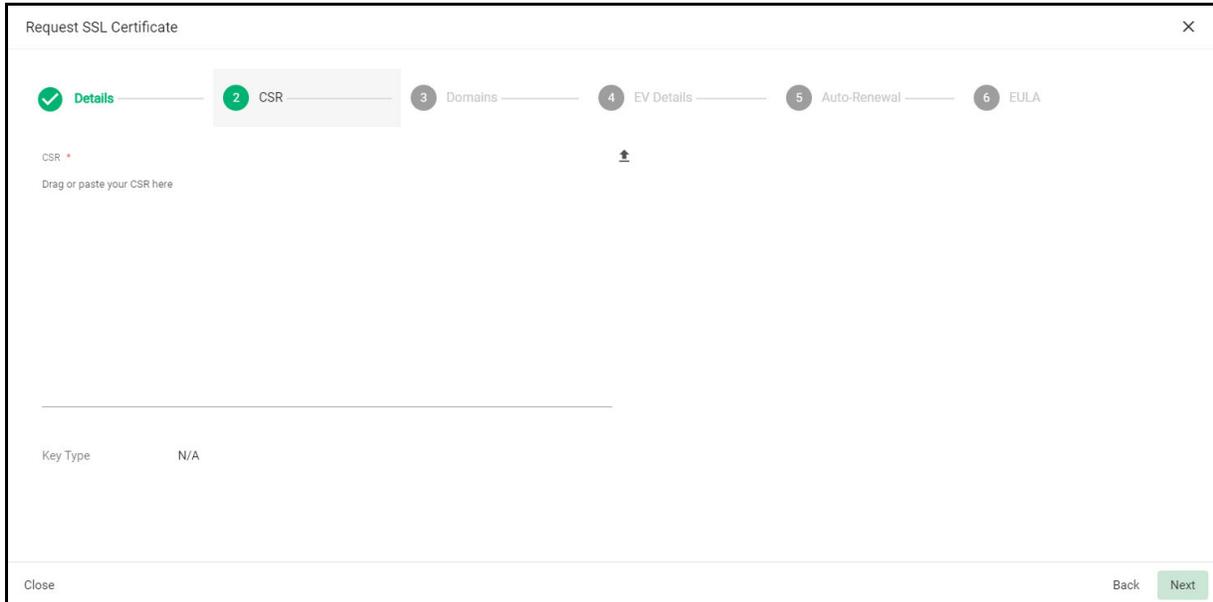
5. Check the Common Name for the domain and click **Next**.

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

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.

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.
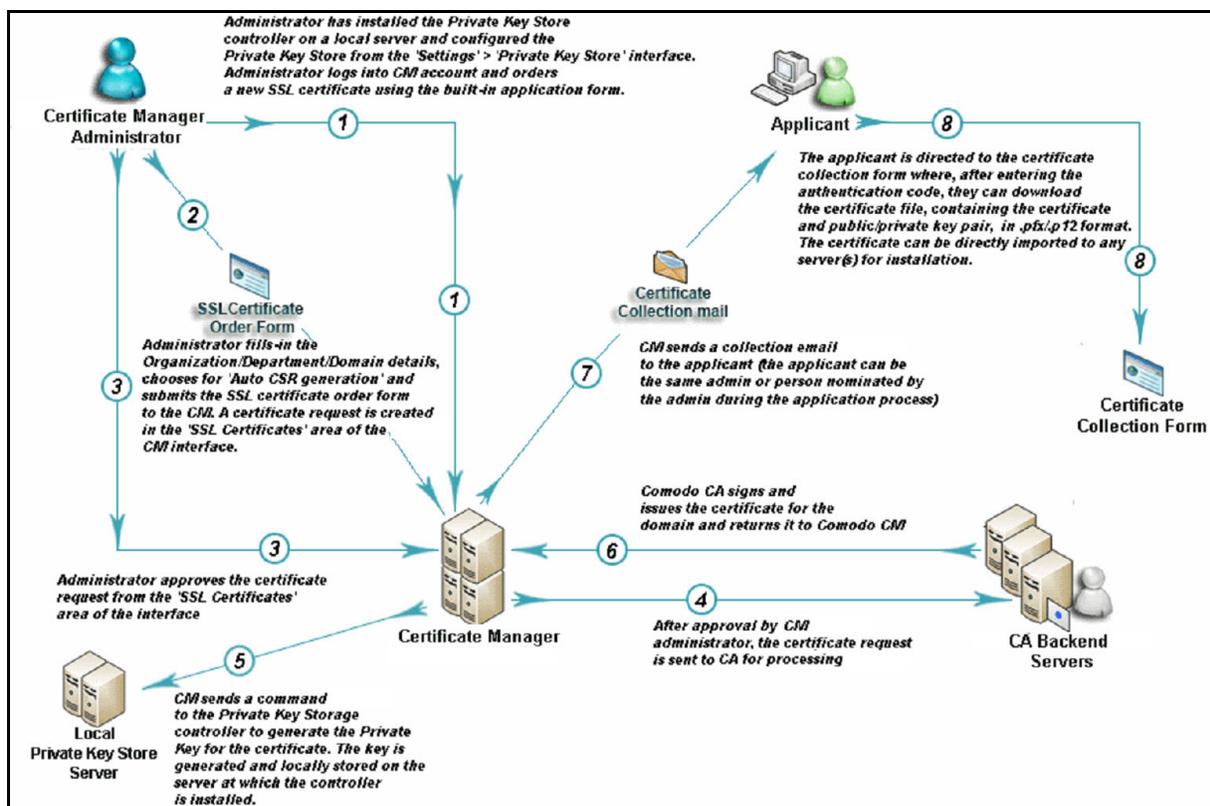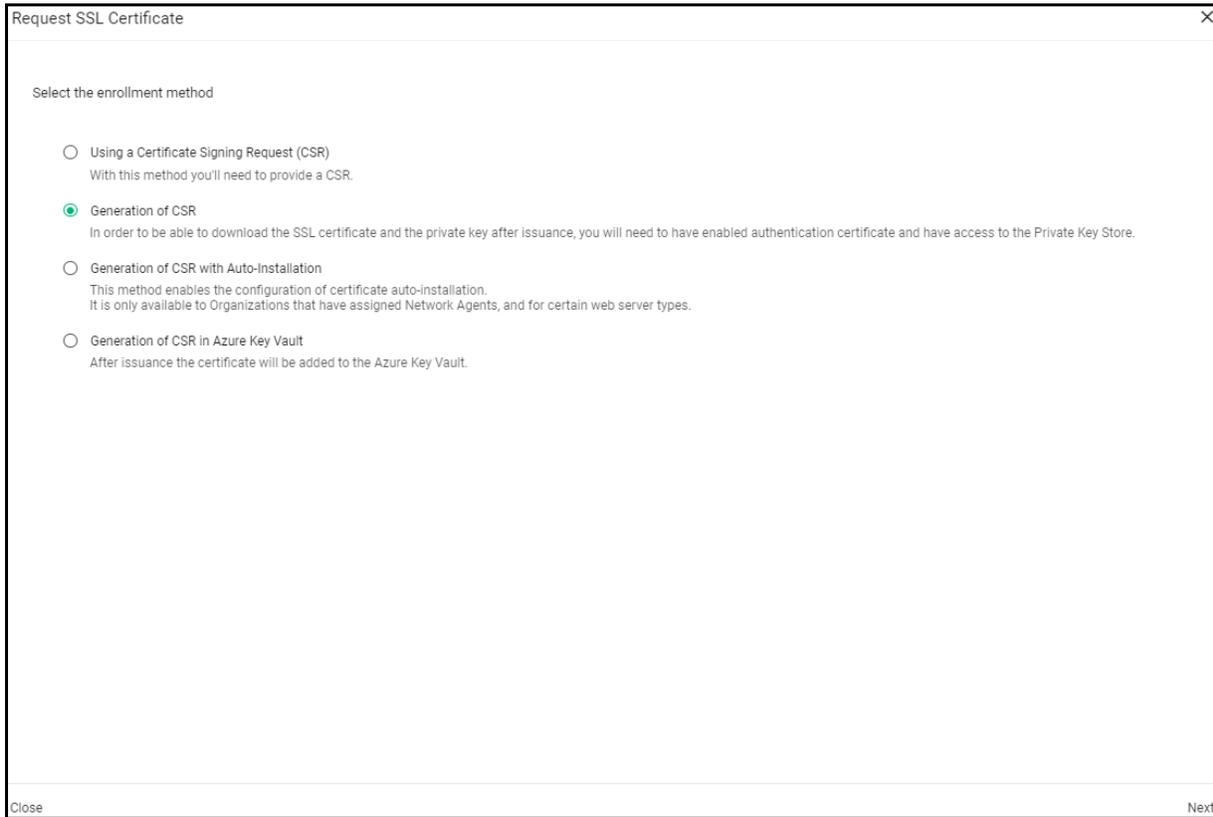

To apply for a new SSL certificate with auto-generated CSR, do the following:

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

3. Fill in the **Details** page based on the table below and click **Next**. Mandatory settings are marked with 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 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**.
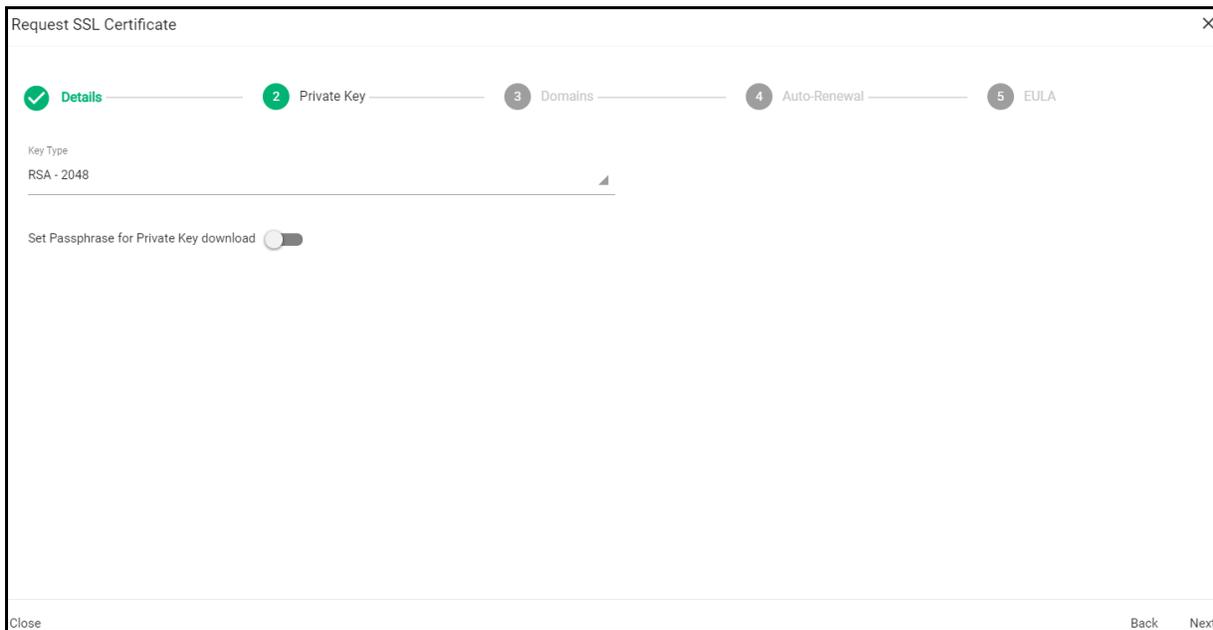
5. Click **Next** to open the **Domains** page and enter the domain name.

6. Click **Next**.

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.

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.

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).
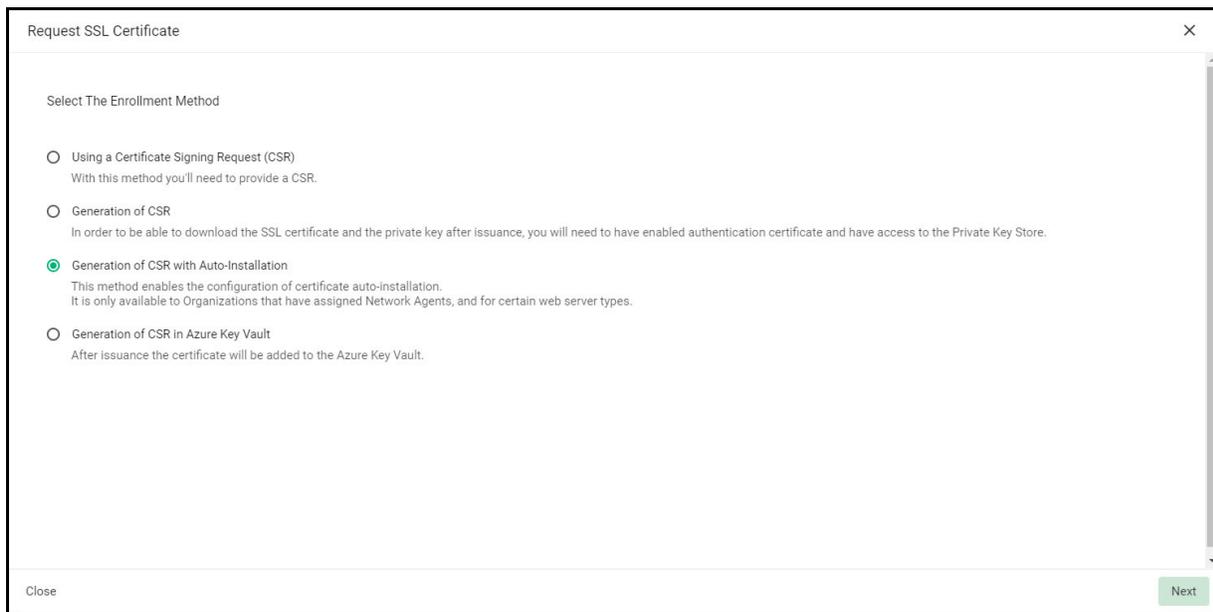
3.2.3.2.3 Generation of CSR with auto-installation

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.

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.

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.

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.

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.

12. Click **Add.**
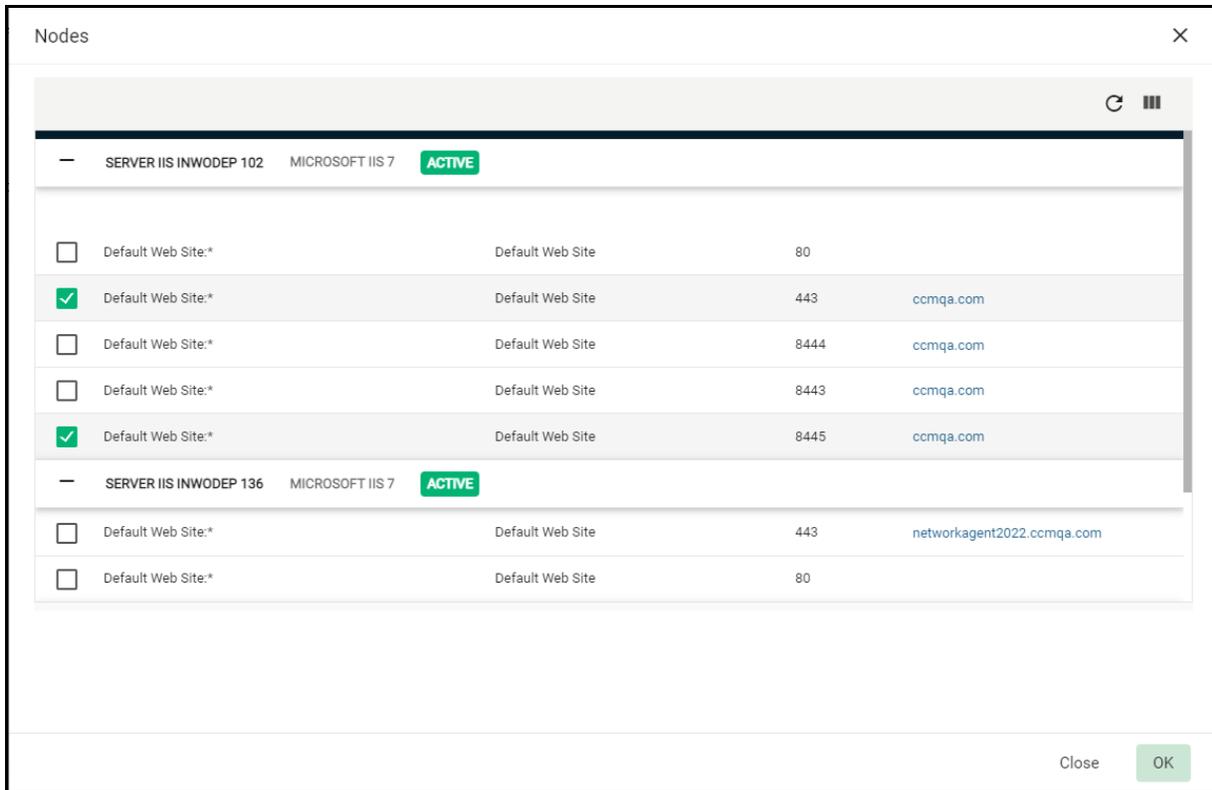
13. Select one or more servers hosting one or more of your target domains and click **OK**.

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.
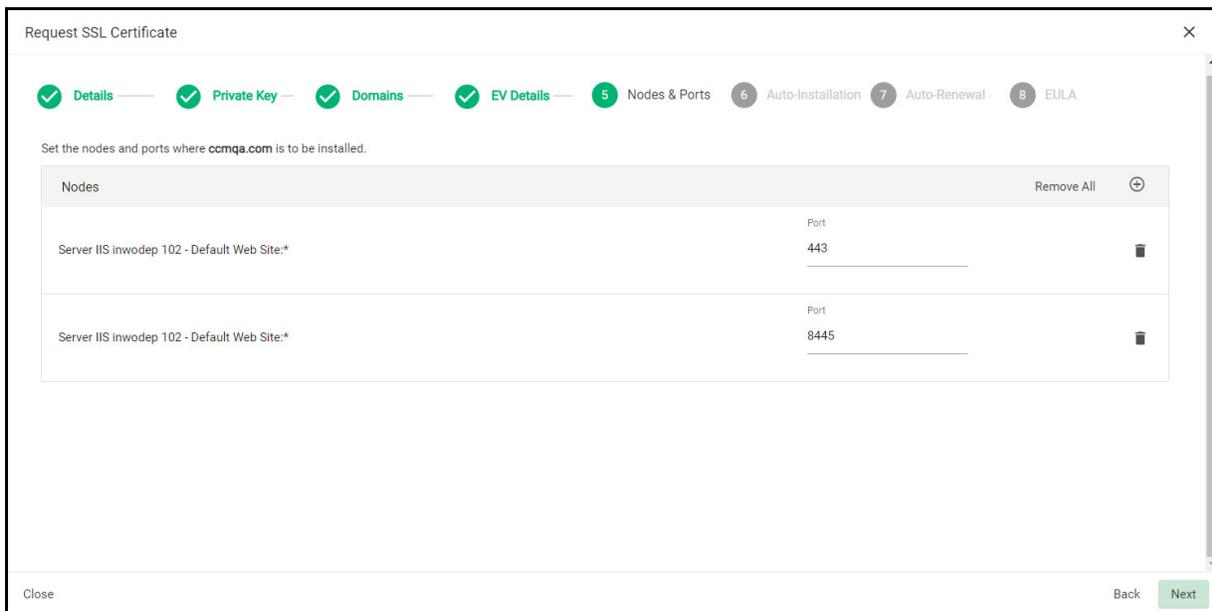
15. Click **Next** to open the **Auto-Installation** page.
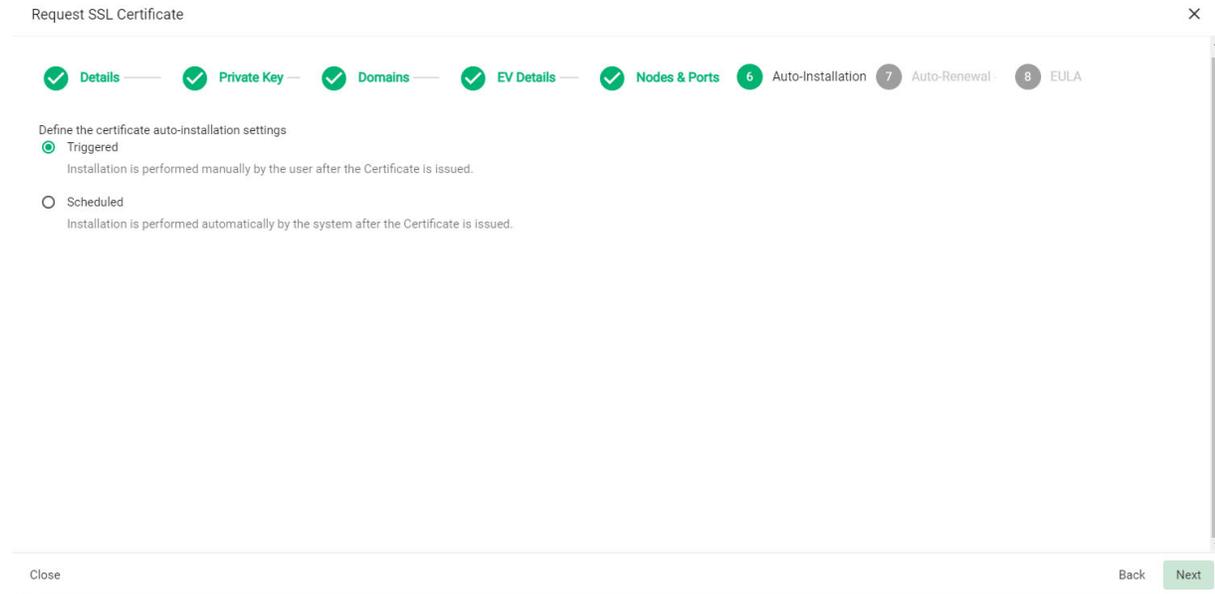
16. Use the **Auto-Installation** page to choose whether you want to start auto-installation manually or schedule it for a later time:

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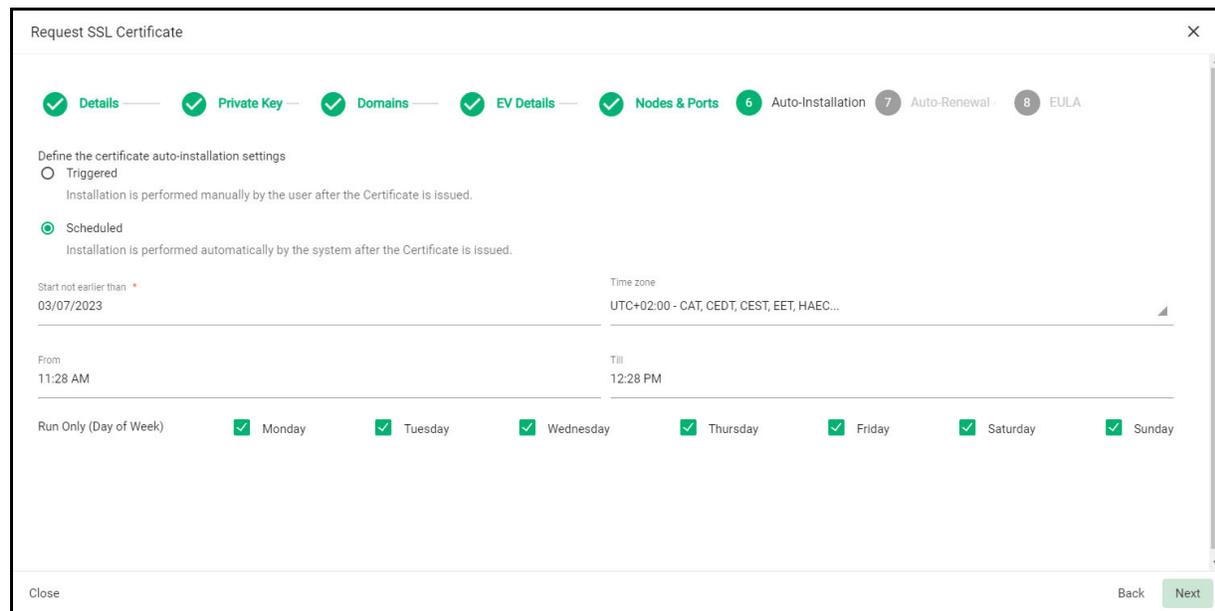
17. If you selected **Scheduled auto-installation**, populate the **Schedule** fields based on the information provided in the following table.

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.

19. 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. 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.

   c. 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.

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**.
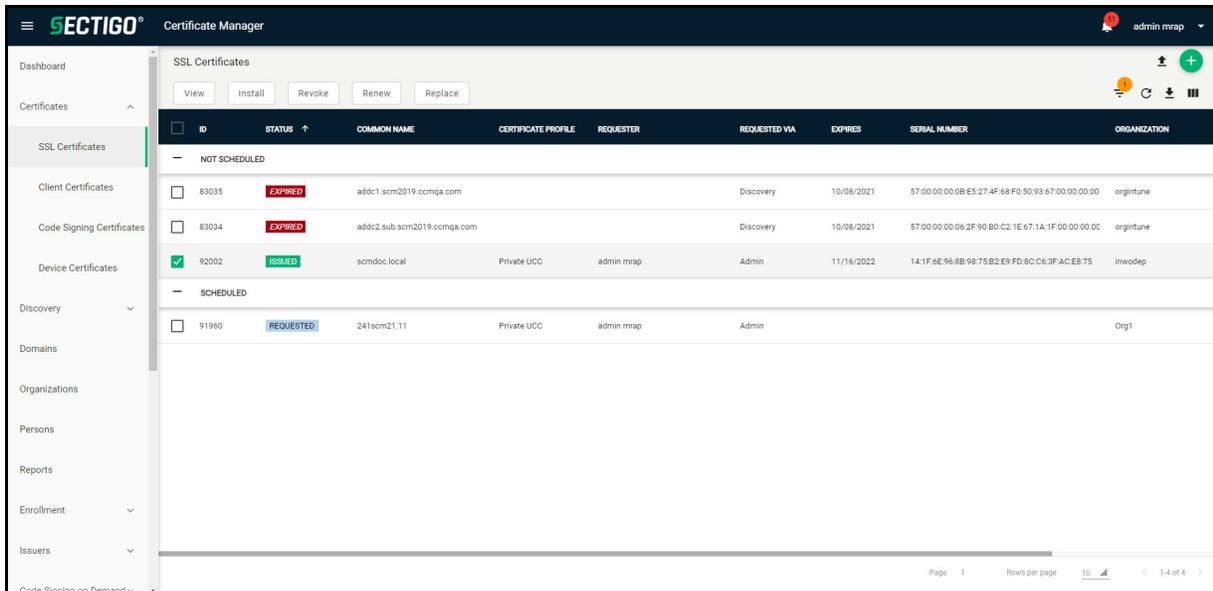
This displays the **SSL certificate auto-installation dialog**.
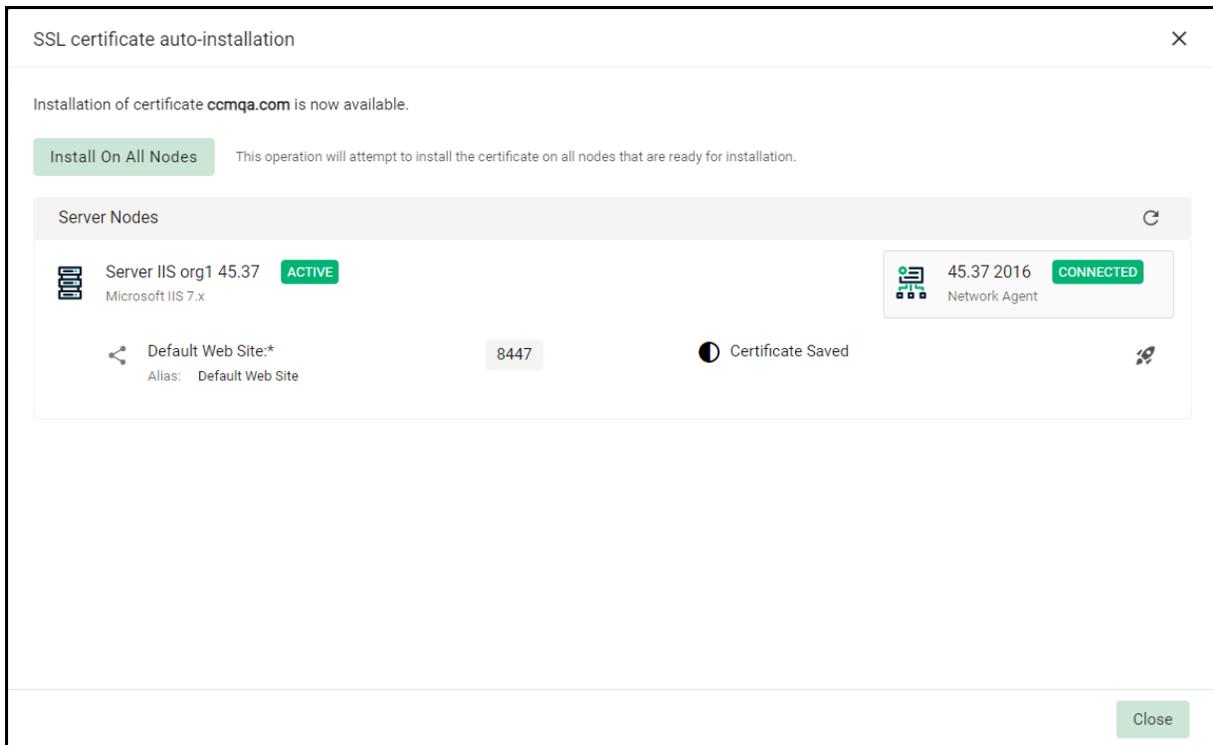
During the auto-installation process, an item can have one of the following statuses:

- **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.
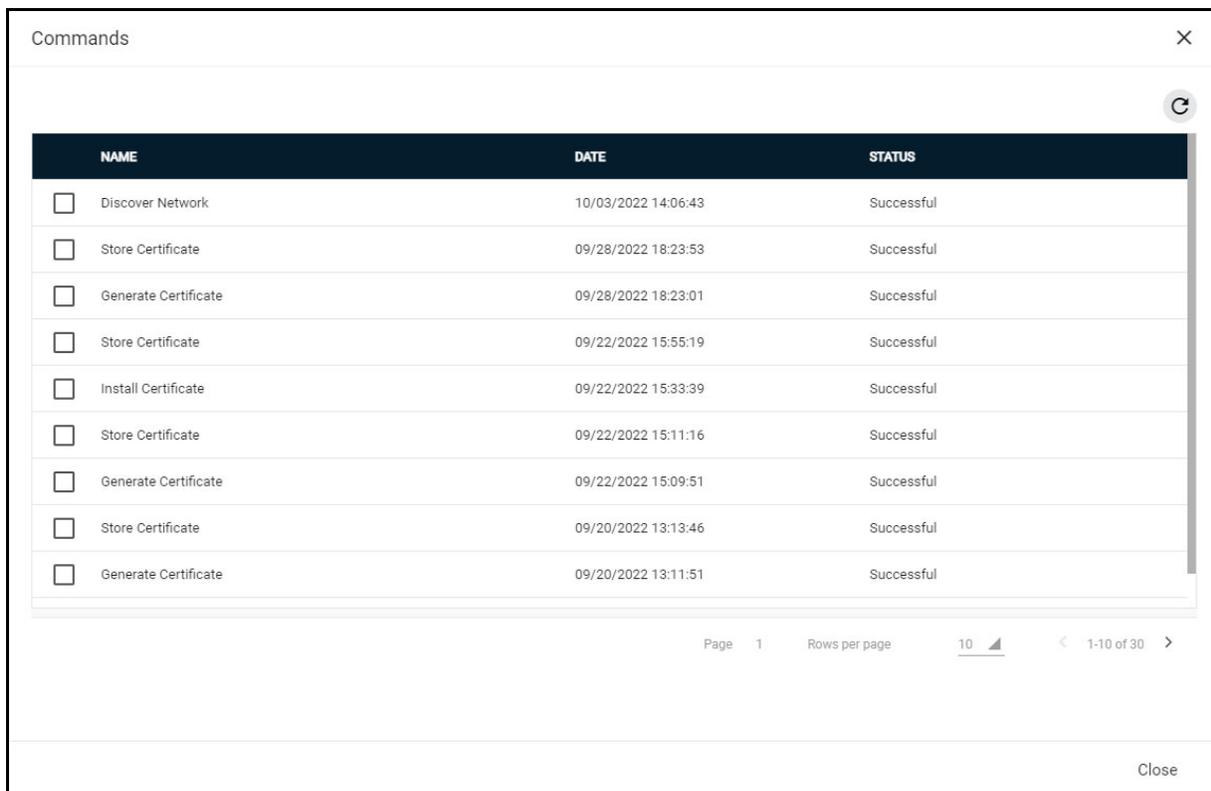
	NAME	DATE	STATUS
☐	Discover Network	10/03/2022 14:06:43	Successful
☐	Store Certificate	09/28/2022 18:23:53	Successful
☐	Generate Certificate	09/28/2022 18:23:01	Successful
☐	Store Certificate	09/22/2022 15:55:19	Successful
☐	Install Certificate	09/22/2022 15:33:39	Successful
☐	Store Certificate	09/22/2022 15:11:16	Successful
☐	Generate Certificate	09/22/2022 15:09:51	Successful
☐	Store Certificate	09/20/2022 13:13:46	Successful
☐	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**.
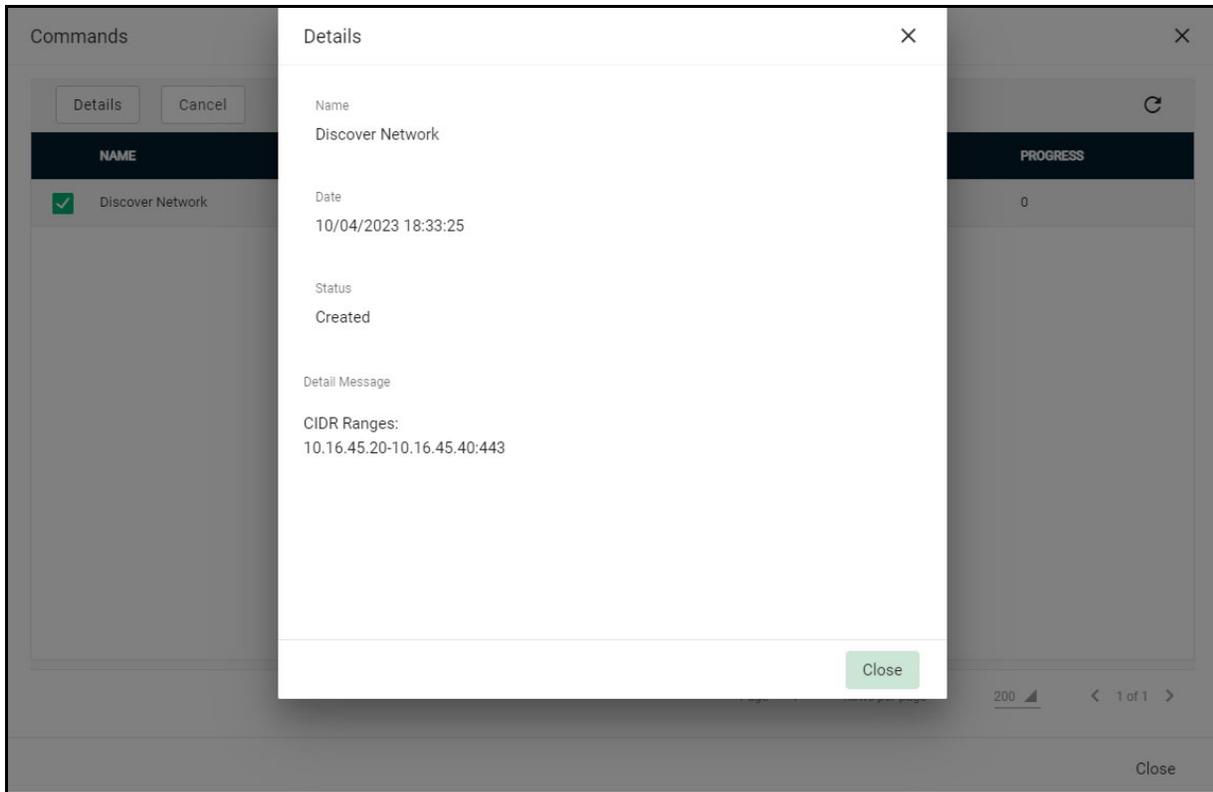
3.2.3.2.4 Generation of CSR in Azure Key Vault

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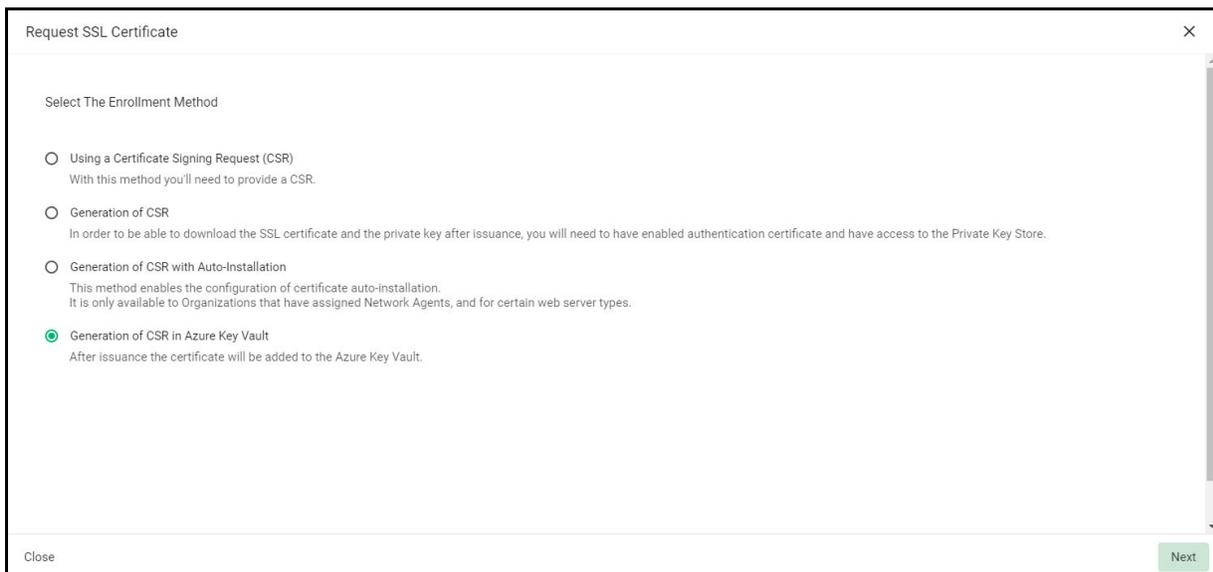
2. Select **Generation of CSR in Azure Key Vault** and click **Next** to open the Details page shown in the following illustration.

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**.
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.
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 *.ccmqa.com, the certificate name in Azure Key Vault is -ccmqa-com.
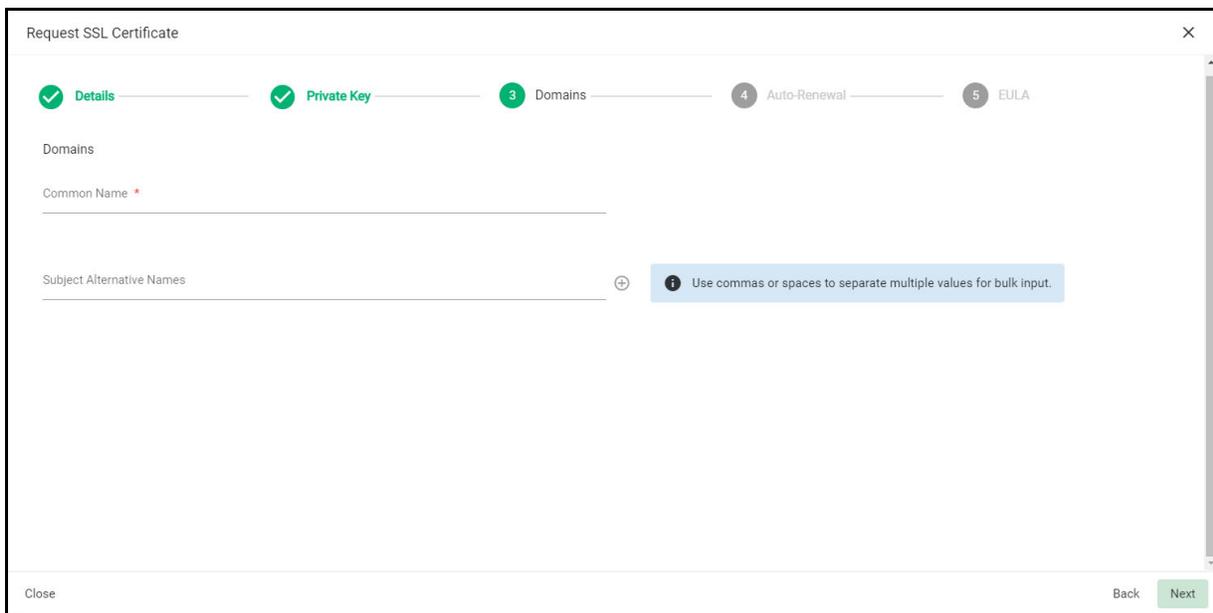
9. Click **Next** to open the **Auto-renewal** page shown in the following illustration.

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.

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.

```
Subject: Enrollment Successful - Your SSL certificate is ready

Hello,
You have successfully enrolled for a SSL certificate.
You now need to complete the following steps:
  * Click the following link to download your SSL certificate
Format(s) most suitable for your server software:
    as Certificate (w/ chain), PEM encoded: https://cert-manager.com/customer/110/ssl?action=download&sslid=84106&format=x509

Other available formats:
    as Certificate only, PEM encoded: https://cert-manager.com/customer/110/ssl?action=download&sslid=84106&format=x509CO
    as PKCS#7, PEM encoded: https://cert-manager.com/customer/110/ssl?action=download&sslid=84106&format=base64
    as PKCS#7: https://cert-manager.com/customer/110/ssl?action=download&sslid=84106&forma=bin

Issuing CA certificates only:
    as Root/Intermediate(s) only, PEM encoded: https://cert-manager.com/customer/110/ssl?action=download&sslid=84106&format=x509IO
    as Intermediate(s)/Root only, PEM encoded: https://cert-manager.com/customer/110/ssl?action=download&sslid=84106&format=x509IOR

  * Import your new certificate into your server (Please contact your administrator for help with this).
  * Your renew id: uuMjRAIGHlxLS36EYcnK

Certificate details
    Common name : sectigo.com
    Subject Alternative Names :
    Number of licenses :
    SSL Type : Instant SSL
    Term : 1 year(s)
    Server : AOL
    Requested : 01/23/2020 16:42 GMT
    Approved : 01/23/2020 16:44 GMT
    Expires : 01/22/2021 23:59 GMT
    Order Number : 2283044
    Self-Enrollment Certificate ID : 84106
    Comments :
```

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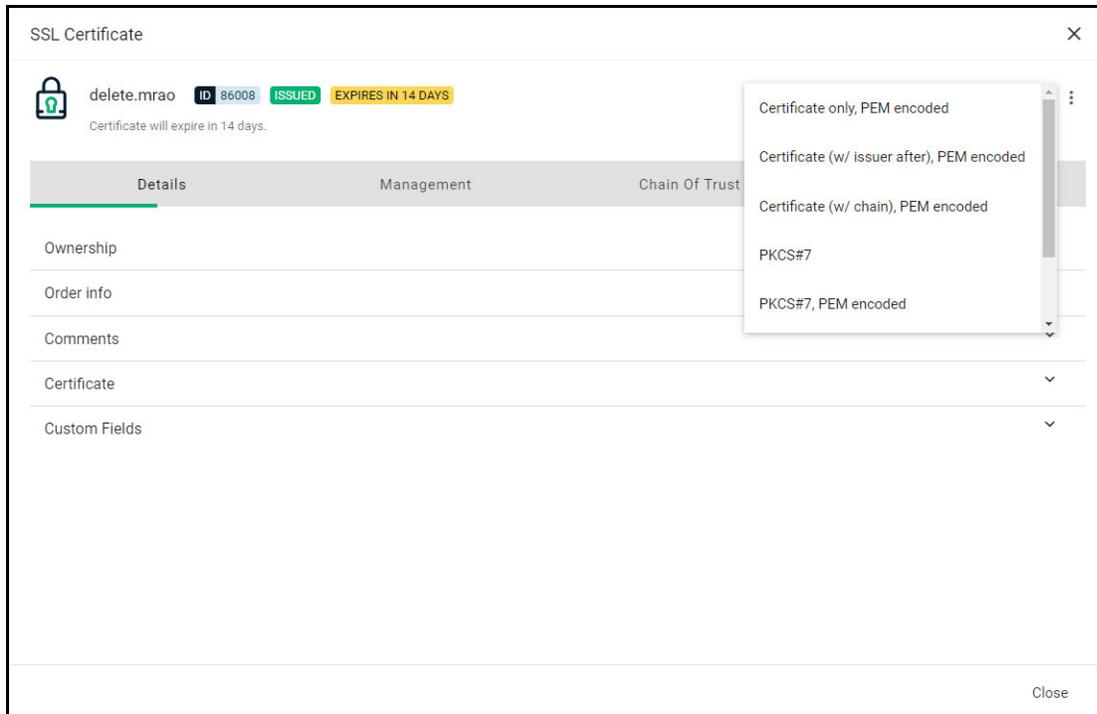
The installation process depends on the web server type. For more information and instructions, select the appropriate installation guide available at the Sectigo support site at sectigo.com/support.

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.

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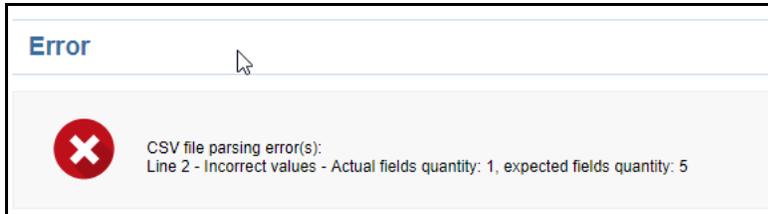
The following table lists errors that may arise during parsing of an SSL Certificate CSV file.

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.

Error ID	Error message	Reason
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 .

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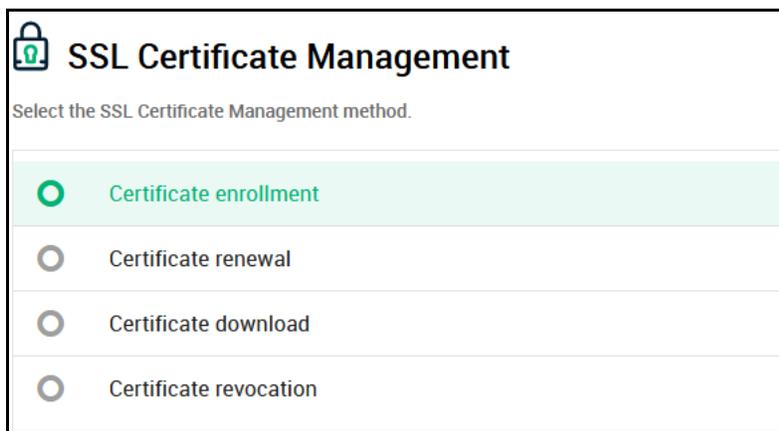
Clicking **Certificate renewal** opens the **SSL Certificate Renewal** form shown in the following illustration.

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**
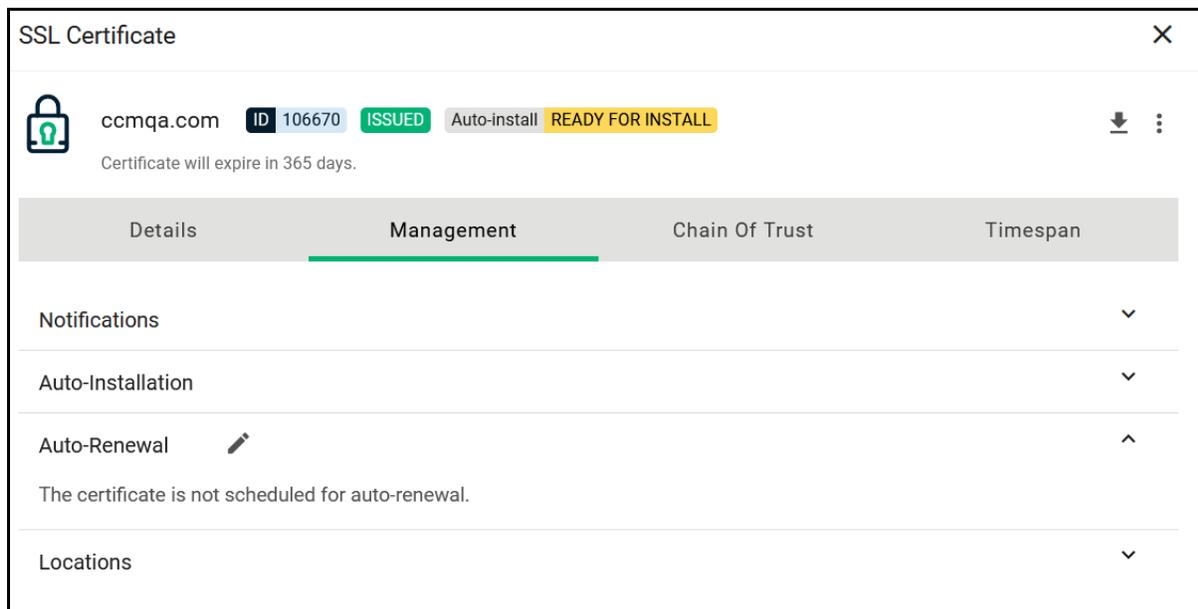
This displays the **Auto-renewal settings for SSL Certificate** dialog.
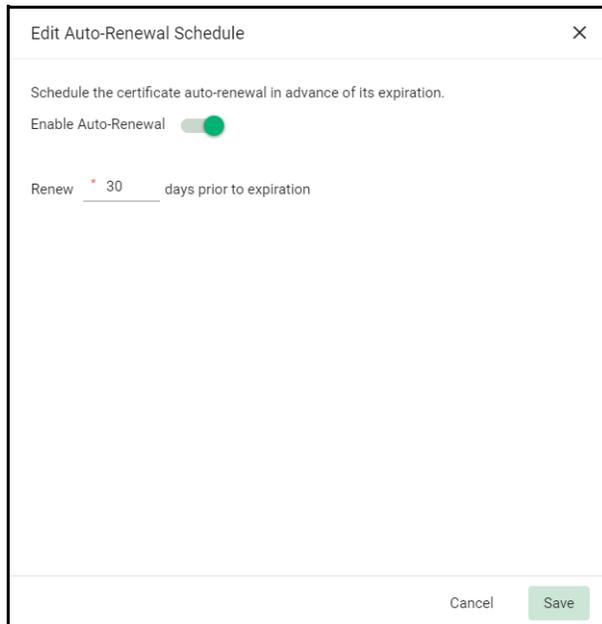
4. Select **Enable Auto-Renewal to** have SCM apply for a new certificate when the current one approaches expiry.

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.
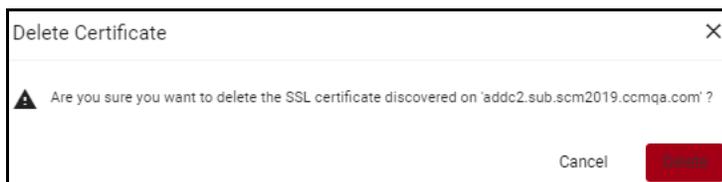
NOTE: You can only delete external certificates.

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.
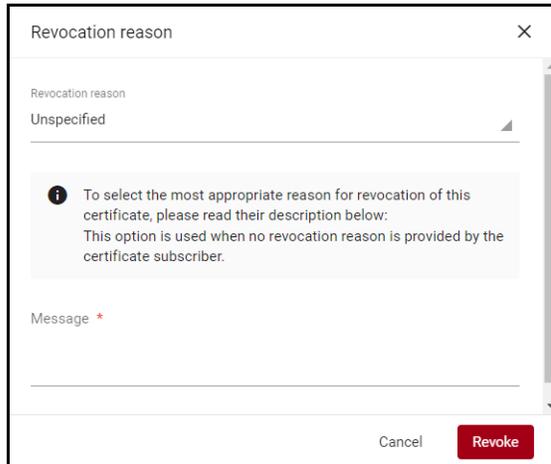
3. Click **Revoke**.

> 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 126.

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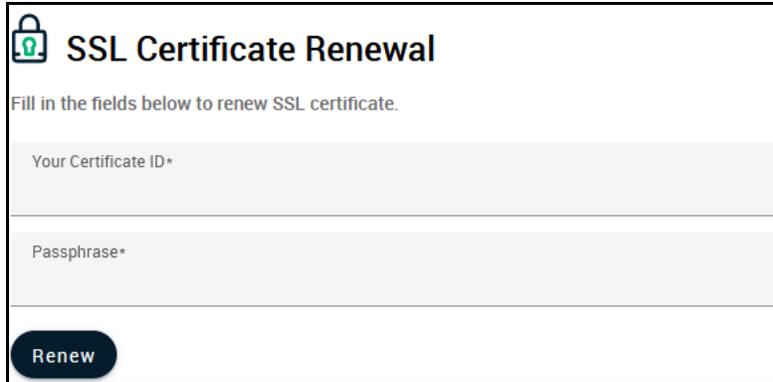
Clicking **Certificate revocation** opens the **SSL Certificate Revocation** form shown in the following illustration.

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.

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, see Understanding persons.

3.3.1 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.
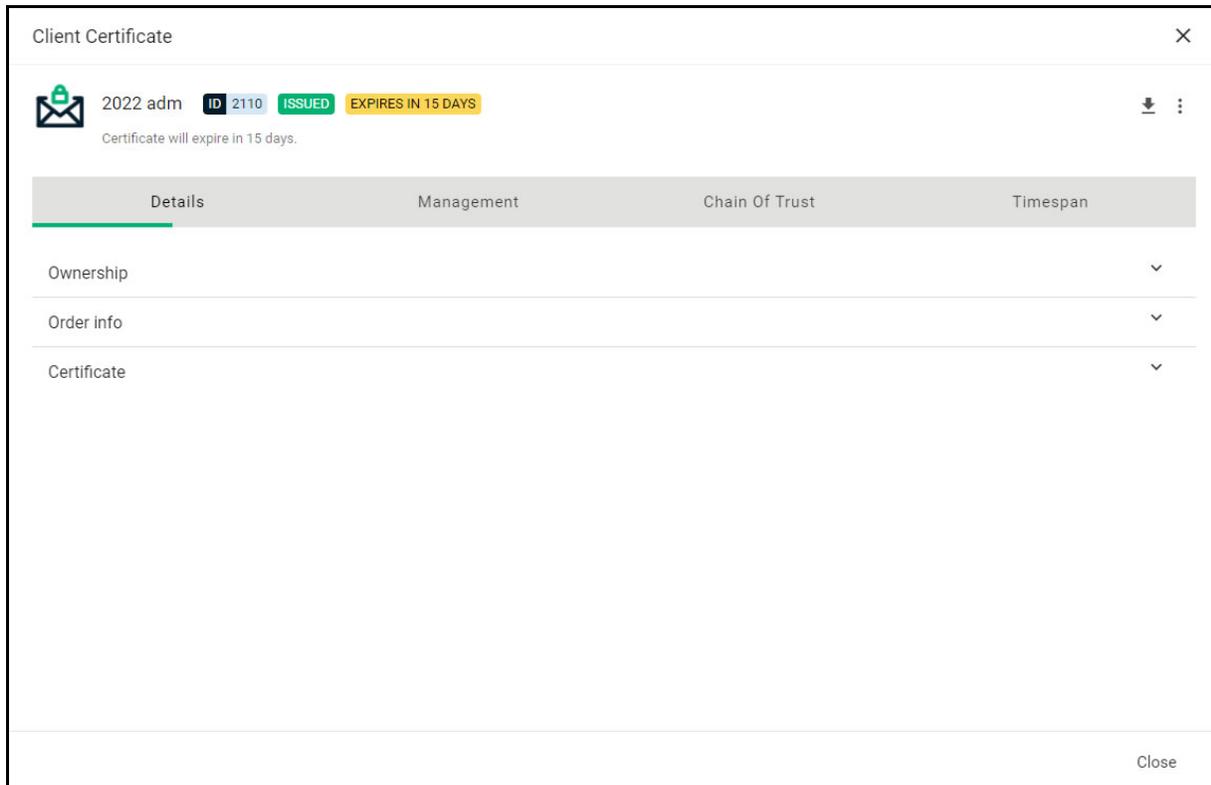
The following table lists fields available in the **Client Certificate** summary.

Field	Description
Status	The current status of the certificate, as follows: • 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	**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
	• Sectigo Key Vault
	  - Client certificates only
	  - Created by SCM if storing private key
	  - Also contains Private Key indicator
	• Legacy Key Vault
	  - Client certificates only
	  - Created by SCM if storing private key
	  - Fields: Escrow Level (CUSTOMER/RAO/DRAO)
	  - 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

3.3.2 How to manage end-users

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 persons
- Adding persons
- Managing persons

3.3.3 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 85 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 90 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 93 for more information.

3.3.3.1 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).

- 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.

4. 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.
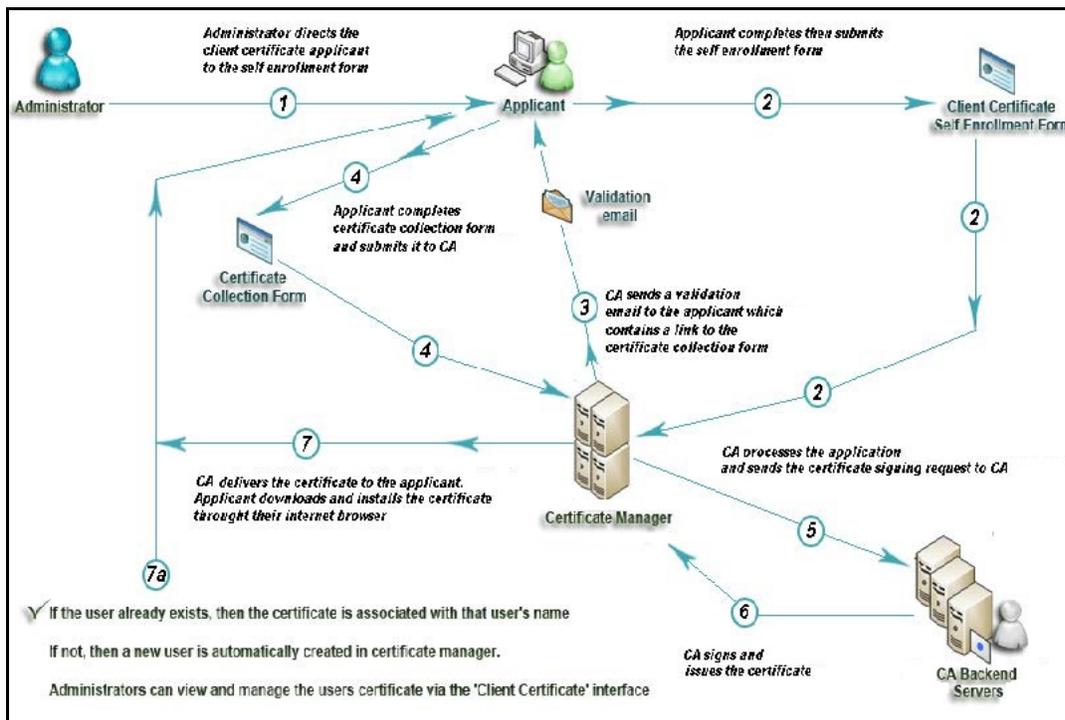
Provide enrollment details to applicants using an out-of-band communication such as email. The communication must contain the following information:

- 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.

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

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 126.

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

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.

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.

3.3.3.2 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). 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.

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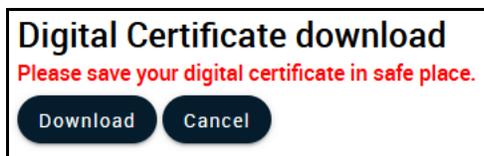
This form enables the end-user to download and save the certificate on their computer.

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.

3.3.3.3 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, see To send an enrollment invitation containing a link to the registration form to the end-user, see Managing persons.

3.3.4 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 Understanding legacy key encryption.

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 Understanding legacy key encryption.

3.3.5 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, see Managing persons.

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.

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: • 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.
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.

Field	Description
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.
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
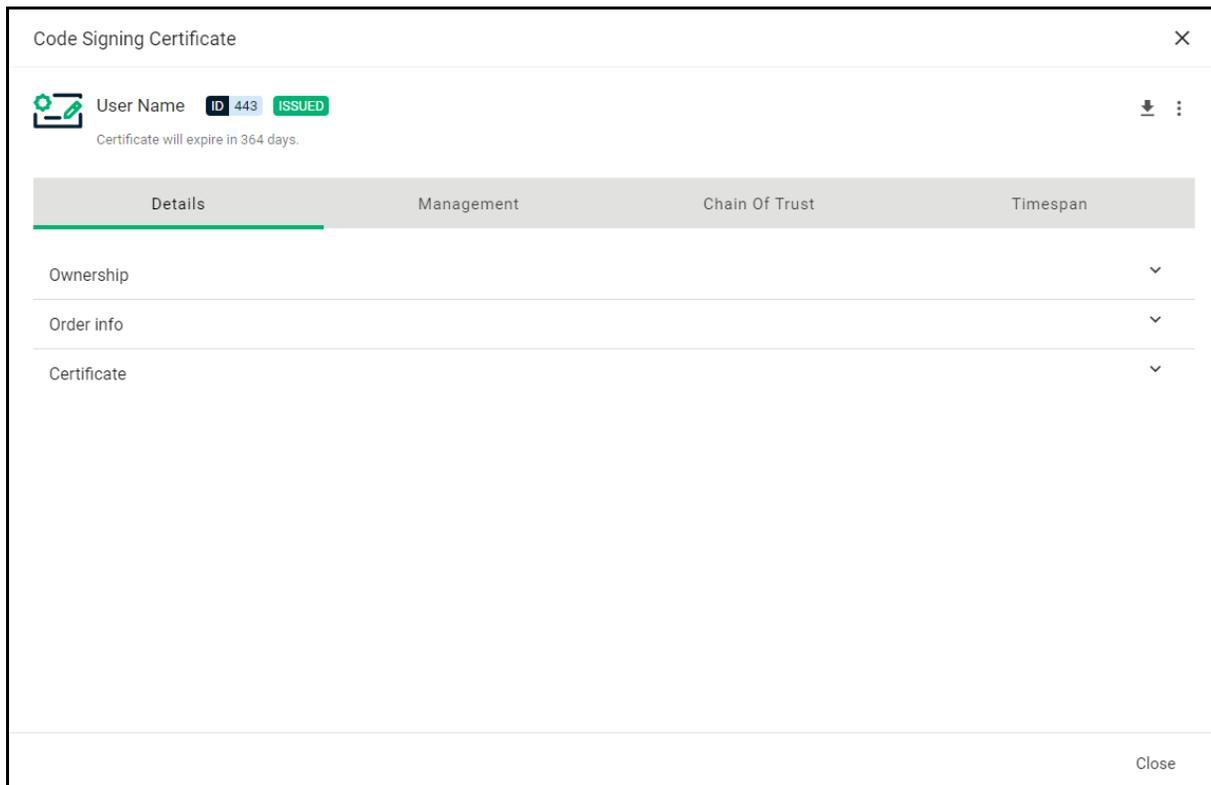
3.4.2 How to request and issue code signing certificates

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.

4. 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:

1. Navigate to **Certificates** > **Code Signing Certificates**.

2. In the upper-right corner, click **Invitations** and then click the **Add** icon to open the **Send Invitation** dialog.
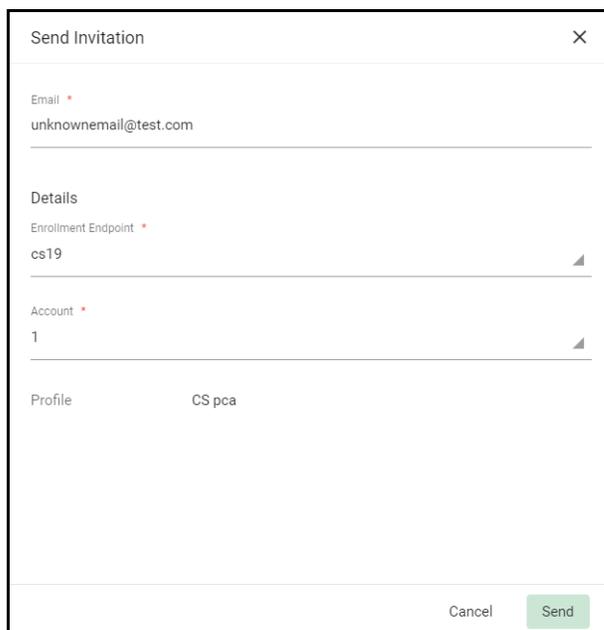
3. Complete the fields based on the information provided in the following table and click **Send**.

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.

3.4.3 Completing the code signing certificate request

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

2. 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.
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

Field	Required	Minimum Characters	Maximum Characters	Format	Supported Characters
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.

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

Column	Description
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.
General	
ID	ID number of the certificate
Status	The current status of the certificate, which can be one of the following: • 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
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

Column	Description
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.
Approver	The name of the person who approved the certificate.
Subject	The Subject Distinguished Name (Subject DN) who was issued the 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 expiration date of the certificate.
Serial Number	A unique number which identifies 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.
Key Algorithm	The type of algorithm used for encryption.
Key Size/Curve	The key size or curve used for encryption.
Signature Algorithm	The signature algorithm of the public key 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.
Comments	Comments that don't fit under any other heading.
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.

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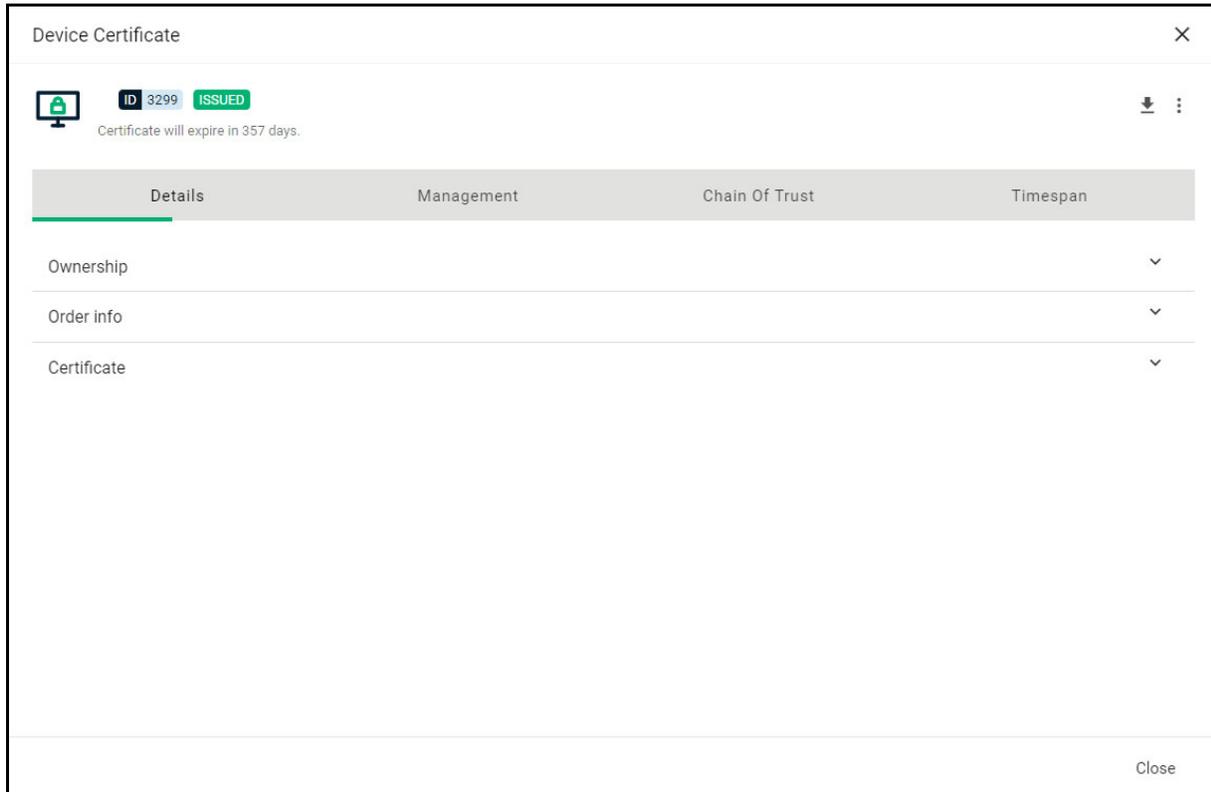
The following table lists the fields and their values available in the **Device Certificate** dialog.

Field	Description
Email	The email of the end-user.
Status	The status of the certificate, as follows: • 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.

Field	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.
Requested	The date the certificate request was sent to Sectigo from SCM or date of certificate request from MS CA by the administrator.
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: • 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 107.
- **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 107 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 107 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 119 and "How to manage certificate profiles".

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 Understanding certificate profiles.
- 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.

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".

- You added a device certificate enrollment endpoint (see "How to map MS AD certificate templates to SCM").
- 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**.

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 112).

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.

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.

Field[a]	Description
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.
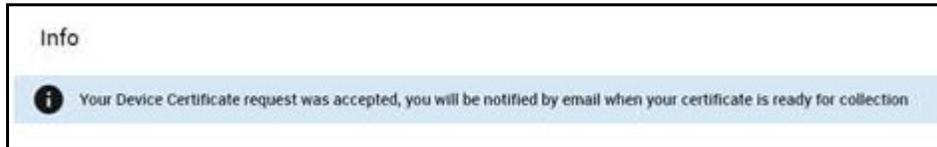
3.5.2.3 Issuing device certificates manually

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".
- 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.

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 112.

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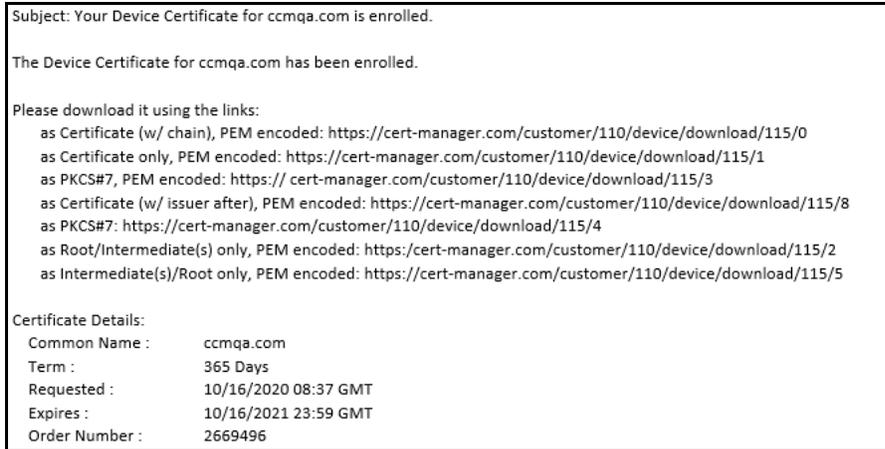3. Click **Approve** or **Decline**.
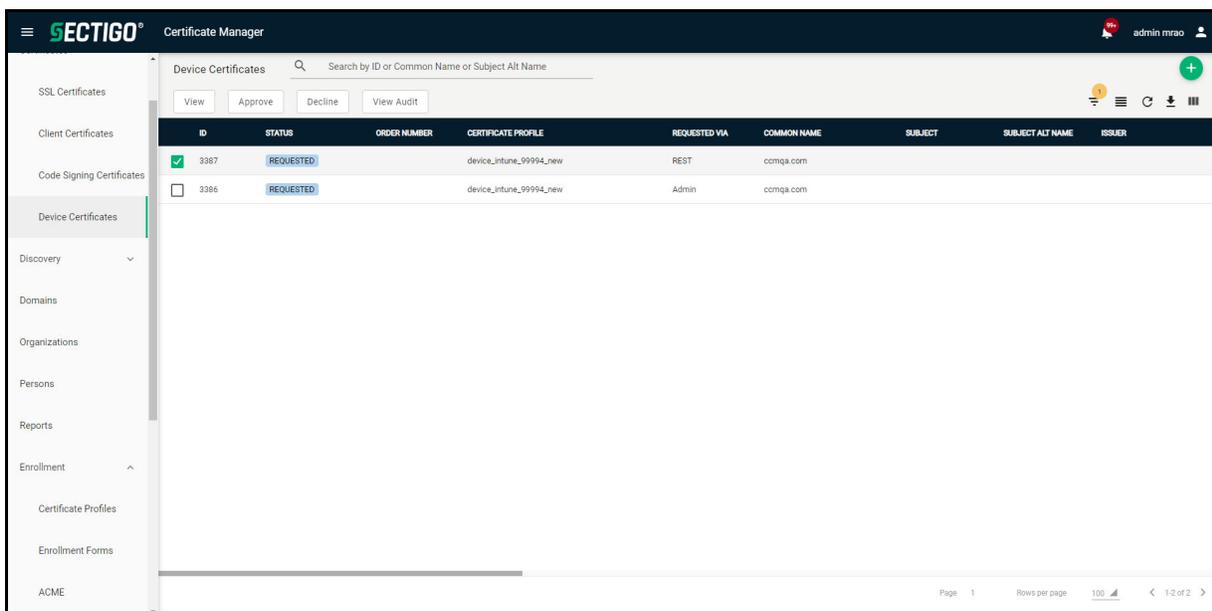
The status of the approved certificate is displayed as **Applied**. Once the certificate is issued, a collection form is sent via email, enabling the user to download and save the certificate.

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.

```
Subject: Your Device Certificate for ccmqa.com is enrolled.

The Device Certificate for ccmqa.com has been enrolled.

Please download it using the links:
    as Certificate (w/ chain), PEM encoded: https://cert-manager.com/customer/110/device/download/115/0
    as Certificate only, PEM encoded: https://cert-manager.com/customer/110/device/download/115/1
    as PKCS#7, PEM encoded: https:// cert-manager.com/customer/110/device/download/115/3
    as Certificate (w/ issuer after), PEM encoded: https://cert-manager.com/customer/110/device/download/115/8
    as PKCS#7: https://cert-manager.com/customer/110/device/download/115/4
    as Root/Intermediate(s) only, PEM encoded: https:/cert-manager.com/customer/110/device/download/115/2
    as Intermediate(s)/Root only, PEM encoded: https://cert-manager.com/customer/110/device/download/115/5

Certificate Details:
    Common Name :        ccmqa.com
    Term :               365 Days
    Requested :          10/16/2020 08:37 GMT
    Expires :            10/16/2021 23:59 GMT
    Order Number :       2669496
```

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 105.

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.

```
Resend Collection Link                           ×

Email  *
test@testdomain.com




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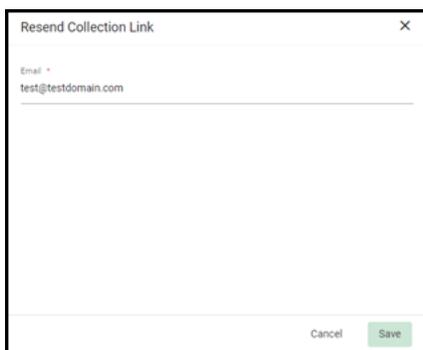
The recipient email address defaults to the address entered during certificate enrollment.

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.
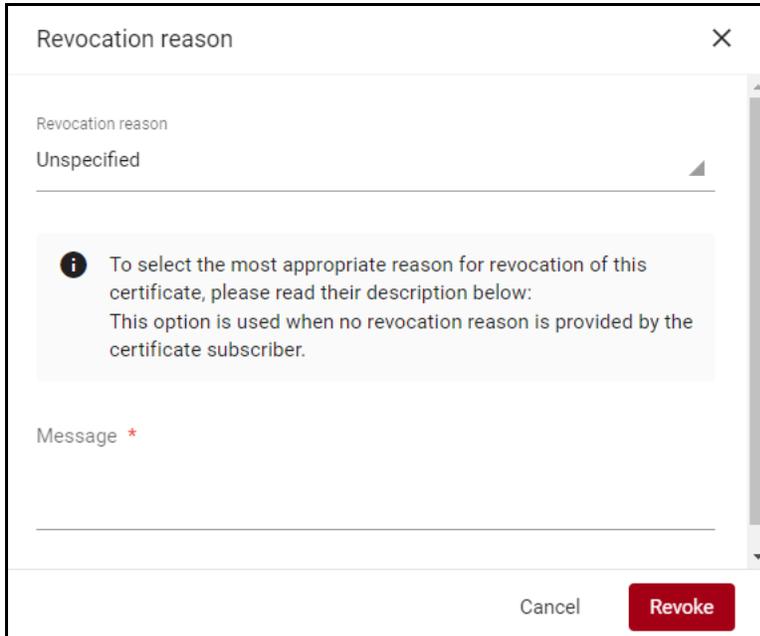
3. Select a reason for revocation from the list, add the message and click **Revoke**.

Upon completion, the certificate is displayed with a status of Revoked.

4

Performing certificate discovery tasks

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 discovery tasks can now be found in the following locations:

- Network discovery tasks
- MS AD discovery tasks
- Assignment rules
- Certificate buckets

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

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:

- Reports

7

Managing enrollments

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the enrollment endpoints can now be found in the following locations:

- Enrollment forms
- Bulk SSL enrollment
- ACME
- SCEP
- EST
- REST
- Certificate profiles

8

Managing issuers

Issuers page contains the following sub-pages:

- CA Backends
- Private CAs

8.1 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

8.2 How to manage private CAs

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the CAs can now be found in the following location:

- Understanding CAs

9

Using SCM with Microsoft Azure and Intune

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 integrations with Microsoft Azure and configuration of Microsoft Intune for enrollment and management of client and device certificates can now be found in the following locations:

- Configuring Azure Key Vault
- Configuring Intune SCEP
- Configuring Intune Exporter
- Understanding Azure accounts
- Understanding Intune Exporter

10

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:

11.1 The settings configuration overview

The **Settings** menu contains multiple areas that vary based on the features enabled for your account and your administrative privileges.
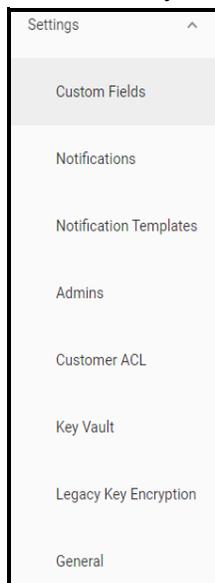
The **Custom Fields** page enables MRAOs to configure custom fields for use in certificate enrollment forms. SSL, client, and device certificates have a set of standard fields that contain information about the owner, domain, organization, department, address, etc. You can use custom fields to track additional information, such as an employee code or telephone number.

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.

The **Notification Templates** page enables MRAOs to customize the contents of templates for event-based notifications.

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.

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 116.

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.

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.

The **General** page enables MRAOs to configure the date format for displaying dates in SCM.

11.2 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.

11.2.1 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

11.3 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

11.4 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

11.5 Configuring Key Escrow and encryption

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the legacy key encryption can now be found in the following location:

- Understanding legacy key encryption

11.6 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

11.7 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.

11.8 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 121.

11.9 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.

11.10 Using Sectigo Key Vault

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about Sectigo Key Vault can now be found in the following location:

- Understanding Sectigo Key Vault

11.11 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 120.

11.12 Managing General settings

The **General** page enables MRAO administrators to change the way in which dates will be displayed globally in SCM.

General	
⚙ Settings	
Date Format	mm/dd/yyyy
Days before expiry validated domain is Action Required	30
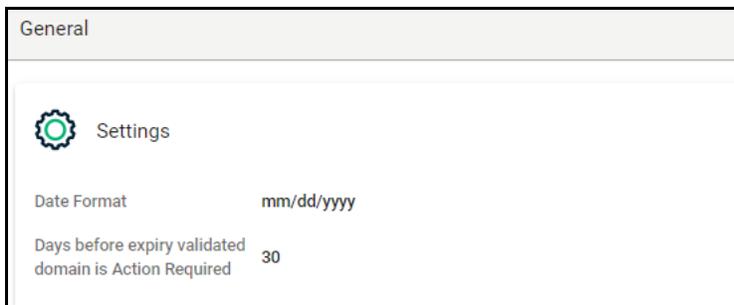
> NOTE: Only affects the way dates are presented in SCM, for all users. This setting does not change the way time is handled on certificates.

12

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
- End-user CSV file format and importing guidelines

A 1: Network discovery task CSV file format

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the network discovery task CSV file format can now be found in the following location:

- Adding network discovery tasks

A.2 SSL certificate CSV file format and importing guidelines

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the SSL certificate CSV file format and importing guidelines can now be found in the following location:

- Bulk enrollment for SSL certificates: CSV format guidelines

A.3 End-user CSV file format and importing guidelines

As part of our ongoing efforts to improve our documentation, the content previously covered in this chapter has been moved online.

Information about the end-user CSV file format and importing guidelines can now be found in the following location:

- End-user CSV file format and importing guidelines

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:

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.