



Trial Quick Start Guide  
for  
**Sectigo® Certificate Manager**  
21.4

April 19, 2021

Sectigo Certificate Manager

Trial Quick Start Guide, SCMTG

Copyright © 2008, 2021, Sectigo.

All rights reserved.

Primary Author: Sectigo

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

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

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

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

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

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

## Preface

This document explains how to set up Sectigo Certificate Manager (SCM) and use it to take full advantage of your SCM trial period. For more detailed information on setting up and using SCM, see *Sectigo Certificate Manager Administrator's Guide*.

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

## Audience

This document is intended for administrators working with a trial version of SCM.

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

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

## Related Documentation

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

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, or text that appears on the screen.
<text>	Chevron brackets indicate the required insertion of user or company specific text.

# 1 Introduction

This document describes the tasks you can perform when you first start using SCM during a trial period, and includes the following topics:

- **Getting Started**
  - Logging into SCM
  - Using the Welcome Dialog
  - Understanding the Main SCM UI
  - Reviewing Your Details
- **Bringing Your Certificates Under SCM Management**
  - Discovering Your Certificates
  - Importing Certificates
  - Reviewing Your Certificates
  - Setting Up Notifications
  - Managing Domains
  - Generating Reports
- **Using a Private CA**
  - Setting Up a Trial Private CA
  - Adding Certificate Profiles
  - Requesting and Issuing SSL Certificates
  - Requesting and Issuing Client Certificates

## 1.1 About SCM

SCM enables administrators to manage the lifespan, issuance, deployment, renewal, and revocation of certificates on an organization, department, and individual basis. By consolidating and automating the often disparate processes involved in complex enterprise-wide PKI deployments, SCM reduces the need for manual certificate management and creates a more efficient, productive, and secure certification environment.

SCM can be used to request and manage the following types of digital certificates:

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

NOTE: Code signing certificates are not available in the trial version of SCM.

## 1.2 About Your SCM Trial

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

The following is a non-exhaustive list of functionality available in the trial version:

- Unlimited logins
- Viewing data in the dashboard
- Managing an unlimited number of SSL, client and device certificates
- Viewing certificates, whether purchased from Sectigo or discovered on your servers
- Viewing and editing certificate details
- Creating organizations and departments
- Adding and delegating domains
- Adding and delegating administrators
- Assigning SSL certificates to an organization
- Adding Private CAs
- Creating network discovery tasks
- Running a weekly certificate discovery scan of public IP addresses
- Generating reports
- Configuring settings

You cannot order publicly trusted certificates or validate domains using the trial version. Certificates issued using the trial private CA have a lifetime of 30 days. During the trial period, you can still purchase certificates through Sectigo websites or by contacting [Sectigo Sales](#). These certificates would be subject to their usual fees.

NOTE: To enable scanning of private IP addresses, place a request with [Sectigo Sales](#).

## 2 Getting Started

The following sections describe how to log in and review your details.

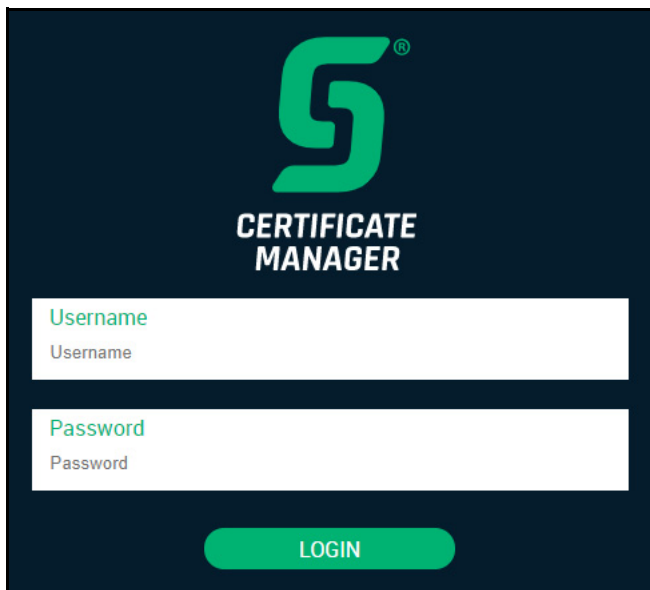
### 2.1 Logging into SCM

Navigate to the URL provided in your welcome email, and log in with the account user name and password that you created when signing up for the trial SCM account.

The default format of this URL is `https://cert-manager.com/customer/<customer URI>/`.

If you are not able to log in, click **SCM Support** to create a support ticket.

NOTE: You can change your password at any time from the **My Profile** dialog. You can access My Profile by clicking your user name in the top-right corner.

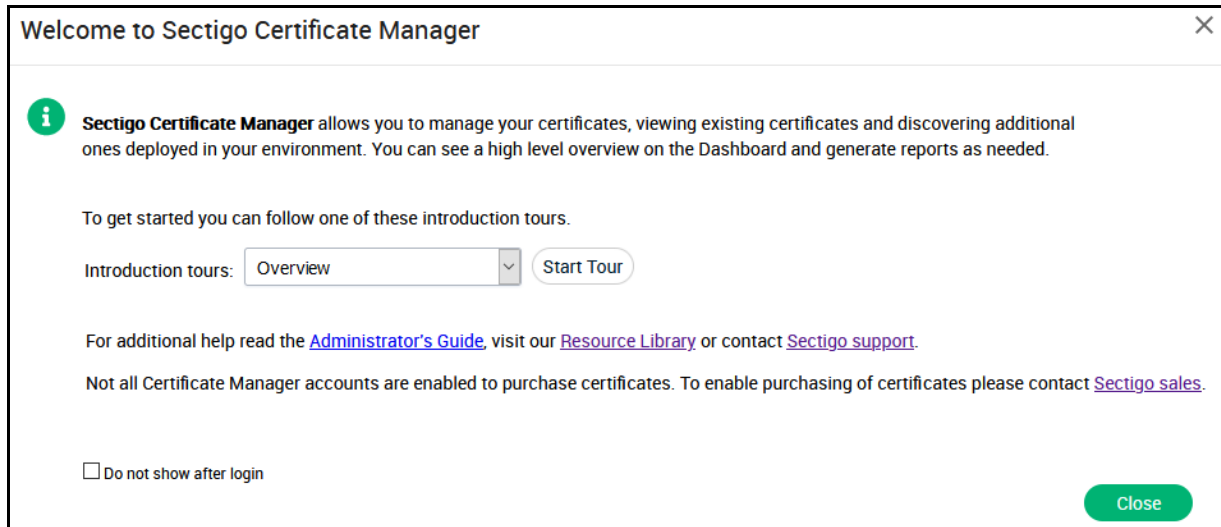


### 2.2 Using the Welcome Dialog

When you first access SCM, you are presented with the **Welcome** dialog shown in the following illustration. This dialog contains links to the following:

- Introduction tour
- *Sectigo Certificate Manager Administrator's Guide*
- Resource library
- Sectigo support
- Sectigo sales

You can launch the **Welcome** dialog at any time by clicking  in the upper-right corner.



## 2.3 Understanding the Main SCM UI

The SCM UI has a tab structure which provides access to most of the settings.



The main functional areas of SCM are presented as a series of tabs:

- **Dashboard**—Displays charts that help you monitor the status of your certificates.
- **Certificates**—Manage and issue certificates.
- **Discovery**—Run scans to discover the certificates on your servers and network.
- **Reports**—Create reports on the status of your certificates and certificate activity.
- **Admins**—Manage the administrators of the organizations and departments.
- **Settings**—Manage a variety of settings, including your organizational structure and domains.
- **About**—Displays information about the features enabled on your account.

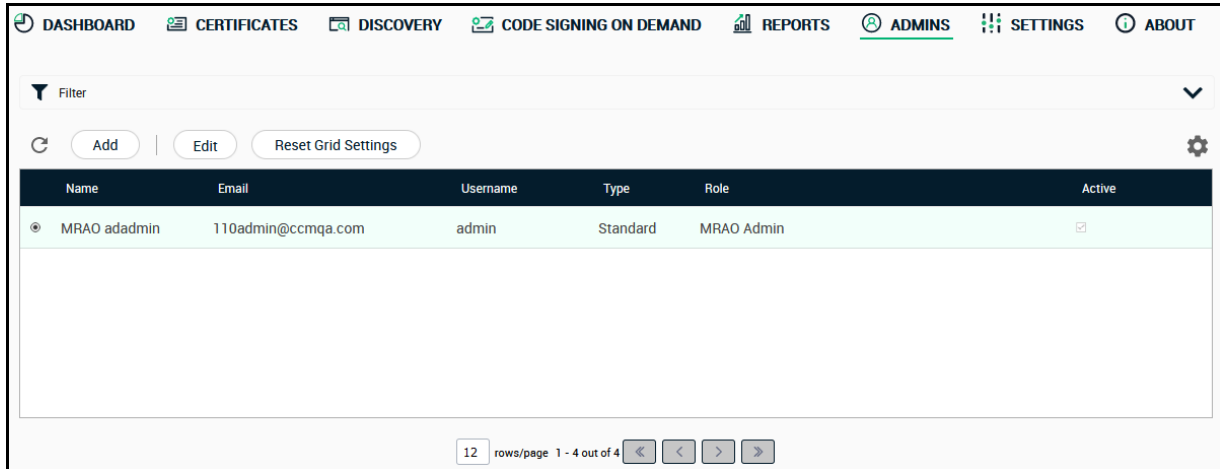
## 2.4 Reviewing Your Details

Your trial comes with the following items configured:

- One MRAO administrator. This is the account you used to log in. An MRAO administrator has full privileges to request certificates, create organizations and departments, create and delegate domains, add users and other administrators, modify SCM settings, and more.
- One organization. The details for this organization are based on the details you provided in the form you submitted when you applied for the trial.

### 2.4.1 How To Review Your Administrator Details

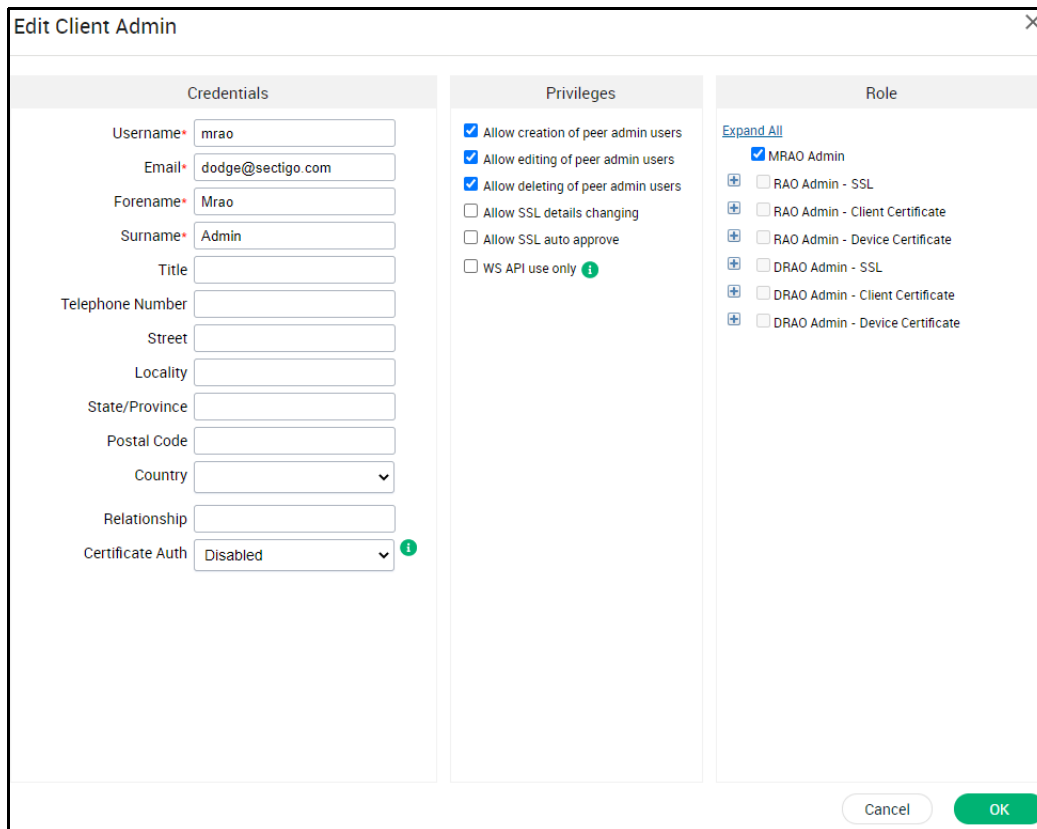
The **Admins** tab enables you to manage administrative personnel. As organizations or departments are added, you can, for example, add administrators with specific roles and permissions to manage them.



To review the administrator details, do the following:

1. Navigate to **Admins**, select the administrator in the list, and click **Edit**.

This displays the **Edit Client Admin** dialog shown in the following illustration.





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

### 2.4.2 How To Review Organization Details and Add a Domain

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

To review the organization details, do the following:

1. Navigate to **Settings > Organizations**, select the organization in the list, and click **Edit**. This displays the **Edit Organization** dialog shown in the following illustration.

The screenshot shows a dialog box titled "Edit Organization: Sectigo Documentation". It has five tabs: "GENERAL", "SSL CERTIFICATE", "CLIENT CERTIFICATE", "DEVICE CERTIFICATE", and "EMAIL TEMPLATE". The "GENERAL" tab is active. The form contains the following fields: "Organization Name" (Sectigo Documentation), "Address1" (501-300 March Rd), "Address2" (empty), "Address3" (empty), "City" (Kanata), "State/Province" (Ontario), "Postal Code" (K2K 2E2), and "Country" (Canada). Below these fields is "OrgID 19550" and an "Access Control List" section with an "Edit" button. At the bottom right are "Cancel" and "OK" buttons.

The **General** tab displays the organization details that you submitted to Sectigo. Certificates, when they are brought under SCM management, are assigned to an organization. Ideally, you want to match certificates to organizations in SCM according to the organization (O) in the subject field of the certificate.

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

Before certificates can be issued to an organization, the organization must be associated with at least one domain.

To delegate a domain to the organization, do the following:

1. Navigate to **Settings > Organizations**, select the organization in the list, and click **Domains**. This displays the **Domains** dialog.
2. Click **Add** to open the **Create Domain** dialog shown in the following illustration.

The screenshot shows a 'Create Domain' dialog box with the following fields and options:

- Domain\***: A text input field.
- Description**: A text input field.
- Active**: A checked checkbox.
- Certificate Type\***: A group of radio buttons with the following options:
  - SSL
  - Client Certificate
  - Code Signing

Buttons: 'Cancel' and 'OK'.

3. Enter the domain name. This should match the common name (CN) in the subject of any certificates that you want to manage under this organization.
4. Enter a description of the domain.
5. Set the domain to be active.
6. Specify the types of certificates that will be used for this domain. Using a Private CA, we will be adding SSL and client certificates, so ensure those are selected.
7. Click **OK**.

The domain is now listed in the **Domains** dialog for the organization. Click **Close** to close the dialog.

## 3 Bringing Your Certificates Under SCM Management

Once you have at least one organization with at least one delegated domain, you can begin bringing certificates under SCM management. This involves the following general steps:

1. Discover your existing certificates using a scan and/or manually import certificates.
2. Evaluate your certificates and manually assign them to organizations if necessary.
3. Set up notifications.
4. Manage the domains.

### 3.1 Discovering Your Certificates

A discovery scan identifies certificates on your network and imports them into SCM for management. Using the trial version, you can schedule a weekly discovery scan of your publicly available hosts.

**NOTE:** Using the full version of SCM, you can run discovery scans of your internal network, and renew or replace discovered certificates with Sectigo equivalents. You can also integrate Active Directory servers into your scans.

Discovered certificates (including those purchased from Sectigo) are given an **External** status, which means they were not ordered through SCM.

You are advised to create the organization or department structure you would like before creating and running a discovery scan. Using assignment rules, on completion of a discovery scan, all identified certificates that match the rules are automatically assigned to the organization or department configured in the rule. You then receive notifications relevant to the certificate for your organization or department (for example, certificate expiry reminders).

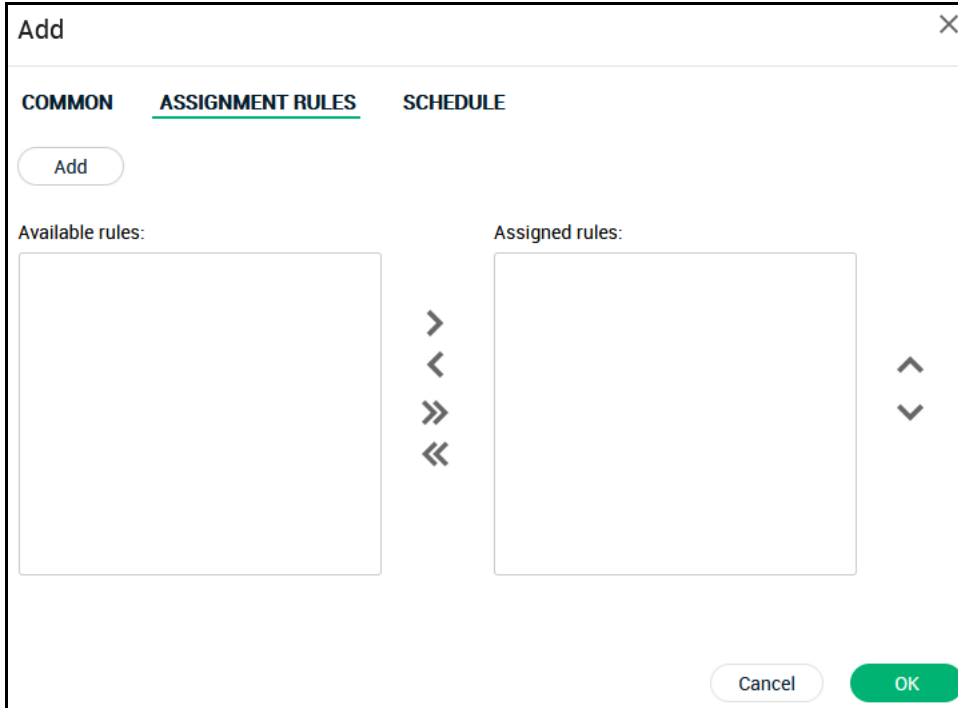
Run a scan at the earliest opportunity so that you can gain a firm inventory of your company's certificate assets.

#### 3.1.1 How To Create a Network Discovery Task

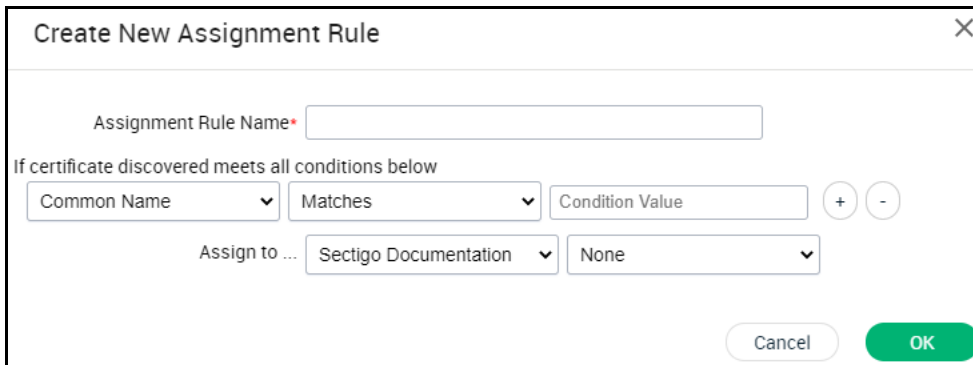
Scan settings are saved as discovery tasks. You create a new discovery task or modify an existing one as follows:

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

3. Enter a name to describe the task.
4. Set the **Agent** field to Auto (this is the default). The Auto agent is run by Sectigo and performs an external scan of publicly accessible servers.
5. Click **Add** to add the host names to be scanned.
6. In the **Add Scan Range** dialog, select Host name and enter a host name.  
 In the case of public scans, host names are preferable to IP addresses so as to be able to retrieve all the certificates in cases where a single IP is hosting multiple host names.
7. Click **OK**.
8. Repeat steps 5-7 for any other host names you want to scan.
9. Select **Assignment Rules**. Assignment Rules enable you to add rules that assign discovered certificates to a specific organization and department based on criteria you define.  
 In this instance, you will want to add a rule that matches certificates for your organization.



10. Click **Add** to add a rule.



11. Enter a name for the rule.
12. Set the conditions for the rule. For example, Organization, Matches, and the name of your organization (assuming it matches the O in the subject of one or more of your certificates).
13. Using the **Assign to** field, assign the matching certificates to your organization.
14. Click **OK**. The rule is added to **Available rules**.
15. Move the rule from the **Available rules** list to the **Assigned rules** list.
16. Click **Schedule**.

**Add**

**COMMON**    **ASSIGNMENT RULES**    **SCHEDULE**

Frequency: Weekly

Day of Week: Sunday

Time zone: UTC-04:00 - AST, ECT, EDT, BOT, CLT...

Time: 11 : 05

Next 5 scans:

09/27/2020	11:05:33	UTC-4
10/04/2020	11:05:33	UTC-4
10/11/2020	11:05:33	UTC-4
10/18/2020	11:05:33	UTC-4
10/25/2020	11:05:33	UTC-4

Cancel    **OK**

Scans can be run manually or automatically (Run Once, Daily, Weekly, Monthly, Quarterly, Semi-Annually and Annually). The trial version is limited to weekly scans.

17. Set the day of the week and time to run the weekly scan.
18. Click **OK**.

Newly created discovery tasks are listed in the **Network Discovery Tasks** tab.

### 3.1.2 How To Run a Discovery Scan

You can launch scans using the task you have created, as follows:

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

While the scan is running, you can click in the Status column to view the progress of the scan.

Navigation: DASHBOARD | CERTIFICATES | DISCOVERY | REPORTS | ADMINS | SETTINGS | ABOUT

Network Assets    Network Discovery Tasks

Filter

Buttons: Add | Import from CSV | Edit | Delete | Cancel | History

Name	Ranges to Scan	Status	Schedule	Last Scanned
Sectigo	sectigo.com	<a href="#">Scan in Progress 0%</a>	Weekly	

When the scan completes, Status is set to Successful.

All discovered certificates are listed under the **Network Assets** tab. See [“How To Use the Network Assets Tab”](#) on page 14.

Matched discovered certificates can also be viewed in the **Certificates > SSL Certificates** tab. The discovered certificates are listed along with details such as the organization or department to which they are assigned. See [“How To Use the SSL Certificates Tab”](#) on page 17.

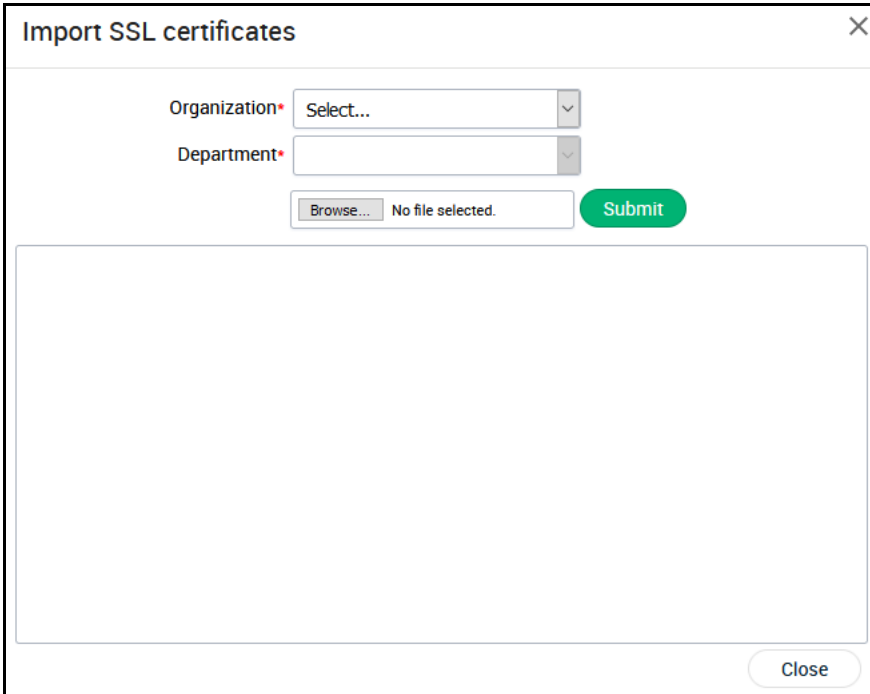
### 3.2 Importing Certificates

You can also bring certificates into SCM by simply importing them. You can manually 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. Click **Import** to open the **Import SSL Certificates** dialog shown in the following illustration.



The screenshot shows a dialog box titled "Import SSL certificates" with a close button (X) in the top right corner. The dialog contains two dropdown menus: "Organization" with "Select..." and "Department" with a blank selection. Below these is a file selection area with a "Browse..." button, the text "No file selected.", and a green "Submit" button. A "Close" button is located at the bottom right of the dialog.

3. Select the organization and department to which the certificates belong.
4. Click **Browse**, choose the archive containing the certificates to be imported and click **OK**.
5. Click **Submit**.

The progress of the import is displayed. When the import is finished, click **Close**.

Imported certificates can be viewed on the **Certificates > SSL Certificates** tab. See [“How To Use the SSL Certificates Tab”](#) on page 17.


### 3.3 Reviewing Your Certificates

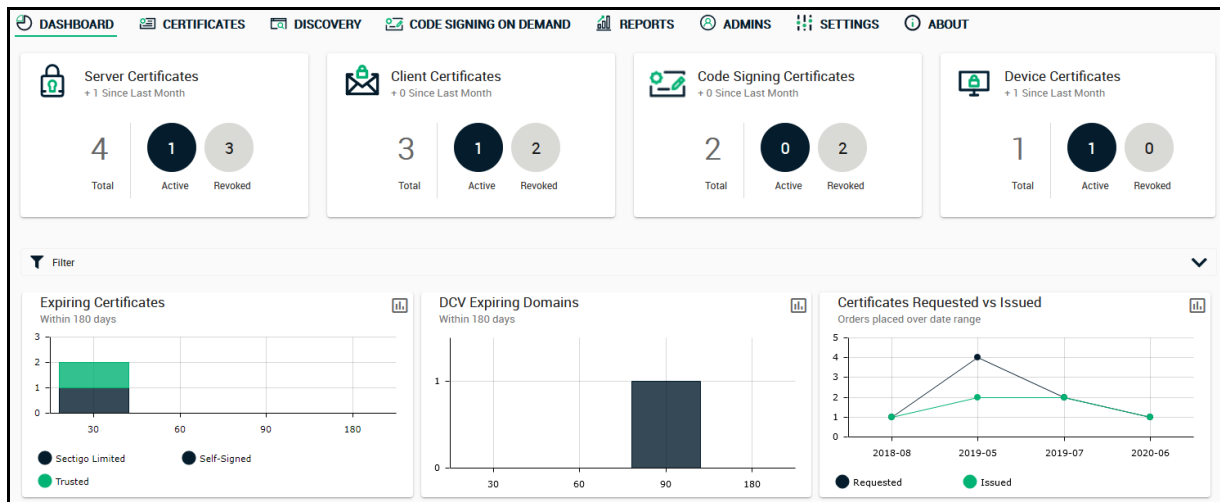
Discovered and imported certificates can be reviewed using the following areas:

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

#### 3.3.1 How To Use the Dashboard

The **Dashboard** tab, shown in the following illustration, contains charts that visualize data on the certificates on your network, such as certificates approaching expiry, issued and requested certificates, domain control validation (DCV) status, breakdown of certificates by types, issuers, and so on. The chart data is updated in real time.

Clicking the chart icon  in a chart displays a report with the breakdown of the chart statistics. In addition, hovering the cursor over a legend or chart sector displays additional information.

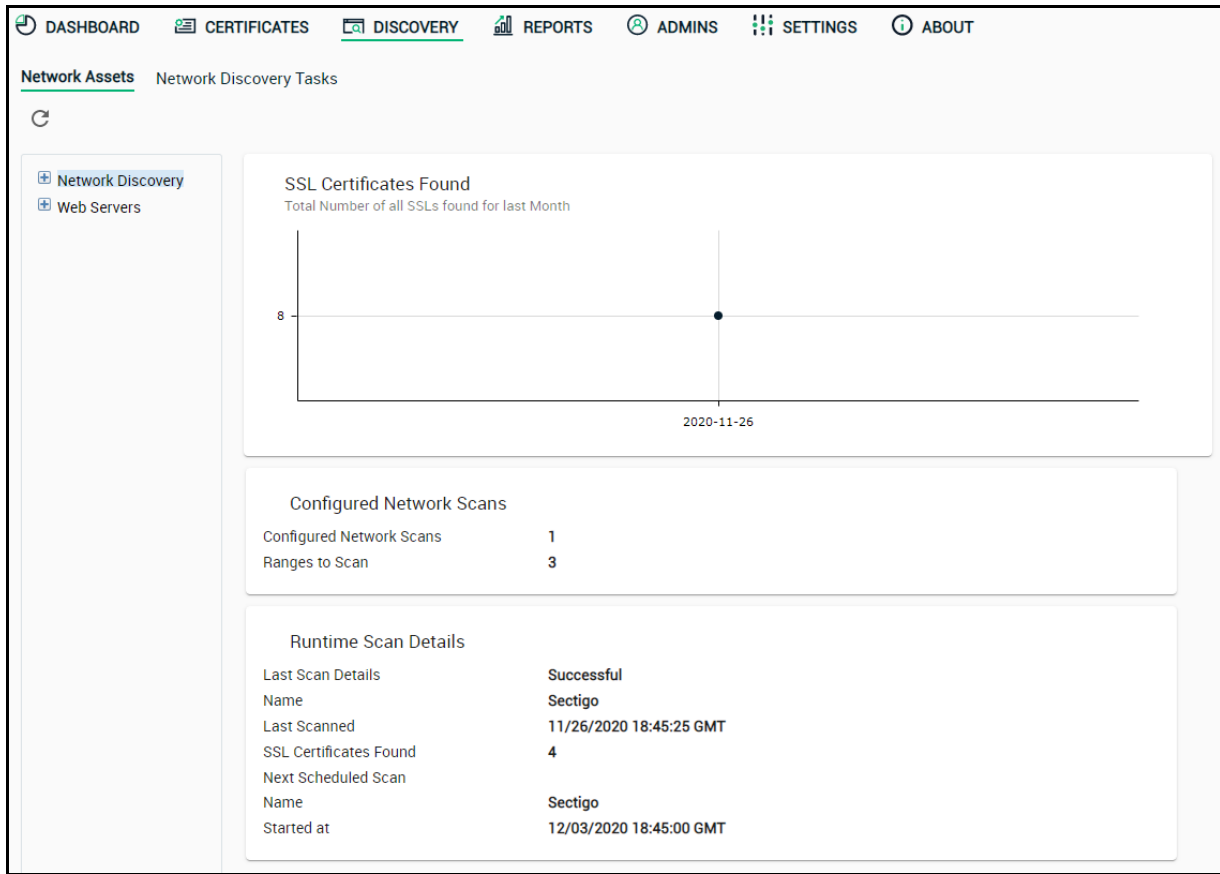


#### 3.3.2 How To Use the Network Assets Tab

After running a scan, all discovered certificates, regardless of whether they were assigned to an organization, are listed in the **Network Assets** tab.

To view a summary of SSL certificates installed on all scanned networks, navigate to **Discovery > Network Assets > Network Discovery**, as shown in the following illustration.

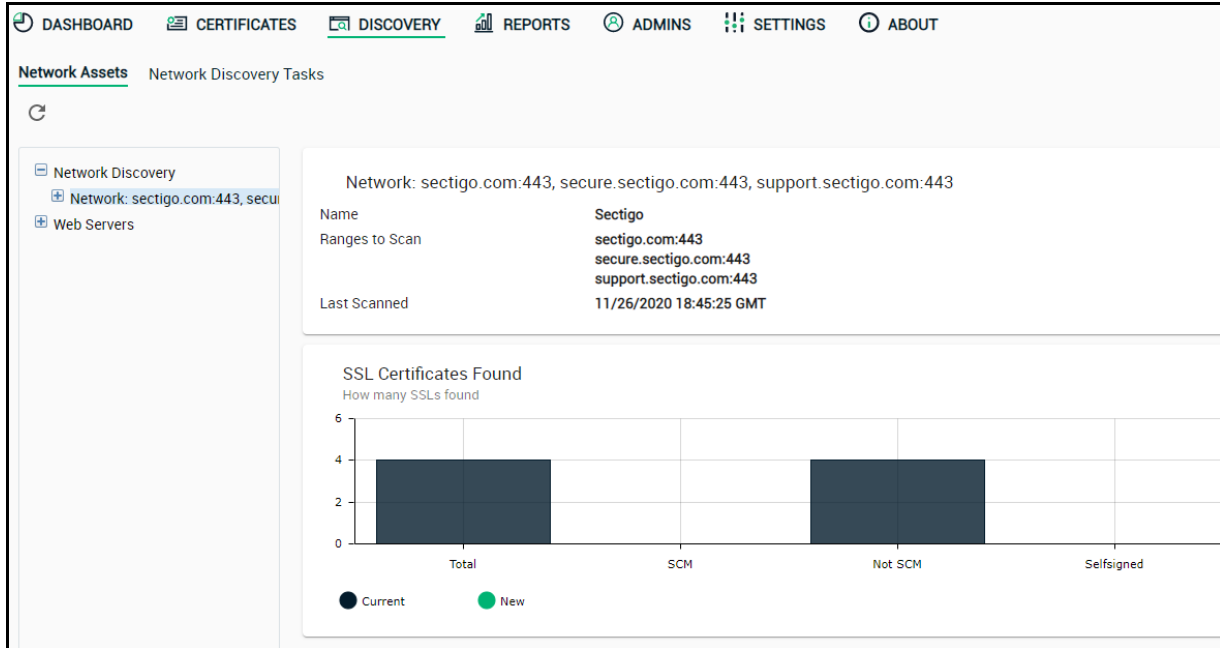




**Network Discovery** displays a time graph of the number of SSL certificates and details of discovery scans run on the networks. Hovering over a date or month shows the number of SSL certificates identified on that date or month.

### 3.3.2.1 Viewing a Summary of SSL Certificates on a Specific Network

To view a summary of SSL certificates installed on a specific network, expand the **Network Discovery** category and select the network, as shown in the following illustration.



The details of the network discovery scan task are displayed, including the name, network, and IP ranges scanned, as well as date and time of the last run scan. A comparison graph of total number of SSL certificates with numbers of certificates that are managed by SCM is displayed, including external certificates and self-signed certificates installed on the network.

### 3.3.2.2 Viewing SSL Certificates Discovered on a Network

To view a list of SSL certificates discovered on a specific network, expand the **Network** category and select **SSL Certificates**, as shown in the following illustration. This displays a list of certificates discovered on the network during the last scan.

The screenshot shows the 'SSL Certificates' view within the 'Network Assets' page. It features a table with the following columns: IP address, Host name, Common Name, Valid To, Valid From, Key Algorithm, Key Size, Signature Algorithm, and Inventory. The table contains four rows of certificate data, with the second row selected.

IP address	Host name	Common Name	Valid To	Valid From	Key Algorithm	Key Size	Signature Algorithm	Inventory
<input type="checkbox"/>	sectigo.com:443	sectigo.com	07/02/2022	07/02/2019	RSA	2048	SHA256WITHRSA	<a href="#">Assigned</a>
<input checked="" type="checkbox"/>	10.17.136.117:443	secure.sectigo.com:44	12/06/2021	12/06/2018	RSA	2048	SHA256WITHRSA	
<input type="checkbox"/>	151.139.128.10:443	sectigo.com:443	*.ssl.hwcdn.net	01/19/2022	01/01/2020	RSA	2048	SHA256WITHRSA
<input type="checkbox"/>	161.71.22.162:443	support.sectigo.com:4	support.sectigo.c	10/02/2022	10/01/2020	RSA	2048	SHA256WITHRSA

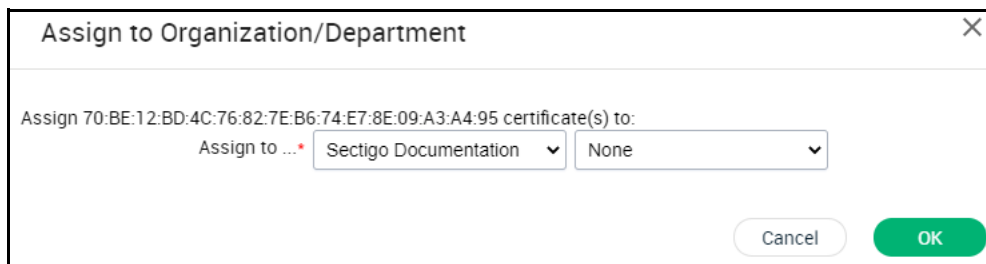
To view **Certificate Details**, select the certificate from the list and click **Details**. Alternatively, you can click **Assigned** or **Managed** in the **Inventory** column. The **Certificate Details** dialog displays the complete details of the selected SSL certificate with its certificate chain details. See [“How To Use the SSL Certificates Tab”](#) on page 17 for more information.

### 3.3.3 How To Manually Assign Certificates to Organizations and Departments

Certificates that fail to match the assignment rules are not assigned to an organization or department, and will not appear in the **Certificates > SSL Certificates** tab. You can manually assign these certificates to organizations and departments.

To manually assign certificates to organizations and departments, do the following:

1. Navigate to **Discovery > Network Assets > Network Discovery** and expand it to view the list of scanned networks.
2. Expand a specific network and select **SSL Certificates** to access a list of SSL certificates installed on the network.
3. Select one or more external certificates from the list and click **Assign To** to open the **Assign to Organization/Department** dialog, as shown in the following illustration.



4. Use the **Assign To** field to specify the organization and, optionally, department to which the certificate(s) should be assigned.
5. Click **OK**.

Once assigned to an organization, the certificates appear in the **Certificates > SSL Certificates** table.

### 3.3.4 How To Use the SSL Certificates Tab

The **SSL Certificates** tab shown in the following illustration lists all certificates that are assigned to organizations.

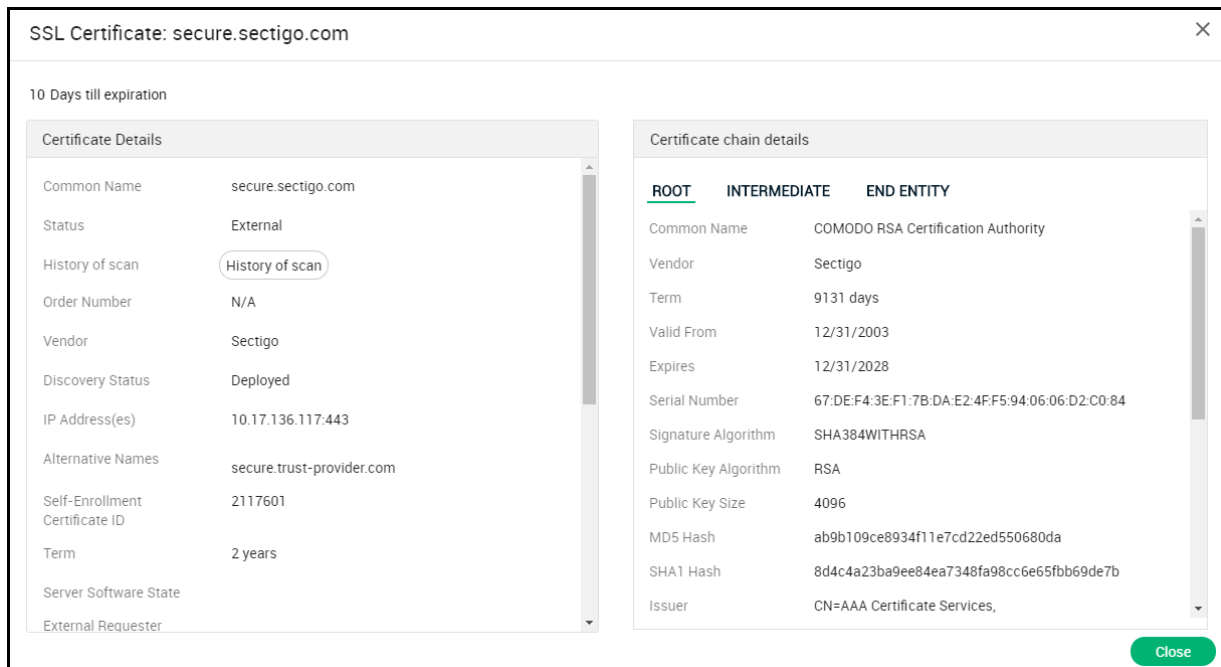
Common Name	Organization	Department	Status	Expires	Install state	Renewal state
<input type="checkbox"/> secure.sectigo.com *	Sectigo Documentation		External (1)	12/06/2020	Not scheduled	Not scheduled
<input type="checkbox"/> sectigo.com *	Sectigo Documentation		External (1)	07/02/2021	Not scheduled	Not scheduled

To view the SSL certificate details, do the following:

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

2. Select a certificate in the list and click **Details**.

This opens the **SSL Certificate** dialog, which has two panels, **Certificate Details** and **Certificate Chain Details**, as shown in the following illustration.



### 3.4 Setting Up Notifications

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

To create or edit a notification, do the following:

1. Navigate to **Settings > Notifications**.
2. Click **Add** or select a notification and click **Edit**. The **Create Notification** dialog is shown in the following illustration.

3. Choose the notification type. For example, SSL Expiration.
4. Enter a description of the notification.
5. To restrict the notification to specific organizations or departments, deselect the **Any** option and select the organizations and departments in the **Organization** and **Department** lists.
6. For SSL-related notifications, you can set the **Certificate Profile** field to restrict the notification to certificates that were created using a specific profile.
7. Enter the number of days in advance of the event to send the notification.
8. Set the frequency for the notification.
9. Choose who to notify. You can add additional email addresses in the **Subscribers** field.
10. Click **OK**.

### 3.5 Managing Domains

The **Domains** tab is used to add and delegate domains to organizations or departments.

NOTE: To issue publicly trusted certificates for a domain, the domain must pass domain control validation (DCV). DCV is only available in the full version of SCM. Privately trusted certificates do not require a domain that has passed DCV.

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

1. Navigate to **Settings > Domains > Delegations**.
2. Click **Add** to open the **Create Domain** dialog shown in the following illustration.

The screenshot shows a 'Create Domain' dialog box with the following elements:

- Domain**: A text input field with a red asterisk indicating it is required.
- Description**: A text input field.
- Active**: A checked checkbox.
- Organizations/Departments**: A table with columns for organization names and three columns for SSL certificate signing options.
- SSL Client Certificate Code Signing**: A table with three columns for signing options.
- Expand All**: A blue link below the table.
- Buttons**: 'Cancel' and 'OK' buttons at the bottom right.

Organizations/Departments	SSL Client Certificate Code Signing			
<input type="checkbox"/> Empty organization	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Encr1_DCV1_Dual0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Org with dept	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> org1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> org2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> org3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> org4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

## 3.6 Generating Reports

Using the **Reports** tab, you can generate reports that reflect an activity and other statistics related to the usage, provisioning, and monitoring of SSL, client, code signing, and device certificates. Depending on the features enabled for your account, the following reports are available:

- **SSL Certificates**—presents a history of all events related to SSL certificates.
- **Client Certificates**—presents a history of all events related to client certificates.
- **Code Signing Certificates**—presents a history of all events related to code signing certificates.
- **Device Certificates**—presents history of all events related to device certificates.
- **Network Discovery Results**—enables you to view information about scan options and discovered SSL certificates.
- **Network Discovery Tasks**—enables MRAO, RAO SSL, and DRAO SSL administrators to view details of configured network discovery tasks.
- **Code Signing Requests**—enables you to view CSoD requests and related activities.
- **Account Activity**—enables MRAOs to view a history of all account activity, including logins, certificate requests and modifications, and more.
- **Sent Notifications**—enables MRAOs to download reports with details about notification emails.
- **Private Key Agent Activity Log**—enables MRAOs to view actions executed by the Private Key Agent installed on the local network. This includes data about CSR generation and private key storage for certificates issued using the auto-CSR generation and PK management tools.
- **DCV**—enables MRAO, RAO SSL, and DRAO SSL administrators to download a report on registered domains and their DCV status.
- **Admins**—enables MRAOs to view a list of all administrators and their privilege levels.
- **Account Structure**—enables MRAOs to download a comprehensive XML report on organizations, departments, administrators, and certificates.

## 4 Using a Private CA

A 30-day SCM trial includes the ability to add and configure trial private CAs.

A private CA allows you to issue your own private trust level certificates. Private trust level certificates can be used to secure enterprise infrastructure, such as:

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

Configuring and using a trial private CA involves the following general steps:

1. Add a root private CA.
2. Add an issuing private CA with the root CA as the parent issuer.
3. Add certificate profiles for the certificate types you want to issue using the private CA, setting the enrolling backend for each profile to the issuing private CA.
4. Issue certificates.

Certificates enrolled during trial have a lifetime of 30 days. For seamless transition from the trial to the full version, ensure that the information you enter during the trial is accurate. Trials are for online root private CAs only, and you cannot transition from an online to offline root.

Five days prior to the scheduled end of your trial, you start receiving daily notification emails from Sectigo. You can contact your Sectigo account manager to request either an extension of the trial or the full private CA feature to be added to your account. Alternatively, you can let the trial expire, in which case you would not be able to order certificates. The certificates ordered during trial are not revoked and continue to be available after the expiration of the trial.

### 4.1 Setting Up a Trial Private CA

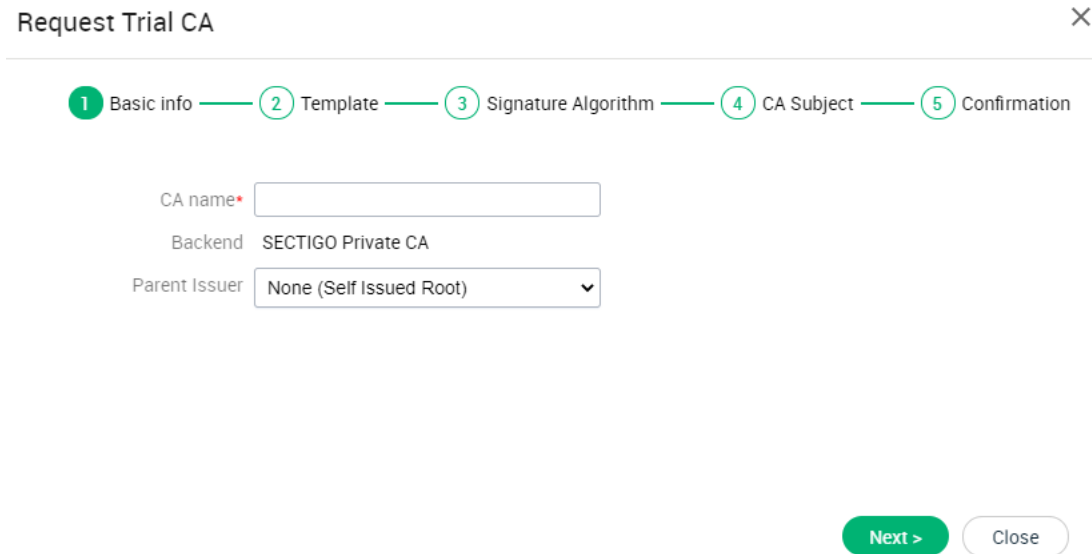
Because end-entity certificates are not issued from a root CA, you first add a root CA, and then an issuing CA that uses the root as its parent. The steps for adding both are the same.

You add a private CA as follows:

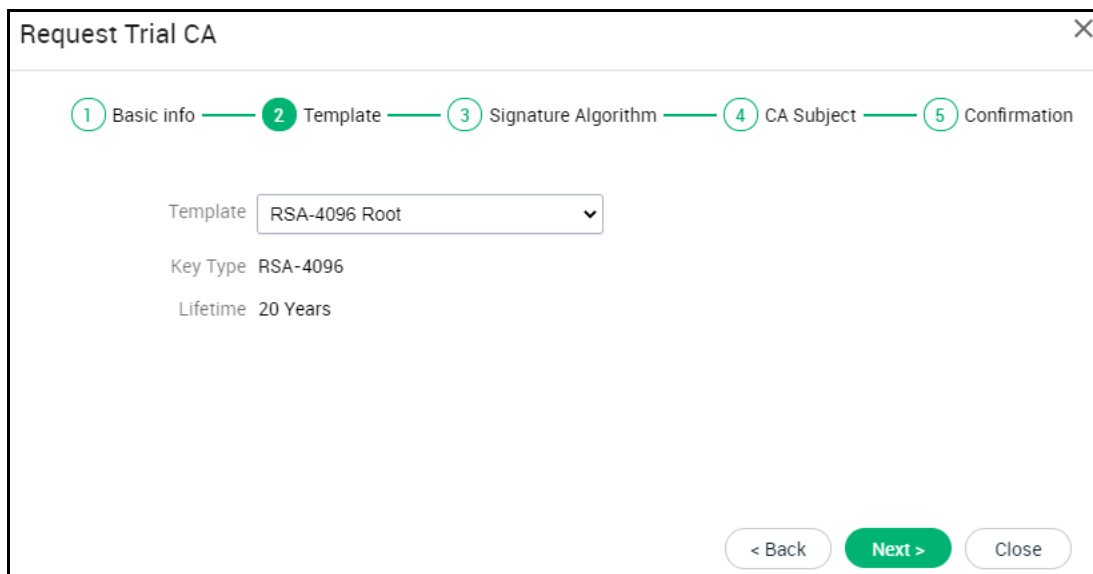
1. Navigate to **Settings > Certificates > Private CAs**.
2. Click **Add** to open the **Request Trial CA** wizard shown in the following illustration.

NOTE: If the Add button is not displayed, your trial is not active and you need to contact Sectigo Support.





3. Enter a name for the CA in the **CA name** field. SCM automatically appends 'Root' to the name of root CAs.
4. Select the **Parent Issuer**.  
To add a root CA, choose **None (Self Issued Root)**.  
To add an issuing CA, choose a root CA you have already added.
5. Click **Next** to open the **Template** page shown in the following illustration.



6. Use the **Template** field to select the template to use. The template determines the key type that the CA will use, as well as the lifetime of the CA certificate.  
The lifetime is 5 years for RSA-2048, and 10 years for all other key types.  
For self-issued roots, RSA-2048 has a fixed expiry of December 31, 2030, and the lifetime is 20 years for all other key types.
7. Click **Next** to open the **Signature Algorithm** page shown in the following illustration.

Request Trial CA

1 Basic info — 2 Template — 3 Signature Algorithm — 4 CA Subject — 5 Confirmation

Signature Algorithm: SHA 256

< Back   Next >   Close

8. Use the **Signature Algorithm** field to select one of the following algorithms:

- SHA-1
- SHA-256
- SHA-384
- SHA-512

For an issuing CA, the algorithm of the parent root CA is automatically selected.

9. Click **Next** to open the **CA Subject** page shown in the following illustration.

Request Trial CA

1 Basic info — 2 Template — 3 Signature Algorithm — 4 CA Subject — 5 Confirmation

Customer Name\*

City or Locality\*

State or Province\*

Country\*

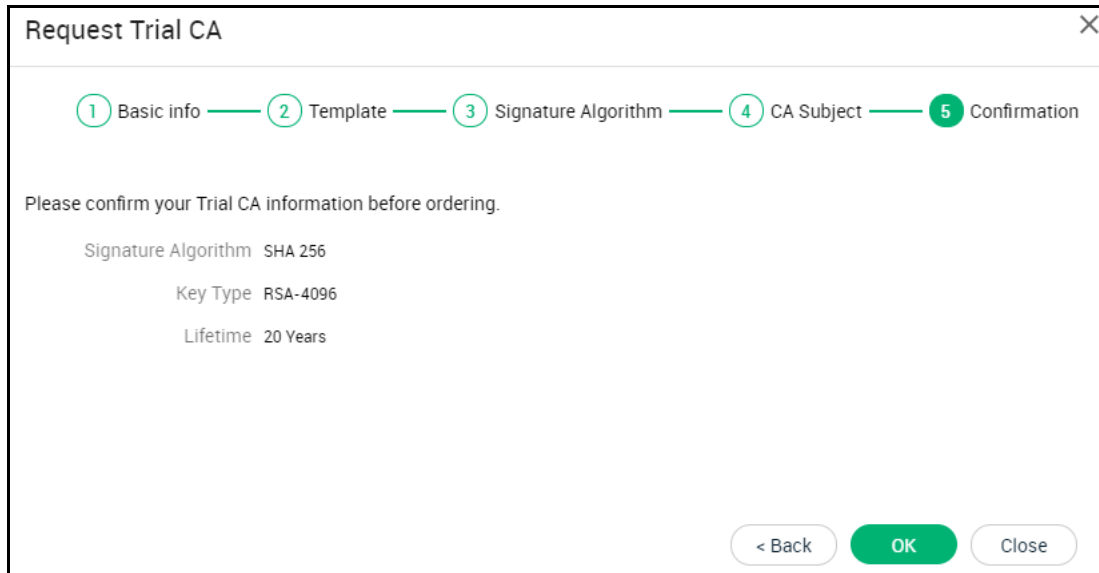
< Back   Next >   Close

10. Enter your customer name in the **Customer Name** field. This value is used for the Organization (O) and Common Name (CN) fields when generating the private CA certificate. In the case of CN, either Root CA or Issuing CA is appended depending on whether the parent issuer is set to self-issued root or another CA.

11. Enter your city in the **City or Locality** field.

12. Enter your state or province in the **State or Province** field.

13. Select your country.
14. Click **Next** to open the **Confirmation** page shown in the following illustration.



15. Click **OK** to confirm your trial.  
The CA is added to the **Private CAs** tab; trial mode is indicated in the **Trial Mode** column.

To download the root CA certificate for installation on your trust store, select the CA and click **Download**. Certificates are downloaded in `.cer` format.

## 4.2 Adding Certificate Profiles

To enroll certificates against a new issuing CA, you first need to add certificate profiles for each type of certificate you want to issue using the new CA. Certificate 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. Certificate templates, one each for client, code signing, SSL, and device profiles, are provided with the trial private CA for this purpose.

**NOTE:** Regardless of any term set for certificate profiles that you create, all certificates enrolled against a trial private CA are limited to 30 days.

You can add or edit certificate profiles for all four certificate types supported by Sectigo (SSL, Client, Code Signing, and Device). To issue SSL and client certificates using the private CA, you will need to add at least one profile of each type.

To add a certificate profile, do the following:

1. Navigate to **Settings > Certificates > Certificate Profiles**.
2. Click **Add** to open the **Add Certificate Profile** dialog shown in the following illustration.

The Enrolling Backend is automatically set to the Sectigo Private CA.

3. Enter a name and description for the profile.
4. Choose the type of certificate that can be issued using this profile (e.g., client or SSL).

The template and term are pre-selected. The term for certificates issued using the trial private CA is 30 days. The remaining fields can be left at default values.

5. Click **OK**.

The profile is added to the **Certificate Profiles** tab.

### 4.3 Requesting and Issuing SSL Certificates

Before you can request an SSL certificate, you need to generate a Certificate Signing Request (CSR). The public key included in the CSR should have at minimum an RSA 2048 key length or ECC p256 curve, and must match one of the key types allowed by the selected certificate profile.

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

- CN—Common name, i.e., 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 ISO code)

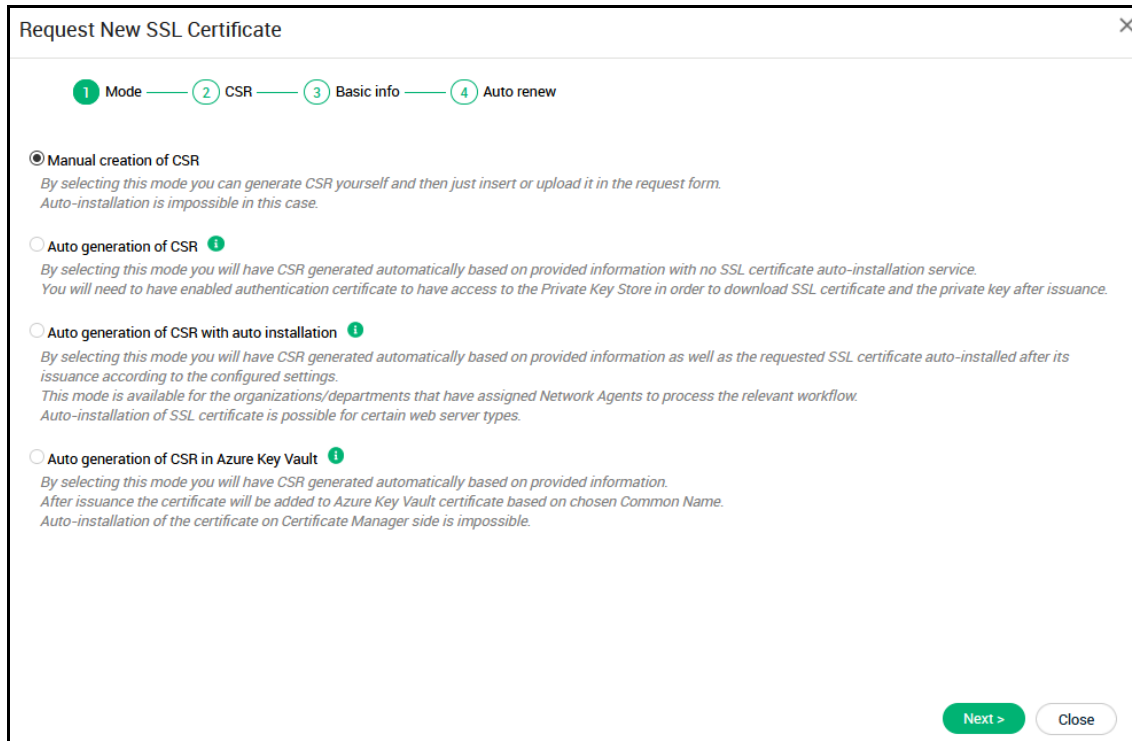
If information is missing from the CSR, or differs from the organization details as specified in SCM, the SCM organization values are used.

Sectigo provides a range of documents about generating CSRs. For a list of these documents, contact Sectigo support.

To request an SSL certificate, do the following:

1. Navigate to **Certificates > SSL Certificates** and click **Add**.

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



2. Select **Manual creation of CSR** and click **Next** to open the **CSR** page shown in the following illustration.

Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Auto renew

CSR\*

Max CSR size is 32K

Upload CSR

< Back Next > Close

3. Paste your CSR into the **CSR** field or upload it as a .txt file.
4. Click **Next** to open the **Basic info** page shown in the following illustration.

Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Auto renew

Organization\* Select... ↕ ↻

Department\* ↕

Certificate Profile\* ↕ ⓘ

Certificate Term\* ↕

Common Name\* www.google.com Get from CSR

Requester MRAO adadmin

External Requester ⓘ

[Click here for advanced options](#)

< Back Next > Close

5. Choose the organization and, optionally, department to which the certificate will be issued.
6. Select the certificate profile to use.  
This should be pre-selected to the SSL certificate profile you created.

7. Choose the term for the certificate.

NOTE: Certificates issued using the trial version of SCM are limited to 30 days regardless of the term that is set.

8. Enter the common name (i.e., domain) for which the certificate is to be issued. You can click **Get from CSR** to fill this field with the CN from the CSR.
9. Click **Next** to open the **Auto renew** page shown in the following illustration.

Request New SSL Certificate

1 Mode — 2 CSR — 3 Basic info — 4 Auto renew — 5 EULA

Here you can set auto-renewal of this certificate in advance of its expiration. These settings can be edited in the certificate details later on.

Enable auto renewal of this certificate

Number of days before expiration to start auto renewal

< Back Next > Close

10. Select **Enable auto renewal of this certificate** to have SCM apply for a new certificate when the current one approaches expiry.
11. 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 parameters as the existing certificate and submit it to the CA.
12. Click **Next** to open the **EULA** page shown in the following illustration.

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

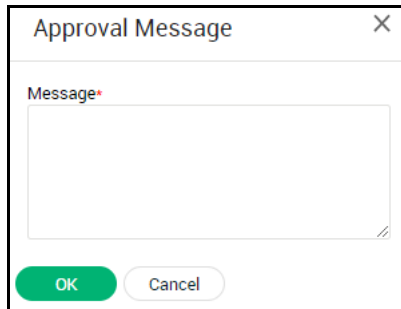
The certificate is added to the **Certificates > SSL Certificates** list with the status of Requested.

Common Name	Organization	Department	Status	Expires	Install state	Renewal state
<input checked="" type="checkbox"/> sectigo.com	Sectigo Documentation		Requested		Not scheduled	Not scheduled
<input type="checkbox"/> secure.sectigo.com *	Sectigo Documentation		External (1)	12/06/2020	Not scheduled	Not scheduled
<input type="checkbox"/> sectigo.com *	Sectigo Documentation		External (1)	07/02/2021	Not scheduled	Not scheduled

The next step is to approve the request, which is done as follows:

1. Navigate to **Certificates > SSL Certificates**.
2. Select the appropriate certificate and click **Approve** to open the **Approval Message** dialog shown in the following illustration.





3. Enter a message to be sent with the approval notification email and click **OK**.

Once the request has been approved, the certificate status changes to **Approved**, then to **Issued**, and a certificate collection email is sent to the applicant. The email contains a summary of the certificate details and links to download the certificate.

You can also download the certificate from the **SSL Certificates** tab as follows:

1. Navigate to **Certificates > SSL Certificates**.
2. Select the certificate and click **Details**.
3. Beside **Download The Certificate**, click **Select**.
4. Click on the appropriate certificate format to download the certificate.

The certificate can now be installed on the server.

## 4.4 Requesting and Issuing Client Certificates

SCM enables you to issue client certificates to enrolled users for domains which have been delegated to an organization or department.

You can add client certificate users to SCM in one of the following ways:

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

This section explains the process of manually adding the users. For more information on importing users or auto-enrolling users through AD Integration, see *Sectigo Certificate Manager Administrator's Guide*.

### 4.4.1 How To Add Users

To add a user manually, do the following:

1. Navigate to **Certificates > Client Certificates**.
2. Click **Add** to open the **Add New Person** dialog shown in the following illustration.

3. Choose the organization and, if applicable, department to which the end user will belong.
4. Choose the domain with which the end user is associated. The end user's email should use this domain.
5. Enter the end user's email address. The domain of the address is automatically set.
6. Enter the end user's personal details.
7. Enter any alternative email addresses separated by commas.
8. Set the validation type to Standard.
9. Click **OK**.

Repeat this process to add more users.

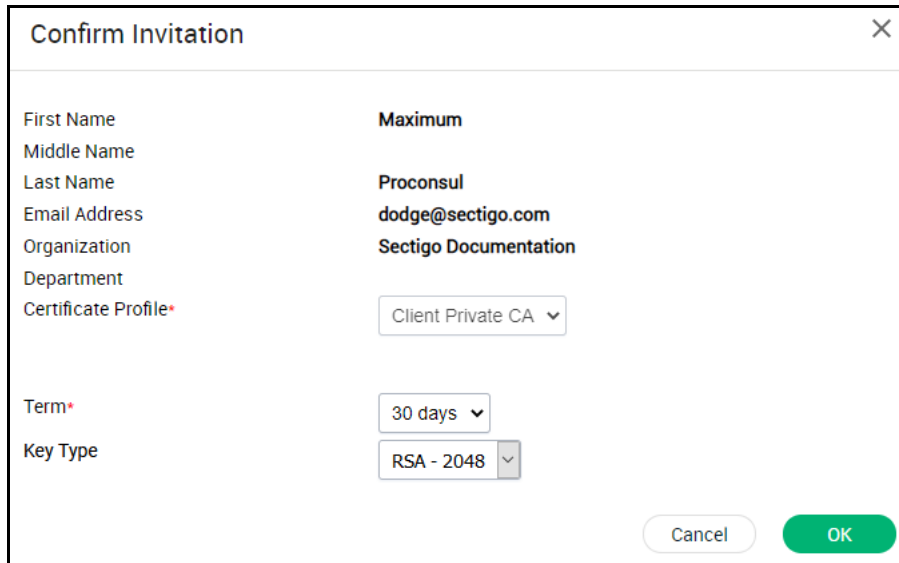
To edit an existing end-user's details, navigate to **Certificates > Client Certificates**, select the end-user and click **Edit**.

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

#### 4.4.2 How To Issue Client Certificates

You can initiate end-user enrollment for client certificates as follows:

1. Navigate to **Certificates > Client Certificates**.
2. Select the appropriate end-user and click **Certificates** to open the **Certificates for** dialog.
3. Click **Send Invitation** to display the **Confirm Invitation** dialog shown in the following illustration. The client certificate profile and term are pre-selected.



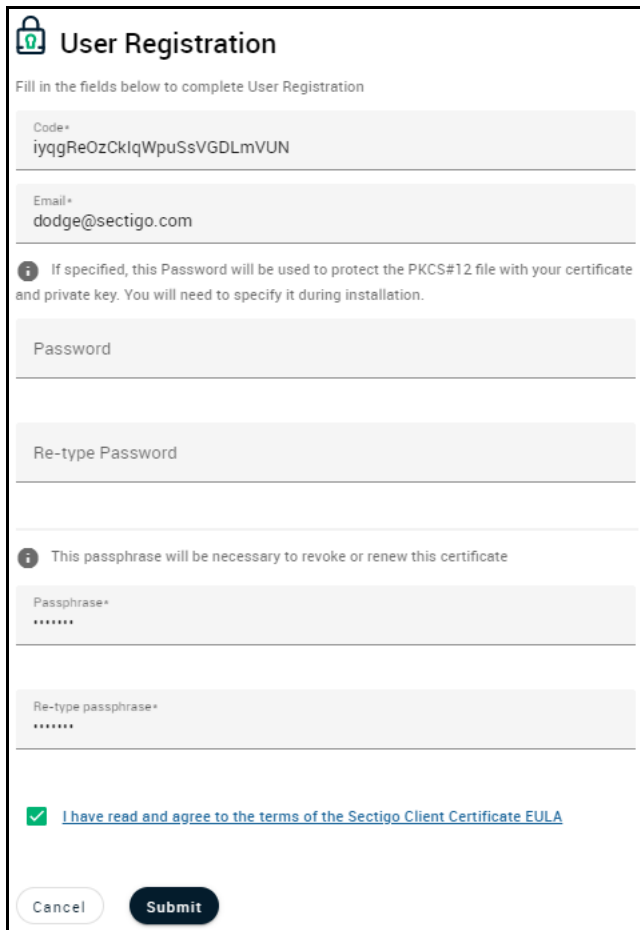
The 'Confirm Invitation' dialog box displays the following information:

First Name	Maximum
Middle Name	
Last Name	Proconsul
Email Address	dodge@sectigo.com
Organization	Sectigo Documentation
Department	
Certificate Profile*	Client Private CA
Term*	30 days
Key Type	RSA - 2048

Buttons: Cancel, OK

4. Click **OK**.

An invitation email is sent to the end-user containing the URL of the **User Registration** form, a request validation code, and instructions for downloading the certificate. Upon clicking the link, the end-user must complete the **User Registration** form shown in the following illustration.



**User Registration**

Fill in the fields below to complete User Registration

Code\*  
iyqgReOzCkIqWpuSsVGDLmVUN

Email\*  
dodge@sectigo.com

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

Password

Re-type Password

*Info* This passphrase will be necessary to revoke or renew this certificate

Passphrase\*  
\*\*\*\*\*

Re-type passphrase\*  
\*\*\*\*\*

I have read and agree to the terms of the Sectigo Client Certificate EULA

Buttons: Cancel, Submit

The **Code** and **Email** fields are pre-populated.

The password is used to protect the client certificate, and is needed when accessing the certificate (for example, when installing the certificate on their computer). A password is recommended, as some applications do not support client certificates that are not password protected.

The passphrase is used when renewing the certificate.

The end-user must then read the EULA, accept the terms, and click **Submit**.

On completion of validation and user registration processes, a certificate collection form shown in the following illustration appears, enabling the user to download and save the certificate.



SCM delivers the certificate to the user in PKCS12 ( .p12 ) format. The user is asked for the password (PIN) when they import the certificate into the certificate store of their computer.